



# **ONTAP 9 Documentation**

## **ONTAP 9**

NetApp  
October 26, 2022

This PDF was generated from <https://docs.netapp.com/us-en/ontap/index.html> on October 26, 2022.  
Always check [docs.netapp.com](https://docs.netapp.com) for the latest.

# Table of Contents

- ONTAP 9 Documentation . . . . . 1
- ONTAP release notes . . . . . 2
- Introduction and concepts . . . . . 3
  - ONTAP concepts . . . . . 3
  - ONTAP and the cloud . . . . . 39
- Set up, upgrade and revert ONTAP and system components . . . . . 49
  - Setup ONTAP . . . . . 49
  - Upgrade ONTAP . . . . . 63
  - Update firmware . . . . . 164
  - Revert ONTAP . . . . . 168
- Cluster administration . . . . . 198
  - Cluster management with System Manager . . . . . 198
  - Cluster management with the CLI . . . . . 209
  - Disk and tier (aggregate) management . . . . . 400
  - FabricPool tier management . . . . . 486
  - SVM data mobility . . . . . 537
  - HA pair management . . . . . 544
  - Rest API management with System Manager . . . . . 567
- Volume administration . . . . . 571
  - Volume and LUN management with System Manager . . . . . 571
  - Logical storage management with the CLI . . . . . 589
  - Provision NAS storage for large file systems using FlexGroup volumes . . . . . 706
  - FlexGroup volumes management with the CLI . . . . . 708
  - Improve performance for multiple clients with FlexCache . . . . . 788
  - FlexCache volumes management with the CLI . . . . . 790
- Network Management . . . . . 809
  - Manage your network with System Manager . . . . . 809
  - Set up NAS path failover with the CLI . . . . . 813
  - Manage your network with the CLI . . . . . 857
- NAS storage management . . . . . 1031
  - Manage NAS protocols with System Manager . . . . . 1031
  - Configure NFS with the CLI . . . . . 1049
  - Manage NFS with the CLI . . . . . 1117
  - Manage NFS over RDMA . . . . . 1227
  - Configure SMB with the CLI . . . . . 1230
  - Manage SMB with the CLI . . . . . 1270
  - SMB configuration for Microsoft Hyper-V and SQL Server . . . . . 1610
- SAN storage management . . . . . 1667
  - SAN administration . . . . . 1667

# ONTAP 9 Documentation

# ONTAP release notes

ONTAP release notes describe new features, enhancements, and known issues for ONTAP 9.5 and later releases. These release notes also provides additional information related to running each of these releases on specific storage systems.

You can access releases notes for ONTAP 9.5 and later [here](#).

ONTAP release notes are formatted as a PDF. You must sign in with your NetApp account or create a NetApp account to access release notes.

# Introduction and concepts

## ONTAP concepts

### Concepts overview

The following concepts inform ONTAP data management software, including cluster storage, high-availability, virtualization, data protection, storage efficiency, and security. You should understand the full range of ONTAP features and benefits before you configure your storage solution.

If you need reference and configuration information about the ONTAP capabilities, refer to the following:

- High availability (HA) configuration

[High Availability](#)

- Cluster and SVM administration

[System administration](#)

- Network and LIF management

[Network management](#)

- Disks and aggregates

[Disk and aggregate management](#)

- FlexVol volumes, FlexClone technology, and storage efficiency features

[Logical storage management](#)

- SAN host provisioning

[SAN administration](#)

- NAS file access

- [NFS management](#)

- [SMB management](#)

- Disaster recovery and archiving

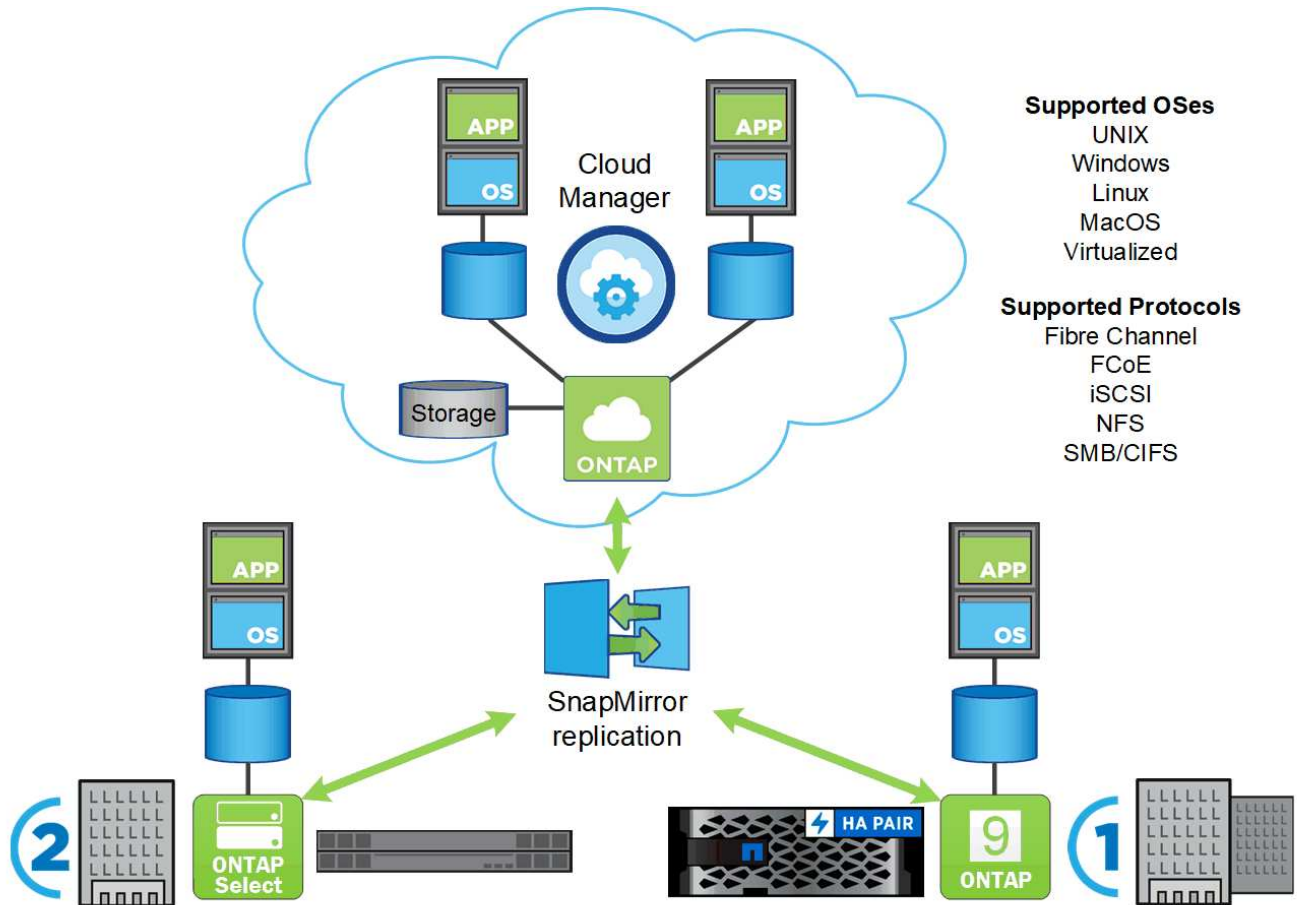
[Data protection](#)

### ONTAP platforms

ONTAP data management software offers unified storage for applications that read and write data over block- or file-access protocols, in storage configurations that range from high-speed flash, to lower-priced spinning media, to cloud-based object storage.

ONTAP implementations run on NetApp-engineered FAS or AFF appliances, on commodity hardware (ONTAP Select), and in private, public, or hybrid clouds (NetApp Private Storage or Cloud Volumes ONTAP). Specialized implementations offer best-in-class converged infrastructure (FlexPod Datacenter) and access to third-party storage arrays (FlexArray Virtualization).

Together these implementations form the basic framework of the *NetApp data fabric*, with a common software-defined approach to data management and fast, efficient replication across platforms.



*Across the NetApp data fabric, you can count on a common set of features and fast, efficient replication across platforms. You can use the same interface and the same data management tools.*

### **About FlexPod Datacenter and FlexArray Virtualization**

Although not represented in the illustration of the NetApp data fabric, FlexPod Datacenter and FlexArray Virtualization are key ONTAP implementations:

- FlexPod integrates best-in-class storage, networking, and compute components in a flexible architecture for enterprise workloads. Its converged infrastructure speeds the deployment of business-critical applications and cloud-based data center infrastructures.
- FlexArray is a front end for third-party and NetApp E-Series storage arrays, offering a uniform set of capabilities and streamlined data management. A FlexArray system looks like any other ONTAP system and offers all the same features.

## Cluster storage

The current iteration of ONTAP was originally developed for NetApp's scale out *cluster* storage architecture. This is the architecture you typically find in datacenter implementations of ONTAP. Because this implementation exercises most of ONTAP's capabilities, it's a good place to start in understanding the concepts that inform ONTAP technology.

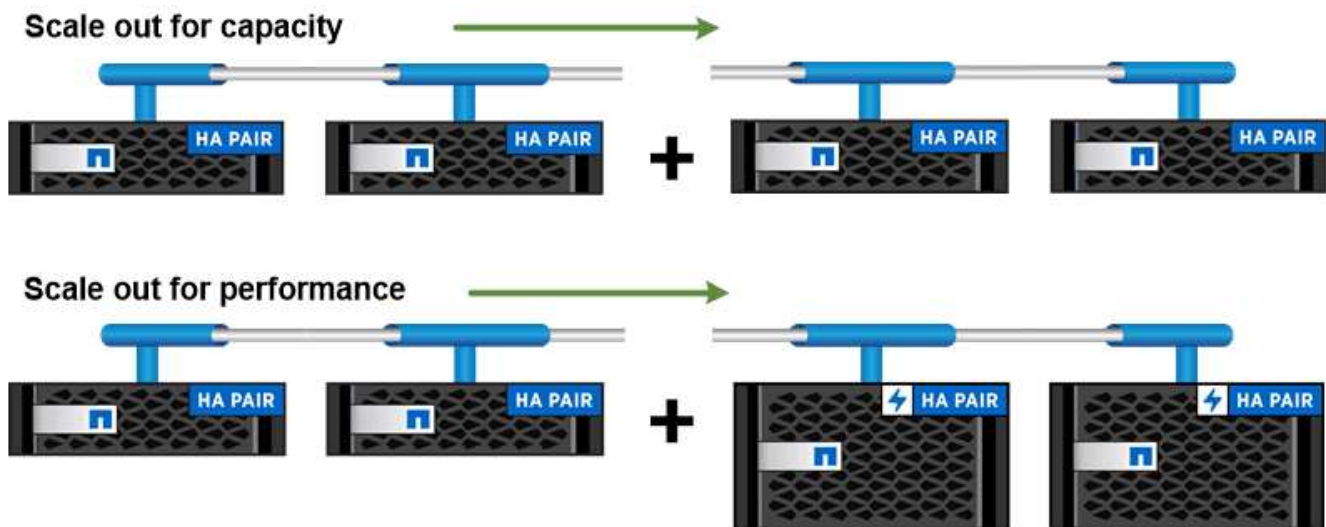
Datacenter architectures usually deploy dedicated FAS or AFF controllers running ONTAP data management software. Each controller, its storage, its network connectivity, and the instance of ONTAP running on the controller is called a *node*.

Nodes are paired for high availability (HA). Together these pairs (up to 12 nodes for SAN, up to 24 nodes for NAS) comprise the cluster. Nodes communicate with each other over a private, dedicated cluster interconnect.

Depending on the controller model, node storage consists of flash disks, capacity drives, or both. Network ports on the controller provide access to data. Physical storage and network connectivity resources are virtualized, visible to cluster administrators only, not to NAS clients or SAN hosts.

Nodes in an HA pair must use the same storage array model. Otherwise you can use any supported combination of controllers. You can scale out for capacity by adding nodes with like storage array models, or for performance by adding nodes with higher-end storage arrays.

Of course you can scale up in all the traditional ways as well, upgrading disks or controllers as needed. ONTAP's virtualized storage infrastructure makes it easy to move data nondisruptively, meaning that you can scale vertically or horizontally without downtime.



*You can scale out for capacity by adding nodes with like controller models, or for performance by adding nodes with higher-end storage arrays, all while clients and hosts continue to access data.*

### ***Single-node clusters***

A single-node cluster is a special implementation of a cluster running on a standalone node. You might want to deploy a single-node cluster in a branch office, for example, assuming the workloads are small enough and that storage availability is not a critical concern.

In this scenario, the single-node cluster would use SnapMirror replication to back up the site's data to your organization's primary data center. ONTAP Select, with its support for ONTAP running on commodity hardware, would be a good candidate for this type of implementation.

### **High-availability pairs**

Cluster nodes are configured in *high-availability (HA) pairs* for fault tolerance and nondisruptive operations. If a node fails or if you need to bring a node down for routine maintenance, its partner can *take over* its storage and continue to serve data from it. The partner *gives back* storage when the node is brought back on line.

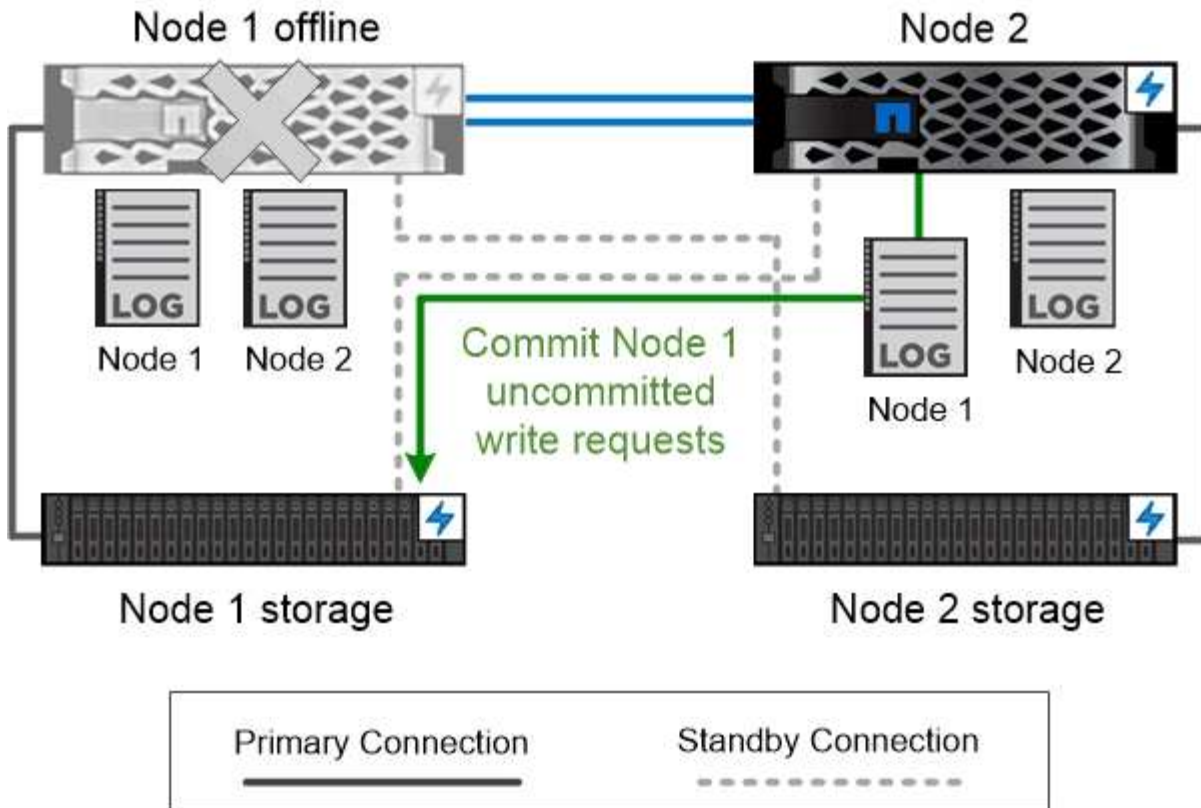
HA pairs always consist of like controller models. The controllers typically reside in the same chassis with redundant power supplies.

An internal HA interconnect allows each node to continually check whether its partner is functioning and to mirror log data for the other's nonvolatile memory. When a write request is made to a node, it is logged in NVRAM on both nodes before a response is sent back to the client or host. On failover, the surviving partner commits the failed node's uncommitted write requests to disk, ensuring data consistency.

Connections to the other controller's storage media allow each node to access the other's storage in the event of a takeover. Network path failover mechanisms ensure that clients and hosts continue to communicate with the surviving node.

To assure availability, you should keep performance capacity utilization on either node at 50% to accommodate the additional workload in the failover case. For the same reason, you may want to configure no more than 50% of the maximum number of NAS virtual network interfaces for a node.





*On failover, the surviving partner commits the failed node's uncommitted write requests to disk, ensuring data consistency.*

#### **Takeover and giveback in virtualized ONTAP implementations**

Storage is not shared between nodes in virtualized “shared-nothing” ONTAP implementations like Cloud Volumes ONTAP for AWS or ONTAP Select. When a node goes down, its partner continues to serve data from a synchronously mirrored copy of the node’s data. It does not take over the node’s storage, only its data serving function.

### **AutoSupport and Active IQ Digital Advisor**

ONTAP offers artificial intelligence-driven system monitoring and reporting through a web portal and through a mobile app. The AutoSupport component of ONTAP sends telemetry that is analyzed by Active IQ Digital Advisor.

Active IQ enables you to optimize your data infrastructure across your global hybrid cloud by delivering actionable predictive analytics and proactive support through a cloud-based portal and mobile app. Data-driven insights and recommendations from Active IQ are available to all NetApp customers with an active SupportEdge contract (features vary by product and support tier).

Here are some things you can do with Active IQ:

- Plan upgrades. Active IQ identifies issues in your environment that can be resolved by upgrading to a newer version of ONTAP and the Upgrade Advisor component helps you plan for a successful upgrade.

- View system wellness. Your Active IQ dashboard reports any issues with wellness and helps you correct those issues. Monitor system capacity to make sure you never run out of storage space.
- Manage performance. Active IQ shows system performance over a longer period than you can see in System Manager. Identify configuration and system issues that are impacting your performance.
- Maximize efficiency. View storage efficiency metrics and identify ways to store more data in less space.
- View inventory and configuration. Active IQ displays complete inventory and software and hardware configuration information. See when service contracts are expiring to ensure you remain covered.

**Related information**

[NetApp Documentation: Active IQ Digital Advisor](#)

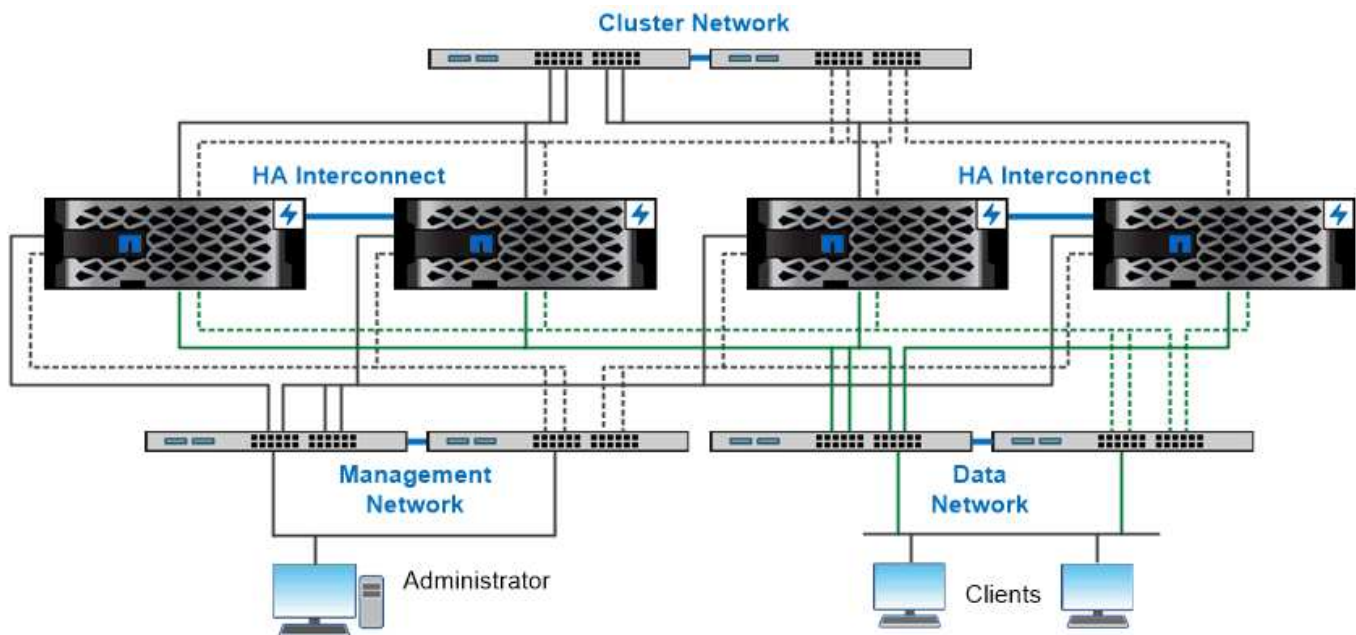
[Launch Active IQ](#)

[SupportEdge Services](#)

**Network architecture**

**Network architecture overview**

The network architecture for an ONTAP datacenter implementation typically consists of a cluster interconnect, a management network for cluster administration, and a data network. NICs (network interface cards) provide physical ports for Ethernet connections. HBAs (host bus adapters) provide physical ports for FC connections.



*The network architecture for an ONTAP datacenter implementation typically consists of a cluster interconnect, a management network for cluster administration, and a data network.*

**Logical ports**

In addition to the physical ports provided on each node, you can use *logical ports* to manage network traffic. Logical ports are interface groups or VLANs.

## Interface groups

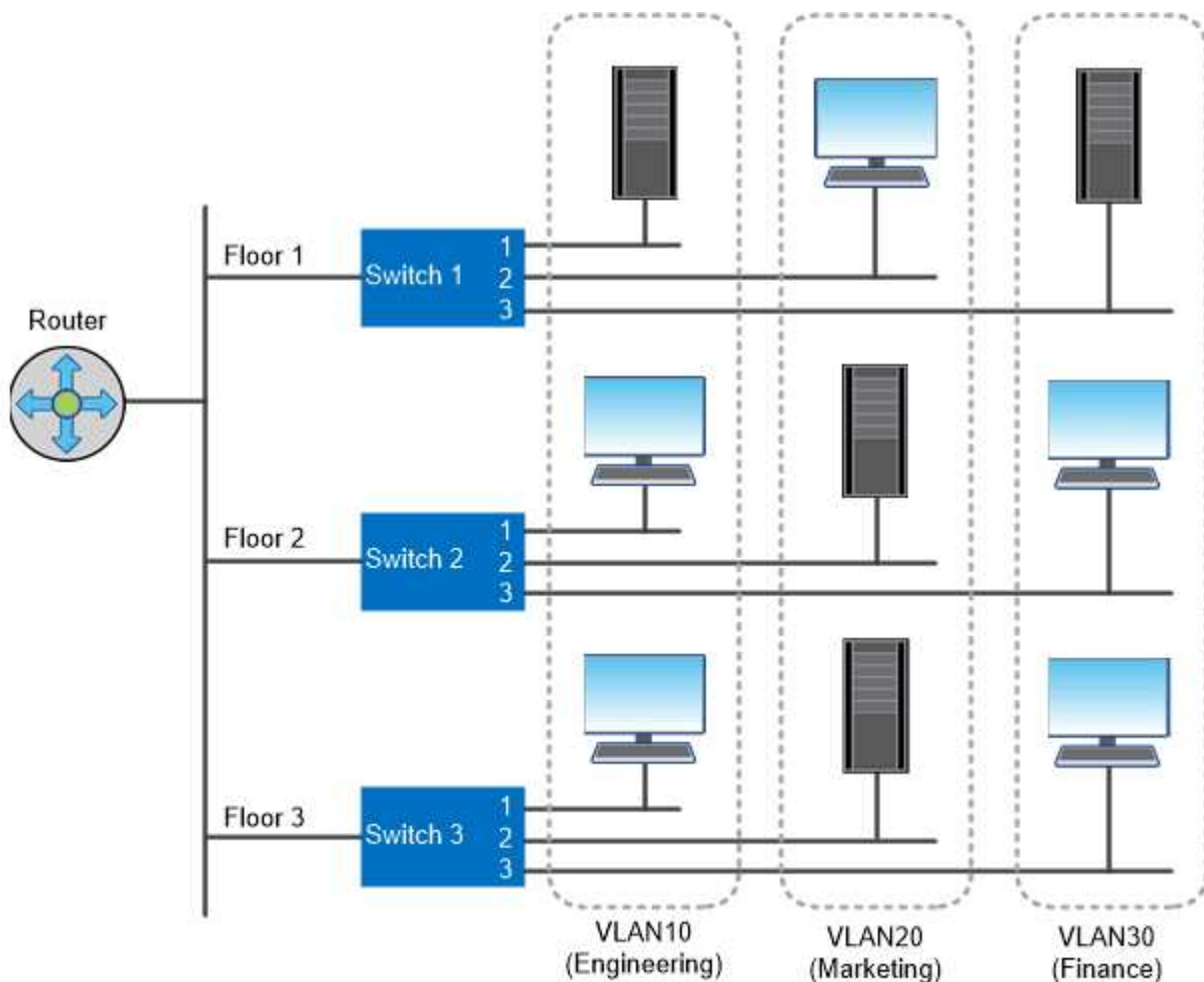
*Interface groups* combine multiple physical ports into a single logical “trunk port.” You might want to create an interface group consisting of ports from NICs in different PCI slots to ensure against a slot failure bringing down business-critical traffic.

An interface group can be single-mode, multimode, or dynamic multimode. Each mode offers differing levels of fault tolerance. You can use either type of multimode interface group to load-balance network traffic.

## VLANs

*VLANs* separate traffic from a network port (which could be an interface group) into logical segments defined on a switch port basis, rather than on physical boundaries. The *end-stations* belonging to a VLAN are related by function or application.

You might group end-stations by department, such as Engineering and Marketing, or by project, such as release1 and release2. Because physical proximity of the end-stations is irrelevant in a VLAN, the end-stations can be geographically remote.



*You can use VLANs to segregate traffic by department.*

## Support for industry-standard network technologies

ONTAP supports all major industry-standard network technologies. Key technologies

include IPspaces, DNS load balancing, and SNMP traps.

Broadcast domains, failover groups, and subnets are described in [NAS path failover](#).

### **IPspaces**

You can use an *IPspace* to create a distinct IP address space for each virtual data server in a cluster. Doing so enables clients in administratively separate network domains to access cluster data while using overlapping IP addresses from the same IP address subnet range.

A service provider, for example, could configure different IPspaces for tenants using the same IP addresses to access a cluster.

### **DNS load balancing**

You can use *DNS load balancing* to distribute user network traffic across available ports. A DNS server dynamically selects a network interface for traffic based on the number of clients that are mounted on the interface.

### **SNMP traps**

You can use *SNMP traps* to check periodically for operational thresholds or failures. SNMP traps capture system monitoring information sent asynchronously from an SNMP agent to an SNMP manager.

### ***FIPS compliance***

ONTAP is compliant with the Federal Information Processing Standards (FIPS) 140-2 for all SSL connections. You can turn on and off SSL FIPS mode, set SSL protocols globally, and turn off any weak ciphers such as RC4.

### **RDMA overview**

If you have latency sensitive or high-bandwidth workloads, you may want to take advantage of ONTAP's Read Direct Memory Access (RDMA) offerings. RDMA allows data to be copied directly between storage system memory and host system memory, circumventing CPU interruptions and overhead.

Beginning with ONTAP 9.10.1, you can configure [NFS over RDMA](#) to enable the use of NVIDIA GPUDirect Storage for GPU-accelerated workloads on hosts with supported NVIDIA GPUs.

ONTAP 9.10.1 also introduces RDMA cluster interconnect for ONTAP users with an A400 or ASA400 storage system with Pensando cluster NICs. RDMA cluster interconnect reduces latency, decreases failover times, and accelerates communication between nodes in a cluster. Given the appropriate storage system set up, no additional configuration is needed.

### **Client protocols**

ONTAP supports all major industry-standard client protocols: NFS, SMB, FC, FCoE, iSCSI, NVMe/FC, and S3.

## **NFS**

NFS is the traditional file access protocol for UNIX and LINUX systems. Clients can access files in ONTAP volumes using the NFSv3, NFSv4, NFSv4.1, and pNFS protocols. You can control file access using UNIX-style permissions, NTFS-style permissions, or a mix of both.

Clients can access the same files using both NFS and SMB protocols.

## **SMB**

SMB is the traditional file access protocol for Windows systems. Clients can access files in ONTAP volumes using the SMB 2.0, SMB 2.1, SMB 3.0, and SMB 3.1.1 protocols. Just like with NFS, a mix of permission styles are supported.

SMB 1.0 is available but disabled by default in ONTAP 9.3 and later releases.

## **FC**

Fibre Channel is the original networked block protocol. Instead of files, a block protocol presents an entire virtual disk to a client. The traditional FC protocol uses a dedicated FC network with specialized FC switches, and requires the client computer to have FC network interfaces.

A LUN represents the virtual disk, and one or more LUNs are stored in an ONTAP volume. The same LUN can be accessed through the FC, FCoE, and iSCSI protocols, but multiple clients can access the same LUN only if they are part of a cluster that prevents write collisions.

## **FCoE**

FCoE is basically the same protocol as FC, but uses a datacenter-grade Ethernet network in place of the traditional FC transport. The client still requires an FCoE-specific network interface.

## **iSCSI**

iSCSI is a block protocol that can run on standard Ethernet networks. Most client operating systems offer a software initiator that runs over a standard Ethernet port. iSCSI is a good choice when you need a block protocol for a particular application, but do not have dedicated FC networking available.

## **NVMe/FC**

The newest block protocol, NVMe/FC, is specifically designed to work with flash-based storage. It offers scalable sessions, a significant reduction in latency, and an increase in parallelism, making it well suited to low-latency and high-throughput applications such as in-memory databases and analytics.

Unlike FC and iSCSI, NVMe does not use LUNs. Instead it uses namespaces, which are stored in an ONTAP volume. NVMe namespaces can be accessed only through the NVMe protocol.

## **S3**

Beginning with ONTAP 9.8, you can enable an ONTAP Simple Storage Service (S3) server in an ONTAP cluster, allowing you to serve data in object storage using S3 buckets.

ONTAP supports two on-premises use case scenarios for serving S3 object storage:

- FabricPool tier to a bucket on local cluster (tier to a local bucket) or remote cluster (cloud tier).

- S3 client app access to a bucket on the local cluster or a remote cluster.



ONTAP S3 is appropriate if you want S3 capabilities on existing clusters without additional hardware and management. For deployments larger than 300TB, NetApp StorageGRID software continues to be the NetApp flagship solution for object storage. Learn about [StorageGRID](#).

## Disks and aggregates

### Local tiers (aggregates) and RAID groups

Modern RAID technologies protect against disk failure by rebuilding a failed disk's data on a spare disk. The system compares index information on a "parity disk" with data on the remaining healthy disks to reconstruct the missing data, all without downtime or a significant performance cost.

A local tier (aggregate) consists of one or more *RAID groups*. The *RAID type* of the local tier determines the number of parity disks in the RAID group and the number of simultaneous disk failures that the RAID configuration protects against.

The default RAID type, RAID-DP (RAID-double parity), requires two parity disks per RAID group and protects against data loss in the event of two disks failing at the same time. For RAID-DP, the recommended RAID group size is between 12 and 20 HDDs and between 20 and 28 SSDs.

You can spread out the overhead cost of parity disks by creating RAID groups at the higher end of the sizing recommendation. This is especially the case for SSDs, which are much more reliable than capacity drives. For local tiers that use HDDs, you should balance the need to maximize disk storage against countervailing factors like the longer rebuild time required for larger RAID groups.

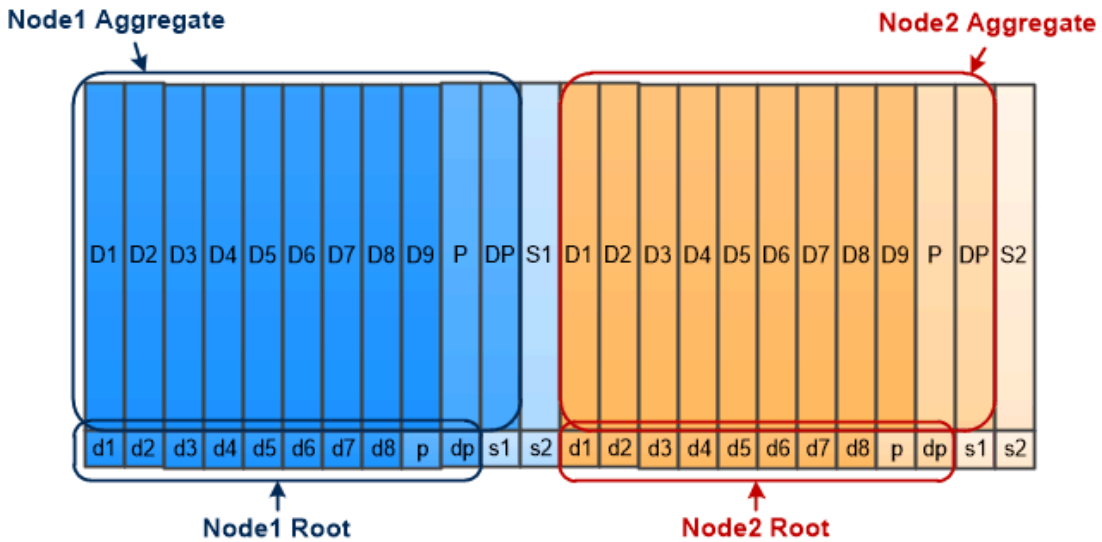
### Root-data partitioning

Every node must have a root aggregate for storage system configuration files. The root aggregate has the RAID type of the data aggregate.

System Manager does not support root-data or root-data-data partitioning.

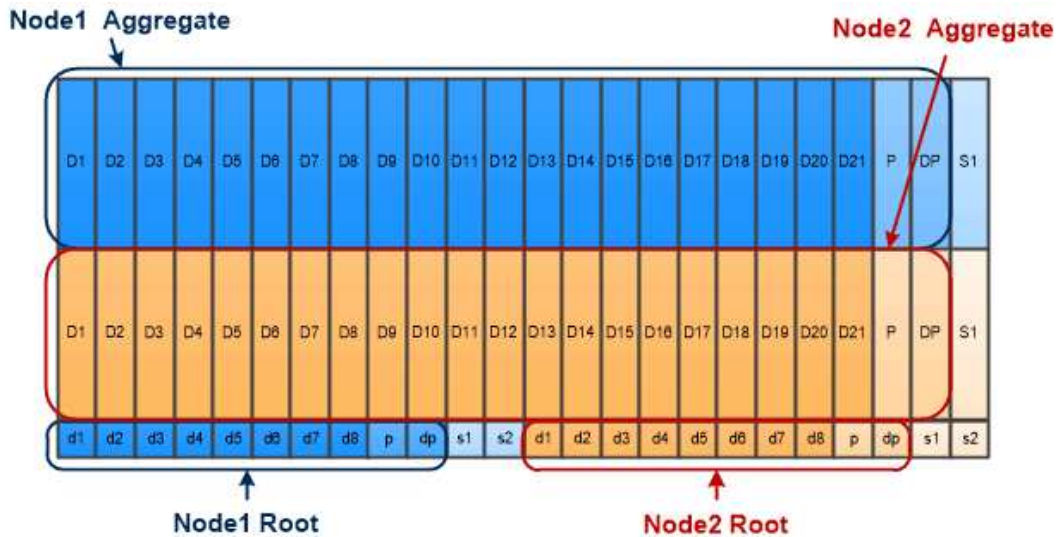
A root aggregate of type RAID-DP typically consists of one data disk and two parity disks. That's a significant "parity tax" to pay for storage system files, when the system is already reserving two disks as parity disks for each RAID group in the aggregate.

*Root-data partitioning* reduces the parity tax by apportioning the root aggregate across disk partitions, reserving one small partition on each disk as the root partition and one large partition for data.



*Root-data partitioning creates one small partition on each disk as the root partition and one large partition on each disk for data.*

As the illustration suggests, the more disks used to store the root aggregate, the smaller the root partition. That's also the case for a form of root-data partitioning called *root-data-data partitioning*, which creates one small partition as the root partition and two larger, equally sized partitions for data.



*Root-data-data partitioning creates one small partition as the root partition and two larger, equally sized partitions for data.*

Both types of root-data partitioning are part of the ONTAP *Advanced Drive Partitioning (ADP)* feature. Both are configured at the factory: root-data partitioning for entry-level FAS2xxx, FAS9000, FAS8200, FAS80xx and AFF systems, root-data-data partitioning for AFF systems only.

#### Drives partitioned and used for the root aggregate

The drives that are partitioned for use in the root aggregate depend on the system configuration. Knowing how many drives are used for the root aggregate helps you to determine how much of the drives' capacity is reserved for the root partition, and how much is available for use in a data aggregate.

The root-data partitioning capability is supported for entry-level platforms, All Flash FAS platforms, and FAS platforms with only SSDs attached.

For entry-level platforms, only the internal drives are partitioned.

For All Flash FAS platforms and FAS platforms with only SSDs attached, all drives that are attached to the controller when the system is initialized are partitioned, up to a limit of 24 per node. Drives that are added after system configuration are not partitioned.

## Volumes, qtrees, files, and LUNs

ONTAP serves data to clients and hosts from logical containers called *FlexVol volumes*. Because these volumes are only loosely coupled with their containing aggregate, they offer greater flexibility in managing data than traditional volumes.

You can assign multiple FlexVol volumes to an aggregate, each dedicated to a different application or service. You can expand and contract a FlexVol volume, move a FlexVol volume, and make efficient copies of a FlexVol volume. You can use *qtrees* to partition a FlexVol volume into more manageable units, and *quotas* to limit volume resource usage.

Volumes contain file systems in a NAS environment and LUNs in a SAN environment. A LUN (logical unit number) is an identifier for a device called a *logical unit* addressed by a SAN protocol.

LUNs are the basic unit of storage in a SAN configuration. The Windows host sees LUNs on your storage system as virtual disks. You can nondisruptively move LUNs to different volumes as needed.

In addition to data volumes, there are a few special volumes you need to know about:

- A *node root volume* (typically “vol0”) contains node configuration information and logs.
- An *SVM root volume* serves as the entry point to the namespace provided by the SVM and contains namespace directory information.
- *System volumes* contain special metadata such as service audit logs.

You cannot use these volumes to store data.





*Volumes contain files in a NAS environment and LUNs in a SAN environment.*

### **FlexGroup volumes**

In some enterprises a single namespace may require petabytes of storage, far exceeding even a FlexVol volume's 100TB capacity.

A *FlexGroup volume* supports up to 400 billion files with 200 constituent member volumes that work collaboratively to dynamically balance load and space allocation evenly across all members.

There is no required maintenance or management overhead with a FlexGroup volume. You simply create the FlexGroup volume and share it with your NAS clients. ONTAP does the rest.

## **Storage virtualization**

### **Storage virtualization overview**

You use *storage virtual machines (SVMs)* to serve data to clients and hosts. Like a virtual machine running on a hypervisor, an SVM is a logical entity that abstracts physical resources. Data accessed through the SVM is not bound to a location in storage. Network access to the SVM is not bound to a physical port.



SVMs were formerly called "vservers." You will still see that term in the ONTAP command line interface (CLI).

An SVM serves data to clients and hosts from one or more volumes, through one or more network *logical interfaces (LIFs)*. Volumes can be assigned to any data aggregate in the cluster. LIFs can be hosted by any physical or logical port. Both volumes and LIFs can be moved without disrupting data service, whether you are performing hardware upgrades, adding nodes, balancing performance, or optimizing capacity across aggregates.

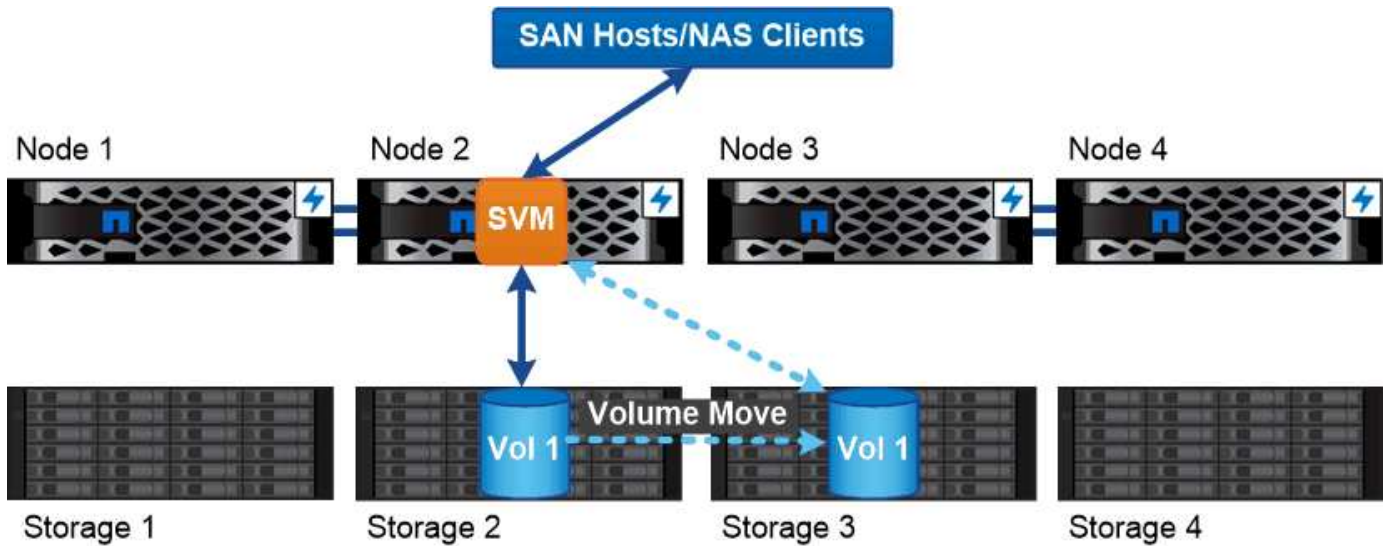
The same SVM can have a LIF for NAS traffic and a LIF for SAN traffic. Clients and hosts need only the

address of the LIF (IP address for NFS, SMB, or iSCSI; WWPN for FC) to access the SVM. LIFs keep their addresses as they move. Ports can host multiple LIFs. Each SVM has its own security, administration, and namespace.

In addition to data SVMs, ONTAP deploys special SVMs for administration:

- An *admin SVM* is created when the cluster is set up.
- A *node SVM* is created when a node joins a new or existing cluster.
- A *system SVM* is automatically created for cluster-level communications in an IPspace.

You cannot use these SVMs to serve data. There are also special LIFs for traffic within and between clusters, and for cluster and node management.



*Data accessed through an SVM is not bound to a physical storage location. You can move a volume without disrupting data service.*

### **Why ONTAP is like middleware**

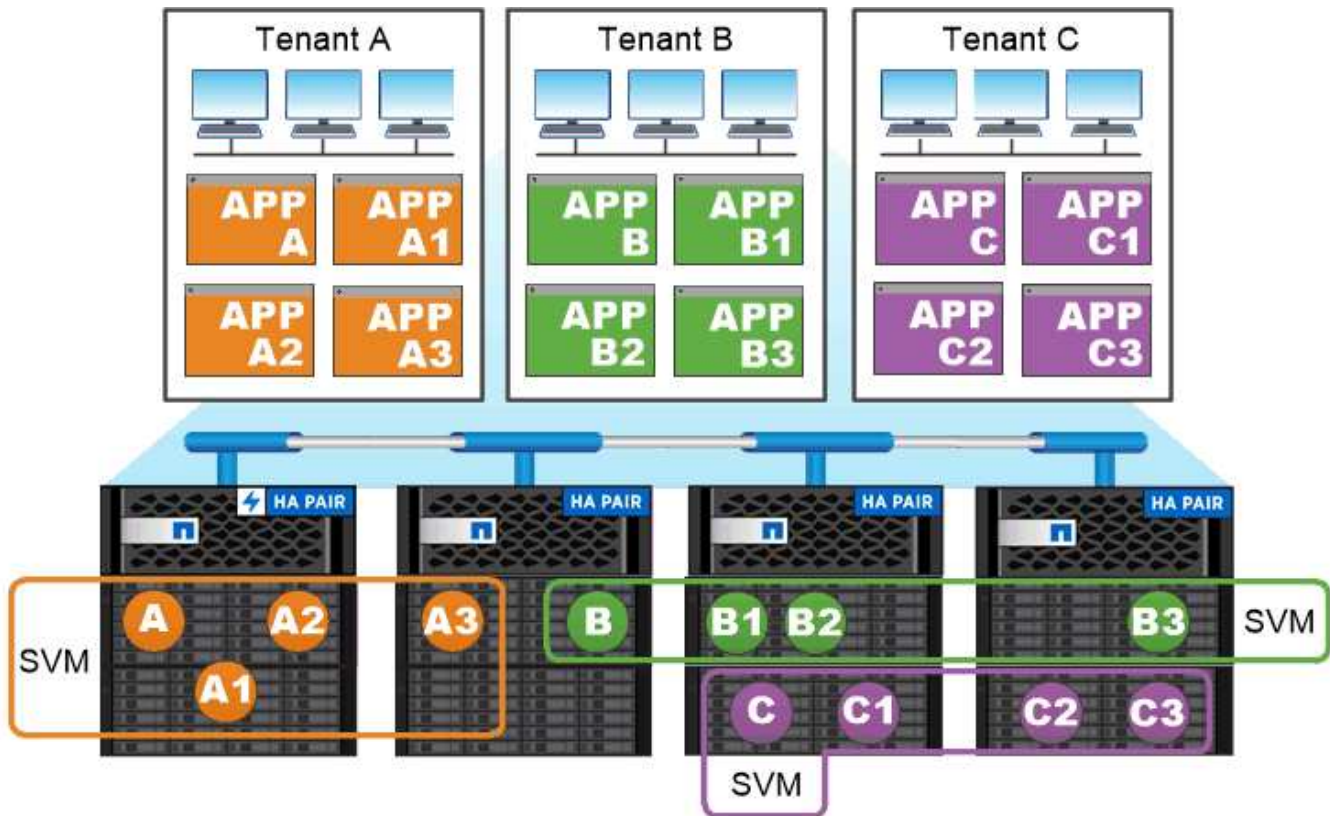
The logical objects ONTAP uses for storage management tasks serve the familiar goals of a well-designed middleware package: shielding the administrator from low-level implementation details and insulating the configuration from changes in physical characteristics like nodes and ports. The basic idea is that the administrator should be able to move volumes and LIFs easily, reconfiguring a few fields rather than the entire storage infrastructure.

### **SVM use cases**

Service providers use SVMs in secure multitenancy arrangements to isolate each tenant's data, to provide each tenant with its own authentication and administration, and to simplify chargeback. You can assign multiple LIFs to the same SVM to satisfy different customer needs, and you can use QoS to protect against tenant workloads "bullying" the workloads of other tenants.

Administrators use SVMs for similar purposes in the enterprise. You might want to segregate data from different departments, or keep storage volumes accessed by hosts in one SVM and user share volumes in another. Some administrators put iSCSI/FC LUNs and NFS datastores in one SVM and SMB shares in

another.



*Service providers use SVMs in multitenant environments to isolate tenant data and simplify chargeback.*

### Cluster and SVM administration

A *cluster administrator* accesses the admin SVM for the cluster. The admin SVM and a cluster administrator with the reserved name `admin` are automatically created when the cluster is set up.

A cluster administrator with the default `admin` role can administer the entire cluster and its resources. The cluster administrator can create additional cluster administrators with different roles as needed.

An *SVM administrator* accesses a data SVM. The cluster administrator creates data SVMs and SVM administrators as needed.

SVM administrators are assigned the `vsadmin` role by default. The cluster administrator can assign different roles to SVM administrators as needed.

### **Role-Based Access Control (RBAC)**

The *role* assigned to an administrator determines the commands to which the administrator has access. You assign the role when you create the account for the administrator. You can assign a different role or define custom roles as needed.

## Namespaces and junction points

A NAS *namespace* is a logical grouping of volumes joined together at *junction points* to create a single file system hierarchy. A client with sufficient permissions can access files in the namespace without specifying the location of the files in storage. Junctioned volumes can reside anywhere in the cluster.

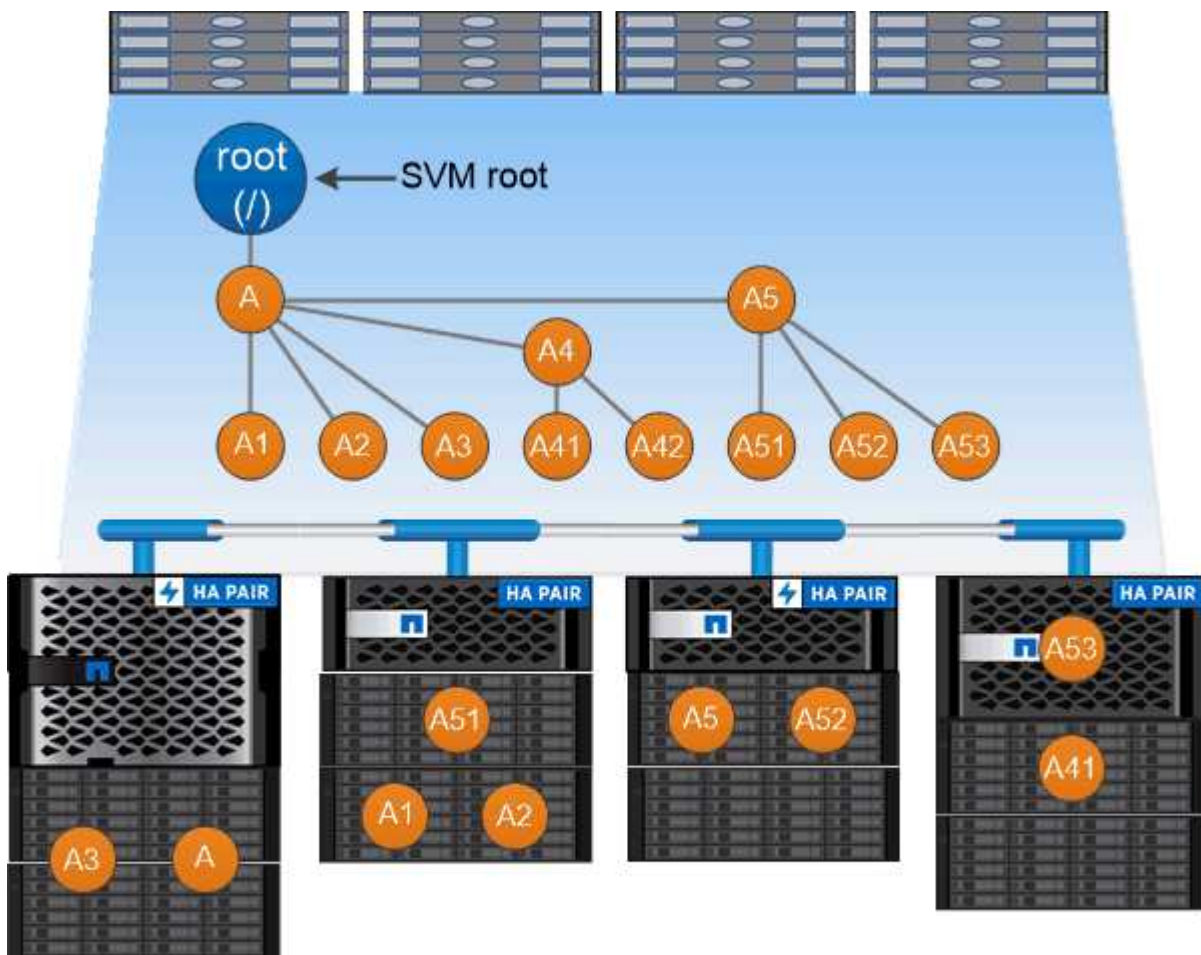
Rather than mounting every volume containing a file of interest, NAS clients mount an NFS *export* or access an SMB *share*. The export or share represents the entire namespace or an intermediate location within the namespace. The client accesses only the volumes mounted below its access point.

You can add volumes to the namespace as needed. You can create junction points directly below a parent volume junction or on a directory within a volume. A path to a volume junction for a volume named “vol3” might be /vol1/vol2/vol3, or /vol1/dir2/vol3, or even /dir1/dir2/vol3. The path is called the *junction path*.

Every SVM has a unique namespace. The SVM root volume is the entry point to the namespace hierarchy.



To ensure that data remains available in the event of a node outage or failover, you should create a *load-sharing mirror copy* for the SVM root volume.



*A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.*

## Example

The following example creates a volume named “home4” located on SVM vs1 that has a junction path /eng/home:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

## Path failover

### Path failover overview

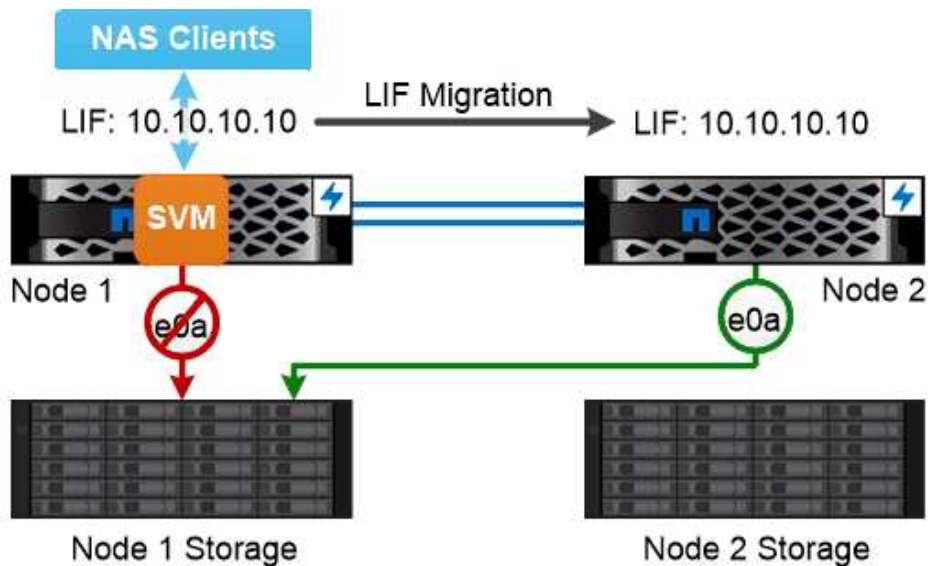
There are important differences in how ONTAP manages path failover in NAS and SAN topologies. A NAS LIF automatically migrates to a different network port after a link failure. A SAN LIF does not migrate (unless you move it manually after the failure). Instead, multipathing technology on the host diverts traffic to a different LIF—on the same SVM, but accessing a different network port.

### NAS path failover

A NAS LIF automatically migrates to a surviving network port after a link failure on its current port. The port to which the LIF migrates must be a member of the *failover group* for the LIF. The *failover group policy* narrows the failover targets for a data LIF to ports on the node that owns the data and its HA partner.

For administrative convenience, ONTAP creates a failover group for each *broadcast domain* in the network architecture. Broadcast domains group ports that belong to the same layer 2 network. If you are using VLANs, for example, to segregate traffic by department (Engineering, Marketing, Finance, and so on), each VLAN defines a separate broadcast domain. The failover group associated with the broadcast domain is automatically updated each time you add or remove a broadcast domain port.

It is almost always a good idea to use a broadcast domain to define a failover group to ensure that the failover group remains current. Occasionally, however, you may want to define a failover group that is not associated with a broadcast domain. For example, you may want LIFs to fail over only to ports in a subset of the ports defined in the broadcast domain.



*A NAS LIF automatically migrates to a surviving network port after a link failure on its current port.*

### Subnets

A *subnet* reserves a block of IP addresses in a broadcast domain. These addresses belong to the same layer 3 network and are allocated to ports in the broadcast domain when you create a LIF. It is usually easier and less error-prone to specify a subnet name when you define a LIF address than it is to specify an IP address and network mask.

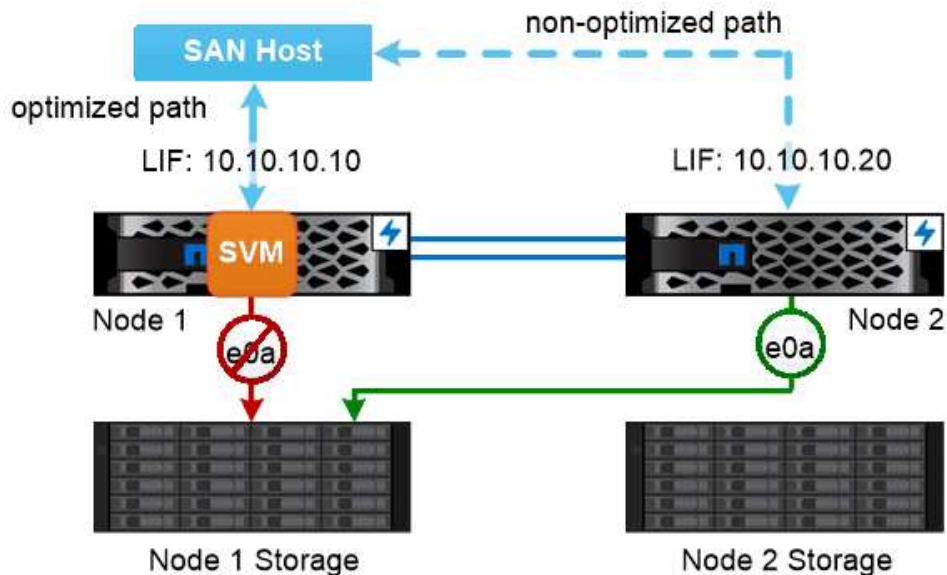
### SAN path failover

A SAN host uses ALUA (Asymmetric Logical Unit Access) and MPIO (multipath I/O) to reroute traffic to a surviving LIF after a link failure. Predefined paths determine the possible routes to the LUN served by the SVM.

In a SAN environment, hosts are regarded as *initiators* of requests to LUN *targets*. MPIO enables multiple paths from initiators to targets. ALUA identifies the most direct paths, called *optimized paths*.

You typically configure multiple optimized paths to LIFs on the LUN's owning node, and multiple non-optimized paths to LIFs on its HA partner. If one port fails on the owning node, the host routes traffic to the surviving ports. If all the ports fail, the host routes traffic over the non-optimized paths.

ONTAP Selective LUN Map (SLM) limits the number of paths from the host to a LUN by default. A newly created LUN is accessible only through paths to the node that owns the LUN or its HA partner. You can also limit access to a LUN by configuring LIFs in a *port set* for the initiator.



A SAN host uses multipathing technology to reroute traffic to a surviving LIF after a link failure.

### Moving volumes in SAN environments

By default, ONTAP *Selective LUN Map (SLM)* limits the number of paths to a LUN from a SAN host. A newly created LUN is accessible only through paths to the node that owns the LUN or its HA partner, the *reporting nodes* for the LUN.

This means that when you move a volume to a node on another HA pair, you need to add reporting nodes for the destination HA pair to the LUN mapping. You can then specify the new paths in your MPIO setup. After the volume move is complete, you can delete the reporting nodes for the source HA pair from the mapping.

## Load balancing

Performance of workloads begins to be affected by latency when the amount of work on a node exceeds the available resources. You can manage an overloaded node by increasing the available resources (upgrading disks or CPU), or by reducing load (moving volumes or LUNs to different nodes as needed).

You can also use ONTAP *storage quality of service (QoS)* to guarantee that performance of critical workloads is not degraded by competing workloads:

- You can set a QoS throughput *ceiling* on a competing workload to limit its impact on system resources (QoS Max).
- You can set a QoS throughput *floor* for a critical workload, ensuring that it meets minimum throughput targets regardless of demand by competing workloads (QoS Min).
- You can set a QoS ceiling and floor for the same workload.

### Throughput ceilings

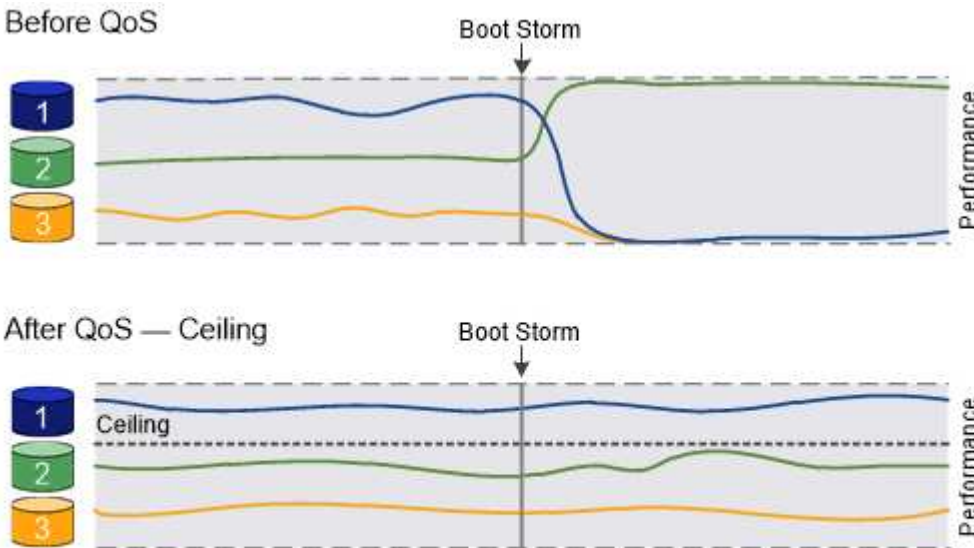
A throughput ceiling limits throughput for a workload to a maximum number of IOPS or MB/s. In the figure

below, the throughput ceiling for workload 2 ensures that it does not “bully” workloads 1 and 3.

A *policy group* defines the throughput ceiling for one or more workloads. A workload represents the I/O operations for a *storage object*: a volume, file, or LUN, or all the volumes, files, or LUNs in an SVM. You can specify the ceiling when you create the policy group, or you can wait until after you monitor workloads to specify it.



Throughput to workloads might exceed the specified ceiling by up to 10 percent, especially if a workload experiences rapid changes in throughput. The ceiling might be exceeded by up to 50% to handle bursts.



*The throughput ceiling for workload 2 ensures that it does not “bully” workloads 1 and 3.*

### Throughput floors

A throughput floor guarantees that throughput for a workload does not fall below a minimum number of IOPS. In the figure below, the throughput floors for workload 1 and workload 3 ensure that they meet minimum throughput targets, regardless of demand by workload 2.



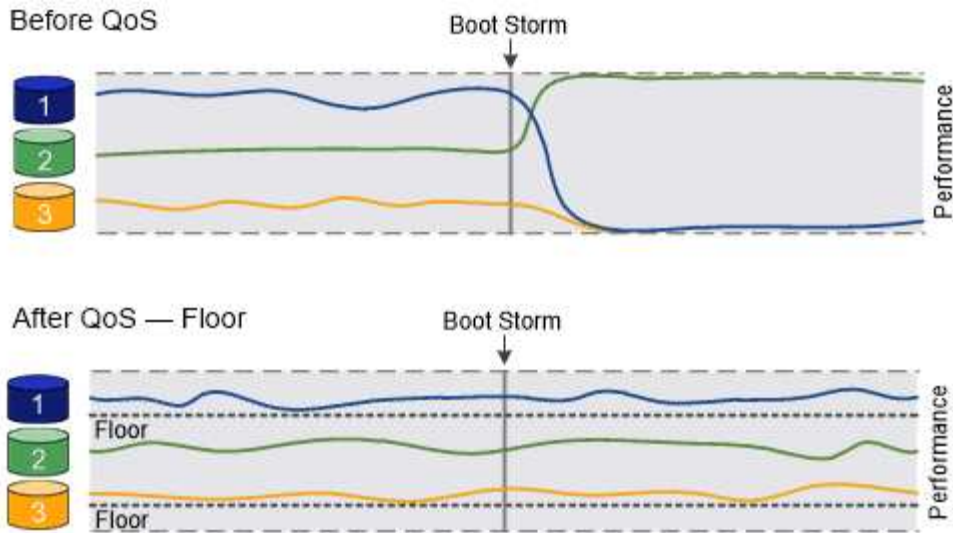
As the examples suggest, a throughput ceiling throttles throughput directly. A throughput floor throttles throughput indirectly, by giving priority to the workloads for which the floor has been set.

A workload represents the I/O operations for a volume, LUN, or, beginning with ONTAP 9.3, file. A policy group that defines a throughput floor cannot be applied to an SVM. You can specify the floor when you create the policy group, or you can wait until after you monitor workloads to specify it.



Throughput to a workload might fall below the specified floor if there is insufficient performance capacity (headroom) on the node or aggregate, or during critical operations like `volume move trigger-cutover`. Even when sufficient capacity is available and critical operations are not taking place, throughput to a workload might fall below the specified floor by up to 5 percent.





*The throughput floors for workload 1 and workload 3 ensure that they meet minimum throughput targets, regardless of demand by workload 2.*

## Adaptive QoS

Ordinarily, the value of the policy group you assign to a storage object is fixed. You need to change the value manually when the size of the storage object changes. An increase in the amount of space used on a volume, for example, usually requires a corresponding increase in the throughput ceiling specified for the volume.

*Adaptive QoS* automatically scales the policy group value to workload size, maintaining the ratio of IOPS to TBs|GBs as the size of the workload changes. That's a significant advantage when you are managing hundreds or thousands of workloads in a large deployment.

You typically use adaptive QoS to adjust throughput ceilings, but you can also use it to manage throughput floors (when workload size increases). Workload size is expressed as either the allocated space for the storage object or the space used by the storage object.



Used space is available for throughput floors in ONTAP 9.5 and later. It is not supported for throughput floors in ONTAP 9.4 and earlier.

- An *allocated space* policy maintains the IOPS/TB|GB ratio according to the nominal size of the storage object. If the ratio is 100 IOPS/GB, a 150 GB volume will have a throughput ceiling of 15,000 IOPS for as long as the volume remains that size. If the volume is resized to 300 GB, adaptive QoS adjusts the throughput ceiling to 30,000 IOPS.
- A *used space* policy (the default) maintains the IOPS/TB|GB ratio according to the amount of actual data stored before storage efficiencies. If the ratio is 100 IOPS/GB, a 150 GB volume that has 100 GB of data stored would have a throughput ceiling of 10,000 IOPS. As the amount of used space changes, adaptive QoS adjusts the throughput ceiling according to the ratio.

## Replication

### Snapshot copies

Traditionally, ONTAP replication technologies served the need for disaster recovery (DR) and data archiving. With the advent of cloud services, ONTAP replication has been

adapted to data transfer between endpoints in the NetApp data fabric. The foundation for all these uses is ONTAP Snapshot technology.

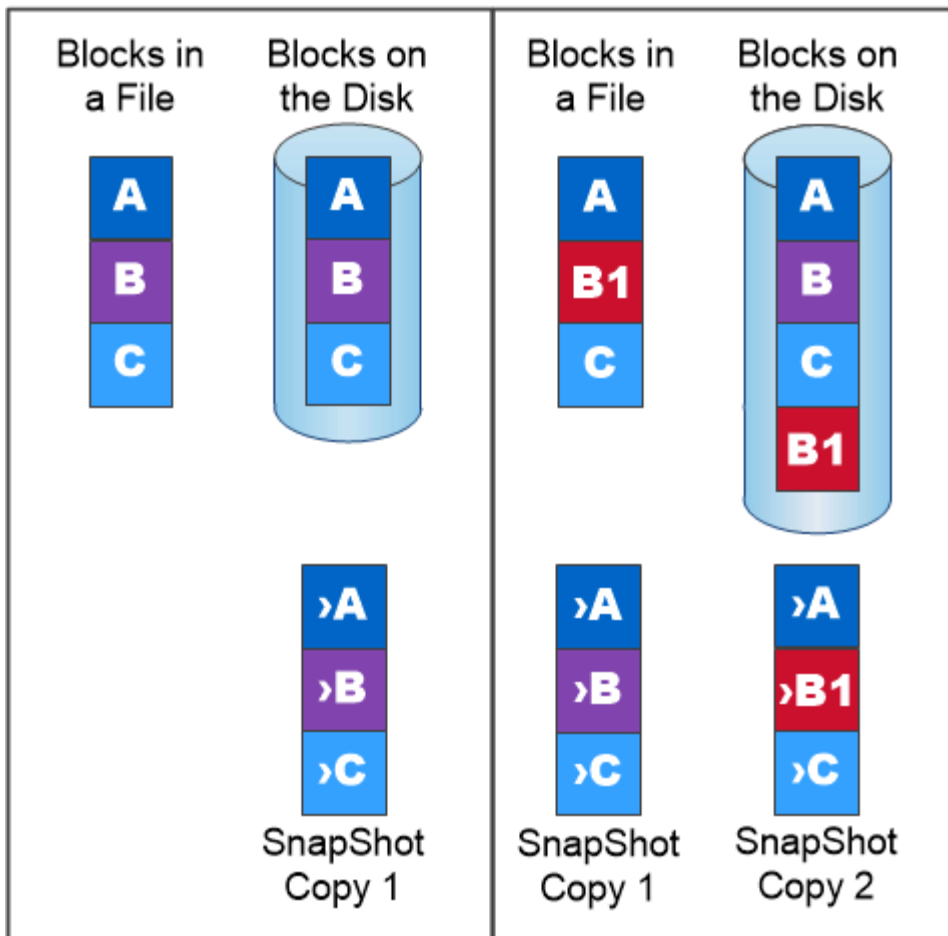
A *Snapshot copy* is a read-only, point-in-time image of a volume. The image consumes minimal storage space and incurs negligible performance overhead because it records only changes to files since the last Snapshot copy was made.

Snapshot copies owe their efficiency to ONTAP's core storage virtualization technology, its *Write Anywhere File Layout (WAFL)*. Like a database, WAFL uses metadata to point to actual data blocks on disk. But, unlike a database, WAFL does not overwrite existing blocks. It writes updated data to a new block and changes the metadata.

It's because ONTAP references metadata when it creates a Snapshot copy, rather than copying data blocks, that Snapshot copies are so efficient. Doing so eliminates the "seek time" that other systems incur in locating the blocks to copy, as well as the cost of making the copy itself.

You can use a Snapshot copy to recover individual files or LUNs, or to restore the entire contents of a volume. ONTAP compares pointer information in the Snapshot copy with data on disk to reconstruct the missing or damaged object, without downtime or a significant performance cost.

A *Snapshot policy* defines how the system creates Snapshot copies of volumes. The policy specifies when to create the Snapshot copies, how many copies to retain, how to name them, and how to label them for replication. For example, a system might create one Snapshot copy every day at 12:10 a.m., retain the two most recent copies, name them "daily" (appended with a timestamp), and label them "daily" for replication.



*A Snapshot copy records only changes to the active file system since the last Snapshot copy.*

### SnapMirror disaster recovery and data transfer

*SnapMirror* is disaster recovery technology, designed for failover from primary storage to secondary storage at a geographically remote site. As its name implies, SnapMirror creates a replica, or *mirror*, of your working data in secondary storage from which you can continue to serve data in the event of a catastrophe at the primary site.

Data is mirrored at the volume level. The relationship between the source volume in primary storage and the destination volume in secondary storage is called a *data protection relationship*. The clusters in which the volumes reside and the SVMs that serve data from the volumes must be *peered*. A peer relationship enables clusters and SVMs to exchange data securely.



You can also create a data protection relationship between SVMs. In this type of relationship, all or part of the SVM's configuration, from NFS exports and SMB shares to RBAC, is replicated, as well as the data in the volumes the SVM owns.

Beginning with ONTAP 9.10.1, you can create data protection relationships between S3 buckets using S3 SnapMirror. Destination buckets can be on local or remote ONTAP systems, or on non-ONTAP systems such as StorageGRID and AWS.

The first time you invoke SnapMirror, it performs a *baseline transfer* from the source volume to the destination volume. The baseline transfer typically involves the following steps:

- Make a Snapshot copy of the source volume.
- Transfer the Snapshot copy and all the data blocks it references to the destination volume.
- Transfer the remaining, less recent Snapshot copies on the source volume to the destination volume for use in case the “active” mirror is corrupted.

Once a baseline transfer is complete, SnapMirror transfers only new Snapshot copies to the mirror. Updates are asynchronous, following the schedule you configure. Retention mirrors the Snapshot policy on the source. You can activate the destination volume with minimal disruption in case of a disaster at the primary site, and reactivate the source volume when service is restored.

Because SnapMirror transfers only Snapshot copies after the baseline is created, replication is fast and nondisruptive. As the failover use case implies, the controllers on the secondary system should be equivalent or nearly equivalent to the controllers on the primary system to serve data efficiently from mirrored storage.



*A SnapMirror data protection relationship mirrors the Snapshot copies available on the source volume.*

### **Using SnapMirror for data transfer**

You can also use SnapMirror to replicate data between endpoints in the NetApp data fabric. You can choose between one-time replication or recurring replication when you create the SnapMirror policy.

### **SnapMirror Cloud backups to object storage**

*SnapMirror Cloud* is a backup and recovery technology designed for ONTAP users who want to transition their data protection workflows to the cloud. Organizations moving away from legacy backup-to-tape architectures can use object storage as an alternative repository for long-term data retention and archiving. SnapMirror Cloud provides ONTAP-to-object storage replication as part of an incremental forever backup strategy.

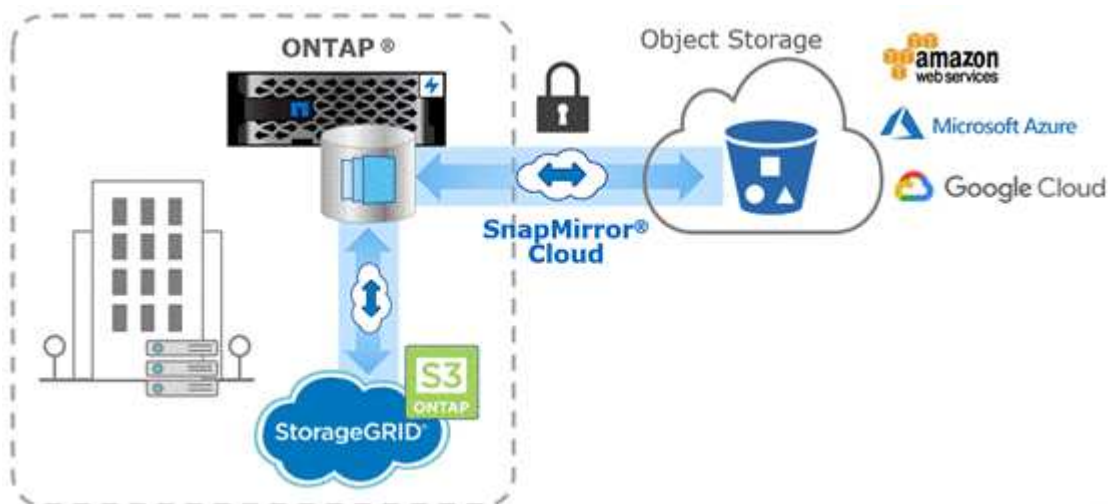
SnapMirror Cloud was introduced in ONTAP 9.8 as an extension to the family of SnapMirror replication technologies. While SnapMirror is frequently used for ONTAP-to-ONTAP backups, SnapMirror Cloud uses the same replication engine to transfer Snapshot copies for ONTAP to S3-compliant object storage backups.

Targeted for backup use cases, SnapMirror Cloud supports both long-term retention and archives workflows. As with SnapMirror, the initial SnapMirror Cloud backup performs a baseline transfer of a volume. For subsequent backups, SnapMirror Cloud generates a snapshot copy of the source volume and transfers the snapshot copy with only the changed data blocks to an object storage target.

SnapMirror Cloud relationships can be configured between ONTAP systems and select on-premises and public cloud object storage targets - including AWS S3, Google Cloud Storage Platform, and Microsoft Azure Blob Storage. Additional on-premises object storage targets include StoragGRID and ONTAP S3.

SnapMirror Cloud replication is a licensed ONTAP feature and requires an approved application to orchestrate data protection workflows. Several orchestration options are available for managing SnapMirror Cloud backups:

- Multiple 3rd party backup partners who offer support for SnapMirror Cloud replication. Participating vendors are available on the [NetApp blog](#).
- Cloud Manager and Cloud Backup for a NetApp-native solution for ONTAP environments
- APIs for developing custom software for data protection workflows or leveraging automation tools



### SnapVault archiving

The SnapMirror license is used to support both SnapVault relationships for backup, and SnapMirror relationships for disaster recovery. SnapVault licenses were deprecated, and SnapMirror licenses can now be used to configure vault, mirror, and mirror-and-vault relationships. SnapMirror replication is used for ONTAP-to-ONTAP replication of Snapshot copies, supporting both backup and disaster recovery use cases.

*SnapVault* is archiving technology, designed for disk-to-disk Snapshot copy replication for standards compliance and other governance-related purposes. In contrast to a SnapMirror relationship, in which the destination usually contains only the Snapshot copies currently in the source volume, a SnapVault destination typically retains point-in-time Snapshot copies created over a much longer period.

You might want to keep monthly Snapshot copies of your data over a 20-year span, for example, to comply with government accounting regulations for your business. Since there is no requirement to serve data from

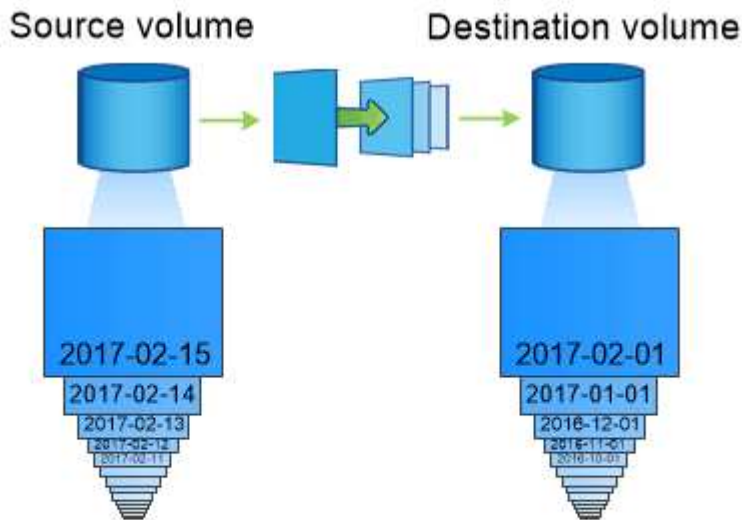
vault storage, you can use slower, less expensive disks on the destination system.

As with SnapMirror, SnapVault performs a baseline transfer the first time you invoke it. It makes a Snapshot copy of the source volume, then transfers the copy and the data blocks it references to the destination volume. Unlike SnapMirror, SnapVault does not include older Snapshot copies in the baseline.

Updates are asynchronous, following the schedule you configure. The rules you define in the policy for the relationship identify which new Snapshot copies to include in updates and how many copies to retain. The labels defined in the policy (“monthly,” for example) must match one or more labels defined in the Snapshot policy on the source. Otherwise, replication fails.



SnapMirror and SnapVault share the same command infrastructure. You specify which method you want to use when you create a policy. Both methods require peered clusters and peered SVMs.



*A SnapVault data protection relationship typically retains point-in-time Snapshot copies created over a longer period than the Snapshot copies on the source volume.*

### Cloud backup and support for traditional backups

In addition to SnapMirror and SnapVault data protection relationships, which were previously disk-to-disk only, there are now several backup solutions that offer a less expensive alternative for long-term data retention.

Numerous third-party data protection applications offer traditional backup for ONTAP-managed data. Veeam, Veritas, and Commvault, among others, all offer integrated backup for ONTAP systems.

Beginning with ONTAP 9.8, SnapMirror Cloud provides asynchronous replication of Snapshot copies from ONTAP instances to object storage endpoints. SnapMirror Cloud replication requires a licensed application for orchestration and management of data protection workflows. SnapMirror Cloud relationships are supported from ONTAP systems to select on-premises and public cloud object storage targets — including AWS S3, Google Cloud Storage Platform, or Microsoft Azure Blob Storage — which provides enhanced efficiency with vendor backup software. Contact your NetApp representative for a list of supported certified applications and object storage vendors.

If you are interested in cloud-native data protection, Cloud Manager can be used to configure SnapMirror or SnapVault relationships between on-premises volumes and Cloud Volumes ONTAP instances in the public cloud.

Cloud Manager also provides backups of Cloud Volumes ONTAP instances using a Software as a Service (SaaS) model. Users can back up their Cloud Volumes ONTAP instances to S3 and S3-compliant public cloud object storage using Cloud Backup found on NetApp Cloud Central.

[Cloud Volumes ONTAP and Cloud Manager documentation resources](#)

[NetApp Cloud Central](#)

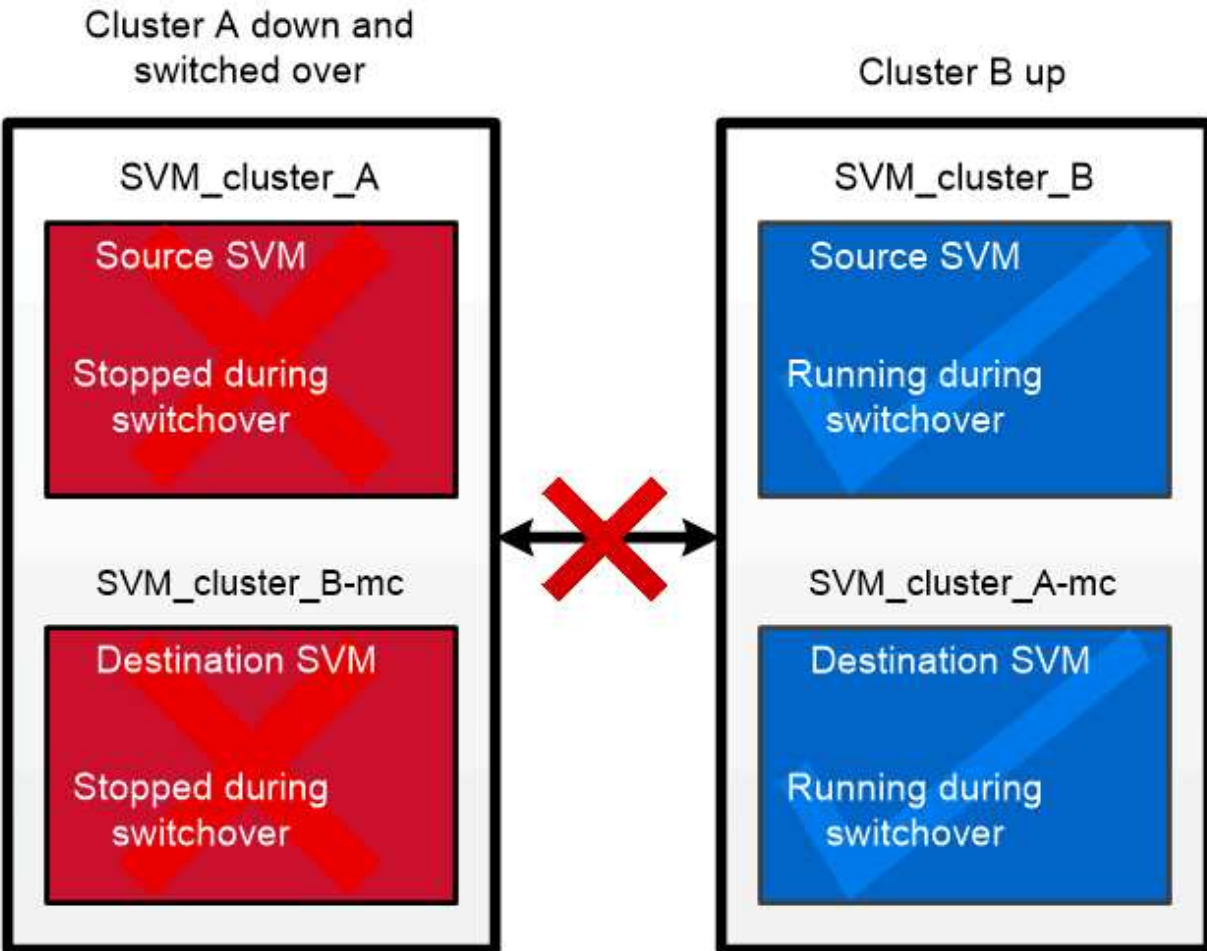
### **MetroCluster continuous availability**

MetroCluster configurations protect data by implementing two physically separate, mirrored clusters. Each cluster synchronously replicates the data and SVM configuration of the other. In the event of a disaster at one site, an administrator can activate the mirrored SVM and begin serving data from the surviving site.

- *Fabric-attached MetroCluster* configurations support metropolitan-wide clusters.
- *Stretch MetroCluster* configurations support campus-wide clusters.

Clusters must be peered in either case.

MetroCluster uses an ONTAP feature called *SyncMirror* to synchronously mirror aggregate data for each cluster in copies, or *plexes*, in the other cluster's storage. If a switchover occurs, the remote plex on the surviving cluster comes online and the secondary SVM begins serving data.



*When a MetroCluster switchover occurs, the remote plex on the surviving cluster comes online and the secondary SVM begins serving data.*

#### **Using SyncMirror in non-MetroCluster implementations**

You can optionally use SyncMirror in a non-MetroCluster implementation to protect against data loss if more disks fail than the RAID type protects against, or if there is a loss of connectivity to RAID group disks. The feature is available for HA pairs only.

Aggregate data is mirrored in plexes stored on different disk shelves. If one of the shelves becomes unavailable, the unaffected plex continues to serve data while you fix the cause of the failure.

Keep in mind that an aggregate mirrored using SyncMirror requires twice as much storage as an unmirrored aggregate. Each plex requires as many disks as the plex it mirrors. You would need 2,880 GB of disk space, for example, to mirror a 1,440 GB aggregate, 1,440 GB for each plex.



SyncMirror is also available for FlexArray Virtualization implementations.

## **Storage efficiency**



## Thin provisioning

ONTAP offers a wide range of storage efficiency technologies in addition to Snapshot copies. Key technologies include thin provisioning, deduplication, compression, and FlexClone volumes, files, and LUNs. Like Snapshot copies, all are built on ONTAP's Write Anywhere File Layout (WAFL).

A *thin-provisioned* volume or LUN is one for which storage is not reserved in advance. Instead, storage is allocated dynamically, as it is needed. Free space is released back to the storage system when data in the volume or LUN is deleted.

Suppose that your organization needs to supply 5,000 users with storage for home directories. You estimate that the largest home directories will consume 1 GB of space.

In this situation, you could purchase 5 TB of physical storage. For each volume that stores a home directory, you would reserve enough space to satisfy the needs of the largest consumers.

As a practical matter, however, you also know that home directory capacity requirements vary greatly across your community. For every large user of storage, there are ten who consume little or no space.

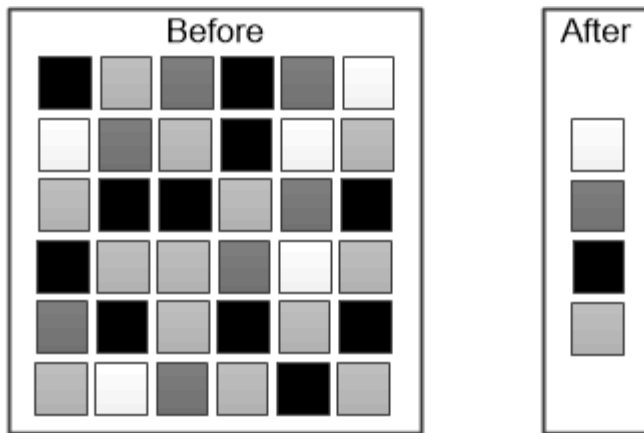
Thin provisioning allows you to satisfy the needs of the large storage consumers without having to purchase storage you might never use. Since storage space is not allocated until it is consumed, you can "overcommit" an aggregate of 2 TB by nominally assigning a size of 1 GB to each of the 5,000 volumes the aggregate contains.

As long as you are correct that there is a 10:1 ratio of light to heavy users, and as long as you take an active role in monitoring free space on the aggregate, you can be confident that volume writes won't fail due to lack of space.

## Deduplication

*Deduplication* reduces the amount of physical storage required for a volume (or all the volumes in an AFF aggregate) by discarding duplicate blocks and replacing them with references to a single shared block. Reads of deduplicated data typically incur no performance charge. Writes incur a negligible charge except on overloaded nodes.

As data is written during normal use, WAFL uses a batch process to create a catalog of *block signatures*. After deduplication starts, ONTAP compares the signatures in the catalog to identify duplicate blocks. If a match exists, a byte-by-byte comparison is done to verify that the candidate blocks have not changed since the catalog was created. Only if all the bytes match is the duplicate block discarded and its disk space reclaimed.



*Deduplication reduces the amount of physical storage required for a volume by discarding duplicate data blocks.*

### Compression

*Compression* reduces the amount of physical storage required for a volume by combining data blocks in *compression groups*, each of which is stored as a single block. Reads of compressed data are faster than in traditional compression methods because ONTAP decompresses only the compression groups that contain the requested data, not an entire file or LUN.

You can perform inline or postprocess compression, separately or in combination:

- *Inline compression* compresses data in memory before it is written to disk, significantly reducing the amount of write I/O to a volume, but potentially degrading write performance. Performance-intensive operations are deferred until the next postprocess compression operation, if any.
- *Postprocess compression* compresses data after it is written to disk, on the same schedule as deduplication.

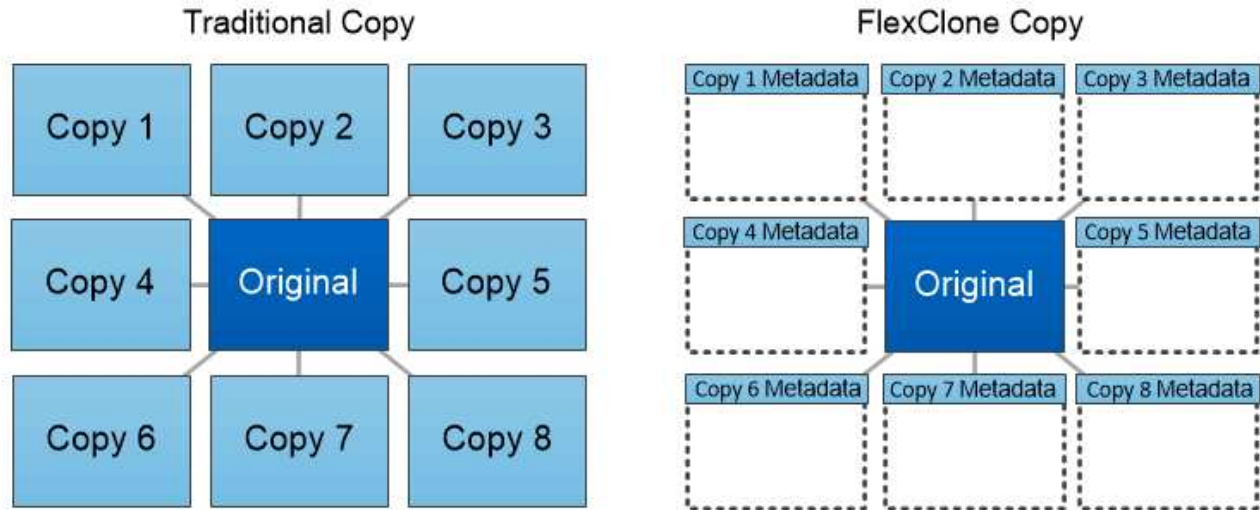
***Inline data compaction*** Small files or I/O padded with zeros are stored in a 4 KB block whether or not they require 4 KB of physical storage. *Inline data compaction* combines data chunks that would ordinarily consume multiple 4 KB blocks into a single 4 KB block on disk. Compaction takes place while data is still in memory, so it is best suited to faster controllers.

### FlexClone volumes, files, and LUNs

*FlexClone* technology references Snapshot metadata to create writable, point-in-time copies of a volume. Copies share data blocks with their parents, consuming no storage except what is required for metadata until changes are written to the copy. FlexClone files and FlexClone LUNs use identical technology, except that a backing Snapshot copy is not required.

Where traditional copies can take minutes or even hours to create, FlexClone software lets you copy even the largest datasets almost instantaneously. That makes it ideal for situations in which you need multiple copies of identical datasets (a virtual desktop deployment, for example) or temporary copies of a dataset (testing an application against a production dataset).

You can clone an existing FlexClone volume, clone a volume containing LUN clones, or clone mirror and vault data. You can *split* a FlexClone volume from its parent, in which case the copy is allocated its own storage.



*FlexClone copies share data blocks with their parents, consuming no storage except what is required for metadata.*

## Security

### Client authentication and authorization

ONTAP uses standard methods to secure client and administrator access to storage and to protect against viruses. Advanced technologies are available for encryption of data at rest and for WORM storage.

ONTAP authenticates a client machine and user by verifying their identities with a trusted source. ONTAP authorizes a user to access a file or directory by comparing the user's credentials with the permissions configured on the file or directory.

### Authentication

You can create local or remote user accounts:

- A local account is one in which the account information resides on the storage system.
- A remote account is one in which account information is stored on an Active Directory domain controller, an LDAP server, or a NIS server.

ONTAP uses local or external name services to look up host name, user, group, netgroup, and name mapping information. ONTAP supports the following name services:

- Local users
- DNS
- External NIS domains
- External LDAP domains

A *name service switch table* specifies the sources to search for network information and the order in which to

search them (providing the equivalent functionality of the `/etc/nsswitch.conf` file on UNIX systems). When a NAS client connects to the SVM, ONTAP checks the specified name services to obtain the required information.

**Kerberos support** Kerberos is a network authentication protocol that provides “strong authentication” by encrypting user passwords in client-server implementations. ONTAP supports Kerberos 5 authentication with integrity checking (`krb5i`) and Kerberos 5 authentication with privacy checking (`krb5p`).

## Authorization

ONTAP evaluates three levels of security to determine whether an entity is authorized to perform a requested action on files and directories residing on an SVM. Access is determined by the effective permissions after evaluation of the security levels:

- Export (NFS) and share (SMB) security

Export and share security applies to client access to a given NFS export or SMB share. Users with administrative privileges can manage export and share-level security from SMB and NFS clients.

- Storage-Level Access Guard file and directory security

Storage-Level Access Guard security applies to SMB and NFS client access to SVM volumes. Only NTFS access permissions are supported. For ONTAP to perform security checks on UNIX users for access to data on volumes for which Storage-Level Access Guard has been applied, the UNIX user must map to a Windows user on the SVM that owns the volume.

- NTFS, UNIX, and NFSv4 native file-level security

Native file-level security exists on the file or directory that represents the storage object. You can set file-level security from a client. File permissions are effective regardless of whether SMB or NFS is used to access the data.

## Administrator authentication and RBAC

Administrators use local or remote login accounts to authenticate themselves to the cluster and SVM. Role-Based Access Control (RBAC) determines the commands to which an administrator has access.

### Authentication

You can create local or remote cluster and SVM administrator accounts:

- A local account is one in which the account information, public key, or security certificate resides on the storage system.
- A remote account is one in which account information is stored on an Active Directory domain controller, an LDAP server, or a NIS server.

Except for DNS, ONTAP uses the same name services to authenticate administrator accounts as it uses to authenticate clients.

## RBAC

The *role* assigned to an administrator determines the commands to which the administrator has access. You assign the role when you create the account for the administrator. You can assign a different role or define custom roles as needed.

## Virus scanning

You can use integrated antivirus functionality on the storage system to protect data from being compromised by viruses or other malicious code. ONTAP virus scanning, called *Vscan*, combines best-in-class third-party antivirus software with ONTAP features that give you the flexibility you need to control which files get scanned and when.

Storage systems offload scanning operations to external servers hosting antivirus software from third-party vendors. The *ONTAP Antivirus Connector*, provided by NetApp and installed on the external server, handles communications between the storage system and the antivirus software.

- You can use *on-access scanning* to check for viruses when clients open, read, rename, or close files over SMB. File operation is suspended until the external server reports the scan status of the file. If the file has already been scanned, ONTAP allows the file operation. Otherwise, it requests a scan from the server.

On-access scanning is not supported for NFS.

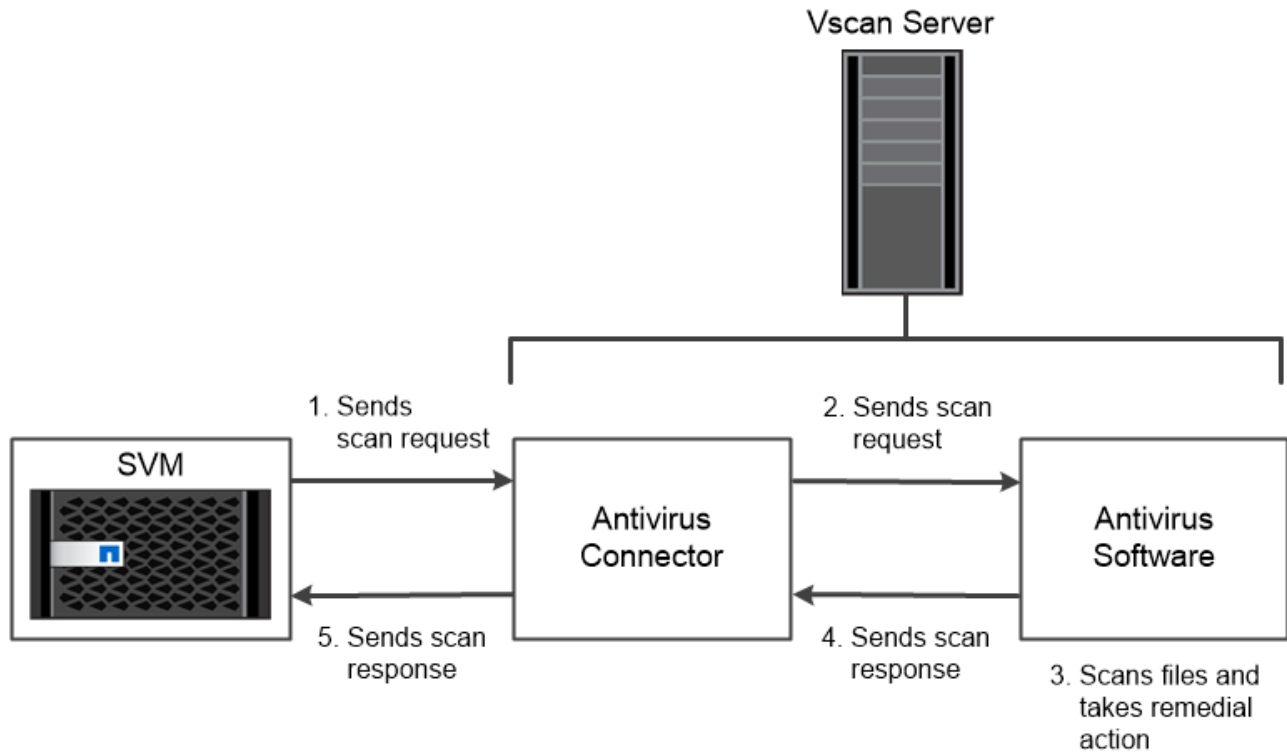
- You can use *on-demand scanning* to check files for viruses immediately or on a schedule. You might want to run scans only in off-peak hours, for example. The external server updates the scan status of the checked files, so that file-access latency for those files (assuming they have not been modified) is typically reduced when they are next accessed over SMB.

You can use on-demand scanning for any path in the SVM namespace, even for volumes that are exported only through NFS.

You typically enable both scanning modes on an SVM. In either mode, the antivirus software takes remedial action on infected files based on your settings in the software.

### ***Virus scanning in disaster recovery and MetroCluster configurations***

For disaster recovery and MetroCluster configurations, you must set up separate Vscan servers for the local and partner clusters.



*The storage system offloads virus scanning operations to external servers hosting antivirus software from third-party vendors.*

## Encryption

ONTAP offers both software- and hardware-based encryption technologies to ensure that data at rest cannot be read if the storage medium is repurposed, returned, misplaced, or stolen.

ONTAP is compliant with the Federal Information Processing Standards (FIPS) 140-2 for all SSL connections. You can use the following encryption solutions:

- Hardware solutions:

- NetApp Storage Encryption (NSE)

NSE is a hardware solution that uses self-encrypting drives (SEDs).

- NVMe SEDs

ONTAP provides full disk encryption for NVMe SEDs that do not have FIPS 140-2 certification.

- Software solutions:

- NetApp Aggregate Encryption (NAE)

NAE is a software solution that enables encryption of any data volume on any drive type where it is enabled with unique keys for each aggregate.

- NetApp Volume Encryption (NVE)

NVE is a software solution that enables encryption of any data volume on any drive type where it is

enabled with a unique key for each volume.

Use both software (NAE or NVE) and hardware (NSE or NVMe SED) encryption solutions to achieve double encryption at rest. Storage efficiency is not affected by NAE or NVE encryption.

### **NetApp Storage Encryption**

NetApp Storage Encryption (NSE) supports SEDs that encrypt data as it is written. The data cannot be read without an encryption key stored on the disk. The encryption key, in turn, is accessible only to an authenticated node.

On an I/O request, a node authenticates itself to an SED using an authentication key retrieved from an external key management server or Onboard Key Manager:

- The external key management server is a third-party system in your storage environment that serves authentication keys to nodes using the Key Management Interoperability Protocol (KMIP).
- The Onboard Key Manager is a built-in tool that serves authentication keys to nodes from the same storage system as your data.

NSE supports self-encrypting HDDs and SSDs. You can use NetApp Volume Encryption with NSE to double encrypt data on NSE drives.

### **NVMe self-encrypting drives**

NVMe SEDs do not have FIPS 140-2 certification, however, these disks use AES 256-bit transparent disk encryption to protect data at rest.

Data encryption operations, such as generating an authentication key, are performed internally. The authentication key is generated the first time the disk is accessed by the storage system. After that, the disks protect data at rest by requiring storage system authentication each time data operations are requested.

### **NetApp Aggregate Encryption**

NetApp Aggregate Encryption (NAE) is a software-based technology for encrypting all data on an aggregate. A benefit of NAE is that volumes are included in aggregate level deduplication, whereas NVE volumes are excluded.

With NAE enabled, the volumes within the aggregate can be encrypted with aggregate keys.

Beginning with ONTAP 9.7, newly created aggregates and volumes are encrypted by default when you have the NVE license and onboard or external key management.

### **NetApp Volume Encryption**

NetApp Volume Encryption (NVE) is a software-based technology for encrypting data at rest one volume at a time. An encryption key accessible only to the storage system ensures that volume data cannot be read if the underlying device is separated from the system.

Both data, including Snapshot copies, and metadata are encrypted. Access to the data is given by a unique XTS-AES-256 key, one per volume. A built-in Onboard Key Manager secures the keys on the same system with your data.

You can use NVE on any type of aggregate (HDD, SSD, hybrid, array LUN), with any RAID type, and in any supported ONTAP implementation, including ONTAP Select. You can also use NVE with NetApp Storage Encryption (NSE) to double encrypt data on NSE drives.

**When to use KMIP servers** Although it is less expensive and typically more convenient to use the Onboard Key Manager, you should set up KMIP servers if any of the following are true:

- Your encryption key management solution must comply with Federal Information Processing Standards (FIPS) 140-2 or the OASIS KMIP standard.
- You need a multi-cluster solution. KMIP servers support multiple clusters with centralized management of encryption keys.

KMIP servers support multiple clusters with centralized management of encryption keys.

- Your business requires the added security of storing authentication keys on a system or in a location different from the data.

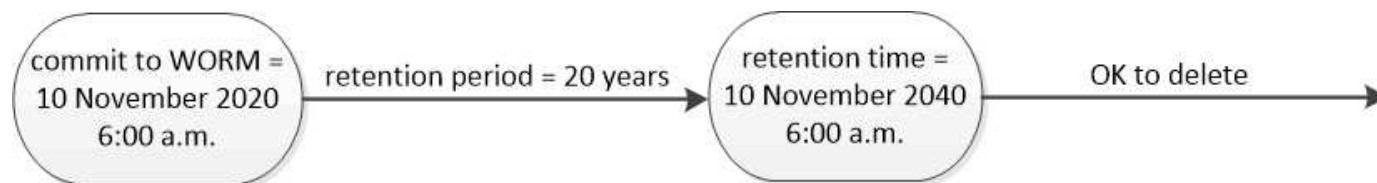
KMIP servers stores authentication keys separately from your data.

## WORM storage

*SnapLock* is a high-performance compliance solution for organizations that use *write once, read many (WORM)* storage to retain critical files in unmodified form for regulatory and governance purposes.

A single license entitles you to use SnapLock in strict *Compliance mode*, to satisfy external mandates like SEC Rule 17a-4, and a looser *Enterprise mode*, to meet internally mandated regulations for the protection of digital assets. SnapLock uses a tamper-proof *ComplianceClock* to determine when the retention period for a WORM file has elapsed.

You can use *SnapLock for SnapVault* to WORM-protect Snapshot copies on secondary storage. You can use SnapMirror to replicate WORM files to another geographic location for disaster recovery and other purposes.



*SnapLock uses a tamper-proof ComplianceClock to determine when the retention period for a WORM file has elapsed.*

## Application aware data management

Application aware data management enables you to describe the application that you want to deploy over ONTAP in terms of the application, rather than in storage terms. The application can be configured and ready to serve data quickly with minimal inputs by using System Manager and REST APIs.

The application aware data management feature provides a way to set up, manage, and monitor storage at the level of individual applications. This feature incorporates relevant ONTAP best practices to optimally provision applications, with balanced placement of storage objects based on desired performance service levels and available system resources.



The application aware data management feature includes a set of application templates, with each template consisting of a set of parameters that collectively describe the configuration of an application. These parameters, which are often preset with default values, define the characteristics that an application administrator could specify for provisioning storage on an ONTAP system, such as database sizes, service levels, protocol access elements such as LIFs as well as local protection criteria and remote protection criteria. Based on the specified parameters, ONTAP configures storage entities such as LUNs and volumes with appropriate sizes and service levels for the application.

You can perform the following tasks for your applications:

- Create applications by using the application templates
- Manage the storage associated with the applications
- Modify or delete the applications
- View applications
- Manage Snapshot copies of the applications
- Create [consistency groups](#) to provide data protection capabilities by selecting multiple LUNs in the same or in different volumes

## ONTAP and the cloud

### ONTAP and the cloud overview

Administrators of on-premises ONTAP systems can start using “the cloud.” ONTAP features are compared to the equivalent products and features in the cloud.

If you are already familiar with ONTAP but are not as familiar with cloud-based products, the following information helps you understand what you can do in the cloud and points you to other resources to learn how:

- Cloud Volumes ONTAP

A software-only storage appliance that runs ONTAP data management software in the cloud.

- Cloud Volume Services

Cloud native file services that provide metered file storage for NAS volumes. Three options are offered:

- Azure NetApp Files
- Cloud Volumes Service for AWS
- Cloud Volumes Service for Google Cloud

#### Related information

Whether you are new to these cloud products or already familiar with them, you can find more information at [NetApp Product Documentation](#).

## Data protection and the cloud

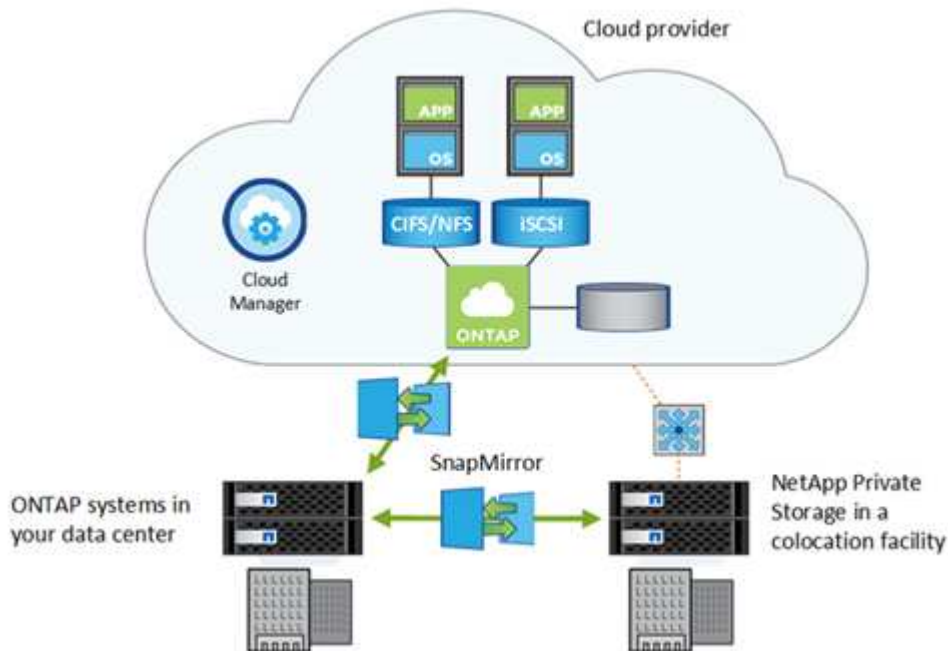
### Data protection and the cloud overview

Data protection is often the first thing customers try when they begin their cloud journey.

Protection can be as simple as asynchronous replication of key data or as complex as a complete hot-backup site. Data protection is based primarily on the familiar NetApp SnapMirror technology.

### Data replication

SnapMirror technology keeps your data synchronized between on-premises and cloud installations by using ONTAP Snapshot copies. SnapMirror performs block-level incremental data transfers to ensure that only the data that has changed is sent to your destination replica.



Similarly, you can use a SnapMirror vault relationship to create a data archive for the local Snapshot copies created on a Cloud Volumes ONTAP system.

NetApp Cloud Backup delivers seamless and cost-effective backup and restore capabilities for protecting and archiving data to object storage in the cloud. Cloud Backup is available for both cloud-based data and for on-premises data.

### Related information

[Setting up a disaster recovery in the cloud with Cloud Volumes ONTAP](#)

[Efficient Data Replication Using Cloud Volumes ONTAP and SnapMirror](#)

[ONTAP Data Protection with the CLI](#)

[NetApp Cloud Backup](#)

### High availability

In an on-premises data center, physical nodes are configured in high-availability (HA) pairs for fault tolerance and nondisruptive operations. If a node fails or if you need to

bring a node down for routine maintenance, its partner takes over its storage and continues to serve data from it.

In a cloud environment, you can create an HA pair of Cloud Volumes ONTAP instances for the same fault tolerance and non-disruptive operations as an on-premises HA pair. These recovery objectives are available with cloud HA pairs:

- The recovery point objective (RPO) is 0 seconds. Your data is transactionally consistent with no data loss.
- The recovery time objective (RTO) is 60 seconds. In the event of an outage, data should be available in 60 seconds or less.

Each cloud provider offers its own HA architecture and configuration options. For Cloud Volumes Service, high availability is guaranteed in the service level agreement.

#### **Related information**

[High-availability pairs in AWS](#)

[High-availability pairs in Azure](#)

#### **Encryption of data at rest**

ONTAP uses the same encryption technology to secure data in the cloud that you use to secure your on-premises data.

Cloud Volumes ONTAP supports NetApp Volume Encryption (NVE) and NetApp Aggregate Encryption (NAE) with an external key manager.

Cloud Volumes ONTAP also supports the following encryption technologies:

- AWS Key Management Service
- Azure Storage Service Encryption
- Google Cloud Platform default encryption

Data is always encrypted at rest when using Azure NetApp Files and NetApp Cloud Volumes Service for Google Cloud.

#### **Related information**

[Encryption of data at rest in Cloud Volumes ONTAP](#)

[NetApp Volume Encryption and NetApp Aggregate Encryption](#)

[Encrypting volumes in Cloud Volumes ONTAP with NetApp encryption solutions](#)

#### **Antivirus protection**

You likely use the integrated antivirus functionality on-premises to protect data from being compromised by viruses or other malicious code. This same antivirus protection is available in the cloud when you use Cloud Volumes ONTAP.

The ONTAP Antivirus Connector, installed on a local server, handles communication between the storage system and the antivirus software. For Cloud Volumes ONTAP, you install the Antivirus Connector on a virtual machine in the same cloud as ONTAP.

## Related information

[Antivirus configuration](#)

## Move entire workloads to the cloud

### Storage protocols

Some customers choose to move entire workloads to the cloud. This can be more complicated than just using the cloud for data protection. But ONTAP makes the move easier because you do not have to rewrite your applications to use cloud-based storage. ONTAP in the cloud works just like your on-premises ONTAP does.

ONTAP offers the same NFS, SMB, and iSCSI protocols in the cloud that you are using today.

### File sharing with NFS and SMB

The NFS and SMB protocols are used to make shares and files available to client applications over a network. Cloud Volumes ONTAP enables you to provide files from a public cloud using either or both of these protocols.

If you choose to move an entire workload to the cloud, Cloud Volumes ONTAP enables your application to work with storage in the cloud exactly as it does on premises. There is no need to change your application, and if you decide to move to a different cloud provider, there is no worry about provider lock in. The same commands and scripts you use to manage file services on premises work in the cloud.

In the cloud, you can scale file shares rapidly, by adding or removing storage and compute instances or by adjusting your service level as needed to respond to changes in client demand without incurring capital expenses. The more resources you use, the more you pay, but only when you are using the resources.

NetApp SnapMirror technology moves and synchronizes your file data between your on-premises ONTAP system and Cloud Volumes ONTAP. You can easily move the data to and from the cloud, and between cloud providers.

## Related information

[Cloud Manager: Provisioning Storage](#)

[Managing volumes for Azure NetApp Files](#)

[Managing Cloud Volumes Service for AWS](#)

### iSCSI

The iSCSI protocol provides block-level storage to clients such as databases and other applications that want block storage instead of files. ONTAP provides the iSCSI protocol in the cloud.

Once iSCSI storage has been provisioned, there is no difference between on-premises iSCSI access and cloud-based iSCSI access.

The same iSCSI SAN features that are available on-premises such as Snapshot copies, deduplication, compression, and thin provisioning are also available and work the same way in the cloud.

## Related information

[Provisioning block storage with Cloud Manager](#)

[Provisioning iSCSI LUNs in Cloud Volumes ONTAP](#)

[Deploying Oracle Databases on Azure/AWS](#)

## AutoSupport and Active IQ Digital Advisor

AutoSupport proactively monitors the health of your system and automatically sends telemetry to NetApp technical support. You can get detailed actionable information about your systems from NetApp Active IQ Digital Advisor.

The same AutoSupport and Active IQ Digital Advisor features you use on-premises are also available in the cloud. While AutoSupport can't collect data about the underlying hardware that powers Cloud Volumes ONTAP, you still get significantly useful information in Active IQ.

## Related information

[NetApp Active IQ](#)

[AutoSupport for Cloud Volumes ONTAP](#)

## Storage VMs

A storage VM (SVM) serves data to clients and hosts. Like a virtual machine running on a hypervisor, an SVM is a logical entity that abstracts physical resources.

In an on-premises ONTAP environment, you use SVMs to separate workloads. In Cloud Volumes ONTAP, you can use multiple SVMs, or you can use multiple instances of Cloud Volumes ONTAP.

## Related information

[Cloud Volumes ONTAP default configuration](#)

## FlexGroup volumes

FlexGroup volumes enable you to present a single volume of virtually unlimited size to an application. FlexGroup volumes are supported for Cloud Volumes ONTAP, enabling you to deploy a FlexGroup volume in Cloud Volumes ONTAP.

## Related information

[FlexGroup volumes management](#)

## Performance and efficiency in the cloud

### Performance and efficiency in the cloud overview

Your on-premises ONTAP system offers data efficiency features that enable you to store more data in less physical space, and to tier rarely used data to lower cost storage. Whether you use a hybrid cloud configuration, or you move an entire workload to the cloud, ONTAP enables you to maximize storage performance and efficiency.

## FabricPool

Many NetApp customers have significant amounts of stored data that is rarely accessed. We call that *cold* data. Customers also have data that is frequently accessed, which we call *hot* data. Ideally, you want to keep your hot data on your fastest storage for best performance. Cold data can move to slower storage as long as it is immediately available if needed. But how do you know which parts of your data are hot and which are cold?

FabricPool is an ONTAP feature that automatically moves data between a high-performance local tier (aggregate) and a cloud tier based on access patterns. Tiering frees up expensive local storage for hot data while keeping cold data readily available from low-cost object storage in the cloud. FabricPool constantly monitors data access and moves data between tiers for best performance and maximum savings.

Using FabricPool to tier cold data to the cloud is one of the easiest ways to gain cloud efficiency and create a hybrid cloud configuration. FabricPool works at the storage block level, so it works with both file and LUN data.

But FabricPool is not just for tiering on-premises data to the cloud. Many customers use FabricPool in Cloud Volumes ONTAP to tier cold data from more-expensive cloud storage to lower-cost object storage within the cloud provider. Beginning with ONTAP 9.8, you can capture analytics on FabricPool-enabled volumes with [File System Analytics](#) or [temperature-sensitive storage efficiency](#).

The applications using the data are not aware that data is tiered, so no changes to your applications are needed. Tiering is fully automatic, so there is no ongoing administration needed.

You can store cold data in object storage from one of the major cloud providers. Or choose NetApp StorageGRID to keep your cold data in your own private cloud for highest performance and complete control over your data.

### Related information

[FabricPool System Manager doc](#)

[Cloud Tiering Service](#)

[FabricPool playlist on NetApp TechComm TV](#)

### Storage Efficiency

The same storage efficiency features of on-premises ONTAP are available in the Cloud. SnapShot copies, deduplication, compression, compaction, thin provisioning, and FlexClone data clones are all available in NetApp Cloud offerings.

When you move data from on-premises ONTAP to the cloud, the existing storage efficiency is preserved. Whether you are moving an entire dataset, or just tiering cold data to the cloud, you won't move uncompressed or duplicate data.

### Related information

[Cloud Volumes ONTAP Feature Spotlight: Storage Efficiency Case Studies](#)

[Using a volume usage profile in Cloud Manager to manage cloud storage efficiency](#)

## Manage ONTAP in the cloud

### Manage ONTAP in the cloud

Whether you use ONTAP in your own datacenter or in the cloud, you use the same interfaces to manage your storage. This means you already know how to manage ONTAP in the cloud. Additionally, NetApp Cloud Manager is a modern, easy-to-use graphical interface for deploying and getting started with Cloud Volumes ONTAP. There are situations when you need to perform advanced management of Cloud Volumes ONTAP or Cloud Volumes Service. You can do so using System Manager, the command line interface (CLI), or REST APIs.

**System Manager** runs on the Cloud Volumes ONTAP or Cloud Volumes Service system, enabling you to perform management tasks.

**The ONTAP CLI** enables you to execute all administrative commands and is a good choice for advanced tasks or if you are more comfortable using the CLI. You connect to the CLI using Secure Shell (SSH).

**ONTAP REST APIs** enable you to create and manage cloud volumes and develop provisioning scripts and tools. The ONTAP capabilities that are available through the Web user interface are also available through REST APIs. For some situations, this programmatic interface is more useful, especially for developers because they can automate processes involving Cloud Manager operations.

#### Related information

[Connecting to Cloud Volumes ONTAP](#)

[Cloud Automation with Cloud Volumes ONTAP and REST](#)

[Cloud Manager REST API](#)

#### Event and performance monitoring

When you move your on-premises workloads to the cloud, you can continue to rely on ONTAP event monitoring. EMS messages, NAS native auditing, FPolicy, and SNMP are all available in the cloud.

If you are already using System Manager or Active IQ Unified Manager for on-premises performance monitoring, you can continue to do so in the cloud. Both System Manager and Unified Manager provide detailed reporting and alerting of Cloud Volumes ONTAP health, capacity, and performance.

#### Related information

[How to Define an Effective Cloud Monitoring Strategy](#)

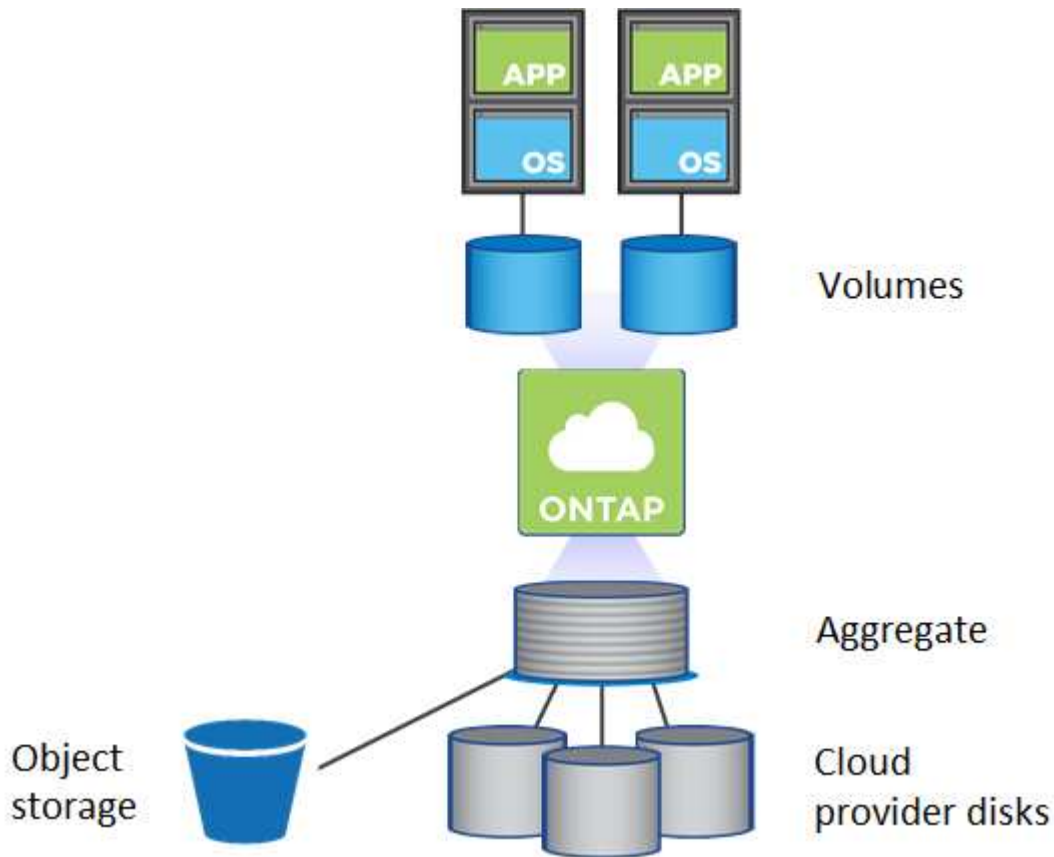
[10 Cloud Monitoring Tools You Should Know](#)

#### Volume management

Flexible and efficient volume management is the heart of the ONTAP cloud solution. ONTAP FlexVol volumes offer the same data fabric benefits, with the same data management processes, regardless of whether they are configured on-prem in the cloud. You can also take advantage of cloud capabilities to rapidly scale workloads, increasing

or decreasing capacity as needed.

Cloud volumes provide the same storage efficiencies as on-prem volumes: deduplication, compression, compaction, thin provisioning, and data tiering. In a cloud environment, this means that you pay less for underlying cloud disk usage.



There are two ways to provision volumes in the cloud:

- Create new cloud volumes.
- Replicate existing on-prem volumes to new cloud volume destination using SnapMirror technology or the Cloud Sync service.

#### **Related information**

[Cloud Manager: Provisioning storage](#)

[Managing volumes for Azure NetApp Files](#)

[Managing Cloud Volumes Service for AWS](#)

[Cloud Sync service](#)

#### **Volume move**

Using ONTAP, you can move a FlexVol volume to a different local tier (aggregate), node, or both within the same storage VM (SVM) to balance storage capacity after you determine that there is a storage capacity imbalance. With Cloud Volumes ONTAP, you can move one or more volumes to another Cloud Volumes ONTAP system or to another



aggregate to avoid capacity issues. You might need to do this if the system reaches its disk limit.

#### **Related information**

[Cloud Volumes ONTAP: Moving volumes to another system to avoid capacity issues](#)

[Cloud Volumes ONTAP: Moving volumes to another aggregate to avoid capacity issues](#)

#### **ONTAP updates**

NetApp releases regular updates to ONTAP to add new features and to fix known issues. You can update ONTAP in the cloud in a similar way to updating your on-premises ONTAP release. For HA configurations in the cloud, the process is nondisruptive.

#### **Related information**

[Upgrading Cloud Volumes ONTAP](#)

### **Compliance and the cloud**

#### **NetApp Cloud Data Sense**

Each industry and each country has different compliance requirements. Whether you have an on-premises system or are working in the cloud, ONTAP helps you maintain compliance.

Powered by artificial intelligence, NetApp offers Cloud Data Sense (formerly Cloud Compliance service) to keep your cloud resources in compliance with many regulations. This always-on service is the best way to navigate complex compliance regulations.

#### **Related information**

[NetApp Cloud Data Sense](#)

#### **Data sovereignty**

Data sovereignty refers to national laws concerning the collection, storage, and transmission of data. The General Data Protection Regulation (GDPR) in Europe and the Health Insurance Portability and Accountability Act (HIPAA) in the US are examples of these laws. Data residency refers to where data is physically stored and is often specified by data sovereignty laws. Personal data about individuals is a primary target of regulations, but other data can be regulated too.

When you store data on premises in your own data center, you have complete control over how and where the data is stored. When you store data in the cloud, you are responsible for understanding how and where that data is physically stored, and you are responsible for ensuring you comply with applicable data sovereignty laws. For hybrid cloud configurations, you need to pay attention to where both the on-premises tiers and the cloud tiers are stored.

The good news is that all the major cloud providers are fully aware of the laws and have procedures and information to help you comply. But it's still important that you select the appropriate products and procedures for your specific needs.

In many cases, storing your data in the cloud makes it possible to keep data within the boundaries of a country where your company has no physical presence.

Here are some examples of the compliance information from NetApp and from cloud providers:

- [Architecting GDPR- and HIPAA-Compliant Storage](#)
- [Questions on data residency and compliance in Microsoft Azure](#)
- [General Data Protection Regulation \(GDPR\) Center for Amazon Web Services](#)
- [Compliance resource center for Google Cloud](#)
- [Alibaba Cloud Security & Compliance Center](#)

### **Cloud WORM storage**

An important aspect of compliance is being able to guarantee that certain data is maintained unchanged for a required period of time. You can activate write once, read many (WORM) storage on a Cloud Volumes ONTAP system to retain files in unmodified form for a specified retention period. Cloud WORM storage is powered by SnapLock technology, which means WORM files are protected at the file level.

Once a file has been committed to WORM storage, it can't be modified, even after the retention period has expired. A tamper-proof clock determines when the retention period for a WORM file has elapsed.

You can activate WORM storage on a Cloud Volumes ONTAP system when you create a new working environment. This includes setting the default retention period for files. You can't activate WORM storage on individual volumes—WORM must be activated at the system level.

### **Related information**

[WORM storage](#)

[Archive and compliance using SnapLock technology](#)

[NetApp Cloud WORM: Enhancing Data Protection with Locking Features](#)

# Set up, upgrade and revert ONTAP and system components

## Setup ONTAP

### Decide whether to use System Manager or the ONTAP CLI for cluster setup

While you can set up new clusters with the ONTAP CLI, NetApp recommends that you use System Manager whenever possible to simplify the cluster setup process. Use these procedures only if your version of System Manager does not support initial cluster setup for your planned ONTAP deployment.

You should be aware of the following System Manager support requirements:

- Cluster setup is supported only for single nodes and HA pairs
- When you set up node management manually using the CLI, System Manager supports only IPv4 and does not support IPv6. However, if you launch System Manager after completing your hardware setup using DHCP with an auto assigned IP address and with Windows discovery, System Manager can configure an IPv6 management address.

In ONTAP 9.6 and earlier, System Manager does not support deployments that require IPv6 networking.

- MetroCluster setup support is for MetroCluster IP configurations with two nodes at each site.

In ONTAP 9.7 and earlier, System Manager does not support new cluster setup for MetroCluster configurations.

If you are configuring a FlexArray on non-NetApp disks, you need to use the ONTAP CLI to configure root volumes on the array LUNs, and then use the Cluster Setup wizard to set up your cluster.

For more information, see the [FlexArray Virtualization installation and requirements](#) documentation.

Before completing any of these procedures, you should have installed, cabled and powered on your new storage system according to the installation and setup instructions for your platform model.

See the [AFF and FAS documentation](#).

### Configure ONTAP on a new cluster

System Manager provides a simple and easy workflow for setting up a new cluster and configuring your storage.

In some cases, such as certain MetroCluster deployments or clusters that require IPv6 network addressing, you might need to use the ONTAP CLI to set up a new cluster. Click [here](#) for more details about these requirements, as well as steps for cluster setup with the ONTAP CLI.

Whether you use System Manager or the CLI for your setup, your system should already be installed and cabled according to the [Installation and Setup Instructions](#) that came with the system. Also, cluster network interfaces should be configured on each node of the cluster for intra-cluster communication.



## Assign a node-management IP address

### Windows System

You should connect your Windows computer to the same subnet as the controllers. This will automatically assign a node-management IP address to your system.

### Step

1. From the Windows system, open the **Network** drive to discover the nodes.
2. Double-click the node to launch the cluster setup wizard.

### Other systems

You should configure the node-management IP address for one of the nodes in your cluster. You can use this node-management IP address to launch the cluster set up wizard.

See [Creating the cluster on the first node](#) for information about assigning a node-management IP address.

## Initialize the cluster

You initialize the cluster by setting an administrative password for the cluster and setting up the cluster management and node management networks. You can also configure services like a DNS server to resolve host names and an NTP server to synchronize time.

### Steps

1. On a web browser, enter the node-management IP address that you have configured: "https://node-management-IP"

System Manager automatically discovers the remaining nodes in the cluster.

2. Initialize the storage system by configuring the cluster management network and node management IP addresses for all the nodes.

## Create your local tier

Create local tiers from the available disks or SSDs in your nodes. System Manager automatically calculates the best tier configuration based on your hardware.

### Steps

1. Click **Dashboard** and then click **Prepare Storage**.

Accept the storage recommendation for your local tier.

## Configure protocols

Depending on the licenses enabled on your cluster, you can enable the desired protocols on your cluster. You then create network interfaces using which you can access the storage.

## Steps

1. Click **Dashboard** and then click **Configure Protocols**.
  - Enable iSCSI or FC for SAN access.
  - Enable NFS or SMB for NAS access.
  - Enable NVMe for FC-NVMe access.

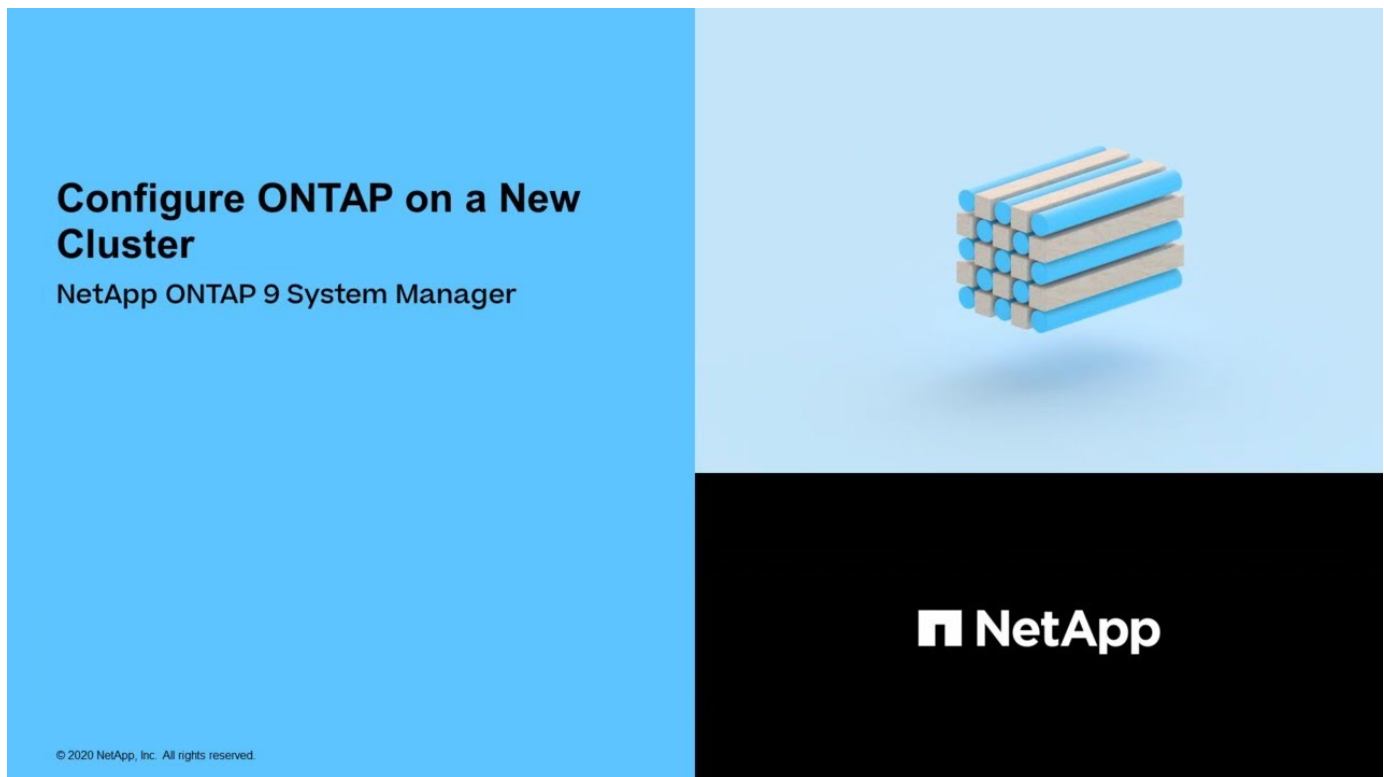
## Provision Storage

You can now provision storage. The options you see depends on the licenses that are installed.

## Steps

1. Click **Dashboard** and then click **Provision Storage**.
  - To [provision SAN access](#), click **Add LUNs**.
  - To [provision NAS access](#), click **Add Volumes**.
  - To [provision NVMe storage](#), click **Add Namespaces**.

## Configure ONTAP on a new cluster video



## Set up the cluster with the ONTAP CLI

Setting up the cluster involves gathering the information needed to configure setting up each node, creating the cluster on the first node, and joining any remaining nodes to the cluster.

Get started by gathering all the relevant information in the cluster setup worksheets.

## Cluster setup worksheets

The cluster setup worksheet enables you to record the values that you need during the cluster setup process. If a default value is provided, you can use that value or else enter your own.

### System defaults

The system defaults are the default values for the private cluster network. It is best to use these default values. However, if they do not meet your requirements, you can use the table to record your own values.



For clusters configured to use network switches, each cluster switch must use the 9000 MTU size.

Types of information	Your values
Private cluster network ports	
Cluster network netmask	
Cluster interface IP addresses (for each cluster network port on each node)  The IP addresses for each node must be on the same subnet.	

### Cluster information


Types of information	Your values
Cluster name  The name must begin with a letter, and it must be fewer than 44 characters. The name can include the following special characters:  . - _	

### Feature license keys

You can find license keys for your initial or add-on software orders at the NetApp Support Site under **My Support > Software Licenses**.

Types of information	Your values
Feature license keys	

### Admin storage virtual machine (SVM)

Types of information	Your values
<p>Cluster administrator password</p> <p>The password for the admin account that the cluster requires before granting cluster administrator access to the console or through a secure protocol.</p> <div style="display: flex; align-items: center; margin-top: 10px;">  <p>For security purposes, recording passwords in this worksheet is not recommended.</p> </div> <p>The default rules for passwords are as follows:</p> <ul style="list-style-type: none"> <li>• A password must be at least eight characters long.</li> <li>• A password must contain at least one letter and one number.</li> </ul>	
<p>Cluster management interface port</p> <p>The physical port that is connected to the data network and enables the cluster administrator to manage the cluster.</p>	
<p>Cluster management interface IP address</p> <p>A unique IPv4 or IPv6 address for the cluster management interface. The cluster administrator uses this address to access the admin SVM and manage the cluster. Typically, this address should be on the data network.</p> <p>You can obtain this IP address from the administrator responsible for assigning IP addresses in your organization.</p> <p>Example: 192.0.2.66</p>	
<p>Cluster management interface netmask (IPv4)</p> <p>The subnet mask that defines the range of valid IPv4 addresses on the cluster management network.</p> <p>Example: 255.255.255.0</p>	

Types of information	Your values
<p>Cluster management interface netmask length (IPv6)</p> <p>If the cluster management interface uses an IPv6 address, then this value represents the prefix length that defines the range of valid IPv6 addresses on the cluster management network.</p> <p>Example: 64</p>	
<p>Cluster management interface default gateway</p> <p>The IP address for the router on the cluster management network.</p>	
<p>DNS domain name</p> <p>The name of your network's DNS domain.</p> <p>The domain name must consist of alphanumeric characters. To enter multiple DNS domain names, separate each name with either a comma or a space.</p>	
<p>Name server IP addresses</p> <p>The IP addresses of the DNS name servers. Separate each address with either a comma or a space.</p>	

**Node information (for each node in the cluster)**

Types of information	Your values
<p>Physical location of the controller (optional)</p> <p>A description of the physical location of the controller. Use a description that identifies where to find this node in the cluster (for example, "Lab 5, Row 7, Rack B").</p>	
<p>Node management interface port</p> <p>The physical port that is connected to the node management network and enables the cluster administrator to manage the node.</p>	



Types of information	Your values
<p>Node management interface IP address</p> <p>A unique IPv4 or IPv6 address for the node management interface on the management network. If you defined the node management interface port to be a data port, then this IP address should be a unique IP address on the data network.</p> <p>You can obtain this IP address from the administrator responsible for assigning IP addresses in your organization.</p> <p>Example: 192.0.2.66</p>	
<p>Node management interface netmask (IPv4)</p> <p>The subnet mask that defines the range of valid IP addresses on the node management network.</p> <p>If you defined the node management interface port to be a data port, then the netmask should be the subnet mask for the data network.</p> <p>Example: 255.255.255.0</p>	
<p>Node management interface netmask length (IPv6)</p> <p>If the node management interface uses an IPv6 address, then this value represents the prefix length that defines the range of valid IPv6 addresses on the node management network.</p> <p>Example: 64</p>	
<p>Node management interface default gateway</p> <p>The IP address for the router on the node management network.</p>	

**NTP server information**

Types of information	Your values
<p>NTP server addresses</p> <p>The IP addresses of the Network Time Protocol (NTP) servers at your site. These servers are used to synchronize the time across the cluster.</p>	

## Create the cluster on the first node

You use the Cluster Setup wizard to create the cluster on the first node. The wizard helps you to configure the cluster network that connects the nodes, create the cluster admin storage virtual machine (SVM), add feature license keys, and create the node management interface for the first node.

1. Power on all the nodes you are adding to the cluster. This is required to enable discovery for your cluster setup.
2. Connect to the console of the first node.

The node boots, and then the Cluster Setup wizard starts on the console.

```
Welcome to the cluster setup wizard....
```

3. Acknowledge the AutoSupport statement.

```
Type yes to confirm and continue {yes}: yes
```



AutoSupport is enabled by default.

4. Follow the instructions on the screen to assign an IP address to the node.
5. If you are using the GUI wizard to perform setup, follow the instructions to complete setup in your web browser. If you are using the CLI wizard to perform setup, press Enter to continue.

```
Use your web browser to complete cluster setup by accessing  
https://10.63.11.29
```

```
Otherwise, press Enter to complete cluster setup using the  
command line interface:
```

```
Do you want to create a new cluster or join an existing cluster?  
{create, join}:
```

6. Create a new cluster: `create`
7. Accept the system defaults or enter your own values.
8. After setup is completed, log in to the cluster and verify that the cluster is active and the first node is healthy by entering the ONTAP CLI command: `cluster show`

The following example shows a cluster in which the first node (cluster1-01) is healthy and eligible to participate:

```
cluster1::> cluster show
Node                Health  Eligibility
-----
cluster1-01        true    true
```

You can access the Cluster Setup wizard to change any of the values you entered for the admin SVM or node SVM by using the `cluster setup` command.

### Join remaining nodes to the cluster

After creating a new cluster, you use the Cluster Setup wizard to join each remaining node to the cluster one at a time. The wizard helps you to configure each node's node management interface.

When you join two nodes in a cluster, you are creating a high availability (HA) pair. If you join 4 nodes, you create two HA pairs. To learn more about HA, see [Learn about HA](#).

You can only join one node to the cluster at a time. When you start to join a node to the cluster, you must complete the join operation for that node, and the node must be part of the cluster before you can start to join the next node.

**Best Practice:** If you have a FAS2720 with 24 or fewer NL-SAS drives, you should verify that the storage configuration default is set to active/passive to optimize performance.

For more information, see [Setting up an active-passive configuration on nodes using root-data partitioning](#)

1. Log in to the node you plan to join in the cluster.

Cluster Setup wizard starts on the console.

```
Welcome to the cluster setup wizard....
```

2. Acknowledge the AutoSupport statement.



AutoSupport is enabled by default.

```
Type yes to confirm and continue {yes}: yes
```

3. Follow the instructions on the screen to assign an IP address to the node.
4. Join the node to the cluster: `join`
5. Follow the instructions on the screen to set up the node and join it to the cluster.
6. After setup is completed, verify that the node is healthy and eligible to participate in the cluster: `cluster show`

The following example shows a cluster after the second node (cluster1-02) has been joined to the cluster:

```
cluster1::> cluster show
Node                Health  Eligibility
-----
cluster1-01        true   true
cluster1-02        true   true
```

You can access the Cluster Setup wizard to change any of the values you entered for the admin SVM or node SVM by using the cluster setup command.

7. Repeat this task for each remaining node.

### Check your cluster with Active IQ Config Advisor

After you have joined all the nodes to your new cluster, you should run Active IQ Config Advisor to validate your configuration and check for common configuration errors.

Config Advisor is a web-based application that you install on your laptop, virtual machine or a server, and works across Windows, Linux, and Mac platforms.

Config Advisor runs a series of commands to validate your installation and check the overall health of the configuration, including the cluster and storage switches.

1. Download and install Active IQ Config Advisor.

#### [Active IQ Config Advisor](#)

2. Launch Active IQ, and set up a passphrase when prompted.
3. Review your settings and click **Save**.
4. On the **Objectives** page, click **ONTAP Post-Deployment Validation**.
5. Choose either Guided or Expert mode.

If you choose Guided mode, connected switches are discovered automatically.

6. Enter the cluster credentials.
7. (Optional) Click **Form Validate**.
8. To begin collecting data, click **Save & Evaluate**.
9. After data collection is complete, under **Job Monitor > Actions**, view the data collected by clicking **Data View** icon, and view the results by clicking the **Results** icon.
10. Resolve the issues identified by Config Advisor.

### Synchronize the system time across the cluster

Synchronizing the time ensures that every node in the cluster has the same time, and prevents CIFS and Kerberos failures.

A Network Time Protocol (NTP) server should be set up at your site. Beginning with ONTAP 9.5, you can set up your NTP server with symmetric authentication.

For more information, see [Managing the cluster time \(cluster administrators only\)](#).

You synchronize the time across the cluster by associating the cluster with one or more NTP servers.

1. Verify that the system time and time zone is set correctly for each node.

All nodes in the cluster should be set to the same time zone.

- a. Use the `cluster date show` command to display the current date, time, and time zone for each node.

```
cluster1::> cluster date show
Node           Date           Time zone
-----
cluster1-01   01/06/2015 09:35:15 America/New_York
cluster1-02   01/06/2015 09:35:15 America/New_York
cluster1-03   01/06/2015 09:35:15 America/New_York
cluster1-04   01/06/2015 09:35:15 America/New_York
4 entries were displayed.
```

- b. Use the `cluster date modify` command to change the date or time zone for all of the nodes.

This example changes the time zone for the cluster to be GMT:

```
cluster1::> cluster date modify -timezone GMT
```

2. Use the `cluster time-service ntp server create` command to associate the cluster with your NTP server.

- To set up your NTP server without symmetric authentication enter the following command: `cluster time-service ntp server create -server server_name`
- To set up your NTP server with symmetric authentication, enter the following command: `cluster time-service ntp server create -server server_ip_address -key-id key_id`



Symmetric authentication is available Beginning with ONTAP 9.5. It is not available in ONTAP 9.4 or earlier.

This example assumes that DNS has been configured for the cluster. If you have not configured DNS, you must specify the IP address of the NTP server:

```
cluster1::> cluster time-service ntp server create -server
ntp1.example.com
```

3. Verify that the cluster is associated with an NTP server: `cluster time-service ntp server show`

```
cluster1::> cluster time-service ntp server show
Server           Version
-----
ntp1.example.com   auto
```

## Related information

[System administration](#)

### Commands for managing symmetric authentication on NTP servers

Beginning with ONTAP 9.5, Network Time Protocol (NTP) version 3 is supported. NTPv3 includes symmetric authentication using SHA-1 keys which increases network security.

To do this...	Use this command...
Configure an NTP server without symmetric authentication	<pre>cluster time-service ntp server create -server server_name</pre>
Configure an NTP server with symmetric authentication	<pre>cluster time-service ntp server create -server server_ip_address -key-id key_id</pre>
Enable symmetric authentication for an existing NTP server  An existing NTP server can be modified to enable authentication by adding the required key-id.	<pre>cluster time-service ntp server modify -server server_name -key-id key_id</pre>
Configure a shared NTP key	<pre>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</pre> <p><b>Note:</b> Shared keys are referred to by an ID. The ID, its type, and value must be identical on both the node and the NTP server</p>
Configure an NTP server with an unknown key ID	<pre>cluster time-service ntp server create -server server_name -key-id key_id</pre>
Configure a server with a key ID not configured on the NTP server.	<pre>cluster time-service ntp server create -server server_name -key-id key_id</pre> <p><b>Note:</b> The key ID, type, and value must be identical to the key ID, type, and value configured on the NTP server.</p>
Disable symmetric authentication	<pre>cluster time-service ntp server modify -server server_name -authentication disabled</pre>

### Additional system configuration tasks to complete

After setting up a cluster, you can use either System Manager or the ONTAP command-line interface (CLI) to continue configuring the cluster.

System configuration task	Resource
Configure networking: <ul style="list-style-type: none"> <li>• Create broadcast domains</li> <li>• Create subnets</li> <li>• Create IP spaces</li> </ul>	<a href="#">Setting up the network</a>
Set up the Service Processor	<a href="#">System administration</a>
Lay out your aggregates	<a href="#">Disk and aggregate management</a>
Create and configure data storage virtual machines (SVMs)	<a href="#">NFS configuration</a> <a href="#">SMB configuration</a> <a href="#">SAN administration</a>
Configure event notifications	<a href="#">EMS configuration</a>

## All SAN Array Software Configuration

Use the following procedures to configure an All SAN Array using System Manager.

### Supported ALL SAN Array configurations

The NetApp All SAN Arrays (ASAs) are all-flash SAN-only solutions built on proven AFF NetApp platforms.

The ASA platforms are available in two-node switched or switchless clusters, can be configured for FC or iSCSI, and use symmetric active-active for multipathing. All paths are active/optimized so in the event of a storage failover, the host does not need to wait for the ALUA transition of the failover paths to resume I/O. This reduces time to failover.



With ONTAP 9.9.1, customers can now scale AFF ASA configurations up to 12 nodes. ASAs are supported in ONTAP 9.7 and later. Supported configurations are listed in the [NetApp Interoperability Matrix Tool](#).

### Related information

[NetApp Technical Report 4515: ONTAP AFF All SAN Array Systems](#)

[NetApp Technical Report 4080: Best Practices for Scalable SAN ONTAP 9](#)

### Set up an ASA

All SAN Arrays (ASAs) follow the same setup procedure as non-ASA systems.

System Manager guides you through the procedures necessary to initialize your cluster, create a local tier, configure protocols, and provision storage for your ASA. See the steps to [Configure ONTAP](#).

## ASA configuration limits

You should use the tested and supported maximum configuration limits established for AFF All SAN Array (ASA) controllers. For reliable operations, you should not exceed the current tested and supported limits listed in [NetApp Hardware Universe](#).

Beginning with ONTAP 9.9.1 AFF ASA controllers can support up to 12 nodes for non-MetroCluster IP configurations and up to 8 nodes for MetroCluster IP configurations.

Also beginning with ONTAP 9.9.1, NVMe-oF protocol is supported on all AFF ASA controllers except those configured for MetroCluster. Metrocluster configurations do not support NVMe-oF.

## Support for persistent ports

Beginning with ONTAP 9.8, persistent ports are enabled by default on All SAN Arrays (ASAs) that are configured to use the FC protocol. Persistent ports are only available for FC and require zone membership identified by World Wide Port Name (WWPN).

Persistent ports reduce the impact of takeovers by creating a shadow LIF on the corresponding physical port of the HA partner. When a node is taken over, the shadow LIF on the partner node assumes the identity of the original LIF, including the WWPN. Before the status of path to the taken over node is changed to faulty, the shadow LIF appears as an Active/Optimized path to the host MPIO stack, and I/O is shifted. This reduces I/O disruption because the host always sees the same number of paths to the target, even during storage failover operations.

For persistent ports, the following FCP port characteristics should be identical within the HA pair:

- FCP port counts
- FCP port names
- FCP port speeds
- FCP LIF WWPN-based zoning

If any of these characteristics are not identical within the HA pair, the following EMS message is generated:

```
EMS : scsiblade.lif.persistent.ports.fcp.init.error
```

For more information on persistent ports, see [NetApp Technical Report 4080: Best Practices for Scalable SAN ONTAP 9](#).

## ASA host settings and utilities

Host settings for setting up All SAN Arrays (ASAs) are the same as those for all other SAN hosts.

You can download the [NetApp Host Utilities software](#) for your specific hosts from the support site.

## Ways to identify an ASA system

You can identify an ASA system using System Manager or using the ONTAP command line interface (CLI).

From the System Manager dashboard, click **Cluster > Overview** and then select the system node. The **PERSONALITY** is displayed as **All SAN Array**.

From the CLI, you can use the `san config show` command. The "All SAN Array" value returns as true for ASA systems.



# Upgrade ONTAP

## Upgrade ONTAP overview

The [method you use to upgrade](#) your ONTAP software depends upon your configuration. If it is supported by your configuration, you should perform an automated nondisruptive upgrade (ANDU) using System Manager.

If you have an active [SupportEdge](#) contract for [Active IQ Digital Advisor](#), before you begin your upgrade, you should launch Upgrade Advisor in Active IQ Digital Advisor to help you plan your upgrade.

The procedures in this section guide you through the steps you should take before and after you upgrade, including the resources you should read and the necessary pre- and post-upgrade checks you should perform.

## What version of ONTAP can I upgrade to?

The version of ONTAP that you can upgrade to varies based on your hardware platform and the version of ONTAP currently running on your cluster's nodes. See [NetApp Hardware Universe](#) to verify that your platform is supported for the target upgrade release.

These guidelines refer only to on-premises ONTAP releases. For information about upgrading ONTAP in the cloud, see [Upgrading Cloud Volumes ONTAP software](#).

To determine your current ONTAP version:

- In System Manager, click **Cluster > Overview**.
- From the command line interface (CLI), use the `cluster image show` command.  
You can also use the `system node image show` command in the advanced privilege level to display details.

## Types of upgrade paths

Automated nondisruptive upgrades (ANDU) are recommended whenever possible. Depending on your current and target releases, your upgrade path will be *direct*, *direct multi-hop*, or *multi-stage*. Unless otherwise noted, these paths apply to all [upgrade methods](#); nondisruptive or disruptive, automated or manual.

- *direct*  
You can always upgrade directly to the next adjacent ONTAP release family using a single software image. For most releases, you can also install a software image that allows you to upgrade directly to releases that are two releases higher than the running release.

For example, you can use the direct update path from 9.8 to 9.9.1, or from 9.8 to 9.10.1.

**Note:** Beginning with ONTAP 9.11.1, software images support upgrading directly to releases that are three releases higher than the running release. For example, you can use the direct upgrade path from 9.8 to 9.11.1.

- *direct multi-hop*  
For some automated nondisruptive upgrades (ANDU) to non-adjacent releases, you can install the software image for an intermediate release as well the target release. The automated upgrade process uses the intermediate image in the background to complete the update to the target release.

For example, if the cluster is running 9.3 and you want to upgrade to 9.7, you would load the ONTAP install packages for both 9.5 and 9.7, then initiate ANDU to 9.7. ONTAP then automatically upgrades the cluster first to 9.5 and then to 9.7. You should expect multiple takeover/giveback operations and related reboots during the process.

The following direct multi-hop upgrade paths are available using the ANDU method:

Source ONTAP release	Target ONTAP release	Images required
9.7	9.11.1	9.8, 9.11.1
	9.10.1	9.8, 9.10.1P1 or later P release
9.6	9.10.1	9.8, 9.10.1P1 or later P release
9.5	9.9.1	9.7, 9.9.1
9.3	9.7	9.5, 9.7

- *multi-stage*

If a direct or direct multi-hop path is not available for your non-adjacent target release, you must first upgrade to a supported intermediate release, and then upgrade to the target release.

For example, if you are currently running 9.6 and you want to upgrade to 9.11.1, you must complete a multi-stage upgrade: first from 9.6 to 9.8, and then from 9.8 to 9.11.1. Upgrades from earlier releases might require three or more stages, with several intermediate upgrades.

**Note:** Before beginning multi-stage upgrades, be sure your target release is supported on your hardware platform.

If you are planning an ONTAP upgrade from an older ONTAP version (such as 9.3), it is a best practice to upgrade first to the latest patch release in the same ONTAP release family and only then upgrade to the next supported major release. This will ensure that any issues in the older version are resolved before upgrading.

For example, if your system is running ONTAP 9.3P9 and you are planning to upgrade to 9.9.1P7, follow this upgrade path:

9.3P9 → 9.3P21 → 9.7P18 → 9.9.1P7

Learn about [Minimum Recommended ONTAP releases on the NetApp Support Site](#).

## Supported upgrade paths

Detailed upgrade paths are available for the following scenarios:

- Automated nondisruptive upgrades (ANDU) within the ONTAP 9 release family (recommended).
- Manual nondisruptive and disruptive upgrades within the ONTAP 9 release family.
- Upgrades from Data ONTAP 8.\* releases to ONTAP 9 releases.

Upgrade images for some earlier releases are no longer available.

## ANDU paths, ONTAP 9

If your current ONTAP release is...	And your target ONTAP release is...	Your ANDU upgrade path is...
9.10.1	9.11.1	direct
9.9.1	9.11.1	direct
	9.10.1	direct
9.8	9.11.1	direct
	9.10.1	direct
	9.9.1	direct
9.7	9.11.1	direct multi-hop (requires images for 9.8 & 9.11.1)
	9.10.1	direct multi-hop (requires images for 9.8 & 9.10.1P1 or later P release)
	9.9.1	direct
	9.8	direct
9.6	9.11.1	multi-stage - 9.6 → 9.8 - 9.8 → 9.11.1
	9.10.1	direct multi-hop (requires images for 9.8 & 9.10.1P1 or later P release)
	9.9.1	multi-stage - 9.6 → 9.8 - 9.8 → 9.9.1
	9.8	direct
	9.7	direct
9.5	9.11.1	multi-stage - 9.5 → 9.9.1 (direct multi-hop, requires images for 9.7 & 9.9.1) - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9.5 → 9.9.1 (direct multi-hop, requires images for 9.7 & 9.9.1) - 9.9.1 → 9.10.1
	9.9.1	direct multi-hop (requires images for 9.7 & 9.9.1)
	9.8	multi-stage - 9.5 → 9.7 - 9.7 → 9.8
	9.7	direct
	9.6	direct

If your current ONTAP release is...	And your target ONTAP release is...	Your ANDU upgrade path is...
9.4	9.11.1	multi-stage - 9.4 → 9.5 - 9.5 → 9.9.1 (direct multi-hop, requires images for 9.7 & 9.9.1) - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9.4 → 9.5 - 9.5 → 9.9.1 (direct multi-hop, requires images for 9.7 & 9.9.1) - 9.9.1 → 9.10.1
	9.9.1	multi-stage - 9.4 → 9.5 - 9.5 → 9.9.1 (direct multi-hop, requires images for 9.7 & 9.9.1)
	9.8	multi-stage - 9.4 → 9.5 - 9.5 → 9.8 (direct multi-hop, requires images for 9.7 & 9.8)
	9.7	multi-stage - 9.4 → 9.5 - 9.5 → 9.7
	9.6	multi-stage - 9.4 → 9.5 - 9.5 → 9.6
	9.5	direct

If your current ONTAP release is...	And your target ONTAP release is...	Your ANDU upgrade path is...
9.3	9.11.1	multi-stage - 9.3 → 9.7 (direct multi-hop, requires images for 9.5 & 9.7) - 9.7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9.3 → 9.7 (direct multi-hop, requires images for 9.5 & 9.7) - 9.7 → 9.10.1 (direct multi-hop, requires images for 9.8 & 9.10.1)
	9.9.1	multi-stage - 9.3 → 9.7 (direct multi-hop, requires images for 9.5 & 9.7) - 9.7 → 9.9.1
	9.8	multi-stage - 9.3 → 9.7 (direct multi-hop, requires images for 9.5 & 9.7) - 9.7 → 9.8
	9.7	direct multi-hop (requires images for 9.5 & 9.7)
	9.6	multi-stage - 9.3 → 9.5 - 9.5 → 9.6
	9.5	direct
	9.4	not available

If your current ONTAP release is...	And your target ONTAP release is...	Your ANDU upgrade path is...
9.2	9.11.1	multi-stage - 9.2 → 9.3 - 9.3 → 9.7 (direct multi-hop, requires images for 9.5 & 9.7) - 9.7 → 9.9.1 (direct multi-hop, requires images for 9.8 & 9.9.1) - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9.2 → 9.3 - 9.3 → 9.7 (direct multi-hop, requires images for 9.5 & 9.7) - 9.7 → 9.10.1 (direct multi-hop, requires images for 9.8 & 9.10.1)
	9.9.1	multi-stage - 9.2 → 9.3 - 9.3 → 9.7 (direct multi-hop, requires images for 9.5 & 9.7) - 9.7 → 9.9.1
	9.8	multi-stage - 9.2 → 9.3 - 9.3 → 9.7 (direct multi-hop, requires images for 9.5 & 9.7) - 9.7 → 9.8
	9.7	multi-stage - 9.2 → 9.3 - 9.3 → 9.7 (direct multi-hop, requires images for 9.5 & 9.7)
	9.6	multi-stage - 9.2 → 9.3 - 9.3 → 9.6 (direct multi-hop, requires images for 9.5 & 9.6)
	9.5	multi-stage - 9.3 → 9.5 - 9.5 → 9.6
	9.4	not available
	9.3	direct

If your current ONTAP release is...	And your target ONTAP release is...	Your ANDU upgrade path is...
9.1	9.11.1	multi-stage - 9.1 → 9.3 - 9.3 → 9.7 (direct multi-hop, requires images for 9.5 & 9.7) - 9.7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9.1 → 9.3 - 9.3 → 9.7 (direct multi-hop, requires images for 9.5 & 9.7) - 9.7 → 9.10.1 (direct multi-hop, requires images for 9.8 & 9.10.1)
	9.9.1	multi-stage - 9.1 → 9.3 - 9.3 → 9.7 (direct multi-hop, requires images for 9.5 & 9.7) - 9.7 → 9.9.1
	9.8	multi-stage - 9.1 → 9.3 - 9.3 → 9.7 (direct multi-hop, requires images for 9.5 & 9.7) - 9.7 → 9.8
	9.7	multi-stage - 9.1 → 9.3 - 9.3 → 9.7 (direct multi-hop, requires images for 9.5 & 9.7)
	9.6	multi-stage - 9.1 → 9.3 - 9.3 → 9.6 (direct multi-hop, requires images for 9.5 & 9.6)
	9.5	multi-stage - 9.1 → 9.3 - 9.3 → 9.5
	9.4	not available
	9.3	direct
	9.2	not available

<b>If your current ONTAP release is...</b>	<b>And your target ONTAP release is...</b>	<b>Your ANDU upgrade path is...</b>
9.0		



	9.3	multi-stage - 9.0 → 9.1 - 9.1 → 9.3
<b>If your current ONTAP release is...</b>	<b>And your target ONTAP release is...</b>	<b>Your ANDU upgrade path is...</b>
		not available
	9.1	direct

### Manual paths, ONTAP 9

<b>If your current ONTAP release is...</b>	<b>And your target ONTAP release is...</b>	<b>Your manual upgrade path is...</b>
9.10.1	9.11.1	direct
9.9.1	9.11.1	direct
	9.10.1	direct
9.8	9.11.1	direct
	9.10.1	direct
	9.9.1	direct
9.7	9.11.1	multi-stage - 9.7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9.7 → 9.9.1 - 9.9.1 → 9.10.1
	9.9.1	direct
	9.8	direct
9.6	9.11.1	multi-stage - 9.6 → 9.8 - 9.8 → 9.11.1
	9.10.1	multi-stage - 9.6 → 9.8 - 9.8 → 9.10.1
	9.9.1	multi-stage - 9.6 → 9.8 - 9.8 → 9.9.1
	9.8	direct
	9.7	direct

If your current ONTAP release is...	And your target ONTAP release is...	Your manual upgrade path is...
9.5	9.11.1	multi-stage - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.10.1
	9.9.1	multi-stage - 9.5 → 9.7 - 9.7 → 9.9.1
	9.8	multi-stage - 9.5 → 9.7 - 9.7 → 9.8
	9.7	direct
	9.6	direct
9.4	9.11.1	multi-stage - 9.4 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9.4 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.10.1
	9.9.1	multi-stage - 9.4 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1
	9.8	multi-stage - 9.4 → 9.5 - 9.5 → 9.7 - 9.7 → 9.8
	9.7	multi-stage - 9.4 → 9.5 - 9.5 → 9.7
	9.6	multi-stage - 9.4 → 9.5 - 9.5 → 9.6
	9.5	direct

If your current ONTAP release is...	And your target ONTAP release is...	Your manual upgrade path is...
9.3	9.11.1	multi-stage - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.10.1
	9.9.1	multi-stage - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1
	9.8	multi-stage - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.8
	9.7	multi-stage - 9.3 → 9.5 - 9.5 → 9.7
	9.6	multi-stage - 9.3 → 9.5 - 9.5 → 9.6
	9.5	direct
	9.4	not available

If your current ONTAP release is...	And your target ONTAP release is...	Your manual upgrade path is...
9.2	9.11.1	multi-stage - 9.2 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9.2 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.10.1
	9.9.1	multi-stage - 9.2 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1
	9.8	multi-stage - 9.2 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.8
	9.7	multi-stage - 9.2 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7
	9.6	multi-stage - 9.2 → 9.3 - 9.3 → 9.5 - 9.5 → 9.6
	9.5	multi-stage - 9.2 → 9.3 - 9.3 → 9.5
	9.4	not available
	9.3	direct

If your current ONTAP release is...	And your target ONTAP release is...	Your manual upgrade path is...
9.1	9.11.1	multi-stage - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.10.1
	9.9.1	multi-stage - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1
	9.8	multi-stage - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.8
	9.7	multi-stage - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7
	9.6	multi-stage - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.6
	9.5	multi-stage - 9.1 → 9.3 - 9.3 → 9.5
	9.4	not available
	9.3	direct
	9.2	not available

<b>If your current ONTAP release is...</b>	<b>And your target ONTAP release is...</b>	<b>Your manual upgrade path is...</b>
9.0		

	9.3	multi-stage - 9.0 → 9.1 - 9.1 → 9.3
<b>If your current ONTAP release is...</b>	<b>And your target ONTAP release is...</b>	<b>Your manual upgrade path is...</b>
	9.1	direct

### Upgrade paths, Data ONTAP 8

Be sure to verify that your platform can run the target ONTAP release by using the [NetApp Hardware Universe](#).

**Note:** The Data ONTAP 8.3 Upgrade Guide erroneously states that in a four-node cluster, you should plan to upgrade the node that holds epsilon last. This is no longer a requirement for upgrades beginning with Data ONTAP 8.2.3. For more information, see [NetApp Bugs Online Bug ID 805277](#).

#### From Data ONTAP 8.3.x

You can upgrade directly to ONTAP 9.1, then upgrade to later releases.

#### From Data ONTAP releases earlier than 8.3.x, including 8.2.x

You must first upgrade to Data ONTAP 8.3.x, then upgrade to ONTAP 9.1, then upgrade to later releases.

## Plan your upgrade with Upgrade Advisor

The Upgrade Advisor service in [Active IQ Digital Advisor](#) provides intelligence that helps you plan your upgrade and minimizes uncertainty and risk.

Active IQ identifies issues in your environment that can be resolved by upgrading to a newer version of ONTAP. The Upgrade Advisor service helps you plan for a successful upgrade and provides a report of issues you might need to be aware of in the ONTAP version you're upgrading to.



An active SupportEdge contract is required for Active IQ.

1. [Launch Active IQ](#)
2. Review the Active IQ health summary to help assess the health of your cluster.
3. Review the recommended upgrade path and generate your upgrade plan.

### Related information

[SupportEdge Services](#)

## Upgrade without Upgrade Advisor

### Plan your upgrade without Upgrade Advisor

It is a best practice to use Upgrade Advisor in [Active IQ](#) to plan your upgrade. If you do not have an active [SupportEdge](#) contract for Active IQ, you should perform the necessary pre-upgrade checks and create your own upgrade plan.

#### How long will my upgrade take?

You should plan for at least 30 minutes to complete preparatory steps, 60 minutes to upgrade each HA pair, and at least 30 minutes to complete post-upgrade steps.



If you are using NetApp Encryption with an external key management server and the Key Management Interoperability Protocol (KMIP), you should expect the upgrade for each HA pair to be longer than one hour.

Our upgrade duration guidelines are based on typical configurations and workloads. You can use these guidelines to estimate the time it will take to perform a nondisruptive upgrade in your environment. However, the actual duration of your upgrade process will depend on your individual environment and the number of nodes.

## Resources to read before you upgrade

If you don't use [Active IQ Upgrade Advisor](#), you need to review a number of NetApp resources before upgrading your ONTAP software. These resources will help you understand issues you must resolve, new system behavior in the target release, and confirm hardware support.

1. Review the *Release Notes* for the target release.

### [ONTAP 9 Release Notes](#)

The “Important cautions” section describes potential issues that you should be aware of before upgrading to the new release. The “New and changed features” and “Known problems and limitations” sections describe new system behavior after upgrading to the new release.

2. Confirm that your hardware platform as well as your cluster and management switches are supported in the target release.

You can upgrade in a transitional state, but ultimately your NX-OS (cluster network switches), IOS (management network switches), and reference configuration file (RCF) software versions should be compatible with the version of ONTAP to which you are upgrading.

### [NetApp Hardware Universe](#)

3. Confirm that your MetroCluster IP switches are supported in the target release.

### [NetApp Interoperability Matrix Tool](#)

4. If your cluster and management switches do not have the minimum software versions for the target ONTAP release, upgrade to supported software versions.

- [NetApp Downloads: Broadcom Cluster Switches](#)
- [NetApp Downloads: Cisco Ethernet Switches](#)
- [NetApp Downloads: NetApp Cluster Switches](#)

5. If your cluster is configured for SAN, confirm that the SAN configuration is fully supported.

All SAN components—including the target ONTAP software version, host OS and patches, required Host Utilities software, multipathing software, and adapter drivers and firmware—should be supported.

### [NetApp Interoperability Matrix Tool](#)

6. If you are transitioning from 7-Mode using the 7-Mode Transition Tool, confirm that the tool supports transition to the ONTAP version to which you are upgrading.



All the projects in the tool must be in the completed or aborted state before you upgrade the 7-Mode Transition Tool that supports the ONTAP version to which you are upgrading.

## [7-Mode Transition Tool installation and administration](#)

### What should I verify before I upgrade without Upgrade Advisor?

#### What to verify before upgrading

If you don't use [Active IQ Upgrade Advisor](#) to plan your upgrade, you should verify your cluster upgrade limits and your cluster activity before you upgrade.

#### Verify cluster upgrade limits

If you don't use [Active IQ Upgrade Advisor](#), you need to verify that your cluster does not exceed the platform system limits. SAN also has limits that you should verify in addition to the platform system limits.

1. Verify that the cluster does not exceed the system limits for your platform.

#### [NetApp Hardware Universe](#)

2. If your cluster is configured for SAN, verify that it does not exceed the configuration limits for FC, FCoE, and iSCSI.

#### [NetApp Hardware Universe](#)

3. Determine the CPU and disk utilization: `node run -node node_name -command sysstat -c 10 -x 3`

You should monitor CPU and disk utilization for 30 seconds. The values in the **CPU** and **Disk Util** columns should not exceed 50% for all 10 measurements reported. No additional load should be added to the cluster until the upgrade is complete.

NOTE: CPU and disk utilization can vary at different times in your environment. Therefore, it is best to check your CPU and disk utilization during the timeframe of your anticipated upgrade window.

#### Verify current cluster activity

If you don't use [Active IQ Upgrade Advisor](#), before upgrading, you should manually verify that no jobs are running and that any CIFS sessions that are not continuously available are terminated.

#### Verify that no jobs are running

Before upgrading the ONTAP software, you must verify the status of cluster jobs. If any aggregate, volume, NDMP (dump or restore), or Snapshot jobs (such as create, delete, move, modify, replicate, and mount jobs) are running or queued, you must allow the jobs to finish successfully or stop the queued entries.

1. Review the list of any running or queued aggregate, volume, or Snapshot jobs: `job show`

```
cluster1::> job show
```

Job ID	Name	Owning Vserver	Node	State
8629	Vol Reaper	cluster1	-	Queued
	Description: Vol Reaper Job			
8630	Certificate Expiry Check	cluster1	-	Queued
	Description: Certificate Expiry Check			
.				
.				
.				

2. If there are any running jobs, allow them to finish successfully.
3. Delete any of the queued aggregate, volume, or Snapshot copy jobs: `job delete -id job_id`

```
cluster1::> job delete -id 8629
```

4. Verify that no aggregate, volume, or Snapshot jobs are running or queued: `job show`

In this example, all running and queued jobs have been deleted:

```
cluster1::> job show
```

Job ID	Name	Owning Vserver	Node	State
9944	SnapMirrorDaemon_7_2147484678	cluster1	node1	Dormant
	Description: Snapmirror Daemon for 7_2147484678			
18377	SnapMirror Service Job	cluster1	node0	Dormant
	Description: SnapMirror Service Job			

2 entries were displayed

## Identifying active CIFS sessions that should be terminated

Before upgrading the ONTAP software, you should identify and gracefully terminate any CIFS sessions that are not continuously available.

Continuously available CIFS shares, which are accessed by Hyper-V or Microsoft SQL Server clients using the SMB 3.0 protocol, do not need to be terminated before upgrading.

1. Identify any established CIFS sessions that are not continuously available: `vserver cifs session show -continuously-available Yes -instance`

This command displays detailed information about any CIFS sessions that have no continuous availability. You should terminate them before proceeding with the ONTAP upgrade.

```
cluster1::> vserver cifs session show -continuously-available Yes
-instance

                Node: node1
                Vserver: vs1
                Session ID: 1
                Connection ID: 4160072788
Incoming Data LIF IP Address: 198.51.100.5
                Workstation IP address: 203.0.113.20
                Authentication Mechanism: NTLMv2
                Windows User: CIFS\user1
                UNIX User: nobody
                Open Shares: 1
                Open Files: 2
                Open Other: 0
                Connected Time: 8m 39s
                Idle Time: 7m 45s
                Protocol Version: SMB2_1
                Continuously Available: No
1 entry was displayed.
```

2. If necessary, identify the files that are open for each CIFS session that you identified: `vserver cifs session file show -session-id session_ID`

```
cluster1::> vserver cifs session file show -session-id 1

Node:          node1
Vserver:       vs1
Connection:    4160072788
Session:       1
File   File           Open Hosting
Continuously
ID     Type             Mode Volume           Share              Available
-----
-----
1      Regular            rw  vol10              homedirshare      No
Path:  \TestDocument.docx
2      Regular            rw  vol10              homedirshare      No
Path:  \file1.txt
2 entries were displayed.
```

## Related information

[Considerations for session-oriented protocols](#)

### How firmware is updated during the ONTAP upgrade

Because upgrading ONTAP includes upgrading your firmware, you do not need to update firmware manually. When you perform an ONTAP upgrade, the firmware for your cluster included with the ONTAP upgrade package is copied to each node's boot device, and the new firmware is installed automatically.

Firmware for the following components is updated automatically if the version in your cluster is older than the firmware that is bundled with the ONTAP upgrade package:

- BIOS/LOADER
- Service Processor (SP) or baseboard management controller (BMC)
- Storage shelf
- Disk
- Flash Cache

If desired, you can also update firmware manually in between ONTAP upgrades.

## What should I verify before I upgrade with or without Upgrade Advisor?

### What to check before upgrading

Even if you use [Active IQ Upgrade Advisor](#) to plan your upgrade, there still are various pre-checks you should perform before you upgrade to verify cluster health, storage health, configuration, and more.

### Verify cluster health

Before you upgrade a cluster, you should verify that the nodes are healthy and eligible to participate in the cluster, and that the cluster is in quorum.

1. Verify that the nodes in the cluster are online and are eligible to participate in the cluster: `cluster show`

```
cluster1::> cluster show
Node                Health  Eligibility
-----
node0                true   true
node1                true   true
```

If any node is unhealthy or ineligible, check EMS logs for errors and take corrective action.

2. If you are operating in a SAN environment, verify that each node is in a SAN quorum: `event log show -severity informational -message-name scsiblade.*`

The most recent scsiblade event message for each node should indicate that the scsi-blade is in quorum.

```
cluster1::*> event log show -severity informational -message-name
scsiblade.*
```

Time	Node	Severity	Event
MM/DD/YYYY TIME	node0	INFORMATIONAL	scsiblade.in.quorum: The scsi-blade ...
MM/DD/YYYY TIME	node1	INFORMATIONAL	scsiblade.in.quorum: The scsi-blade ...

## Related information

[System administration](#)

## Verify storage health

Before and after you upgrade a cluster, you should verify the status of your disks, aggregates, and volumes.

1. Verify disk status:

To check for...	Do this...
Broken disks	<ol style="list-style-type: none"> <li>a. Display any broken disks:  <code>storage disk show -state broken</code></li> <li>b. Remove or replace any broken disks.</li> </ol>
Disks undergoing maintenance or reconstruction	<ol style="list-style-type: none"> <li>a. Display any disks in maintenance, pending, or reconstructing states:  <code>storage disk show -state maintenance pending reconstructing</code></li> <li>b. Wait for the maintenance or reconstruction operation to finish before proceeding.</li> </ol>

2. Verify that all aggregates are online by displaying the state:

```
storage aggregate show -state !online
```

This command displays the aggregates that are *not* online. All aggregates must be online before and after performing a major upgrade or reversion.

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

3. Verify that all volumes are online by displaying any volumes that are *not* online:

```
volume show -state !online
```

All volumes must be online before and after performing a major upgrade or reversion.

```
cluster1::> volume show -state !online
There are no entries matching your query.
```

#### 4. Verify that there are no inconsistent volumes:

```
volume show -is-inconsistent true
```

See the Knowledge Base article [Volume Showing WAFL Inconsistent](#) on how to address the inconsistent volumes.

### Related information

[Logical storage management](#)

### Verify SVM routing configuration

It is a best practice to configure one default route for an SVM. To avoid disruption, you should ensure that the default route is able to reach any network address that is not reachable by a more specific route. For more information, see [SU134: Network access might be disrupted by incorrect routing configuration in clustered ONTAP](#).

The routing table for an SVM determines the network path the SVM uses to communicate with a destination. It's important to understand how routing tables work so that you can prevent network problems before they occur.

Routing rules are as follows:

- ONTAP routes traffic over the most specific available route.
- ONTAP routes traffic over a default gateway route (having 0 bits of netmask) as a last resort, when more specific routes are not available.

In the case of routes with the same destination, netmask, and metric, there is no guarantee that the system will use the same route after a reboot or after an upgrade. This is especially an issue if you have configured multiple default routes.

### Verifying the LIF failover configuration

Before you perform an upgrade, you must verify that the failover policies and failover groups are configured correctly.



During the upgrade process, LIFs are migrated based on the upgrade method. Depending upon the upgrade method, the LIF failover policy might or might not be used.

If you have 8 or more nodes in your cluster, the automated upgrade is performed using the batch method. The batch upgrade method involves dividing the cluster into multiple upgrade batches, upgrading the set of nodes in the first batch, upgrading their high-availability (HA) partners, and then repeating the process for the remaining batches. In ONTAP 9.7 and earlier, if the batch method is used, LIFs are migrated to the HA partner of the node being upgraded. In ONTAP 9.8 and later, if the batch method is used, LIFs are migrated to the other batch group.

If you have less than 8 nodes in your cluster, the automated upgrade is performed using the rolling method. The rolling upgrade method involves initiating a failover operation on each node in an HA pair, updating the "failed" node, initiating giveback, and then repeating the process for each HA pair in the cluster. If the rolling

method is used, LIFs are migrated to the failover target node as defined by the LIF failover policy.

1. Display the failover policy for each data LIF:

If your ONTAP version is...	Use this command
9.6 or later	<code>network interface show -service-policy data -failover</code>
9.5 or earlier	<code>network interface show -role data -failover</code>

This example shows the default failover configuration for a two-node cluster with two data LIFs:

```
cluster1::> network interface show -role data -failover
          Logical          Home          Failover          Failover
Vserver  Interface        Node:Port        Policy           Group
-----  -
vs0
          lif0            node0:e0b        nextavail        system-
defined
                                     Failover Targets: node0:e0b, node0:e0c,
                                                         node0:e0d, node0:e0e,
                                                         node0:e0f, node1:e0b,
                                                         node1:e0c, node1:e0d,
                                                         node1:e0e, node1:e0f
vs1
          lif1            node1:e0b        nextavail        system-
defined
                                     Failover Targets: node1:e0b, node1:e0c,
                                                         node1:e0d, node1:e0e,
                                                         node1:e0f, node0:e0b,
                                                         node0:e0c, node0:e0d,
                                                         node0:e0e, node0:e0f
```

The **Failover Targets** field shows a prioritized list of failover targets for each LIF. For example, if lif0 fails over from its home port (e0b on node0), it's first attempts to fail over to port e0c on node0. If lif0 cannot fail over to e0c, it next attempts to fail over to port e0d on node0, and so on.

2. If the failover policy is set to disabled for any LIFs, other than SAN LIFs, use the `network interface modify` command to enable failover.
3. For each LIF, verify that the **Failover Targets** field includes data ports from a different node that will remain up while the LIF's home node is being upgraded.

You can use the `network interface failover-groups modify` command to add a failover target to the failover group.

## Example

```
network interface failover-groups modify -vserver vs0 -failover-group
fg1 -targets sti8-vsimsim-ucs572q:e0d,sti8-vsimsim-ucs572r:e0d
```

## Related information

[Network and LIF management](#)

## Verify status

Before you upgrade, you should verify the following:

- HA pair status
- LDAP status (for ONTAP 9.2 or later)
- DNS server status (for ONTAP 9.2 or later),
- Networking and storage status (for MetroCluster configurations)

### Verifying HA status

Before performing a nondisruptive upgrade, you should verify that storage failover is enabled for each HA pair. If the cluster consists of only two nodes, you should also verify that cluster HA is enabled.

You do not need to verify the HA status if you plan to perform a disruptive upgrade, because this upgrade method does not require storage failover.

1. Verify that storage failover is enabled and possible for each HA pair: `storage failover show`

This example shows that storage failover is enabled and possible on node0 and node1:

```
cluster1::> storage failover show

Node           Partner           Takeover
-----
Possible State
-----
node0          node1             true          Connected to node1
node1          node0             true          Connected to node0
2 entries were displayed.
```

If necessary, you can enable storage failover by using the `storage failover modify` command.

2. If the cluster consists of only two nodes (a single HA pair), verify that cluster HA is configured: `cluster ha show`

This example shows that cluster HA is configured:



```
cluster1::> cluster ha show
High Availability Configured: true
```

If necessary, you can enable cluster HA by using the `cluster ha modify` command.

### Verifying LDAP status (ONTAP 9.2 and later)

Beginning with ONTAP 9.2, if LDAP is used by your storage virtual machines (SVMs), you must have an established LDAP connection to perform a nondisruptive upgrade. You should verify the LDAP connection before you begin the upgrade.

The task does not apply if you are upgrading from ONTAP 9.1 or earlier.

1. Check the LDAP status: `ldap check -vserver vserver_name`
2. If the LDAP status is down, modify it: `ldap client modify -client-config LDAP_client -ldap -servers ip_address`
3. Verify that the LDAP status is up: `ldap check -vserver vserver_name`

### Verifying DNS server status (ONTAP 9.2 and later)

Beginning with ONTAP 9.2 and later, you should verify the status of your Domain Name Service (DNS) server before and after performing a nondisruptive upgrade.

The task does not apply if you are upgrading from ONTAP 9.1 or earlier.

1. Check the status of your DNS servers: `dns check -vserver vserver_name`

An up status indicates the service is running. A down status indicates that the service is not running.

2. If the DNS server is down, modify it: `dns modify -vserver vserver_name -domains domain_name -name-servers name_server_ipaddress`
3. Verify the status of the DNS server is up.

### Verify all LIFS are on home ports before upgrade

During a reboot, some LIFs might have been migrated to their assigned failover ports. Before and after you upgrade a cluster, you must enable and revert any LIFs that are not on their home ports.

The `network interface revert` command reverts a LIF that is not currently on its home port back to its home port, provided that the home port is operational. A LIF's home port is specified when the LIF is created; you can determine the home port for a LIF by using the `network interface show` command.

1. Display the status of all LIFs: `network interface show`

This example displays the status of all LIFs for a storage virtual machine (SVM).

```

cluster1::> network interface show -vserver vs0
          Logical      Status      Network      Current
Current Is
Vserver   Interface  Admin/Oper  Address/Mask  Node      Port
Home
-----
vs0
          data001    down/down  192.0.2.120/24  node0     e0e
true
          data002    down/down  192.0.2.121/24  node0     e0f
true
          data003    down/down  192.0.2.122/24  node0     e2a
true
          data004    down/down  192.0.2.123/24  node0     e2b
true
          data005    down/down  192.0.2.124/24  node0     e0e
false
          data006    down/down  192.0.2.125/24  node0     e0f
false
          data007    down/down  192.0.2.126/24  node0     e2a
false
          data008    down/down  192.0.2.127/24  node0     e2b
false
8 entries were displayed.

```

If any LIFs appear with a Status Admin status of down or with an Is home status of false, continue with the next step.

2. Enable the data LIFs: `network interface modify {-role data} -status-admin up`

```

cluster1::> network interface modify {-role data} -status-admin up
8 entries were modified.

```

3. Revert LIFs to their home ports: `network interface revert *`

This command reverts all LIFs back to their home ports.

```

cluster1::> network interface revert *
8 entries were acted on.

```

4. Verify that all LIFs are in their home ports: `network interface show`

This example shows that all LIFs for SVM vs0 are on their home ports.

```

cluster1::> network interface show -vserver vs0
          Logical      Status      Network      Current
Current Is
Vserver   Interface  Admin/Oper  Address/Mask  Node      Port
Home
-----
vs0
          data001      up/up      192.0.2.120/24  node0     e0e
true
          data002      up/up      192.0.2.121/24  node0     e0f
true
          data003      up/up      192.0.2.122/24  node0     e2a
true
          data004      up/up      192.0.2.123/24  node0     e2b
true
          data005      up/up      192.0.2.124/24  node1     e0e
true
          data006      up/up      192.0.2.125/24  node1     e0f
true
          data007      up/up      192.0.2.126/24  node1     e2a
true
          data008      up/up      192.0.2.127/24  node1     e2b
true
8 entries were displayed.

```

### Use Active IQ Config Advisor to verify there are no common configuration errors

Before you upgrade, you can use the Active IQ Config Advisor tool to check for common configuration errors.

Active IQ Config Advisor is a configuration validation and health check tool for NetApp systems. This tool can be deployed at both secure sites and nonsecure sites for data collection and system analysis.



Support for Active IQ Config Advisor is limited and is available only online.

1. Log in to the NetApp Support Site, and then click **TOOLS > Tools**.
2. Under **Active IQ Config Advisor**, click [Download App](#).
3. Download, install, and run Active IQ Config Advisor by following the directions on the web page.
4. After running Active IQ Config Advisor, review the tool's output, and follow the recommendations that are provided to address any issues that are discovered by the tool.

### Special considerations

## Pre-upgrade checks

Depending on your environment, you need to consider certain factors before you start your upgrade. Get started by reviewing the table below to see what special considerations you need to consider.

Ask yourself...	If your answer is yes, then do this...
Do I have a mixed version cluster?	<a href="#">Check mixed version requirements</a>
Do I have a SAN configuration?	<a href="#">Verify the SAN configuration</a>
Do I have a MetroCluster configuration?	<ul style="list-style-type: none"><li>• <a href="#">Review specific upgrade requirements for MetroCluster configurations</a></li><li>• <a href="#">Verify networking and storage status</a></li></ul>
Are nodes on my cluster using root-data partitioning and root-data-data-partitioning?	<a href="#">Examine upgrade considerations for root-data and root-data-data partitioning</a>
Do I have deduplicated volumes and aggregates?	<a href="#">Verify you have enough free space for your deduplicated volumes and aggregates</a>
Is my cluster running SnapMirror?	<ul style="list-style-type: none"><li>• <a href="#">Review upgrade requirements for SnapMirror</a></li><li>• <a href="#">Prepare your SnapMirror relationships for upgrade</a></li></ul>
Is my cluster running SnapLock?	<a href="#">Review upgrade considerations for SnapLock</a>
Am I upgrading from ONTAP 8.3 and have load-sharing mirrors?	<a href="#">Prepare all load-sharing mirrors for upgrade</a>
Am I using NetApp Storage Encryption with external key management servers?	<a href="#">Delete any existing key management server connections</a>
Do I have netgroups loaded into SVMs?	<a href="#">Verify that the netgroup file is present on each node</a>
Do I have LDAP clients using SSLv3?	<a href="#">Configure LDAP clients to use TLS</a>
Am I using session-oriented protocols?	<a href="#">Review considerations for session-oriented protocols</a>
Is SSL FIPS mode enabled on a cluster where administrator accounts authenticate with an SSH public key?	<a href="#">Review requirements for SSH public keys</a>

## Mixed version requirements

Beginning with ONTAP 9.3, by default, you cannot join new nodes to the cluster that are running a version of ONTAP that is different from the version running on the existing nodes.

If you plan to add new nodes to your cluster that are running a version of ONTAP that is later than the nodes in your existing cluster, you should upgrade the nodes in your cluster to the later version first, then add the new nodes.

Mixed version clusters are not recommended, but in certain cases you might need to temporarily enter a mixed version state. For example, you need to enter a mixed version state if you are upgrading to a later version of

ONTAP that is not supported on certain nodes in your existing cluster. In this case, you should upgrade the nodes that do support the later version of ONTAP, then unjoin the nodes that do not support the version of ONTAP you are upgrading to using the advanced privilege `cluster unjoin -skip-lastlow-version -node check` command.

You might also need to enter a mixed version state for a technical refresh or an interrupted upgrade. In such cases you can override ONTAP default behavior and join nodes of a different version using the following advanced privilege commands:

- `cluster join -allow-mixed-version-join`
- `cluster add-node -allow-mixed-version-join`

When you have to enter a mixed version state, you should complete the upgrade as quickly as possible. An HA pair must not run an ONTAP version from a release that is different from other HA pairs in the cluster for more than seven days. For correct cluster operation, the period the cluster is in a mixed version state should be as short as possible.

When the cluster is in a mixed version state, you should not enter any commands that alter the cluster operation or configuration except as necessary to satisfy the upgrade requirements.

### Verifying the SAN configuration

Upgrading in a SAN environment changes which paths are direct. Therefore, before performing an upgrade, you should verify that each host is configured with the correct number of direct and indirect paths, and that each host is connected to the correct LIFs.

1. On each host, verify that a sufficient number of direct and indirect paths are configured, and that each path is active.

Each host must have a path to each node in the cluster.

2. Verify that each host is connected to a LIF on each node.

You should record the list of initiators for comparison after the upgrade.

For...	Enter...
iSCSI	<code>iscsi initiator show -fields igroup,initiator-name,tpgroup</code>
FC	<code>fcp initiator show -fields igroup,wwpn,lif</code>

### MetroCluster configurations

#### Upgrade requirements for MetroCluster configurations

If you have to upgrade a MetroCluster configuration, you should be aware of some important requirements.

## Required methods for performing major and minor upgrades of MetroCluster configurations

Patch upgrades to MetroCluster configurations can be performed with automatic non-disruptive upgrade (NDU) procedure.

Beginning with ONTAP 9.3, major upgrades to MetroCluster configurations can be performed with automatic non-disruptive upgrade (NDU) procedure. On systems running ONTAP 9.2 or earlier, major upgrades to MetroCluster configurations must be performed with the NDU procedure that is specific to MetroCluster configurations.

### General requirements

- Both clusters must be running the same version of ONTAP.

You can verify the ONTAP version by using the version command.

- The MetroCluster configuration must be in either normal or switchover mode.



Upgrade in switchover mode is only supported in minor patch upgrades.

- For all configurations except two-node clusters, you can nondisruptively upgrade both clusters at the same time.

For nondisruptive upgrade in two-node clusters, the clusters must be upgraded one node at a time.

- The aggregates in both clusters must not be in resyncing RAID status.

During MetroCluster healing, the mirrored aggregates are resynchronized. You can verify if the MetroCluster configuration is in this state by using the `storage aggregate plex show -in -progress true` command. If any aggregates are being synchronized, you should not perform an upgrade until the resynchronization is complete.

- Negotiated switchover operations will fail while the upgrade is in progress.

To avoid issues with upgrade or revert operations, do not attempt an unplanned switchover during an upgrade or revert operation unless all nodes on both clusters are running the same version of ONTAP.

### Configuration requirements for normal operation

- The source SVM LIFs must be up and located on their home nodes.

Data LIFs for the destination SVMs are not required to be up or to be on their home nodes.

- All aggregates at the local site must be online.
- All root and data volumes owned by the local cluster's SVMs must be online.

### Configuration requirements for switchover

- All LIFs must be up and located on their home nodes.
- All aggregates must be online, except for the root aggregates at the DR site.

Root aggregates at the DR site are offline during certain phases of switchover.

- All volumes must be online.

## Related information

[Verifying networking and storage status for MetroCluster configurations](#)

## Verify networking and storage status for MetroCluster configurations

Before performing an upgrade in a MetroCluster configuration, you should verify the status of the LIFs, aggregates, and volumes for each cluster.

1. Verify the LIF status: `network interface show`

In normal operation, LIFs for source SVMs must have an admin status of up and be located on their home nodes. LIFs for destination SVMs are not required to be up or located on their home nodes. In switchover, all LIFs have an admin status of up, but they do not need to be located on their home nodes.

```

cluster1::> network interface show
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper  Address/Mask  Node      Port
Home
-----
Cluster
      cluster1-a1_clus1
              up/up      192.0.2.1/24      cluster1-01
              e2a
true
      cluster1-a1_clus2
              up/up      192.0.2.2/24      cluster1-01
              e2b
true
cluster1-01
      clus_mgmt      up/up      198.51.100.1/24      cluster1-01
              e3a
true
      cluster1-a1_inet4_intercluster1
              up/up      198.51.100.2/24      cluster1-01
              e3c
true
      ...

27 entries were displayed.

```

2. Verify the state of the aggregates: `storage aggregate show -state !online`

This command displays any aggregates that are *not* online. In normal operation, all aggregates located at the local site must be online. However, if the MetroCluster configuration is in switchover, root aggregates at the disaster recovery site are permitted to be offline.

This example shows a cluster in normal operation:

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

This example shows a cluster in switchover, in which the root aggregates at the disaster recovery site are offline:

```
cluster1::> storage aggregate show -state !online
Aggregate      Size Available Used% State  #Vols  Nodes           RAID
Status
-----
aggr0_b1
      0B      0B    0% offline    0 cluster2-01
raid_dp,
mirror
degraded
aggr0_b2
      0B      0B    0% offline    0 cluster2-02
raid_dp,
mirror
degraded
2 entries were displayed.
```

### 3. Verify the state of the volumes: `volume show -state !online`

This command displays any volumes that are *not* online.

If the MetroCluster configuration is in normal operation (it is not in switchover state), the output should show all volumes owned by the cluster's secondary SVMs (those with the SVM name appended with "-mc").

Those volumes come online only in the event of a switchover.

This example shows a cluster in normal operation, in which the volumes at the disaster recovery site are not online.



```

cluster1::> volume show -state !online
  (volume show)
Vserver   Volume           Aggregate      State      Type      Size
Available Used%
-----
vs2-mc    vol1             aggr1_b1      -          RW        -
-         -
vs2-mc    root_vs2        aggr0_b1      -          RW        -
-         -
vs2-mc    vol2             aggr1_b1      -          RW        -
-         -
vs2-mc    vol3             aggr1_b1      -          RW        -
-         -
vs2-mc    vol4             aggr1_b1      -          RW        -
-         -
5 entries were displayed.

```

4. Verify that there are no inconsistent volumes: `volume show -is-inconsistent true`

If any inconsistent volumes are returned, you must contact NetApp Support before you precede with the upgrade.

#### Related information

[Upgrade requirements for MetroCluster configurations](#)

#### Upgrade considerations for root-data partitioning and root-data-data partitioning

Root-data partitioning and root-data-data-partitioning is supported for some platform models and configurations. This partitioning capability is enabled during system initialization; it cannot be applied to existing aggregates.

For information about migrating your data to a node that is configured for root-data partitioning or root-data-data partitioning, contact your account team or partner organization.

#### Related information

[ONTAP concepts](#)

#### Verify that deduplicated volumes and aggregates contain sufficient free space

Before upgrading ONTAP, you must verify that any deduplicated volumes and the aggregates that contain them have sufficient free space for the deduplication metadata. If there is insufficient free space, deduplication will be disabled when the ONTAP upgrade is completed.

Each deduplicated volume must contain at least 4% free space. Each aggregate that contains a deduplicated volume must contain at least 3% free space.

1. Determine which volumes are deduplicated: `volume efficiency show`
2. Determine the free space available on each volume that you identified: `vol show -vserver Vserver_name -volume volume_name -fields volume, size, used, available, percent-used, junction-path`

Each deduplicated volume must not contain more than 96% used capacity. If necessary, you can increase the sizes of any volumes that exceed this capacity.

### Logical storage management

In this example, the percent-used field displays the percentage of used space on the deduplicated volume.:

```
vserver      volume size      junction-path available used    percent-used
-----
cluster1-01 vo10    22.99GB -          14.11GB    7.73GB 35%
cluster1-02 vo10    22.99GB -          12.97GB    8.87GB 40%
2 entries were displayed.
```

3. Identify the free space available on each aggregate that contains a deduplicated volume: `aggr show -aggregate aggregate_name -fields aggregate, size, usedsize, availsize, percent-used`

Each aggregate must not contain more than 97% used capacity. If necessary, you can increase the sizes of any aggregates that exceed this capacity.

### Disk and aggregate management

In this example, the percent-used field displays the percentage of used space on the aggregate containing the deduplicated volume (`aggr_2`):

```
aggr show -aggregate aggregate_name -fields
aggregate, size, usedsize, availsize, percent-used
aggregate          availsize percent-used size      usedsize
-----
aggr0_cluster1_01  1.11GB   95%          24.30GB 23.19GB
aggr0_cluster1_02 1022MB   96%          24.30GB 23.30GB
2 entries were displayed.
```

## SnapMirror

### Upgrade requirements for SnapMirror

You must perform certain tasks to successfully upgrade a cluster that is running SnapMirror.

- If you are upgrading clusters with DP SnapMirror relationships, you must upgrade the destination cluster/nodes before you upgrade the source cluster/nodes.

- Before upgrading a cluster that is running SnapMirror, SnapMirror operations must be quiesced for each node that contains destination volumes, and each peered SVM must have a unique name across the clusters.

To prevent SnapMirror transfers from failing, you must suspend SnapMirror operations and, in some cases, upgrade destination nodes before upgrading source nodes. The following table describes the two options for suspending SnapMirror operations.

Option	Description	Upgrade destination nodes before source nodes?
Suspend SnapMirror operations for the duration of the NDU (nondisruptive upgrade).	The simplest method for upgrading in a SnapMirror environment is to suspend all SnapMirror operations, perform the upgrade, and then resume the SnapMirror operations. However, no SnapMirror transfers will occur during the entire NDU. You must use this method if your cluster contains nodes that are mirroring volumes to each other.	No, the nodes can be upgraded in any order.
Suspend SnapMirror operations one destination volume at a time.	You can suspend SnapMirror transfers for a particular destination volume, upgrade the node (or HA pair) that contains the destination volume, upgrade the node (or HA pair) that contains the source volume, and then resume the SnapMirror transfers for the destination volume. By using this method, SnapMirror transfers for all other destination volumes can continue while the nodes that contain the original destination and source volumes are upgraded.	Yes.

SVM peering requires SVM names to be unique across clusters. It is best practice to name SVMs with a unique fully qualified domain name (FQDN), for example, “dataVserver.HQ” or “mirrorVserver.Offsite”. Using the FQDN naming style makes it much easier to make sure of uniqueness.

**Related information**

[ONTAP concepts](#)

**Prepare SnapMirror relationships for a nondisruptive upgrade**

It is recommended that you quiesce your SnapMirror operations before performing a nondisruptive upgrade of ONTAP.

1. Use the `snapmirror show` command to determine the destination path for each SnapMirror relationship.

2. For each destination volume, suspend future SnapMirror transfers: `snapmirror quiesce -destination-path destination`

If there are no active transfers for the SnapMirror relationship, this command sets its status to Quiesced. If the relationship has active transfers, the status is set to Quiescing until the transfer is completed, and then the status becomes Quiesced.

This example quiesces transfers involving the destination volume vol1 from SVMvs0.example.com:

```
cluster1::> snapmirror quiesce -destination-path vs0.example.com:vol1
```

3. Verify that all SnapMirror relationships are quiesced: `snapmirror show -status !Quiesced`

This command displays any SnapMirror relationships that are *not* quiesced.

This example shows that all SnapMirror relationships are quiesced:

```
cluster1::> snapmirror show -status !Quiesced
There are no entries matching your query.
```

4. If any SnapMirror relationships are currently being transferred, do one of the following options:

Option	Description
Wait for the transfers to finish before performing the ONTAP upgrade.	After each transfer finishes, the relationship changes to Quiesced status.
Stop the transfers: <code>snapmirror abort -destination-path destination -h</code> <b>Note:</b> You must use the <code>-foreground true</code> parameter if you are aborting load-sharing mirror transfers.	This command stops the SnapMirror transfer and restores the destination volume to the last Snapshot copy that was successfully transferred. The relationship is set to Quiesced status.

## Related information

[Upgrade requirements for SnapMirror](#)

## Upgrade considerations for SnapLock

SnapLock does not allow the download of certain kernel versions if these are qualified as bad SnapLock releases or if SnapLock is disabled in those releases. These download restrictions only apply if the node has SnapLock data.

## Prepare all load-sharing mirrors for a major upgrade

Before performing a major upgrade from ONTAP 8.3, you should move all of the load-sharing mirror source volumes to an aggregate on the node that you will upgrade last. This ensures that load-sharing mirror destination volumes are the same or later versions of ONTAP.

1. Record the locations of all load-sharing mirror source volumes.

Knowing where the load-sharing mirror source volumes came from helps facilitate returning them to their original locations after the major upgrade.

2. Determine the node and aggregate to which you will move the load-sharing mirror source volumes.
3. Move the load-sharing mirror source volumes to the node and aggregate by using the volume move start command.

#### Delete existing external key management server connections before upgrading

If you are using NetApp Storage Encryption (NSE) on ONTAP 9.2 or earlier and upgrading to ONTAP 9.3 or later, you must use the command line interface (CLI) to delete any existing external key management (KMIP) server connections before performing the upgrade.

1. Verify that the NSE drives are unlocked, open, and set to the default manufacture secure ID 0x0:

```
storage encryption disk show -disk*
```

2. Enter the advanced privilege mode:

```
set -privilege advanced
```

3. Use the default manufacture secure ID 0x0 to assign the FIPS key to the self-encrypting disks (SEDs):

```
storage encryption disk modify -fips-key-id 0x0 -disk *
```

4. Verify that assigning the FIPS key to all disks is complete: `storage encryption disk show-status`

5. Verify that the **mode** for all disks is set to `data`: `storage encryption disk show`

6. View the configured KMIP servers: `security key-manager show`

7. Delete the configured KMIP servers: `security key-manager delete -address kmip_ip_address`

8. Delete the external key manager configuration: `security key-manager delete-kmip-config`



This step does not remove the NSE certificates.

After the upgrade is complete, you must reconfigure the KMIP server connections.

#### Related information

[Reconfiguring KMIP server connections after upgrading to ONTAP 9.3 or later](#)

#### Verifying that the netgroup file is present on all nodes

If you have loaded netgroups into storage virtual machines (SVMs), before you upgrade or revert, you must verify that the netgroup file is present on each node. A missing netgroup file on a node can cause an upgrade or revert to fail.

[NFS management](#) contains more information about netgroups and loading them from a URI.

1. Set the privilege level to advanced: `set -privilege advanced`
2. Display the netgroup status for each SVM: `vserver services netgroup status`
3. Verify that for each SVM, each node shows the same netgroup file hash value: `vserver services name-service netgroup status`

If this is the case, you can skip the next step and proceed with the upgrade or revert. Otherwise, proceed to the next step.

4. On any one node of the cluster, manually load the netgroup file: `vserver services netgroup load -vserver vserver_name -source uri`

This command downloads the netgroup file on all nodes. If a netgroup file already exists on a node, it is overwritten.

### Configure LDAP clients to use TLS for highest security

Before upgrading to the target ONTAP release, you must configure LDAP clients using SSLv3 for secure communications with LDAP servers to use TLS. SSL will not be available after the upgrade.

By default, LDAP communications between client and server applications are not encrypted. You must disallow the use of SSL and enforce the use of TLS.

1. Verify that the LDAP servers in your environment support TLS.

If they do not, do not proceed. You should upgrade your LDAP servers to a version that supports TLS.

2. Check which ONTAP LDAP client configurations have LDAP over SSL/TLS enabled: `vserver services name-service ldap client show`

If there are none, you can skip the remaining steps. However, you should consider using LDAP over TLS for better security.

3. For each LDAP client configuration, disallow SSL to enforce the use of TLS: `vserver services name-service ldap client modify -vserver vserver_name -client-config ldap_client_config_name -allow-ssl false`

4. Verify that the use of SSL is no longer allowed for any LDAP clients: `vserver services name-service ldap client show`

### Related information

[NFS management](#)

### Considerations for session-oriented protocols

Clusters and session-oriented protocols might cause adverse effects on clients and applications in certain areas during upgrades.

If you are using session-oriented protocols, consider the following:

- SMB

If you serve continuously available (CA) shares with SMBv3, you can use the automated nondisruptive upgrade method (with System Manager or the CLI), and no disruption is experienced by the client.

If you are serving shares with SMBv1 or SMBv2, or non-CA shares with SMBv3, client sessions are disrupted during upgrade takeover and reboot operations. You should direct users to end their sessions before you upgrade.

For more information, see [TR-4100: Nondisruptive Operations with SMB File Shares ONTAP 9.x](#).

Hyper-V and SQL Server over SMB support nondisruptive operations (NDOs). If you configured a Hyper-V or SQL Server over SMB solution, the application servers and the contained virtual machines or databases remain online and provide continuous availability during the ONTAP upgrade.

- NFSv4.x

NFSv4.x clients will automatically recover from connection losses experienced during the upgrade using normal NFSv4.x recovery procedures. Applications might experience a temporary I/O delay during this process.

- NDMP

State is lost and the client user must retry the operation.

- Backups and restores

State is lost and the client user must retry the operation.



Do not initiate a backup or restore during or immediately before an upgrade. Doing so might result in data loss.

- Applications (for example, Oracle or Exchange)

Effects depend on the applications. For timeout-based applications, you might be able to change the timeout setting to longer than the ONTAP reboot time to minimize adverse effects.

#### Considerations for session-oriented protocols

If SSL FIPS mode is enabled on a cluster where administrator accounts authenticate with an SSH public key, you must ensure that the host key algorithm is supported on the target release before upgrading ONTAP.

**Note:** Host key algorithm support has changed in ONTAP 9.11.1 and later releases.

ONTAP release	Supported key types	Unsupported key types
9.11.1 and later	ecdsa-sha2-nistp256	rsa-sha2-512 rsa-sha2-256 ssh-ed25519 ssh-dss ssh-rsa

9.10.1 and earlier	ecdsa-sha2-nistp256 ssh-ed25519	ssh-dss ssh-rsa
--------------------	------------------------------------	--------------------

Existing SSH public key accounts without the supported key algorithms must be reconfigured with a supported key type before enabling upgrading, or administrator authentication will fail.

[Learn more about enabling SSH public key accounts.](#)

## Download and install the ONTAP software image

You must first download the ONTAP software from the NetApp Support site; then you can install it using the automatic nondisruptive upgrade (ANDU) or manual upgrade process.

### Download the software image

Depending on your ONTAP release, you can copy the ONTAP software image from the NetApp Support Site to one of the following locations: an HTTP, HTTPS or FTP server on your network, or a local folder.

You should note the following important information:

- Software images are specific to platform models.

You must obtain the correct image for your cluster. Software images, firmware version information, and the latest firmware for your platform model are available on the NetApp Support Site.

- Software images include the latest version of system firmware that was available when a given version of ONTAP was released.
- If you are upgrading a system with NetApp Volume Encryption to ONTAP 9.5 or later, you must download the ONTAP software image for non-restricted countries, which includes NetApp Volume Encryption.

If you use the ONTAP software image for restricted countries to upgrade a system with NetApp Volume Encryption, the system panics and you lose access to your volumes.

- If you are upgrading from ONTAP 9.5 to 9.9.1, you must copy the software image for ONTAP 9.7 and 9.9.1.
- If you are upgrading from ONTAP 9.3 to 9.7, you must copy the software image for ONTAP 9.5 and 9.7.

### Steps

1. Locate the target ONTAP software in the [Software Downloads](#) area of the NetApp Support Site.
2. Copy the software image (for example, 97\_q\_image.tgz) to the appropriate location.

Depending on your ONTAP release, the location will be a directory an HTTP, HTTPS or FTP server from which the image will be served to the local system, or to a local folder on the storage system.

You can copy the image to this location...	If you are running these ONTAP releases...
An HTTP or FTP server	ONTAP 9.0 and later
A local folder	ONTAP 9.4 and later
An HTTPS server The server's CA certificate must be installed on the local system.	ONTAP 9.6 and later



## Install the software image

You must install the target software image on the cluster's nodes.

- If you are upgrading a system with NetApp Volume Encryption to ONTAP 9.5 or later, you must have downloaded the ONTAP software image for non-restricted countries, which includes NetApp Volume Encryption.

If you use the ONTAP software image for restricted countries to upgrade a system with NetApp Volume Encryption, the system panics and you lose access to your volumes.

- If you are upgrading from ONTAP 9.5 directly to 9.9.1, you must download the software image for ONTAP 9.7 and 9.9.1. If you are upgrading from ONTAP 9.3 directly to 9.7, you must download the software image for ONTAP 9.5 and 9.7.

The automated upgrade process uses both images in the background to complete the upgrade.

### For automatic nondisruptive upgrade (ANDU)

1. Check the image repository and delete any previous images.

```
cluster image package show-repository
```

```
cluster image package show-repository\  
<<name_of_vsim|There are no packages in the repository.\r\n
```

2. Download the image.

```
cluster image package get -url url_to_image_on_nss
```

#### Example

```
cluster image package get -url http://10.60.132.98/x/eng/rlse/DOT/9.7P13X2/  
promo/9.7P13X2/x86\_64.optimize/image.tgz
```

3. Verify the package is downloaded.

```
cluster image package show-repository
```

#### Example

```
cluster image package show-repository -fields download-ver\  
<<name_of_vsim| download-verX;X\r\n  
<<name_of_vsim| Downloaded VersionX;X\r\n  
<<name_of_vsim| ONTAP 9.10.1.X;X\r\n
```

### For manual upgrades

1. Set the privilege level to advanced, entering **y** when prompted to continue: `set -privilege advanced`

The advanced prompt (**\*>**) appears.

## 2. Download the image.

- a. If you are upgrading a cluster without a MetroCluster configuration or a two-node MetroCluster configuration, use the following command to download the image:

```
system node image update -node * -package location -replace-package true  
-setdefault true -background true
```

*location* can be a web server or a local folder, depending on the ONTAP version. See the `system node image update` man page for details.

This command downloads and installs the software image on all of the nodes simultaneously. To download and install the image on each node one at a time, do not specify the `-background` parameter.

- b. If you are upgrading a four or eight-node MetroCluster configuration, you must issue the following command on both clusters:

```
system node image update -node * -package location -replace-package true  
-background true -setdefault false
```

This command uses an extended query to change the target software image, which is installed as the alternate image on each node.

## 3. Enter `y` to continue when prompted.

## 4. Verify that the software image is downloaded and installed on each node.

```
system node image show-update-progress -node *
```

This command displays the current status of the software image download and installation. You should continue to run this command until all nodes report a **Run Status** of **Exited**, and an **Exit Status** of **Success**.

The `system node image update` command can fail and display error or warning messages. After resolving any errors or warnings, you can run the command again.

This example shows a two-node cluster in which the software image is downloaded and installed successfully on both nodes:

```

cluster1::*> system node image show-update-progress -node *
There is no update/install in progress
Status of most recent operation:
    Run Status:      Exited
    Exit Status:     Success
    Phase:           Run Script
    Exit Message:    After a clean shutdown, image2 will be set as
the default boot image on node0.
There is no update/install in progress
Status of most recent operation:
    Run Status:      Exited
    Exit Status:     Success
    Phase:           Run Script
    Exit Message:    After a clean shutdown, image2 will be set as
the default boot image on node1.
2 entries were acted on.

```

## Which upgrade method should I use?

### Which upgrade method should I use?

The method you use to upgrade — nondisruptive or disruptive, automated or manual — depends upon your configuration. If available, the automated nondisruptive upgrade (ANDU) using System Manager is the preferred method.

### Nondisruptive upgrades

Nondisruptive upgrades take advantage of ONTAP's high-availability (HA) failover technology to ensure that clusters continue to serve data during the upgrade. There are two types of nondisruptive upgrade processes.

- *Batch* updates

In a batch update, the cluster is divided into several batches, each of which contains multiple HA pairs. In the first batch, half of the nodes are upgraded, followed by their HA partners. The process is then repeated sequentially for the remaining batches.

- *Rolling* updates

In a rolling update, a node is taken offline and upgraded while its partner takes over its storage. When the node upgrade is complete, the partner node gives control back to the original owning node and the process is repeated, this time on the partner node. Each additional HA pair is upgraded in sequence until all HA pairs are running the target release.

**Note:** The term *rolling upgrade* is frequently used in the software industry for software upgrades that don't cause disruptions in service and hence is often synonymous with "nondisruptive upgrade". In ONTAP 9 upgrades, a *rolling update* is one of the processes that can be used for nondisruptive upgrades.

Nondisruptive upgrades can be performed using an *automated* or *manual* method.

- **Automated nondisruptive upgrade (ANDU)**

- When an administrator initiates an ANDU, ONTAP automatically installs the target ONTAP image on each node, validates the cluster components to ensure that the cluster can be upgraded

nondisruptively, and then executes a batch or rolling update in the background.

- Batch updates are the default for clusters of 8 nodes or more.
- Rolling updates are the default for clusters with fewer than 8 nodes. Rolling updates can also be selected explicitly for clusters with 8 nodes or more.
- An ANDU can be executed using System Manager or the ONTAP command line interface (CLI). If available for your configuration, ANDU using System Manager is the recommended method of upgrade.

• **Manual nondisruptive upgrade**

- An administrator must manually confirm upgrade readiness of the cluster components on each node, then manually perform rolling update process steps in the foreground.
- Manual nondisruptive upgrades are executed using the ONTAP CLI.
- You should only use a manual method if ANDU is not supported for your configuration.

**Disruptive upgrades**

In a disruptive upgrade, storage failover is disabled for each HA pair, and then each node is rebooted one at a time. Disruptive upgrades can be performed more quickly than nondisruptive upgrades, and require fewer steps to complete. However, you should not perform a disruptive upgrade unless you can take the cluster offline for the duration of the upgrade. If you are operating in a SAN environment, you should be prepared to shut down or suspend all SAN clients before performing a disruptive upgrade. Disruptive upgrades are performed using the ONTAP CLI.

**Methods for non-MetroCluster configurations**

Clusters with 2 or more nodes can use any of the following upgrade methods, which are listed in order of recommended usage.

- [Automated nondisruptive using System Manager](#)
- [Automated nondisruptive using the CLI](#)
- [Manual nondisruptive using the CLI](#)
- [Manual disruptive using the CLI](#)

Single node clusters must use one of disruptive methods, although the automated method is recommended.

- [Automated disruptive using the CLI](#)
- [Manual disruptive using the CLI](#)

**Methods for MetroCluster configurations**

The upgrade methods available for each configuration are listed in order of recommended usage.

ONTAP version	Number of nodes	Upgrade method
9.3 or later	2,4	<ul style="list-style-type: none"><li>• <a href="#">Automated nondisruptive using System Manager</a></li><li>• <a href="#">Automated nondisruptive using the CLI</a></li><li>• <a href="#">Manual disruptive using the CLI</a></li></ul>

ONTAP version	Number of nodes	Upgrade method
9.3 or later	8	<ul style="list-style-type: none"> <li>Automated nondisruptive using the CLI</li> <li>Manual nondisruptive using the CLI</li> <li>Manual disruptive using the CLI</li> </ul>
9.2 or earlier	2	<ul style="list-style-type: none"> <li>Manual nondisruptive (for 2-node clusters) using the CLI</li> <li>Manual disruptive using the CLI</li> </ul>
9.2 or earlier	4, 8	<ul style="list-style-type: none"> <li>Manual nondisruptive using the CLI</li> <li>Manual disruptive using the CLI</li> </ul>
9.0 or later	4, 8 (patch only)	Automated nondisruptive using System Manager
9.2 or earlier	2, 4, 8 (patch only)	Automated nondisruptive using System Manager

### Automated nondisruptive update using System Manager

You can nondisruptively update the version of ONTAP on your cluster using System Manager.

The update process checks your hardware platform and configuration to verify that your system is supported by the ONTAP version to which you are upgrading. ONTAP automatically shifts workloads during an upgrade between clusters so you can continue serving data.

This procedure updates your system to the specified version of ONTAP. It is assumed that your hardware platform and configuration is supported for the target release.

Beginning with ONTAP 9.10.1, if you have a cluster with 8 or more nodes you can select to have them updated one HA pair at a time. This allows you, if needed, to correct upgrade issues on the first HA pair before moving to subsequent pairs.



If issues are encountered during your automated upgrade, you can view EMS messages and details in System Manager: Click **Events & Jobs > Events**.


### Steps

1. If you want to download the software image to an HTTP or FTP server on your network, copy the software image from the NetApp support site to the directory on the HTTP or FTP server from which the image will be served.

If you want to download the software image to a local folder, then click the software image on the NetApp support site, select **Save As**, and then choose the local folder to place the image.

- Depending on the ONTAP version that you are running, perform one of the following steps:

ONTAP version	Steps
ONTAP 9.8 or later	Click <b>Cluster &gt; Overview</b> .
ONTAP 9.5, 9.6, and 9.7	Click <b>Configuration &gt; Cluster &gt; Update</b> .
ONTAP 9.4 or earlier	Click <b>Configuration &gt; Cluster Update</b> .

- In the right corner of the Overview pane, click .
- Click **ONTAP Update**.
- In the Cluster Update tab, add a new image or select an available image.

If you want to...	Then...
Add a new software image from the local client  <b>Note:</b> You should have already downloaded the image to the local client.  <a href="#">Download and install the ONTAP software images</a>	a. Under Available Software Images, click <b>Add from Local</b> .  b. Browse to the location you saved the software image, select the image, and then click <b>Open</b> .  The software image uploads after you click <b>Open</b> .
Add a new software image from the NetApp Support Site	a. Click <b>Add from Server</b> .  b. In the Add a New Software Image dialog box, enter the URL of the HTTP server or FTP server on which you have saved the image that was downloaded from the NetApp Support Site.  For anonymous FTP, you must specify the URL in the <a href="#">ftp://anonymous@ftpserver</a> format.  c. Click <b>Add</b> .
Select an available image	Choose one of the listed images.

- Click **Validate** to run the pre-update validation checks to verify whether the cluster is ready for an update.

The validation operation checks the cluster components to validate that the update can be completed nondisruptively, and then displays any errors or warnings. It also displays any required remedial action that you must perform before updating the software.



You must perform all of the required remedial actions for the errors before proceeding with the update. Although you can ignore the remedial actions for the warnings, the best practice is to perform all of the remedial actions before proceeding with the update.

7. Click **Next**.
8. Click **Update**.

Validation is performed again.

- When the validation is complete, a table displays any errors and warnings, along with any required remedial actions to be taken before proceeding.
- If the validation is completed with warnings, you can choose to select **Update with warnings**.



If you prefer to have your nodes updated one HA pair at a time instead of a batch update of all the HA pairs in your cluster, select **Update one HA pair at a time**. This option is only available in ONTAP 9.10.1 or later for clusters of eight or more nodes.

When the validation is complete and the update is in progress, the update might be paused because of errors. You can click the error message to view the details, and then perform the remedial actions before resuming the update.

After the update is completed successfully, the node reboots, and you are redirected to the System Manager login page. If the node takes a long time to reboot, you must refresh your browser.

#### Resuming an upgrade (using System Manager) after an error in the automated upgrade process

If an automated upgrade pauses because of an error, you can resolve the error and resume the automated upgrade, or you can cancel the automated upgrade and complete the process manually. If you choose to continue the automated upgrade, do not perform any of the upgrade steps manually.

1. Depending on the ONTAP version that you are running, perform one of the following steps:
  - ONTAP 9.8 or later: Click **Cluster > Overview**
  - ONTAP 9.5, 9.6, or 9.7: Click **Configuration > Cluster > Update**.
  - ONTAP 9.4 or earlier: Click **Configuration > Cluster Update**.

Then in the right corner of the Overview pane, click the three blue vertical dots, and **ONTAP Update**.

2. Continue the automated update or cancel it and continue manually.

If you want to...	Then...
Resume the automated update	Click <b>Resume</b> .
Cancel the automated update and continue manually	Click <b>Cancel</b> .

#### Video: Upgrades made easy

Take a look at the simplified ONTAP upgrade capabilities of System Manager in ONTAP 9.8.

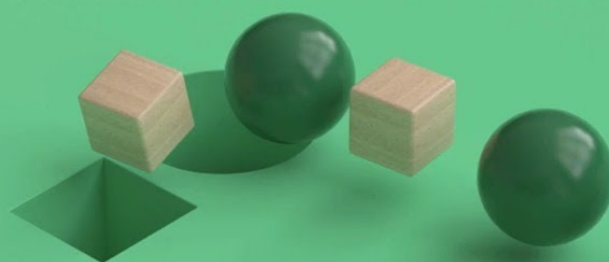
## ONTAP Upgrades Made Easy

Get the transformative features you've paid for!



### Tech Clip

© 2020 NetApp, Inc. All rights reserved.



### Automated nondisruptive ONTAP upgrade using the CLI

You can use the command line interface (CLI) to verify that the cluster can be upgraded nondisruptively, install the target ONTAP image on each node, and then execute an upgrade in the background.

After you upgrade, you should verify your cluster version, cluster health, and storage health.



If you are using a MetroCluster FC configuration, you also need to verify that the cluster is enabled for automatic unplanned switchover.

If you do not plan to monitor the progress of the upgrade process, it is a good practice to [request EMS notifications of errors that might require manual intervention](#).

### Before you begin

- You should launch Active IQ Digital Advisor.

The Upgrade Advisor component of Active IQ Digital Advisor helps you plan for a successful upgrade.

Data-driven insights and recommendations from Active IQ Digital Advisor are provided to all NetApp customers with an active **SupportEdge** contract (features vary by product and support tier).

- You must have met the upgrade preparation requirements.
- For each HA pair, each node should have one or more ports on the same broadcast domain.

When a set of nodes is upgraded during a batch upgrade, the LIFs are migrated to the HA partner nodes. If the partners do not have any ports in the same broadcast domain, then the LIF migration fails.

- If you are upgrading from ONTAP 9.3 to 9.7, you must have obtained the software image for 9.5 and 9.7.



- If you are upgrading from ONTAP 9.5 to 9.9.1, you must have obtained the software image for 9.7 and 9.9.1.

### About this task

The `cluster image validate` command checks the cluster components to validate that the upgrade can be completed nondisruptively, and then it provides the status of each check and any required action you must take before performing the software upgrade.



Modifying the setting of the `storage failover modify-auto-giveback` command option before the start of an automatic nondisruptive upgrade (ANDU) has no impact on the upgrade process. The ANDU process ignores any preset value to this option during the takeover/giveback required for the update. For example, setting `-autogiveback` to `false` prior to beginning ANDU does not interrupt the automatic upgrade before giveback.

1. Delete the previous ONTAP software package:

```
cluster image package delete -version previous_ONTAP_Version
```

2. Download the target ONTAP software package:

```
cluster image package get -url location
```



If you are upgrading from ONTAP 9.3 to 9.7, download the software package for ONTAP 9.5, and then use the same command to download the software package for 9.7. If you are upgrading from ONTAP 9.5 to 9.9.1, download the software package for ONTAP 9.7, and then use the same command to download the software package for 9.9.1.

```
cluster1::> cluster image package get -url
http://www.example.com/software/9.7/image.tgz
```

```
Package download completed.
Package processing completed.
```

3. Verify that the software package is available in the cluster package repository:

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository
```

```
Package Version  Package Build Time
-----
9.7              MM/DD/YYYY 10:32:15
```

4. Verify that the cluster is ready to be upgraded nondisruptively:

```
cluster image validate -version package_version_number
```

- If you are upgrading a two-node or four-node MetroCluster configuration, you must run this command on both clusters before proceeding.

- If you are upgrading from ONTAP 9.3 to 9.7, use the 9.7 package for verification. You do not need to validate the 9.5 package separately.
- If you are upgrading from ONTAP 9.5 to 9.9.1, use the 9.9.1 package for verification. You do not need to validate the 9.7 package separately.

```
cluster1::> cluster image validate -version 9.7
```

```
WARNING: There are additional manual upgrade validation checks that must  
be performed after these automated validation checks have completed...
```

5. Monitor the progress of the validation:

```
cluster image show-update-progress
```

6. Complete all required actions identified by the validation.

7. Generate a software upgrade estimate:

```
cluster image update -version package_version_number -estimate-only
```

The software upgrade estimate displays details about each component to be updated, and the estimated duration of the upgrade.

8. Perform the software upgrade:

```
cluster image update -version package_version_number
```

- If you are upgrading from ONTAP 9.3 to 9.7, use the 9.7 `package_version_number` in the above command.
- If you are upgrading from ONTAP 9.5 to 9.9.1, use the 9.9.1 `package_version_number` in the above command.
- For any MetroCluster configuration, except a 2-node MetroCluster system, the ONTAP upgrade process starts simultaneously on the HA pairs at both sites (the local site and the disaster recovery site) after the user initiates and provides confirmation on the command line. For a 2-node MetroCluster system, the update is started first on the disaster recovery site, that is, the site where the upgrade is not initiated. After the update is fully completed on the disaster recovery site, the upgrade begins on the local site.
- If the cluster consists of 2 to 6 nodes, a rolling upgrade is performed. If the cluster consists of 8 or more nodes, a batch upgrade is performed by default. If desired, you can use the `-force-rolling` parameter to specify a rolling upgrade instead.
- After completing each takeover and giveback, the upgrade waits for 8 minutes to enable client applications to recover from the pause in I/O that occurs during the takeover and giveback. If your environment requires more or less time for client stabilization, you can use the `-stabilize-minutes` parameter to specify a different amount of stabilization time.

```

cluster1::> cluster image update -version 9.7

Starting validation for this update. Please wait..

It can take several minutes to complete validation...

WARNING: There are additional manual upgrade validation checks...

Pre-update Check      Status      Error-Action
-----
.....
...
20 entries were displayed

Would you like to proceed with update ? {y|n}: y
Starting update...

cluster-1::>

```

9. Display the cluster update progress:

```
cluster image show-update-progress
```



If you are upgrading a 4-node or 8-node MetroCluster configuration, the `cluster image show-update-progress` command only displays the progress for the node on which you run the command. You must run the command on each node to see individual node progress.

10. Verify that the upgrade was completed successfully on each node.

```

cluster1::> cluster image show-update-progress

Update Phase      Status      Estimated      Elapsed
-----
Pre-update checks  completed   00:10:00      00:02:07
Data ONTAP updates completed   01:31:00      01:39:00
Post-update checks completed   00:10:00      00:02:00
3 entries were displayed.

Updated nodes: node0, node1.

cluster1::>

```

11. Trigger an AutoSupport notification:

```
autosupport invoke -node * -type all -message "Finishing_NDU"
```

If your cluster is not configured to send AutoSupport messages, a copy of the notification is saved locally.

12. Verify that the cluster is enabled for automatic unplanned switchover:



This procedure is performed only for MetroCluster FC configurations. If you are using a MetroCluster IP configuration, skip this procedure.

a. Check whether automatic unplanned switchover is enabled:

```
metrocluster show
```

If automatic unplanned switchover is enabled, the following statement appears in the command output:

```
AUSO Failure Domain      auso-on-cluster-disaster
```

b. If the statement does not appear in the output, enable automatic unplanned switchover:

```
metrocluster modify -auto-switchover-failure-domain auso-on-cluster-disaster
```

c. Verify that automatic unplanned switchover has been enabled by repeating Step 1.

### Resuming an upgrade (using the CLI) after an error in the automated upgrade process

If an automated upgrade pauses because of an error, you can resolve the error and resume the automated upgrade, or you can cancel the automated upgrade and complete the process manually. If you choose to continue the automated upgrade, do not perform any of the upgrade steps manually.

#### About this task

If you want to manually complete the upgrade, use the `cluster image cancel-update` command to cancel the automated process and proceed manually. If you want to continue the automated upgrade, complete the following steps.

#### Steps

1. View the upgrade error:

```
cluster image show-update-progress
```

2. Resolve the error.

3. Resume the update:

```
cluster image resume-update
```

#### Related information

[Launch Active IQ](#)

[Active IQ documentation](#)

## Automated disruptive using the CLI (single-node cluster only)

Beginning with ONTAP 9.2, you can perform an automated update of a single-node cluster. Because single-node clusters lack redundancy, updates are always disruptive.

- You must have satisfied upgrade preparation requirements.

1. Delete the previous ONTAP software package: `cluster image package delete -version previous_package_version`
2. Download the target ONTAP software package: `cluster image package get -url location`

```
cluster1::> cluster image package get -url
http://www.example.com/software/9.7/image.tgz
```

```
Package download completed.
Package processing completed.
```

3. Verify that the software package is available in the cluster package repository: `cluster image package show-repository`

```
cluster1::> cluster image package show-repository
Package Version  Package Build Time
-----
9.7              M/DD/YYYY 10:32:15
```

4. Verify that the cluster is ready to be upgraded: `cluster image validate -version package_version_number`

```
cluster1::> cluster image validate -version 9.7
```

```
WARNING: There are additional manual upgrade validation checks that
must be performed after these automated validation checks have
completed...
```

5. Monitor the progress of the validation: `cluster image show-update-progress`
6. Complete all required actions identified by the validation.
7. Optionally, generate a software upgrade estimate: `cluster image update -version package_version_number -estimate-only`

The software upgrade estimate displays details about each component to be updated, and the estimated duration of the upgrade.

8. Perform the software upgrade: `cluster image update -version package_version_number`



If an issue is encountered, the update pauses and prompts you to take corrective action. You can use the `cluster image show-update-progress` command to view details about any issues and the progress of the update. After correcting the issue, you can resume the update by using the `cluster image resume-update` command.

9. Display the cluster update progress: `cluster image show-update-progress`

The node is rebooted as part of the update and cannot be accessed while rebooting.

10. Trigger a notification: `autosupport invoke -node * -type all -message "Finishing_Upgrade"`

If your cluster is not configured to send messages, a copy of the notification is saved locally.

## Manual nondisruptive using the CLI

### Manual nondisruptive upgrade using the CLI (non-MetroCluster systems)

To upgrade a cluster of two or more nodes using the manual nondisruptive method, you must initiate a failover operation on each node in an HA pair, update the “failed” node, initiate giveback, and then repeat the process for each HA pair in the cluster.

You must have satisfied upgrade preparation requirements.

1. Update the first node in an HA pair

You upgrade the first node in an HA pair by initiating a takeover by the node’s partner. The partner serves the node’s data while the first node is upgraded.

2. Update the second node in an HA pair

After upgrading or downgrading the first node in an HA pair, you upgrade its partner by initiating a takeover on it. The first node serves the partner’s data while the partner node is upgraded.

3. Repeat these steps for each additional HA pair.

You should complete post-upgrade tasks.

### Updating the first node in an HA pair

You can update the first node in an HA pair by initiating a takeover by the node’s partner. The partner serves the node’s data while the first node is upgraded.

If you are performing a major upgrade, the first node to be upgraded must be the same node on which you configured the data LIFs for external connectivity and installed the first ONTAP image.

After upgrading the first node, you should upgrade the partner node as quickly as possible. Do not allow the two nodes to remain in a state of version mismatch longer than necessary.

1. Update the first node in the cluster by invoking an AutoSupport message: `autosupport invoke -node * -type all -message "Starting_NDU"`

This AutoSupport notification includes a record of the system status just prior to update. It saves useful

troubleshooting information in case there is a problem with the update process.

If the cluster is not configured to send AutoSupport messages, a copy of the notification is saved locally.

2. Set the privilege level to advanced, entering **y** when prompted to continue: `set -privilege advanced`

The advanced prompt (`*>`) appears.

3. Set the new ONTAP software image to be the default image: `system image modify {-node nodenameA -iscurrent false} -isdefault true`

The `system image modify` command uses an extended query to change the new ONTAP software image (which is installed as the alternate image) to the default image for the node.

4. Monitor the progress of the update: `system node upgrade-revert show`
5. Verify that the new ONTAP software image is set as the default image: `system image show`

In the following example, `image2` is the new ONTAP version and is set as the default image on `node0`:

```
cluster1::*> system image show
Node      Image      Is      Is      Install
          Image    Default Current Version Date
-----
node0
  image1  false    true    X.X.X   MM/DD/YYYY TIME
  image2  true     false   Y.Y.Y   MM/DD/YYYY TIME
node1
  image1  true     true    X.X.X   MM/DD/YYYY TIME
  image2  false   false   Y.Y.Y   MM/DD/YYYY TIME
4 entries were displayed.
```

6. Disable automatic giveback on the partner node if it is enabled: `storage failover modify -node nodenameB -auto-giveback false`

If the cluster is a two-node cluster, a message is displayed warning you that disabling automatic giveback prevents the management cluster services from going online in the event of an alternating-failure scenario. Enter **y** to continue.

7. Verify that automatic giveback is disabled for node's partner: `storage failover show -node nodenameB -fields auto-giveback`

```
cluster1::> storage failover show -node node1 -fields auto-giveback
node      auto-giveback
-----
node1     false
1 entry was displayed.
```

- Run the following command twice to determine whether the node to be updated is currently serving any clients  
`system node run -node nodenameA -command uptime`

The uptime command displays the total number of operations that the node has performed for NFS, SMB, FC, and iSCSI clients since the node was last booted. For each protocol, you must run the command twice to determine whether the operation counts are increasing. If they are increasing, the node is currently serving clients for that protocol. If they are not increasing, the node is not currently serving clients for that protocol.

**NOTE:** You should make a note of each protocol that has increasing client operations so that after the node is updated, you can verify that client traffic has resumed.

The following example shows a node with NFS, SMB, FC, and iSCSI operations. However, the node is currently serving only NFS and iSCSI clients.

```
cluster1::> system node run -node node0 -command uptime
  2:58pm up 7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster1::> system node run -node node0 -command uptime
  2:58pm up 7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

- Migrate all of the data LIFs away from the node:  
`network interface migrate-all -node nodenameA`
- Verify any LIFs that you migrated:  
`network interface show`

For more information about parameters you can use to verify LIF status, see the `network interface show man` page.

The following example shows that node0's data LIFs migrated successfully. For each LIF, the fields included in this example enable you to verify the LIF's home node and port, the current node and port to which the LIF migrated, and the LIF's operational and administrative status.

```
cluster1::> network interface show -data-protocol nfs|cifs -role data
-home-node node0 -fields home-node,curr-node,curr-port,home-port,status-
admin,status-oper
vserver lif      home-node home-port curr-node curr-port status-oper
status-admin
-----
vs0      data001 node0      e0a      node1    e0a      up        up
vs0      data002 node0      e0b      node1    e0b      up        up
vs0      data003 node0      e0b      node1    e0b      up        up
vs0      data004 node0      e0a      node1    e0a      up        up
4 entries were displayed.
```



11. Initiate a takeover: `storage failover takeover -ofnode nodenameA`

Do not specify the `-option immediate` parameter, because a normal takeover is required for the node that is being taken over to boot onto the new software image. If you did not manually migrate the LIFs away from the node, they automatically migrate to the node's HA partner to ensure that there are no service disruptions.

The first node boots up to the Waiting for giveback state.

**NOTE:** If AutoSupport is enabled, an AutoSupport message is sent indicating that the node is out of cluster quorum. You can ignore this notification and proceed with the update.

12. Verify that the takeover is successful: `storage failover show`

You might see error messages indicating version mismatch and mailbox format problems. This is expected behavior and it represents a temporary state in a major nondisruptive upgrade and is not harmful.

The following example shows that the takeover was successful. Node `node0` is in the Waiting for giveback state, and its partner is in the In takeover state.

```
cluster1::> storage failover show
Node           Partner           Takeover
-----
-----
node0          node1             -           Waiting for giveback (HA
mailboxes)
node1          node0             false      In takeover
2 entries were displayed.
```

13. Wait at least eight minutes for the following conditions to take effect:

- Client multipathing (if deployed) is stabilized.
- Clients are recovered from the pause in an I/O operation that occurs during takeover.

The recovery time is client specific and might take longer than eight minutes, depending on the characteristics of the client applications.

14. Return the aggregates to the first node: `storage failover giveback -ofnode nodenameA`

The giveback first returns the root aggregate to the partner node and then, after that node has finished booting, returns the non-root aggregates and any LIFs that were set to automatically revert. The newly booted node begins to serve data to clients from each aggregate as soon as the aggregate is returned.

15. Verify that all aggregates have been returned: `storage failover show-giveback`

If the Giveback Status field indicates that there are no aggregates to give back, then all aggregates have been returned. If the giveback is vetoed, the command displays the giveback progress and which subsystem vetoed the giveback.

16. If any aggregates have not been returned, perform the following steps:

- a. Review the veto workaround to determine whether you want to address the “veto” condition or override the veto.

#### High-availability configuration

- b. If necessary, address the “veto” condition described in the error message, ensuring that any identified operations are terminated gracefully.
- c. Rerun the storage failover giveback command.

If you decided to override the “veto” condition, set the `-override-vetoes` parameter to true.

17. Wait at least eight minutes for the following conditions to take effect:

- Client multipathing (if deployed) is stabilized.
- Clients are recovered from the pause in an I/O operation that occurs during giveback.

The recovery time is client specific and might take longer than eight minutes, depending on the characteristics of the client applications.

18. Verify that the update was completed successfully for the node:

- a. Go to the advanced privilege level: `set -privilege advanced`
- b. Verify that update status is complete for the node: `system node upgrade-revert show -node nodenameA`

The status should be listed as complete.

If the status is not complete, contact technical support.

- c. Return to the admin privilege level: `set -privilege admin`

19. Verify that the node’s ports are up: `network port show -node nodenameA`

You must run this command on a node that is upgraded to the higher version of ONTAP 9.

The following example shows that all of the node’s ports are up:

```
cluster1::> network port show -node node0
```

							Speed
(Mbps)							
Node	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper	
-----							
node0							
	e0M	Default	-	up	1500	auto/100	
	e0a	Default	-	up	1500	auto/1000	
	e0b	Default	-	up	1500	auto/1000	
	e1a	Cluster	Cluster	up	9000	auto/10000	
	e1b	Cluster	Cluster	up	9000	auto/10000	

5 entries were displayed.

20. Revert the LIFs back to the node: `network interface revert *`

This command returns the LIFs that were migrated away from the node.

```
cluster1::> network interface revert *
8 entries were acted on.
```

21. Verify that the node's data LIFs successfully reverted back to the node, and that they are up: `network interface show`

The following example shows that all of the data LIFs hosted by the node have successfully reverted back to the node, and that their operational status is up:

```
cluster1::> network interface show
Current Is
Vserver   Logical   Status    Network    Current
Home      Interface Admin/Oper Address/Mask Node        Port
-----
vs0
true      data001   up/up     192.0.2.120/24 node0       e0a
true      data002   up/up     192.0.2.121/24 node0       e0b
true      data003   up/up     192.0.2.122/24 node0       e0b
true      data004   up/up     192.0.2.123/24 node0       e0a
4 entries were displayed.
```

22. If you previously determined that this node serves clients, verify that the node is providing service for each protocol that it was previously serving: `system node run -node nodenameA -command uptime`

The operation counts reset to zero during the update.

The following example shows that the updated node has resumed serving its NFS and iSCSI clients:

```
cluster1::> system node run -node node0 -command uptime
3:15pm up 0 days, 0:16 129 NFS ops, 0 CIFS ops, 0 HTTP ops, 0 FCP
ops, 2 iSCSI ops
```

23. Reenable automatic giveback on the partner node if it was previously disabled: `storage failover modify -node nodenameB -auto-giveback true`

You should proceed to update the node's HA partner as quickly as possible. If you must suspend the update process for any reason, both nodes in the HA pair should be running the same ONTAP version.

### Updating the partner node in an HA pair

After updating the first node in an HA pair, you update its partner by initiating a takeover on it. The first node serves the partner's data while the partner node is upgraded.

1. Set the privilege level to advanced, entering **y** when prompted to continue: `set -privilege advanced`

The advanced prompt (**\*>**) appears.

2. Set the new ONTAP software image to be the default image: `system image modify {-node nodenameB -iscurrent false} -isdefault true`

The `system image modify` command uses an extended query to change the new ONTAP software image (which is installed as the alternate image) to be the default image for the node.

3. Monitor the progress of the update: `system node upgrade-revert show`
4. Verify that the new ONTAP software image is set as the default image: `system image show`

In the following example, `image2` is the new version of ONTAP and is set as the default image on the node:

```
cluster1::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date
node0					
	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME
node1					
	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

5. Disable automatic giveback on the partner node if it is enabled: `storage failover modify -node nodenameA -auto-giveback false`

If the cluster is a two-node cluster, a message is displayed warning you that disabling automatic giveback prevents the management cluster services from going online in the event of an alternating-failure scenario. Enter **y** to continue.

6. Verify that automatic giveback is disabled for the partner node: `storage failover show -node nodenameA -fields auto-giveback`

```
cluster1::> storage failover show -node node0 -fields auto-giveback
node      auto-giveback
-----  -
node0     false
1 entry was displayed.
```

7. Run the following command twice to determine whether the node to be updated is currently serving any clients: `system node run -node nodenameB -command uptime`

The `uptime` command displays the total number of operations that the node has performed for NFS, SMB, FC, and iSCSI clients since the node was last booted. For each protocol, you must run the command twice to determine whether the operation counts are increasing. If they are increasing, the node is currently serving clients for that protocol. If they are not increasing, the node is not currently serving clients for that protocol.

**NOTE:** You should make a note of each protocol that has increasing client operations so that after the node is updated, you can verify that client traffic has resumed.

The following example shows a node with NFS, SMB, FC, and iSCSI operations. However, the node is currently serving only NFS and iSCSI clients.

```
cluster1::> system node run -node node1 -command uptime
 2:58pm up 7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster1::> system node run -node node1 -command uptime
 2:58pm up 7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

8. Migrate all of the data LIFs away from the node: `network interface migrate-all -node nodenameB`
9. Verify the status of any LIFs that you migrated: `network interface show`

For more information about parameters you can use to verify LIF status, see the `network interface show man` page.

The following example shows that `node1`'s data LIFs migrated successfully. For each LIF, the fields included in this example enable you to verify the LIF's home node and port, the current node and port to which the LIF migrated, and the LIF's operational and administrative status.

```

cluster1::> network interface show -data-protocol nfs|cifs -role data
-home-node node1 -fields home-node,curr-node,curr-port,home-port,status-
admin,status-oper
vserver lif      home-node home-port curr-node curr-port status-oper
status-admin
-----
-----
vs0      data001 node1      e0a      node0    e0a      up       up
vs0      data002 node1      e0b      node0    e0b      up       up
vs0      data003 node1      e0b      node0    e0b      up       up
vs0      data004 node1      e0a      node0    e0a      up       up
4 entries were displayed.

```

- Initiate a takeover: `storage failover takeover -ofnode nodenameB -option allow-version-mismatch`

Do not specify the `-option immediate` parameter, because a normal takeover is required for the node that is being taken over to boot onto the new software image. If you did not manually migrate the LIFs away from the node, they automatically migrate to the node's HA partner so that there are no service disruptions.

The node that is taken over boots up to the Waiting for giveback state.

**NOTE:** If AutoSupport is enabled, an AutoSupport message is sent indicating that the node is out of cluster quorum. You can ignore this notification and proceed with the update.

- Verify that the takeover was successful: `storage failover show`

The following example shows that the takeover was successful. Node node1 is in the Waiting for giveback state, and its partner is in the In takeover state.

```

cluster1::> storage failover show
Node          Partner          Takeover
Possible State Description
-----
-----
node0         node1             -           In takeover
node1         node0             false      Waiting for giveback (HA
mailboxes)
2 entries were displayed.

```

- Wait at least eight minutes for the following conditions to take effect:
  - Client multipathing (if deployed) is stabilized.
  - Clients are recovered from the pause in I/O that occurs during takeover.

The recovery time is client-specific and might take longer than eight minutes, depending on the characteristics of the client applications.

13. Return the aggregates to the partner node: `storage failover giveback -ofnode nodenameB`

The giveback operation first returns the root aggregate to the partner node and then, after that node has finished booting, returns the non-root aggregates and any LIFs that were set to automatically revert. The newly booted node begins to serve data to clients from each aggregate as soon as the aggregate is returned.

14. Verify that all aggregates are returned: `storage failover show-giveback`

If the Giveback Status field indicates that there are no aggregates to give back, then all aggregates are returned. If the giveback is vetoed, the command displays the giveback progress and which subsystem vetoed the giveback operation.

15. If any aggregates are not returned, perform the following steps:
  - a. Review the veto workaround to determine whether you want to address the “veto” condition or override the veto.

#### [High-availability configuration](#)

- b. If necessary, address the “veto” condition described in the error message, ensuring that any identified operations are terminated gracefully.
  - c. Rerun the storage failover giveback command.

If you decided to override the “veto” condition, set the `-override-vetoes` parameter to true.

16. Wait at least eight minutes for the following conditions to take effect:

- Client multipathing (if deployed) is stabilized.
- Clients are recovered from the pause in an I/O operation that occurs during giveback.

The recovery time is client specific and might take longer than eight minutes, depending on the characteristics of the client applications.

17. Verify that the update was completed successfully for the node:

- a. Go to the advanced privilege level: `set -privilege advanced`
- b. Verify that update status is complete for the node: `system node upgrade-revert show -node nodenameB`

The status should be listed as complete.

If the status is not complete, from the node, run the `system node upgrade-revert upgrade` command. If the command does not complete the update, contact technical support.

- c. Return to the admin privilege level: `set -privilege admin`

18. Verify that the node’s ports are up: `network port show -node nodenameB`

You must run this command on a node that has been upgraded to ONTAP 9.4.

The following example shows that all of the node’s data ports are up:

```
cluster1::> network port show -node node1
```

(Mbps)							Speed
Node	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper	
-----							
node1							
	e0M	Default	-	up	1500	auto/100	
	e0a	Default	-	up	1500	auto/1000	
	e0b	Default	-	up	1500	auto/1000	
	e1a	Cluster	Cluster	up	9000	auto/10000	
	e1b	Cluster	Cluster	up	9000	auto/10000	

5 entries were displayed.

19. Revert the LIFs back to the node: `network interface revert *`

This command returns the LIFs that were migrated away from the node.

```
cluster1::> network interface revert *
8 entries were acted on.
```

20. Verify that the node's data LIFs successfully reverted back to the node, and that they are up: `network interface show`

The following example shows that all of the data LIFs hosted by the node is successfully reverted back to the node, and that their operational status is up:

```
cluster1::> network interface show
```

Current Is	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Port
-----					
vs0					
true	data001	up/up	192.0.2.120/24	node1	e0a
true	data002	up/up	192.0.2.121/24	node1	e0b
true	data003	up/up	192.0.2.122/24	node1	e0b
true	data004	up/up	192.0.2.123/24	node1	e0a

4 entries were displayed.



21. If you previously determined that this node serves clients, verify that the node is providing service for each protocol that it was previously serving: `system node run -node nodenameB -command uptime`

The operation counts reset to zero during the update.

The following example shows that the updated node has resumed serving its NFS and iSCSI clients:

```
cluster1::> system node run -node node1 -command uptime
  3:15pm up  0 days, 0:16 129 NFS ops, 0 CIFS ops, 0 HTTP ops, 0 FCP
ops, 2 iSCSI ops
```

22. If this was the last node in the cluster to be updated, trigger an AutoSupport notification: `autosupport invoke -node * -type all -message "Finishing_NDU"`

This AutoSupport notification includes a record of the system status just prior to update. It saves useful troubleshooting information in case there is a problem with the update process.

If the cluster is not configured to send AutoSupport messages, a copy of the notification is saved locally.

23. Confirm that the new ONTAP software is running on both nodes of the HA pair: `system node image show`

In the following example, image2 is the updated version of ONTAP and is the default version on both nodes:

```
cluster1::*> system node image show
Node      Image      Is Default  Is Current  Version  Install Date
-----
node0
  image1  false     false    X.X.X    MM/DD/YYYY TIME
  image2  true      true     Y.Y.Y    MM/DD/YYYY TIME
node1
  image1  false     false    X.X.X    MM/DD/YYYY TIME
  image2  true      true     Y.Y.Y    MM/DD/YYYY TIME
4 entries were displayed.
```

24. Reenable automatic giveback on the partner node if it was previously disabled: `storage failover modify -node nodenameA -auto-giveback true`
25. Verify that the cluster is in quorum and that services are running by using the `cluster show` and `cluster ring show` (advanced privilege level) commands.

You must perform this step before upgrading any additional HA pairs.

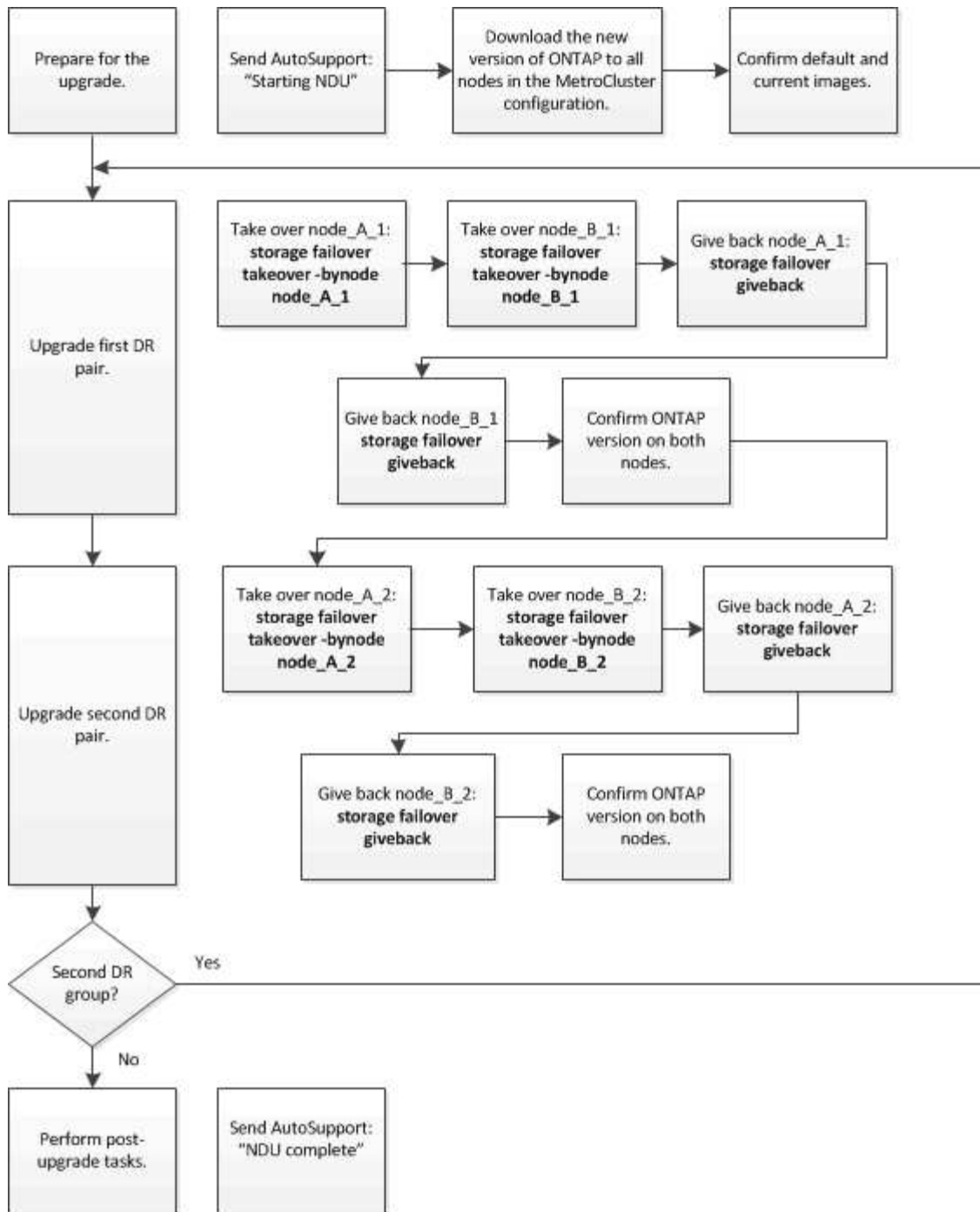
26. Return to the admin privilege level: `set -privilege admin`

Upgrade any additional HA pairs.

### Manual nondisruptive upgrade of a four- or eight-node MetroCluster configuration using the CLI

The manual update procedure for upgrading or downgrading a four- or eight-node MetroCluster configuration involves preparing for the update, updating the DR pairs in each of the one or two DR groups simultaneously, and performing some post-update tasks.

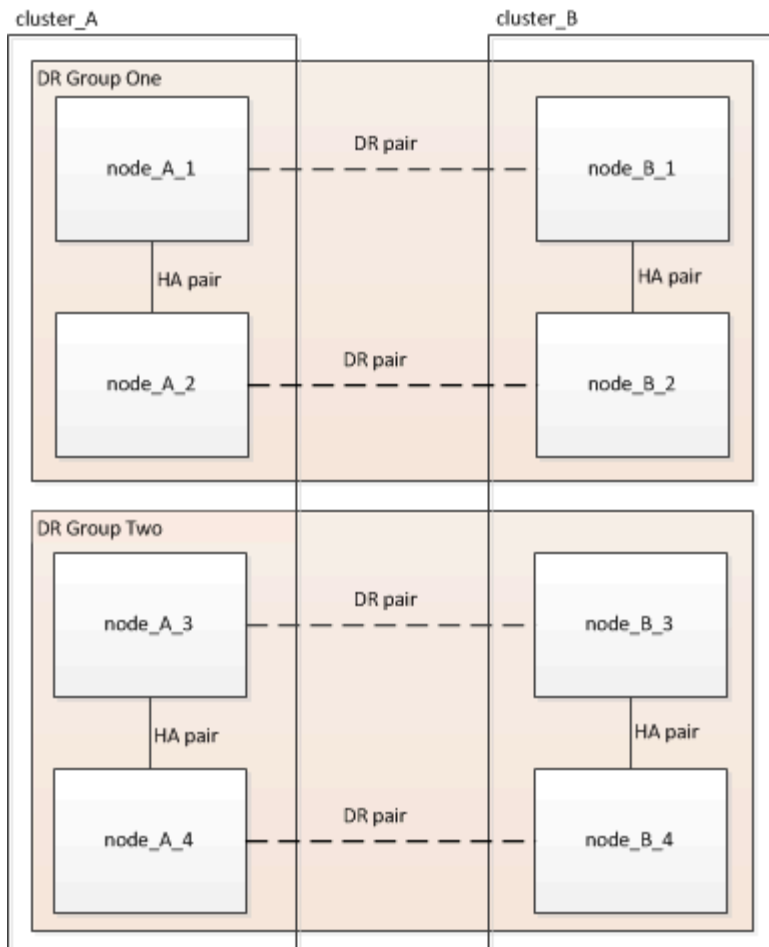
- This task applies to the following configurations:
  - Four-node MetroCluster FC or IP configurations running ONTAP 9.2 or earlier
  - Eight-node MetroCluster FC configurations, regardless of ONTAP version
- If you have a two-node MetroCluster configuration, do not use this procedure.
- The following tasks refer to the old and new versions of ONTAP.
  - When upgrading, the old version is a previous version of ONTAP, with a lower version number than the new version of ONTAP.
  - When downgrading, the old version is a later version of ONTAP, with a higher version number than the new version of ONTAP.
- This task uses the following high-level workflow:



### Differences when updating software on an eight-node or four-node MetroCluster configuration

The MetroCluster software update process differs, depending on whether there are eight or four nodes in the MetroCluster configuration.

A MetroCluster DR configuration consists of one or two DR groups. Each DR group consists of two HA pairs, one HA pair at each MetroCluster cluster. An eight-node MetroCluster includes two DR groups:



The MetroCluster software update procedure involves upgrading or downgrading one DR group at a time.

For four-node MetroCluster configurations:

1. Update DR Group One:
  - a. Update node\_A\_1 and node\_B\_1.
  - b. Update node\_A\_2 and node\_B\_2.

For eight-node MetroCluster configurations, you perform the DR group update procedure twice:

1. Update DR Group One:
  - a. Update node\_A\_1 and node\_B\_1.
  - b. Update node\_A\_2 and node\_B\_2.
2. Update DR Group Two:
  - a. Update node\_A\_3 and node\_B\_3.
  - b. Update node\_A\_4 and node\_B\_4.

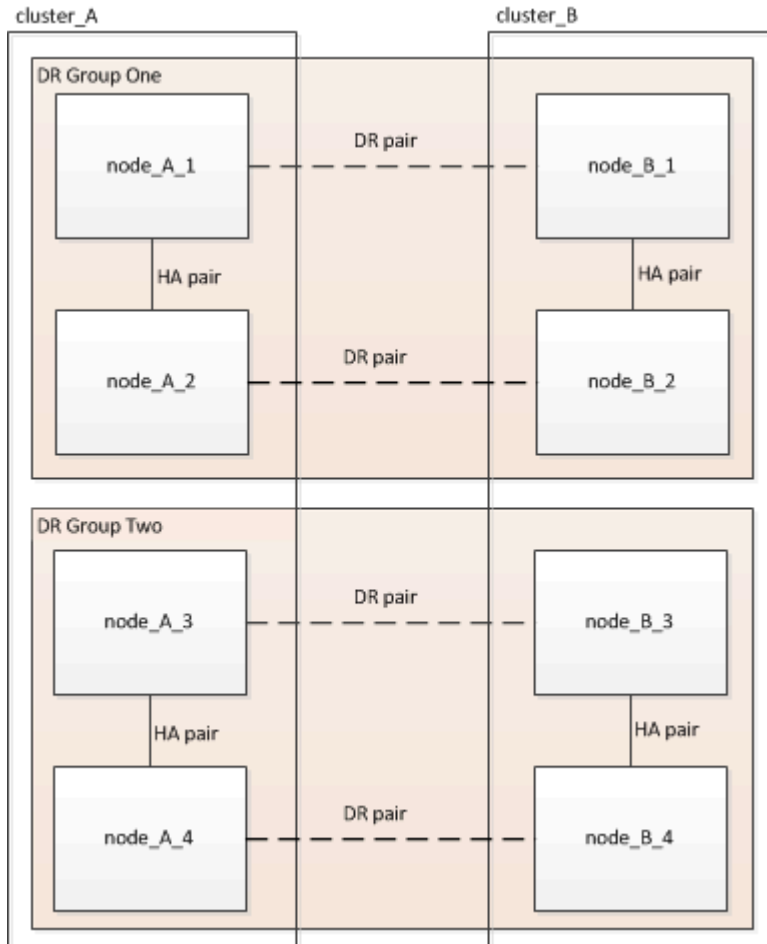
### Preparing to update a MetroCluster DR group

Before you actually update the software on the nodes, you must identify the DR relationships among the nodes, send an AutoSupport message that you are initiating an update, and confirm the ONTAP version running on each node.

You must have [downloaded and installed the software images](#).

This task must be repeated on each DR group. If the MetroCluster configuration consists of eight nodes, there are two DR groups. Thereby, this task must be repeated on each DR group.

The examples provided in this task use the names shown in the following illustration to identify the clusters and nodes:



1. Identify the DR pairs in the configuration: `metrocluster node show -fields dr-partner`

```
cluster_A::> metrocluster node show -fields dr-partner
(metrocluster node show)
dr-group-id cluster      node          dr-partner
-----
1           cluster_A    node_A_1     node_B_1
1           cluster_A    node_A_2     node_B_2
1           cluster_B    node_B_1     node_A_1
1           cluster_B    node_B_2     node_A_2
4 entries were displayed.

cluster_A::>
```

2. Set the privilege level from admin to advanced, entering **y** when prompted to continue: `set -privilege advanced`

The advanced prompt (**\*>**) appears.

3. Confirm the ONTAP version running on each node:

- a. Confirm the version on cluster\_A: `system image show`

```
cluster_A::*> system image show
           Is      Is      Install
Node      Image   Default Current Version  Date
-----
node_A_1
  image1  true    true   X.X.X   MM/DD/YYYY TIME
  image2  false   false  Y.Y.Y   MM/DD/YYYY TIME
node_A_2
  image1  true    true   X.X.X   MM/DD/YYYY TIME
  image2  false   false  Y.Y.Y   MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

- b. Confirm the version on cluster\_B: `system image show`

```
cluster_B::*> system image show
           Is      Is      Install
Node      Image   Default Current Version  Date
-----
node_B_1
  image1  true    true   X.X.X   MM/DD/YYYY TIME
  image2  false   false  Y.Y.Y   MM/DD/YYYY TIME
node_B_2
  image1  true    true   X.X.X   MM/DD/YYYY TIME
  image2  false   false  Y.Y.Y   MM/DD/YYYY TIME
4 entries were displayed.

cluster_B::>
```

4. Trigger an AutoSupport notification: `autosupport invoke -node * -type all -message "Starting_NDU"`

This AutoSupport notification includes a record of the system status before the update. It saves useful troubleshooting information if there is a problem with the update process.

If your cluster is not configured to send AutoSupport messages, then a copy of the notification is saved locally.

5. For each node in the first set, set the target ONTAP software image to be the default image: `system image modify {-node nodename -iscurrent false} -isdefault true`

This command uses an extended query to change the target software image, which is installed as the alternate image, to be the default image for the node.

6. Verify that the target ONTAP software image is set as the default image:

- a. Verify the images on cluster\_A: `system image show`

In the following example, image2 is the new ONTAP version and is set as the default image on each of the nodes in the first set:

```
cluster_A::*> system image show
      Is      Is      Install
Node   Image   Default Current Version Date
-----
node_A_1
      image1  false   true    X.X.X   MM/DD/YYYY TIME
      image2  true    false   Y.Y.Y   MM/DD/YYYY TIME
node_A_2
      image1  false   true    X.X.X   MM/DD/YYYY TIME
      image2  true    false   Y.Y.Y   MM/DD/YYYY TIME

2 entries were displayed.
```

- b. Verify the images on cluster\_B: `system image show`

The following example shows that the target version is set as the default image on each of the nodes in the first set:

```
cluster_B::*> system image show
      Is      Is      Install
Node   Image   Default Current Version Date
-----
node_A_1
      image1  false   true    X.X.X   MM/DD/YYYY TIME
      image2  true    false   Y.Y.Y   MM/YY/YYYY TIME
node_A_2
      image1  false   true    X.X.X   MM/DD/YYYY TIME
      image2  true    false   Y.Y.Y   MM/DD/YYYY TIME

2 entries were displayed.
```

7. Determine whether the nodes to be upgraded are currently serving any clients twice for each node: `system node run -node target-node -command uptime`

The uptime command displays the total number of operations that the node has performed for NFS, CIFS, FC, and iSCSI clients since the node was last booted. For each protocol, you need to run the command twice to determine whether the operation counts are increasing. If they are increasing, the node is currently serving clients for that protocol. If they are not increasing, the node is not currently serving clients for that protocol.

**NOTE:** You should make a note of each protocol that has increasing client operations so that after the node is upgraded, you can verify that client traffic has resumed.

This example shows a node with NFS, CIFS, FC, and iSCSI operations. However, the node is currently serving only NFS and iSCSI clients.

```
cluster_x::> system node run -node node0 -command uptime
  2:58pm up 7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster_x::> system node run -node node0 -command uptime
  2:58pm up 7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

### Updating the first DR pair in a MetroCluster DR group

You must perform a takeover and giveback of the nodes in the correct order to make the new version of ONTAP the current version of the node.

All nodes must be running the old version of ONTAP.

In this task, node\_A\_1 and node\_B\_1 are updated.

If you have updated the ONTAP software on the first DR group, and are now updating the second DR group in an eight-node MetroCluster configuration, in this task you would be updating node\_A\_3 and node\_B\_3.

1. If MetroCluster Tiebreaker software is enabled, disabled it.
2. For each node in the HA pair, disable automatic giveback: `storage failover modify -node target-node -auto-giveback false`

This command must be repeated for each node in the HA pair.

3. Verify that automatic giveback is disabled: `storage failover show -fields auto-giveback`

This example shows that automatic giveback has been disabled on both nodes:

```
cluster_x::> storage failover show -fields auto-giveback
node      auto-giveback
-----  -
node_x_1  false
node_x_2  false
2 entries were displayed.
```



4. Ensure that I/O is not exceeding ~50% for each controller. Ensure that CPU utilization is not exceeding ~50% per controller.
5. Initiate a takeover of the target node on cluster\_A:

Do not specify the `-option immediate` parameter, because a normal takeover is required for the nodes that are being taken over to boot onto the new software image.

- a. Take over the DR partner on cluster\_A (node\_A\_1): `storage failover takeover -ofnode node_A_1`

The node boots up to the "Waiting for giveback" state.



If AutoSupport is enabled, then an AutoSupport message is sent indicating that the nodes are out of cluster quorum. You can ignore this notification and proceed with the upgrade.

- b. Verify that the takeover is successful: `storage failover show`

The following example shows that the takeover is successful. Node\_A\_1 is in the "Waiting for giveback" state and node\_A\_2 is in the "In takeover" state.

```
cluster1::> storage failover show
Node           Partner           Takeover
-----
node_A_1       node_A_2          -           Waiting for giveback (HA
mailboxes)
node_A_2       node_A_1          false       In takeover
2 entries were displayed.
```

6. Take over the DR partner on cluster\_B (node\_B\_1):

Do not specify the `-option immediate` parameter, because a normal takeover is required for the nodes that are being taken over to boot onto the new software image.

- a. Take over node\_B\_1: `storage failover takeover -ofnode node_B_1`

The node boots up to the "Waiting for giveback" state.



If AutoSupport is enabled, then an AutoSupport message is sent indicating that the nodes are out of cluster quorum. You can ignore this notification and proceed with the upgrade.

- b. Verify that the takeover is successful: `storage failover show`

The following example shows that the takeover is successful. Node\_B\_1 is in the "Waiting for giveback" state and node\_B\_2 is in the "In takeover" state.

```

cluster1::> storage failover show
                                Takeover
Node           Partner           Possible State Description
-----
node_B_1      node_B_2           -      Waiting for giveback (HA
mailboxes)
node_B_2      node_B_1           false  In takeover
2 entries were displayed.

```

7. Wait at least eight minutes to ensure the following conditions:

- Client multipathing (if deployed) is stabilized.
- Clients are recovered from the pause in I/O that occurs during takeover.

The recovery time is client-specific and might take longer than eight minutes depending on the characteristics of the client applications.

8. Return the aggregates to the target nodes:

After upgrading MetroCluster IP configurations to ONTAP 9.5 or later, the aggregates will be in a degraded state for a short period before resynchronizing and returning to a mirrored state.

- a. Give back the aggregates to the DR partner on cluster\_A: `storage failover giveback -ofnode node_A_1`
- b. Give back the aggregates to the DR partner on cluster\_B: `storage failover giveback -ofnode node_B_1`

The giveback operation first returns the root aggregate to the node and then, after the node has finished booting, returns the non-root aggregates.

9. Verify that all aggregates have been returned by issuing the following command on both clusters: `storage failover show-giveback`

If the Giveback Status field indicates that there are no aggregates to give back, then all aggregates have been returned. If the giveback is vetoed, the command displays the giveback progress and which subsystem vetoed the giveback.

10. If any aggregates have not been returned, do the following:

- a. Review the veto workaround to determine whether you want to address the “veto” condition or override the veto.
- b. If necessary, address the “veto” condition described in the error message, ensuring that any identified operations are terminated gracefully.
- c. Reenter the storage failover giveback command.

If you decided to override the “veto” condition, set the `-override-vetoes` parameter to true.

11. Wait at least eight minutes to ensure the following conditions:

- Client multipathing (if deployed) is stabilized.

- Clients are recovered from the pause in I/O that occurs during giveback.

The recovery time is client-specific and might take longer than eight minutes depending on the characteristics of the client applications.

12. Set the privilege level from admin to advanced, entering **y** when prompted to continue: `set -privilege advanced`

The advanced prompt (**\*>**) appears.

13. Confirm the version on cluster\_A: `system image show`

The following example shows that System image2 should be the default and current version on node\_A\_1:

```
cluster_A::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date
node_A_1					
	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME
node_A_2					
	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

```
cluster_A::>
```

14. Confirm the version on cluster\_B: `system image show`

The following example shows that System image2 (ONTAP 9.0.0) is the default and current version on node\_A\_1:

```
cluster_A::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date
node_B_1					
	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME
node_B_2					
	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

```
cluster_A::>
```

## Updating the second DR pair in a MetroCluster DR group

You must perform a takeover and giveback of the node in the correct order to make the new version of ONTAP the current version of the node.

You should have upgraded the first DR pair (node\_A\_1 and node\_B\_1).

In this task, node\_A\_2 and node\_B\_2 are updated.

If you have updated the ONTAP software on the first DR group, and are now updating the second DR group in an eight-node MetroCluster configuration, in this task you are updating node\_A\_4 and node\_B\_4.

### 1. Initiate a takeover of the target node on cluster\_A:

Do not specify the `-option immediate` parameter, because a normal takeover is required for the nodes that are being taken over to boot onto the new software image.

#### a. Take over the DR partner on cluster\_A:

```
storage failover takeover -ofnode node_A_2 -option allow-version-mismatch
```



The `allow-version-mismatch` option is not required for upgrades from ONTAP 9.0 to ONTAP 9.1 or for any patch upgrades.

The node boots up to the "Waiting for giveback" state.

If AutoSupport is enabled, then an AutoSupport message is sent indicating that the nodes are out of cluster quorum. You can ignore this notification and proceed with the upgrade.

#### b. Verify that the takeover is successful: `storage failover show`

The following example shows that the takeover is successful. Node\_A\_2 is in the "Waiting for giveback" state and node\_A\_1 is in the "In takeover" state.

```
cluster1::> storage failover show
                                     Takeover
Node           Partner           Possible State Description
-----
node_A_1       node_A_2           false      In takeover
node_A_2       node_A_1           -          Waiting for giveback (HA
mailboxes)
2 entries were displayed.
```

### 2. Initiate a takeover of the target node on cluster\_B:

Do not specify the `-option immediate` parameter, because a normal takeover is required for the nodes that are being taken over to boot onto the new software image.

#### a. Take over the DR partner on cluster\_B (node\_B\_2):

If you are upgrading from...	Enter this command...
ONTAP 9.2 or ONTAP 9.1	<code>storage failover takeover -ofnode node_B_2</code>
ONTAP 9.0 or Data ONTAP 8.3.x	<code>storage failover takeover -ofnode node_B_2 -option allow-version-mismatch</code> <b>NOTE:</b> The <code>allow-version-mismatch</code> option is not required for upgrades from ONTAP 9.0 to ONTAP 9.1 or for any patch upgrades.

The node boots up to the "Waiting for giveback" state.

+  
**NOTE:** If AutoSupport is enabled, an AutoSupport message is sent indicating that the nodes are out of cluster quorum. You can safely ignore this notification and proceed with the upgrade.

- a. Verify that the takeover is successful: `storage failover show`

The following example shows that the takeover is successful. Node\_B\_2 is in the "Waiting for giveback" state and node\_B\_1 is in the "In takeover" state.

```
cluster1::> storage failover show
Node           Partner           Takeover
-----
Possible State Description
-----
node_B_1       node_B_2           false      In takeover
node_B_2       node_B_1           -          Waiting for giveback (HA
mailboxes)
2 entries were displayed.
```

1. Wait at least eight minutes to ensure the following conditions:
  - Client multipathing (if deployed) is stabilized.
  - Clients are recovered from the pause in I/O that occurs during takeover.

The recovery time is client-specific and might take longer than eight minutes depending on the characteristics of the client applications.

2. Return the aggregates to the target nodes:

After upgrading MetroCluster IP configurations to ONTAP 9.5, the aggregates will be in a degraded state for a short period before resynchronizing and returning to a mirrored state.

- b. Give back the aggregates to the DR partner on cluster\_A: `storage failover giveback -ofnode node_A_2`

- c. Give back the aggregates to the DR partner on cluster\_B: `storage failover giveback -ofnode node_B_2`

The giveback operation first returns the root aggregate to the node and then, after the node has finished booting, returns the non-root aggregates.

1. Verify that all aggregates have been returned by issuing the following command on both clusters:  
`storage failover show-giveback`

If the Giveback Status field indicates that there are no aggregates to give back, then all aggregates have been returned. If the giveback is vetoed, the command displays the giveback progress and which subsystem vetoed the giveback.

2. If any aggregates have not been returned, do the following:

- d. Review the veto workaround to determine whether you want to address the “veto” condition or override the veto.
- e. If necessary, address the “veto” condition described in the error message, ensuring that any identified operations are terminated gracefully.
- f. Reenter the storage failover giveback command.

If you decided to override the “veto” condition, set the `-override-vetoes` parameter to true.

. Wait at least eight minutes to ensure the following conditions:

**Client multipathing (if deployed) is stabilized.**

Clients are recovered from the pause in I/O that occurs during giveback.

+

The recovery time is client-specific and might take longer than eight minutes depending on the characteristics of the client applications.

1. Set the privilege level from admin to advanced, entering **y** when prompted to continue: `set -privilege advanced`

The advanced prompt (`*>`) appears.

2. Confirm the version on cluster\_A: `system image show`

The following example shows that System image2 (target ONTAP image) is the default and current version on node\_A\_2:

```

cluster_B::*> system image show
          Is      Is
Node      Image  Default Current Version  Install
-----  -
node_A_1
  image1  false   false   X.X.X   MM/DD/YYYY TIME
  image2  true     true    Y.Y.Y   MM/DD/YYYY TIME
node_A_2
  image1  false   false   X.X.X   MM/DD/YYYY TIME
  image2  true     true    Y.Y.Y   MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>

```

3. Confirm the version on cluster\_B: system image show

The following example shows that System image2 (target ONTAP image) is the default and current version on node\_B\_2:

```

cluster_B::*> system image show
          Is      Is
Node      Image  Default Current Version  Install
-----  -
node_B_1
  image1  false   false   X.X.X   MM/DD/YYYY TIME
  image2  true     true    Y.Y.Y   MM/DD/YYYY TIME
node_B_2
  image1  false   false   X.X.X   MM/DD/YYYY TIME
  image2  true     true    Y.Y.Y   MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>

```

4. For each node in the HA pair, enable automatic giveback: `storage failover modify -node target-node -auto-giveback true`

This command must be repeated for each node in the HA pair.

5. Verify that automatic giveback is enabled: `storage failover show -fields auto-giveback`

This example shows that automatic giveback has been enabled on both nodes:

```
cluster_x::> storage failover show -fields auto-giveback
node      auto-giveback
-----
node_x_1  true
node_x_2  true
2 entries were displayed.
```

## Manual nondisruptive upgrade of a two-node MetroCluster configuration in ONTAP 9.2 or earlier using the CLI

You can upgrade ONTAP nondisruptively for a two-node MetroCluster configuration. This method has several steps: initiating a negotiated switchover, updating the cluster at the “failed” site, initiating switchover, and then repeating the process on the cluster at the other site.

This procedure is for two-node MetroCluster configurations running ONTAP 9.2 or earlier only.

+

Do not use this procedure if you have a four-node MetroCluster configuration.

+

If you have a two-node MetroCluster configuration running ONTAP 9.3 or later, perform an [automated nondisruptive upgrade using System Manager](#).

1. Set the privilege level to advanced, entering **y** when prompted to continue: `set -privilege advanced`

The advanced prompt (`*>`) appears.

2. On the cluster to be upgraded, install the new ONTAP software image as the default: `system node image update -package package_location -setdefault true -replace-package true`

```
cluster_B::*> system node image update -package
http://www.example.com/NewImage.tgz -setdefault true -replace-package
true
```

3. Verify that the target software image is set as the default image: `system node image show`

The following example shows that `NewImage` is set as the default image:



```

cluster_B::*> system node image show

```

Node	Image	Is Default	Is Current	Version	Install Date
node_B_1	OldImage	false	true	X.X.X	MM/DD/YYYY TIME
	NewImage	true	false	Y.Y.Y	MM/DD/YYYY TIME

```

2 entries were displayed.

```

4. If the target software image is not set as the default image, then change it: `system image modify {-node * -iscurrent false} -isdefault true`
5. Verify that all cluster SVMs are in a health state: `metrocluster vserver show`
6. On the cluster that is not being updated, initiate a negotiated switchover: `metrocluster switchover`

The operation can take several minutes. You can use the `metrocluster operation show` command to verify that the switchover is completed.

In the following example, a negotiated switchover is performed on the remote cluster ("cluster\_A"). This causes the local cluster ("cluster\_B") to halt so that you can update it.

```

cluster_A::> metrocluster switchover

```

Warning: negotiated switchover is about to start. It will stop all the data

Vservers on cluster "cluster\_B" and automatically re-start them on cluster "cluster\_A". It will finally gracefully shutdown cluster "cluster\_B".

Do you want to continue? {y|n}: y

7. Verify that all cluster SVMs are in a health state: `metrocluster vserver show`
8. Resynchronize the data aggregates on the "surviving" cluster: `metrocluster heal -phase aggregates`

After upgrading MetroCluster IP configurations to ONTAP 9.5 or later, the aggregates will be in a degraded state for a short period before resynchronizing and returning to a mirrored state.

```

cluster_A::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.

```

9. Verify that the healing operation was completed successfully: `metrocluster operation show`

```
cluster_A::> metrocluster operation show
Operation: heal-aggregates
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

10. Resynchronize the root aggregates on the “surviving” cluster: `metrocluster heal -phase root-aggregates`

```
cluster_A::> metrocluster heal -phase root-aggregates
[Job 131] Job succeeded: Heal Root Aggregates is successful.
```

11. Verify that the healing operation was completed successfully: `metrocluster operation show`

```
cluster_A::> metrocluster operation show
Operation: heal-root-aggregates
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

12. On the halted cluster, boot the node from the LOADER prompt: `boot_ontap`
13. Wait for the boot process to finish, and then verify that all cluster SVMs are in a health state: `metrocluster vserver show`
14. Perform a switchback from the “surviving” cluster: `metrocluster switchback`
15. Verify that the switchback was completed successfully: `metrocluster operation show`

```
cluster_A::> metrocluster operation show
Operation: switchback
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

16. Verify that all cluster SVMs are in a health state: `metrocluster vserver show`
17. Repeat all previous steps on the other cluster.
18. Verify that the MetroCluster configuration is healthy:
  - a. Check the configuration: `metrocluster check run`

```

cluster_A::> metrocluster check run
Last Checked On: MM/DD/YYYY TIME
Component          Result
-----
nodes              ok
lifs               ok
config-replication ok
aggregates        ok
4 entries were displayed.

```

Command completed. Use the "metrocluster check show -instance" command or sub-commands in "metrocluster check" directory for detailed results.

To check if the nodes are ready to do a switchover or switchback operation, run "metrocluster switchover -simulate" or "metrocluster switchback -simulate", respectively.

- b. If you want to view more detailed results, use the metrocluster check run command: metrocluster check aggregate show metrocluster check config-replication show metrocluster check lif show` metrocluster check node show
- c. Set the privilege level to advanced: set -privilege advanced
- d. Simulate the switchover operation: metrocluster switchover -simulate
- e. Review the results of the switchover simulation: metrocluster operation show

```

cluster_A::*> metrocluster operation show
Operation: switchover
State: successful
Start time: MM/DD/YYYY TIME
End time: MM/DD/YYYY TIME
Errors: -

```

- f. Return to the admin privilege level: set -privilege admin
- g. Repeat these substeps on the other cluster.

You should perform any post-upgrade tasks.

#### Related information

[MetroCluster Disaster recovery](#)

#### Manual disruptive upgrade using the CLI

If you can take your cluster offline to upgrade to a new ONTAP release, then you can use the disruptive upgrade method. This method has several steps: disabling storage failover for each HA pair, rebooting each node in the cluster, and then reenabling storage failover.

- You must have satisfied preparation requirements.

In particular, you must download and install the software image using the procedure [for manual upgrades](#).

- If you are operating in a SAN environment, all SAN clients must be shut down or suspended until the upgrade is complete.

If SAN clients are not shut down or suspended prior to a disruptive upgrade, then the client file systems and applications suffer errors that might require manual recovery after the upgrade is completed.

In a disruptive upgrade, downtime is required because storage failover is disabled for each HA pair, and each node is updated. When storage failover is disabled, each node behaves as a single-node cluster; that is, system services associated with the node are interrupted for as long as it takes the system to reboot.

1. Set the privilege level from admin to advanced, entering **y** when prompted to continue: `set -privilege advanced`

The advanced prompt (**\*>**) appears.

2. Set the new ONTAP software image to be the default image: `system image modify {-node * -iscurrent false} -isdefault true`

This command uses an extended query to change the target ONTAP software image (which is installed as the alternate image) to be the default image for each node.

3. Verify that the new ONTAP software image is set as the default image: `system image show`

In the following example, image 2 is the new ONTAP version and is set as the default image on both nodes:

```
cluster1::*> system image show
Node      Image      Is      Is      Install
          Image    Default Current Version  Date
-----
node0
  image1   false     true    X.X.X    MM/DD/YYYY TIME
  image2   true      false   Y.Y.Y    MM/DD/YYYY TIME
node1
  image1   false     true    X.X.X    MM/DD/YYYY TIME
  image2   true      false   Y.Y.Y    MM/DD/YYYY TIME
4 entries were displayed.
```

4. Perform either one of the following steps:

If the cluster consists of...	Do this...
One node	Continue to the next step.

If the cluster consists of...	Do this...
Two nodes	<p>a. Disable cluster high availability: <code>cluster ha modify -configured false</code></p> <p>Enter <code>y</code> to continue when prompted.</p> <p>b. Disable storage failover for the HA pair:  <code>storage failover modify -node * -enabled false</code></p>
More than two nodes	<p>Disable storage failover for each HA pair in the cluster: <code>storage failover modify -node * -enabled false</code></p>

5. Reboot a node in the cluster: `system node reboot -node nodename -ignore-quorum-warnings`



Do not reboot more than one node at a time.

The node boots the new ONTAP image. The ONTAP login prompt appears, indicating that the reboot process is complete.

6. After the node or set of nodes has rebooted with the new ONTAP image, confirm that the new software is running: `system node image show`

In the following example, `image1` is the new ONTAP version and is set as the current version on `node0`:

```
cluster1::*> system node image show
Node      Image      Is Default Is Current Version      Install Date
-----
node0
  image1  true      true  X.X.X  MM/DD/YYYY TIME
  image2  false     false Y.Y.Y  MM/DD/YYYY TIME
node1
  image1  true      false X.X.X  MM/DD/YYYY TIME
  image2  false     true  Y.Y.Y  MM/DD/YYYY TIME
4 entries were displayed.
```

7. Verify that the upgrade is completed successfully:
  - a. Set the privilege level to advanced: `set -privilege advanced`
  - b. Verify that the upgrade status is complete for each node: `system node upgrade-revert show -node nodename`

The status should be listed as complete.

If the status is not complete, [contact NetApp Support](#) immediately.

c. Return to the admin privilege level: `set -privilege admin`

8. Repeat Steps 2 through 7 for each additional node.

9. If the cluster consists of two or more nodes, enable storage failover for each HA pair in the cluster:  
`storage failover modify -node * -enabled true`

10. If the cluster consists of only two nodes, enable cluster high availability: `cluster ha modify -configured true`

## What should I do after my upgrade?

### What to do after upgrading

After upgrading your ONTAP software, there are several tasks you should perform to verify your cluster readiness.

### Post-upgrade cluster verification

After you upgrade, you should verify your cluster version, cluster health, and storage health.



#### Before you begin

If you are using a MetroCluster FC configuration, you also need to verify that the cluster is enabled for automatic unplanned switchover.

### Verify cluster version

After all of the HA pairs have been upgraded, you must use the version command to verify that all of the nodes are running the target release.

The cluster version is the lowest version of ONTAP running on any node in the cluster. If the cluster version is not the target ONTAP release, you can upgrade your cluster.

1. Verify that the cluster version is the target ONTAP release:

```
version
```

2. If the cluster version is not the target ONTAP release, you can verify the upgrade status of all nodes:

```
system node upgrade-revert show
```

### Verify cluster health

After you upgrade a cluster, you should verify that the nodes are healthy and eligible to participate in the cluster, and that the cluster is in quorum.

1. Verify that the nodes in the cluster are online and are eligible to participate in the cluster:

```
cluster show
```

```
cluster1::> cluster show
Node                Health  Eligibility
-----
node0               true   true
node1               true   true
```

If any node is unhealthy or ineligible, check EMS logs for errors and take corrective action.

2. Set the privilege level to advanced:

```
set -privilege advanced
```

Enter “y” to continue.

3. Verify the configuration details for each RDB process.

- The relational database epoch and database epochs should match for each node.
- The per-ring quorum master should be the same for all nodes.

Note that each ring might have a different quorum master.

To display this RDB process...	Enter this command...
Management application	<code>cluster ring show -unitname mgmt</code>
Volume location database	<code>cluster ring show -unitname vldb</code>
Virtual-Interface manager	<code>cluster ring show -unitname vifmgr</code>
SAN management daemon	<code>cluster ring show -unitname bcomd</code>

This example shows the volume location database process:

```
cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch    DB Epoch DB Trnxs Master  Online
-----
node0     vldb     154      154      14847   node0   master
node1     vldb     154      154      14847   node0   secondary
node2     vldb     154      154      14847   node0   secondary
node3     vldb     154      154      14847   node0   secondary
4 entries were displayed.
```

4. If you are operating in a SAN environment, verify that each node is in a SAN quorum: `event log show -severity informational -message-name scsiblade.*`

The most recent scsiblade event message for each node should indicate that the scsi-blade is in quorum.

```
cluster1::*> event log show -severity informational -message-name
scsiblade.*
```

Time	Node	Severity	Event
MM/DD/YYYY TIME	node0	INFORMATIONAL	scsiblade.in.quorum: The scsi-blade ...
MM/DD/YYYY TIME	node1	INFORMATIONAL	scsiblade.in.quorum: The scsi-blade ...

## Related information

### [System administration](#)

#### Verify that automatic unplanned switchover is enabled

After you upgrade a cluster, you should verify that automatic unplanned switchover is enabled.



#### About this task

This procedure is performed only for MetroCluster FC configurations. If you are using a MetroCluster IP configuration, skip this procedure.

#### Steps

1. Check whether automatic unplanned switchover is enabled:

```
metrocluster show
```

If automatic unplanned switchover is enabled, the following statement appears in the command output:

```
AUSO Failure Domain  auso-on-cluster-disaster
```

2. If the statement does not appear, enable an automatic unplanned switchover:

```
metrocluster modify -auto-switchover-failure-domain auso-on-cluster-disaster
```

3. Verify that an automatic unplanned switchover has been enabled by repeating Step 1.

#### Verify storage health

After you upgrade a cluster, you should verify the status of your disks, aggregates, and volumes.

1. Verify disk status:

To check for...	Do this...
-----------------	------------



Broken disks	<p>a. Display any broken disks:</p> <pre>storage disk show -state broken</pre> <p>b. Remove or replace any broken disks.</p>
Disks undergoing maintenance or reconstruction	<p>a. Display any disks in maintenance, pending, or reconstructing states:</p> <pre>storage disk show -state maintenance pending reconstructing</pre> <p>b. Wait for the maintenance or reconstruction operation to finish before proceeding.</p>

- Verify that all aggregates are online by displaying the state of physical and logical storage, including storage aggregates:

```
storage aggregate show -state !online
```

This command displays the aggregates that are *not* online. All aggregates must be online before and after performing a major upgrade or reversion.

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

- Verify that all volumes are online by displaying any volumes that are *not* online:

```
volume show -state !online
```

All volumes must be online before and after performing a major upgrade or reversion.

```
cluster1::> volume show -state !online
There are no entries matching your query.
```

- Verify that there are no inconsistent volumes:

```
volume show -is-inconsistent true
```

See the Knowledge Base article [Volume Showing WAFL Inconsistent](#) on how to address the inconsistent volumes.

## Related information

[Disk and aggregate management](#)

## Verify all LIFS are on home ports after upgrade

During a reboot, some LIFs might have been migrated to their assigned failover ports.

After you upgrade a cluster, you must enable and revert any LIFs that are not on their home ports.

The network interface revert command reverts a LIF that is not currently on its home port back to its home port, provided that the home port is operational. A LIF's home port is specified when the LIF is created; you can determine the home port for a LIF by using the network interface show command.

1. Display the status of all LIFs: `network interface show -fields home-ports,curr-port`

This example displays the status of all LIFs for a storage virtual machine (SVM).

```

cluster1::> network interface show -fields home-port,curr-port
vserver                lif                home-port curr-port
-----
C1_sti96-vsim-ucs539g_1622463615 clus_mgmt e0d          e0d
C1_sti96-vsim-ucs539g_1622463615 sti96-vsim-ucs539g_cluster_mgmt_inet6
e0d e0d
C1_sti96-vsim-ucs539g_1622463615 sti96-vsim-ucs539g_mgmt1 e0c e0c
C1_sti96-vsim-ucs539g_1622463615 sti96-vsim-ucs539g_mgmt1_inet6 e0c e0c
C1_sti96-vsim-ucs539g_1622463615 sti96-vsim-ucs539h_cluster_mgmt_inet6
e0d e0d
C1_sti96-vsim-ucs539g_1622463615 sti96-vsim-ucs539h_mgmt1 e0c e0c
C1_sti96-vsim-ucs539g_1622463615 sti96-vsim-ucs539h_mgmt1_inet6 e0c e0c
Cluster                sti96-vsim-ucs539g_clus1 e0a e0a
Cluster                sti96-vsim-ucs539g_clus2 e0b e0b
Cluster                sti96-vsim-ucs539h_clus1 e0a e0a
Cluster                sti96-vsim-ucs539h_clus2 e0b e0b
vs0                    sti96-vsim-ucs539g_data1 e0d e0d
vs0                    sti96-vsim-ucs539g_data1_inet6 e0d e0d
vs0                    sti96-vsim-ucs539g_data2 e0e e0e
vs0                    sti96-vsim-ucs539g_data2_inet6 e0e e0e
vs0                    sti96-vsim-ucs539g_data3 e0f e0f
vs0                    sti96-vsim-ucs539g_data3_inet6 e0f e0f
vs0                    sti96-vsim-ucs539g_data4 e0d e0d
vs0                    sti96-vsim-ucs539g_data4_inet6 e0d e0d
vs0                    sti96-vsim-ucs539g_data5 e0e e0e
vs0                    sti96-vsim-ucs539g_data5_inet6 e0e e0e
vs0                    sti96-vsim-ucs539g_data6 e0f e0f
vs0                    sti96-vsim-ucs539g_data6_inet6 e0f e0f
vs0                    sti96-vsim-ucs539h_data1 e0d e0d
vs0                    sti96-vsim-ucs539h_data1_inet6 e0d e0d
vs0                    sti96-vsim-ucs539h_data2 e0e e0e
vs0                    sti96-vsim-ucs539h_data2_inet6 e0e e0e
vs0                    sti96-vsim-ucs539h_data3 e0f e0f
vs0                    sti96-vsim-ucs539h_data3_inet6 e0f e0f
vs0                    sti96-vsim-ucs539h_data4 e0d e0d
vs0                    sti96-vsim-ucs539h_data4_inet6 e0d e0d
vs0                    sti96-vsim-ucs539h_data5 e0e e0e
vs0                    sti96-vsim-ucs539h_data5_inet6 e0e e0e
vs0                    sti96-vsim-ucs539h_data6 e0f e0f
vs0                    sti96-vsim-ucs539h_data6_inet6 e0f e0f
35 entries were displayed.

```

If any LIFs appear with a Status Admin status of "down" or with an Is home status of "false", continue with the next step.

2. Enable the data LIFs: `network interface modify {-role data} -status-admin up`

```
cluster1::> network interface modify {-role data} -status-admin up
8 entries were modified.
```

3. Revert LIFs to their home ports: `network interface revert *`

This command reverts all LIFs back to their home ports.

```
cluster1::> network interface revert *
8 entries were acted on.
```

4. Verify that all LIFs are in their home ports: `network interface show`

This example shows that all LIFs for SVM vs0 are on their home ports.

```
cluster1::> network interface show -vserver vs0
      Logical      Status      Network      Current      Current      Is
Vserver Interface  Admin/Oper  Address/Mask  Node         Port         Home
-----
vs0
      data001      up/up      192.0.2.120/24  node0        e0e          true
      data002      up/up      192.0.2.121/24  node0        e0f          true
      data003      up/up      192.0.2.122/24  node0        e2a          true
      data004      up/up      192.0.2.123/24  node0        e2b          true
      data005      up/up      192.0.2.124/24  node1        e0e          true
      data006      up/up      192.0.2.125/24  node1        e0f          true
      data007      up/up      192.0.2.126/24  node1        e2a          true
      data008      up/up      192.0.2.127/24  node1        e2b          true
8 entries were displayed.
```

## Verify special configurations

### Post upgrade checks for special configurations

If your cluster is configured with any of the following features you might need to perform additional steps after you upgrade.

Ask yourself...	If your answer is yes, then do this...
Did I upgrade to ONTAP 9.8 or later from ONTAP 9.7 or earlier	<a href="#">Verify your network configuration</a>  <a href="#">Remove the EMS LIF service from network service polices that do not provide reachability to the EMS destination</a>

Ask yourself...	If your answer is yes, then do this...
Do I have a MetroCluster configuration?	<a href="#">Verify your networking and storage status</a>
Do I have a SAN configuration?	<a href="#">Verify your SAN configuration</a>
Am I using NetApp Storage Encryption and I upgraded to ONTAP 9.3 or later?	<a href="#">Reconfigure KMIP server connections</a>
Do I have load-sharing mirrors?	<a href="#">Relocate moved load-sharing mirror source volumes</a>
Am I using SnapMirror?	<a href="#">Resume SnapMirror operations</a>
Did I upgrade from ONTAP 8.3.0?	<a href="#">Set the desired NT ACL permissions display level for NFS clients</a>
Do I have administrator accounts created prior to ONTAP 9.0?	<a href="#">Enforce SHA-2 on administrator passwords</a>
Do I have user accounts for Service Processor (SP) access created prior to ONTAP 9.9.1?	<a href="#">Verify the change in accounts that can access the Service Processor</a>

### Verifying your network configuration after upgrade

ONTAP 9.8 and later automatically monitors layer 2 reachability. After you upgrade from ONTAP 9.7x or earlier to ONTAP 9.8 or later, you should verify that each .network port has reachability to its expected broadcast domain.

1. Verify each port has reachability to its expected domain: `network port reachability show -detail`

A reachability-status of ok indicates that the port has layer 2 reachability to its assigned domain.

### Verify networking and storage status for MetroCluster configurations

After performing an update in a MetroCluster configuration, you should verify the status of the LIFs, aggregates, and volumes for each cluster.

1. Verify the LIF status: `network interface show`

In normal operation, LIFs for source SVMs must have an admin status of up and be located on their home nodes. LIFs for destination SVMs are not required to be up or located on their home nodes. In switchover, all LIFs have an admin status of up, but they do not need to be located on their home nodes.

```

cluster1::> network interface show
          Logical      Status      Network      Current
Current Is
Vserver   Interface  Admin/Oper  Address/Mask  Node      Port
Home
-----
-----
Cluster
          cluster1-a1_clus1
          up/up    192.0.2.1/24  cluster1-01
          true
          e2a
          cluster1-a1_clus2
          up/up    192.0.2.2/24  cluster1-01
          true
          e2b
cluster1-01
          clus_mgmt    up/up    198.51.100.1/24  cluster1-01
          true
          e3a
          cluster1-a1_inet4_intercluster1
          up/up    198.51.100.2/24  cluster1-01
          true
          e3c
          ...

27 entries were displayed.

```

## 2. Verify the state of the aggregates: `storage aggregate show -state !online`

This command displays any aggregates that are *not* online. In normal operation, all aggregates located at the local site must be online. However, if the MetroCluster configuration is in switchover, root aggregates at the disaster recovery site are permitted to be offline.

This example shows a cluster in normal operation:

```

cluster1::> storage aggregate show -state !online
There are no entries matching your query.

```

This example shows a cluster in switchover, in which the root aggregates at the disaster recovery site are offline:

```

cluster1::> storage aggregate show -state !online
Aggregate      Size Available Used% State  #Vols  Nodes          RAID
Status
-----
-----
aggr0_b1
          0B          0B    0% offline    0 cluster2-01
raid_dp,
mirror
degraded
aggr0_b2
          0B          0B    0% offline    0 cluster2-02
raid_dp,
mirror
degraded
2 entries were displayed.

```

3. Verify the state of the volumes: `volume show -state !online`

This command displays any volumes that are *not* online.

If the MetroCluster configuration is in normal operation (it is not in switchover state), the output should show all volumes owned by the cluster's secondary SVMs (those with the SVM name appended with "-mc").

Those volumes come online only in the event of a switchover.

This example shows a cluster in normal operation, in which the volumes at the disaster recovery site are not online.

```

cluster1::> volume show -state !online
  (volume show)
Vserver   Volume           Aggregate      State      Type      Size
Available Used%
-----
vs2-mc    vol1             aggr1_b1      -          RW        -
-         -
vs2-mc    root_vs2        aggr0_b1      -          RW        -
-         -
vs2-mc    vol2             aggr1_b1      -          RW        -
-         -
vs2-mc    vol3             aggr1_b1      -          RW        -
-         -
vs2-mc    vol4             aggr1_b1      -          RW        -
-         -
5 entries were displayed.

```

4. Verify that there are no inconsistent volumes: `volume show -is-inconsistent true`

See the Knowledge Base article [Volume Showing WAFL Inconsistent](#) on how to address the inconsistent volumes.

#### Verify the SAN configuration after an upgrade

If you are upgrading in a SAN environment, then after the upgrade, you should verify that each initiator that was connected to a LIF before the upgrade has successfully reconnected to the LIF.

1. Verify that each initiator is connected to the correct LIF.

You should compare the list of initiators to the list you made during the upgrade preparation.

For...	Enter...
iSCSI	<code>iscsi initiator show -fields igroup,initiator-name,tpgroup</code>
FC	<code>fcp initiator show -fields igroup,wwpn,lif</code>

#### Reconfiguring KMIP server connections after upgrading to ONTAP 9.3 or later

After performing an upgrade to ONTAP 9.3 or later, you must reconfigure your external key management (KMIP) server connections.



1. Configure the key manager connectivity: `security key-manager setup`
2. Add your KMIP servers: `security key-manager add -address key_management_server_ip_address`
3. Verify that KMIP servers are connected: `security key-manager show -status`
4. Query the key servers: `security key-manager query`
5. Create a new authentication key and passphrase: `security key-manager create-key -prompt -for-key true`

The passphrase must have a minimum of 32 characters.

6. Query the new authentication key: `security key-manager query`
7. Assign the new authentication key to your self-encrypting disks (SEDs): `storage encryption disk modify -disk disk_ID -data-key-id key_ID`



Make sure you are using the new authentication key from your query.

8. If needed, assign a FIPS key to the SEDs: `storage encryption disk modify -disk disk_id -fips-key-id fips_authentication_key_id`

If your security setup requires you to use different keys for data authentication and FIPS 140-2 authentication, you should create a separate key for each. If that is not the case, you can use the same authentication key for FIPS compliance that you use for data access.

### Relocating moved load-sharing mirror source volumes

After successfully completing a nondisruptive upgrade, you can move load-sharing mirror source volumes back to the locations they were in originally before the upgrade.

1. Identify the location to which you are moving the load-sharing mirror source volume by using the record you created before moving the load-sharing mirror source volume.
2. Move the load-sharing mirror source volume back to its original location by using the `volume move start` command.

### Resuming SnapMirror operations

After completing a nondisruptive upgrade, you must resume any SnapMirror relationships that were suspended.

Existing SnapMirror relationships must have been suspended by using the `snapmirror quiesce` command, and the cluster must have been nondisruptively upgraded.

1. Resume transfers for each SnapMirror relationship that was previously quiesced: `snapmirror resume *`

This command resumes the transfers for all quiesced SnapMirror relationships.

2. Verify that the SnapMirror operations have resumed: `snapmirror show`

```

cluster1::> snapmirror show

Source          Destination  Mirror  Relationship  Total
Last
Path           Type  Path          State   Status          Progress  Healthy
Updated
-----
-----
cluster1-vs1:dp_src1
          DP  cluster1-vs2:dp_dst1
                               Snapmirrored
                               Idle             -         true     -
cluster1-vs1:xdp_src1
          XDP cluster1-vs2:xdp_dst1
                               Snapmirrored
                               Idle             -         true     -
cluster1://cluster1-vs1/ls_src1
          LS  cluster1://cluster1-vs1/ls_mr1
                               Snapmirrored
                               Idle             -         true     -
          cluster1://cluster1-vs1/ls_mr2
                               Snapmirrored
                               Idle             -         true     -

4 entries were displayed.

```

For each SnapMirror relationship, verify that the Relationship Status is **Idle**. If the status is **Transferring**, wait for the SnapMirror transfer to complete, and then reenter the command to verify that the status has changed to **Idle**.

For each SnapMirror relationship that is configured to run on a schedule, you should verify that the first scheduled SnapMirror transfer completes successfully.

#### Setting the desired NT ACL permissions display level for NFS clients

After upgrading from ONTAP 8.3.0, the default handling for displaying NT ACL permissions to NFS clients has changed. You should check the setting and change it to the desired setting for your environment if necessary. This task does not apply if you are upgrading from ONTAP 8.3.1 or later.

In multiprotocol environments, ONTAP displays to NFS clients the permissions of NTFS security-style files and directories based on the access granted by the NT ACL to any user. In ONTAP 8.3.0, ONTAP by default displayed to NFS clients the permission based on the maximum access granted by the NT ACL. After upgrading, the default setting changes to display permissions based on the minimum access granted by the NT ACL. This change applies to new and existing storage virtual machines (SVMs).

1. Set the privilege level to advanced: `set -privilege advanced`

2. Check the setting for displaying NT ACL permissions for NFS clients: `vserver nfs show -vserver vserver_name -fields ntacl-display-permissive-perms`

After upgrading from 8.3.0, the value for this new parameter is disabled, meaning ONTAP displays the minimum permissions.

3. If you prefer to display the maximum permissions, change the setting individually for each SVM as desired: `vserver nfs modify -vserver vserver_name -ntacl-display-permissive-perms enabled`
4. Verify that the change took effect: `vserver nfs show -vserver vserver_name -fields ntacl-display-permissive-perms`
5. Return to the admin privilege level: `set -privilege admin`

### Enforcing SHA-2 on administrator account passwords

Administrator accounts created prior to ONTAP 9.0 continue to use MD5 passwords after the upgrade, until the passwords are manually changed. MD5 is less secure than SHA-2. Therefore, after upgrading, you should prompt users of MD5 accounts to change their passwords to use the default SHA-512 hash function.

The password hash functionality enables you to do the following:

- Display user accounts that match the specified hash function.
- Expire accounts that use a specified hash function (for example, MD5), forcing the users to change their passwords in their next login.
- Lock accounts whose passwords use the specified hash function.
- When reverting to a release earlier than ONTAP 9, reset the cluster administrator's own password for it to be compatible with the hash function (MD5) that is supported by the earlier release.

ONTAP accepts pre-hashed SHA-2 passwords only by using NetApp Manageability SDK (`security-login-create` and `security-login-modify-password`).

### Manageability enhancements

1. Migrate the MD5 administrator accounts to the SHA-512 password hash function:
  - a. Expire all MD5 administrator accounts: `security login expire-password -vserver * -username * -hash-function md5`

Doing so forces MD5 account users to change their passwords upon next login.

- b. Ask users of MD5 accounts to log in through a console or SSH session.

The system detects that the accounts are expired and prompts users to change their passwords. SHA-512 is used by default for the changed passwords.

2. For MD5 accounts whose users do not log in to change their passwords within a period of time, force the account migration:
  - a. Lock accounts that still use the MD5 hash function (advanced privilege level): `security login expire-password -vserver * -username * -hash-function md5 -lock-after integer`

After the number of days specified by `-lock-after`, users cannot access their MD5 accounts.

- b. Unlock the accounts when the users are ready to change their passwords: `security login unlock -vserver vserver_name -username user_name`
- c. Have users log in to their accounts through a console or SSH session and change their passwords when the system prompts them to do so.

#### Change in user accounts that can access the Service Processor

If you created user accounts in ONTAP 9.8 and earlier releases that can access the Service Processor (SP) with a non-admin role and you upgrade to ONTAP 9.9.1 or later, any non-admin value in the `-role` parameter is modified to `admin`.

For more information, see [Accounts that can access the SP](#).

#### Remove EMS LIF service from network service policies

If you have Event Management System (EMS) messages set up before you upgrade from ONTAP 9.7 or earlier to ONTAP 9.8 or later, after the upgrade, your EMS messages might not be delivered.

During the upgrade, `management-ems`, which is the the EMS LIF service, is added to all existing service policies. This allows EMS messages to be sent from any of the LIFs associated with any of the service policies. If the selected LIF does not have reachability to the event notification destination, the message is not delivered.

To prevent this, after the upgrade, you should remove the EMS LIF service from the network service policies that do not provide reachability to the destination.

#### Steps

1. Identify the LIFs and associated network service policies through which EMS messages can be sent:

```
network interface show -fields service-policy -services management-ems
```

```
vserver      lif          service-policy
-----
cluster-1    cluster_mgmt          default-management
cluster-1    node1-mgmt           default-management
cluster-1    node2-mgmt           default-management
cluster-1    inter_cluster        default-intercluster
4 entries were displayed.
```

2. Check each LIF for connectivity to the EMS destination:

```
network ping -lif lif_name -vserver svm_name -destination destination_address
```

Perform this on each node.

### Examples

```
cluster-1::> network ping -lif node1-mgmt -vserver cluster-1
-destination 10.10.10.10
10.10.10.10 is alive

cluster-1::> network ping -lif inter_cluster -vserver cluster-1
-destination 10.10.10.10
no answer from 10.10.10.10
```

### 3. Enter advanced privilege level:

```
set advanced
```

### 4. For the LIFs that do not have reachability, remove the management-ems LIF service from the corresponding service policies:

```
network interface service-policy remove-service -vserver svm_name -policy
service_policy_name -service management-ems
```

### 5. Verify that the management-ems LIF is now only associated with the LIFs that provide reachability to the EMS destination:

```
network interface show -fields service-policy -services management-ems
```

### Related Links

[LIFs and service policies in ONTAP 9.6 and later](#)

### When you need to update the Disk Qualification Package

The Disk Qualification Package (DQP) adds full support for newly qualified drives.

ONTAP treats disk drives differently than normally expected, for example, ONTAP allocates different sector sizes than those specified by manufacturers. The DQP contains the proper parameters for ONTAP for all newly qualified drives. Therefore, if you are running a version of ONTAP with a DQP that does not contain information for a newly qualified drive, ONTAP will not have the information to properly configure the drive.

You need to download and install the DQP in the following situations. A best practice is to also update the DQP regularly; for example, every quarter or semi-annually.

- Whenever you upgrade to a new version of ONTAP.

The DQP is not updated as part of an ONTAP upgrade.

- Whenever you add a new drive type or size to the node

For example, if you already have 1-TB drives and add 2-TB drives, you need to check for the latest DQP update.

- Whenever you update the disk firmware

- Whenever newer disk firmware or DQP files are available

#### Related information

[NetApp Downloads: Disk Qualification Package](#)

[NetApp Downloads: Disk Drive Firmware](#)

## Update firmware

With System Manager, you can apply a firmware update to supported devices in your cluster, such as disks, disk shelves, the Disk Qualification Package (DQP), the service processor (SP), or the Baseboard Management Controller (BMC).

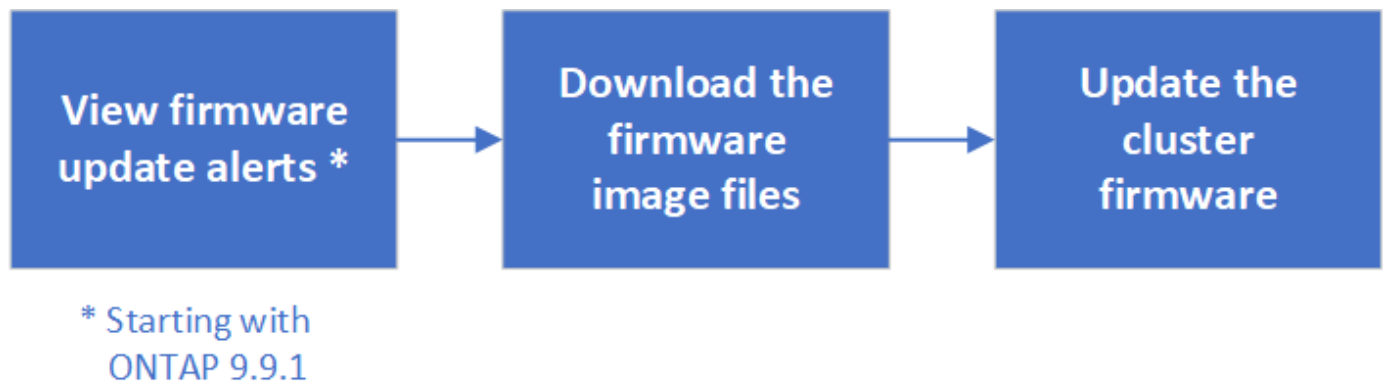
You can apply firmware updates manually or automatically. Select either procedure:

- [Update firmware manually](#)
- [Update firmware automatically](#)

### Update firmware manually

#### About this task

Beginning with ONTAP 9.9.1, you can receive alerts from Active IQ that inform you when firmware updates are pending on the cluster. Then, you can download the firmware image and upload it using System Manager.



#### View firmware update alerts from Active IQ

Beginning with ONTAP 9.9.1, you can receive alerts in System Manager from Active IQ Unified Manager that inform you when firmware updates are pending on the cluster.



When working with ONTAP 9.9.1, to receive alerts about firmware updates, you must be registered with Active IQ Unified Manager. Refer to [Active IQ Unified Manager documentation resources](#).

#### Steps

1. Go to **Dashboard**.

In the **Health** section, a message displays if there are any recommended firmware updates for the cluster.

2. Click on the alert message.

The **Firmware Update** tab is displayed in the **Update** page.

### Download the cluster firmware



For ONTAP 9.8, you must navigate to the NetApp Support Site to download an updated firmware image package.

Beginning with ONTAP 9.9.1, you can use System Manager to download firmware updates from the **Update** page when you view firmware alerts (see [View firmware update alerts from Active IQ.](#)).

### Steps

Perform the procedure that is appropriate for the version of ONTAP that is installed on the cluster.

<b>For ONTAP 9.8 and ONTAP 9.9.1, if you are not registered with Active IQ, then perform these steps...</b>	<b>Beginning with ONTAP 9.9.1, if you are registered with Active IQ, then perform these steps...</b>
<ol style="list-style-type: none"> <li>1. Navigate to the NetApp Support Site.</li> <li>2. Log into the NetApp Support Site.</li> <li>3. Select the firmware package that you want to use to update your cluster firmware.</li> <li>4. Copy the files to an HTTP or FTP server on your network or to a local folder.</li> </ol>	<ol style="list-style-type: none"> <li>1. On the <b>Update</b> page, for the firmware update that you want to perform, click on the link that says "Download from NetApp Support Site".  The NetApp Support Site is displayed.</li> <li>2. Log into the NetApp Support Site.</li> <li>3. Download the firmware image package you want to update with.</li> <li>4. Copy the files to an HTTP or FTP server on your network or to a local folder.</li> </ol>

### Update the cluster firmware

After the firmware package files are downloaded, you can update the cluster firmware.

### Steps

1. In System Manager, click **Cluster > Overview**.
2. In the right corner of the **Overview** pane, click **More** and select **ONTAP Update**.
3. Click the **Firmware Update** tab, and then perform one of the following procedures, depending on which version of ONTAP you are using:

<b>ONTAP version</b>	<b>Procedure</b>
ONTAP 9.10.0 or earlier	<ol style="list-style-type: none"> <li>1. Select <b>From Server</b> or <b>Local Client</b></li> <li>2. Provide the server URL or the file location.</li> </ol>

ONTAP 9.10.1

**Note:** To schedule fixes and updates to occur automatically and receive recommendations about updating, see [Update firmware automatically](#).

1. In the list of recommended updates, select the **Actions** button to perform the following tasks:

- **Update:** Install the update.
- **Schedule:** Set a schedule for installing the update.
- **Dismiss:** Remove the recommendation notice from the list.

If the update has been schedule, the options of the **Actions** button are:

- **Update:** Install the update now.
- **Edit Schedule:** Change the schedule date for the update.
- **Cancel Schedule:** Cancel the scheduled date for the update.

2. If you want to update manually, select the **Update Firmware** button.



You can monitor or verify updates under **Firmware Update Summary**. Updates that were dismissed or failed to install can be viewed in System Manager. Go to **Cluster > Settings > Automatic Update > View All Automatic Updates**.

## Update firmware automatically

Beginning with ONTAP 9.10.1, you can use System Manager to enable the Automatic Update feature, which allows ONTAP to automatically download and install recommended firmware patches, upgrades, and updates provided by NetApp (the default behavior).

### Before you begin

The Automatic Update feature requires AutoSupport connectivity over HTTPS. To troubleshoot connectivity problems, see [Troubleshoot AutoSupport message delivery over HTTP or HTTPS](#).

### About this task

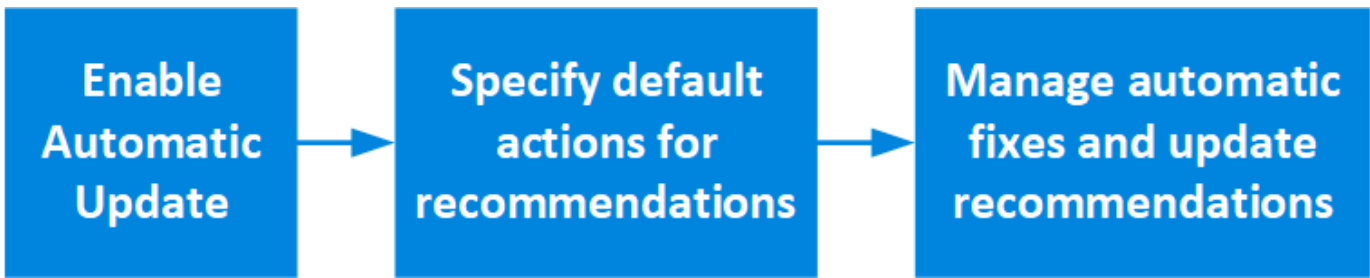
Updates include firmware patches, upgrades, and updates for the following categories:

- **Storage firmware:** Storage devices, Disk Qualification Package (DQP), disks, and disk shelves
- **SP/BMC firmware:** Service processors and BMC modules

In System Manager, you can change the default behavior per category so that you receive recommendations for updates to firmware, allowing you to decide which ones to install and to set the schedule when you want them to install. You can also turn off the feature.

To schedule updates to occur automatically and to receive recommendations about updating, you perform the following workflow tasks:





- Ensure the Automatic Update feature is enabled
- Specify default actions for update recommendations
- Manage automatic update recommendations

### Ensure the Automatic Update feature is enabled

In System Manager, to enable the Automatic Update feature, you must accept the terms and conditions specified by NetApp.

#### Before you begin

The Automatic Update feature requires that AutoSupport is enabled and using the HTTPS protocol.

#### Steps

1. In System Manager, click **Events**.
2. In the **Overview** section, under **Recommended Actions**, click **Action** next to **Enable automatic update**.
3. Click **Enable**.

Information is displayed about the Automatic Update feature. It describes the default behavior (automatically download and install updates) and notifies you that you can modify the default behavior. The information also contains terms and conditions to which you must agree if you want to use this feature.

4. To accept the terms and conditions, and to enable the feature, click the checkbox, then click **Save**.

### Specify default actions for update recommendations

ONTAP automatically detects when an update is available. It initiates the download and installation without any intervention. However, you can specify a different default behavior to be performed for storage firmware updates and SP/BMC firmware updates.

#### Steps




1. In System Manager, click **Cluster > Settings**.
2. In the **Automatic Update** section, click **⋮** to view a list of actions.
3. Click **Edit Automatic Update Settings**.
4. Select default actions for both categories of updates.

### Manage automatic update recommendations


In System Manager, you can view a list of recommendations and perform actions on each one or on all of them at once.

#### Steps

1. Use either method to view the list of recommendations:

View from the Overview page	View from the Settings page
<ol style="list-style-type: none"> <li>1. Click <b>Cluster &gt; Overview</b>.</li> <li>2. In the <b>Overview</b> section, click <b>More</b> , then click <b>ONTAP Update</b>.</li> <li>3. Select the <b>Firmware Update</b> tab.</li> <li>4. On the <b>Firmware Update</b> tab, click <b>More</b> , then click <b>View All Automatic Updates</b>.</li> </ol>	<ol style="list-style-type: none"> <li>1. Click <b>Cluster &gt; Settings</b>.</li> <li>2. In the <b>Automatic Update</b> section, click , then click <b>View All Automatic Updates</b>.</li> </ol>

The Automatic Update Log displays the recommendations and details about each one, including a description, a category, a scheduled time to install, status, and any errors.

2. Click  next to the description to view a list of actions you can perform on the recommendation.

You can perform one of the following actions, depending on the state of the recommendation:

If the update is in this state...	You can perform...
Has not been scheduled	<p><b>Update:</b> Starts the updating process.</p> <p><b>Schedule:</b> Lets you set a date for starting the updating process.</p> <p><b>Dismiss:</b> Removes the recommendation from the list.</p>
Has been scheduled	<p><b>Update:</b> Starts the updating process.</p> <p><b>Edit Schedule:</b> Lets you modify the scheduled date for starting the updating process.</p> <p><b>Cancel Schedule:</b> Cancels the scheduled date.</p>
Has been dismissed	<p><b>Undismiss:</b> Returns the recommendation to the list.</p>
Is being applied or is being downloaded	<p><b>Cancel:</b> Cancels the update.</p>



Updates that were dismissed or failed to install can be viewed in System Manager. Go to **Cluster > Settings > Automatic Update > View All Automatic Updates**.

## Revert ONTAP

### Revert ONTAP overview

To transition a cluster to an earlier ONTAP release, you must perform a reversion.

The information in this section will guide you through the steps you should take before and after you revert, including the resources you should read and the necessary pre- and post-revert checks you should perform.



If you need to transition a cluster from ONTAP 9.1 to ONTAP 9.0, you need to use the downgrade procedure documented [here](#).

## Do I need technical support to revert?

You can revert without assistance on new or test clusters. You should call technical support to revert production clusters. You should also call technical support if you experience any of the following:

- You are in a production environment and revert fails or you encounter any problems before or after the revert such as:
  - The revert process fails and cannot finish.
  - The revert process finishes, but the cluster is unusable in a production environment.
  - The revert process finishes and the cluster goes into production, but you are not satisfied with its behavior.
- You created volumes in ONTAP 9.5 or later and you need to revert to an earlier version. Volumes using adaptive compression must be uncompressed before reverting.

## Revert paths

The version of ONTAP that you can revert to varies based on the version of ONTAP currently running on your nodes. You can use the `system image show` command to determine the version of ONTAP running on each node.

These guidelines refer only to on-premises ONTAP releases. For information about reverting ONTAP in the cloud, see [Reverting or downgrading Cloud Volumes ONTAP](#).

You can revert from...	To...
ONTAP 9.11.1	ONTAP 9.10.1
ONTAP 9.10.1	ONTAP 9.9.1
ONTAP 9.9.1	ONTAP 9.8
ONTAP 9.8	ONTAP 9.7
ONTAP 9.7	ONTAP 9.6
ONTAP 9.6	ONTAP 9.5
ONTAP 9.5	ONTAP 9.4
ONTAP 9.4	ONTAP 9.3
ONTAP 9.3	ONTAP 9.2

You can revert from...	To...
ONTAP 9.2	ONTAP 9.1
ONTAP 9.1 or ONTAP 9	Data ONTAP 8.3.x



If you need to change from ONTAP 9.1 to 9.0, you should follow the [downgrade process](#) documented here.

## What should I read before I revert?

### Resources to review before you revert

Before you revert ONTAP, you should confirm hardware support and review resources to understand issues you might encounter or need to resolve.

1. Review the [ONTAP 9 Release Notes](#) for the target release.

The “Important cautions” section describes potential issues that you should be aware of before downgrading or reverting.

2. Confirm that your hardware platform is supported in the target release.

[NetApp Hardware Universe](#)

3. Confirm that your cluster and management switches are supported in the target release.

You must verify that the NX-OS (cluster network switches), IOS (management network switches), and reference configuration file (RCF) software versions are compatible with the version of ONTAP to which you are reverting.

[NetApp Downloads: Cisco Ethernet Switch](#)

4. If your cluster is configured for SAN, confirm that the SAN configuration is fully supported.

All SAN components—including target ONTAP software version, host OS and patches, required Host Utilities software, and adapter drivers and firmware—should be supported.

[NetApp Interoperability Matrix Tool](#)

### Revert considerations

You need to consider the revert issues and limitations before beginning an ONTAP reversion.

- Reversion is disruptive.

No client access can occur during the reversion. If you are reverting a production cluster, be sure to include this disruption in your planning.

- Reversion affects all nodes in the cluster.

The reversion affects all nodes in the cluster; however, the reversion must be performed and completed on each HA pair before other HA pairs are reverted.

- The reversion is complete when all nodes are running the new target release.

When the cluster is in a mixed-version state, you should not enter any commands that alter the cluster operation or configuration except as necessary to satisfy reversion requirements; monitoring operations are permitted.



If you have reverted some, but not all of the nodes, do not attempt to upgrade the cluster back to the source release.

- When you revert a node, it clears the cached data in a Flash Cache module.

Because there is no cached data in the Flash Cache module, the node serves initial read requests from disk, which results in decreased read performance during this period. The node repopulates the cache as it serves read requests.

- A LUN that is backed up to tape running on ONTAP 9.x can be restored only to 9.x and later releases and not to an earlier release.
- If your current version of ONTAP supports In-Band ACP (IBACP) functionality, and you revert to a version of ONTAP that does not support IBACP, the alternate path to your disk shelf is disabled.
- If LDAP is used by any of your storage virtual machines (SVMs), LDAP referral must be disabled before reversion.
- In MetroCluster IP systems using switches which are MetroCluster compliant but not MetroCluster validated, the reversion from ONTAP 9.7 to 9.6 is disruptive as there is no support for systems using ONTAP 9.6 and earlier.

## Things to verify before you revert

Before revert, you should verify your cluster health, storage health, and system time. You should also delete any cluster jobs that are running and gracefully terminate any SMB sessions that are not continuously available.

### Verify cluster health

Before you revert cluster, you should verify that the nodes are healthy and eligible to participate in the cluster, and that the cluster is in quorum.

1. Verify that the nodes in the cluster are online and are eligible to participate in the cluster: `cluster show`

```
cluster1::> cluster show
Node                Health  Eligibility
-----
node0                true   true
node1                true   true
```

If any node is unhealthy or ineligible, check EMS logs for errors and take corrective action.

2. Set the privilege level to advanced:

```
set -privilege advanced
```

Enter `y` to continue.

3. Verify the configuration details for each RDB process.

- The relational database epoch and database epochs should match for each node.
- The per-ring quorum master should be the same for all nodes.

Note that each ring might have a different quorum master.

To display this RDB process...	Enter this command...
Management application	<code>cluster ring show -unitname mgmt</code>
Volume location database	<code>cluster ring show -unitname vl原因</code>
Virtual-Interface manager	<code>cluster ring show -unitname vifmgr</code>
SAN management daemon	<code>cluster ring show -unitname bcomd</code>

This example shows the volume location database process:

```
cluster1::*> cluster ring show -unitname vl原因
Node      UnitName Epoch    DB Epoch DB Trnxs Master    Online
-----
node0     vl原因      154      154      14847   node0     master
node1     vl原因      154      154      14847   node0     secondary
node2     vl原因      154      154      14847   node0     secondary
node3     vl原因      154      154      14847   node0     secondary
4 entries were displayed.
```

4. Return to the admin privilege level:

```
set -privilege admin
```

5. If you are operating in a SAN environment, verify that each node is in a SAN quorum: `event log show -severity informational -message-name scsibl原因.*`

The most recent scsibl原因 event message for each node should indicate that the scsi-blade is in quorum.

```
cluster1::*> event log show -severity informational -message-name
scsiblade.*
```

Time	Node	Severity	Event
MM/DD/YYYY TIME	node0	INFORMATIONAL	scsiblade.in.quorum: The scsi-blade ...
MM/DD/YYYY TIME	node1	INFORMATIONAL	scsiblade.in.quorum: The scsi-blade ...

## Related information

[System administration](#)

## Verify storage health

Before you revert a cluster, you should verify the status of your disks, aggregates, and volumes.

### 1. Verify disk status:

To check for...	Do this...
Broken disks	<ol style="list-style-type: none"> <li>Display any broken disks: <code>storage disk show -state broken</code></li> <li>Remove or replace any broken disks.</li> </ol>
Disks undergoing maintenance or reconstruction	<ol style="list-style-type: none"> <li>Display any disks in maintenance, pending, or reconstructing states: <code>storage disk show -state maintenance pending reconstructing</code></li> <li>Wait for the maintenance or reconstruction operation to finish before proceeding.</li> </ol>

### 2. Verify that all aggregates are online by displaying the state of physical and logical storage, including storage aggregates: `storage aggregate show -state !online`

This command displays the aggregates that are *not* online. All aggregates must be online before and after performing a major upgrade or reversion.

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

### 3. Verify that all volumes are online by displaying any volumes that are *not* online: `volume show -state !online`

All volumes must be online before and after performing a major upgrade or reversion.

```
cluster1::> volume show -state !online
There are no entries matching your query.
```

4. Verify that there are no inconsistent volumes: `volume show -is-inconsistent true`

See the Knowledge Base article [Volume Showing WAFL Inconsistent](#) on how to address the inconsistent volumes.

### Related information

[Disk and aggregate management](#)

### Verifying the system time

Before you revert, you should verify that NTP is configured, and that the time is synchronized across the cluster.

1. Verify that the cluster is associated with an NTP server: `cluster time-service ntp server show`
2. Verify that each node has the same date and time: `cluster date show`

```
cluster1::> cluster date show
Node          Date                Timezone
-----
node0         4/6/2013 20:54:38   GMT
node1         4/6/2013 20:54:38   GMT
node2         4/6/2013 20:54:38   GMT
node3         4/6/2013 20:54:38   GMT
4 entries were displayed.
```

### Verify that no jobs are running

Before you revert the ONTAP software, you must verify the status of cluster jobs. If any aggregate, volume, NDMP (dump or restore), or Snapshot jobs (such as create, delete, move, modify, replicate, and mount jobs) are running or queued, you must allow the jobs to finish successfully or stop the queued entries.

1. Review the list of any running or queued aggregate, volume, or Snapshot jobs: `job show`



```
cluster1::> job show
```

Job ID	Name	Owning Vserver	Node	State
8629	Vol Reaper Description: Vol Reaper Job	cluster1	-	Queued
8630	Certificate Expiry Check Description: Certificate Expiry Check	cluster1	-	Queued
.				
.				
.				

2. Delete any running or queued aggregate, volume, or Snapshot copy jobs: `job delete -id job_id`

```
cluster1::> job delete -id 8629
```

3. Verify that no aggregate, volume, or Snapshot jobs are running or queued: `job show`

In this example, all running and queued jobs have been deleted:

```
cluster1::> job show
```

Job ID	Name	Owning Vserver	Node	State
9944	SnapMirrorDaemon_7_2147484678 Description: Snapmirror Daemon for 7_2147484678	cluster1	node1	Dormant
18377	SnapMirror Service Job Description: SnapMirror Service Job	cluster1	node0	Dormant

2 entries were displayed

### SMB sessions that should be terminated

Before you revert, you should identify and gracefully terminate any SMB sessions that are not continuously available.

Continuously available SMB shares, which are accessed by Hyper-V or Microsoft SQL Server clients using the SMB 3.0 protocol, do not need to be terminated before upgrading or downgrading.

1. Identify any established SMB sessions that are not continuously available: `vserver cifs session show -continuously-available Yes -instance`

This command displays detailed information about any SMB sessions that have no continuous availability.

You should terminate them before proceeding with the ONTAP downgrade.

```
cluster1::> vserver cifs session show -continuously-available Yes
-instance

                Node: node1
                Vserver: vs1
                Session ID: 1
                Connection ID: 4160072788
Incoming Data LIF IP Address: 198.51.100.5
                Workstation IP address: 203.0.113.20
                Authentication Mechanism: NTLMv2
                Windows User: CIFSLAB\user1
                UNIX User: nobody
                Open Shares: 1
                Open Files: 2
                Open Other: 0
                Connected Time: 8m 39s
                Idle Time: 7m 45s
                Protocol Version: SMB2_1
                Continuously Available: No
1 entry was displayed.
```

2. If necessary, identify the files that are open for each SMB session that you identified: `vserver cifs session file show -session-id session_ID`

```
cluster1::> vserver cifs session file show -session-id 1

Node:          node1
Vserver:       vs1
Connection:    4160072788
Session:       1
File   File      Open Hosting
Continuously
ID     Type        Mode Volume          Share                Available
-----
-----
1      Regular    rw  vol10             homedirshare         No
Path:  \TestDocument.docx
2      Regular    rw  vol10             homedirshare         No
Path:  \file1.txt
2 entries were displayed.
```

## What else should I check before I revert?

### Pre-revert checks

Depending on your environment, you need to consider certain factors before revert. Get started by reviewing the table below to see what special considerations you need to consider.

Ask yourself...	If your answer is yes, then do this...
Is my cluster running SnapMirror?	<ul style="list-style-type: none"><li>• <a href="#">Review considerations for reverting systems with SnapMirror Synchronous relationships</a></li><li>• <a href="#">Review reversion requirements for SnapMirror and SnapVault relationships</a></li></ul>
Is my cluster running SnapLock?	<a href="#">Set autocommit periods</a>
Do I have Split FlexClone volumes?	<a href="#">Reverse physical block sharing</a>
Do I have FlexGroup volumes?	<a href="#">Disable qtree functionality</a>
Do I have CIFS servers in workgroup mode?	<a href="#">Move or delete CIFS servers in workgroup mode</a>
Do I have deduplicated volumes?	<a href="#">Verify volume contains enough free space</a>
Do I have a 2 or 4-node MetroCluster configuration?	<a href="#">Disable automatic unplanned switchover</a>
Do I have Snapshot copies?	<a href="#">Prepare Snapshot copies</a>
Am I reverting to ONTAP 8.3.x?	<a href="#">Identify user accounts that use SHA-2 hash function</a>
Is anti-ransomware protection configured for ONTAP 9.11.1 or later?	<a href="#">Check anti-ransomware licensing</a>

### SnapMirror

#### Considerations for reverting systems with SnapMirror Synchronous relationships

You must be aware of the considerations for SnapMirror Synchronous relationships before reverting from ONTAP 9.6 to ONTAP 9.5.

Before reverting, you must take the following steps if you have SnapMirror Synchronous relationships:

- You must delete any SnapMirror Synchronous relationship in which the source volume is serving data using NFSv4 or SMB.

ONTAP 9.5 does not support NFSv4 and SMB.

- You must delete any SnapMirror Synchronous relationships in a mirror-mirror cascade deployment.

A mirror-mirror cascade deployment is not supported for SnapMirror Synchronous relationships in ONTAP 9.5.

- If the common Snapshot copies in ONTAP 9.5 are not available during revert, you must initialize the SnapMirror Synchronous relationship after reverting.

After two hours of upgrade to ONTAP 9.6, the common Snapshot copies from ONTAP 9.5 are automatically replaced by the common Snapshot copies in ONTAP 9.6. Therefore, you cannot resynchronize the SnapMirror Synchronous relationship after reverting if the common Snapshot copies from ONTAP 9.5 are not available.

### Reversion requirements for SnapMirror and SnapVault relationships

The system node `revert-to` command notifies you of any SnapMirror and SnapVault relationships that need to be deleted or reconfigured for the reversion process to be completed. However, you should be aware of these requirements before you begin the reversion.

- All SnapVault and data protection mirror relationships must be quiesced and then broken.

After the reversion is completed, you can resynchronize and resume these relationships if a common Snapshot copy exists.

- SnapVault relationships must not contain the following SnapMirror policy types:
  - `async-mirror`

You must delete any relationship that uses this policy type.

- `MirrorAndVault`

If any of these relationships exist, you should change the SnapMirror policy to `mirror-vault`.

- All load-sharing mirror relationships and destination volumes must be deleted.
- SnapMirror relationships with FlexClone destination volumes must be deleted.
- Network compression must be disabled for each SnapMirror policy.
- The `all_source_snapshot` rule must be removed from any `async-mirror` type SnapMirror policies.



The Single File Snapshot Restore (SFSR) and Partial File Snapshot Restore (PFSR) operations are deprecated on the root volume.

- Any currently running single file and Snapshot restore operations must be completed before the reversion can proceed.

You can either wait for the restore operation to finish, or you can abort it.

- Any incomplete single file and Snapshot restore operations must be removed by using the `snapmirror restore` command.

### Set autocommit periods for SnapLock volumes before reverting

To revert from ONTAP 9, the value of the autocommit period for SnapLock volumes must be set in hours, not days. Before attempting to revert, you must check the autocommit value for your SnapLock volumes and modify it from days to hours, if necessary.

1. Verify that there are SnapLock volumes in the cluster that have unsupported autocommit periods:

```
volume  
snaplock show -autocommit-period *days
```

2. Modify the unsupported autocommit periods to hours: `volume snaplock modify -vserver vserver_name -volume volume_name -autocommit-period value hours`

### Reverse physical block sharing in split FlexClone volumes

If you have split a FlexClone volume from its parent volume, you must undo the sharing of any physical block between the clone and its parent volume before reverting from ONTAP 9.4 or later to an earlier version of ONTAP.

This task is applicable only for AFF systems when split has been run on any of the FlexClone volumes.

1. Log in to the advanced privilege level: `set -privilege advanced`
2. Identify the split FlexClone volumes with shared physical blocks: `volume clone sharing-by-split show`

```
cluster1::> volume clone sharing-by-split show
Node           Vserver  Volume      Aggregate
-----
node1          vs1      vol_clone1  aggr1
node2          vs2      vol_clone2  aggr2
2 entries were displayed.
```

3. Undo the physical block sharing in all of the split FlexClone volumes across the cluster: `volume clone sharing-by-split undo start-all`
4. Verify that there are no split FlexClone volumes with shared physical blocks: `volume clone sharing-by-split show`

```
cluster1::> volume clone sharing-by-split show
This table is currently empty.
```

### Disable qtree functionality in FlexGroup volumes before reverting

Qtrees for FlexGroup volumes are not supported prior to ONTAP 9.3. You must disable the qtree functionality on FlexGroup volumes before reverting from ONTAP 9.3 to an earlier version of ONTAP.

The qtree functionality is enabled either when you create a qtree or if you modify the security-style and oplock-mode attributes of the default qtree.

1. Identify and delete all of the non-default qtrees in each FlexGroup volume that are enabled with the qtree functionality:
  - a. Log in to the advanced privilege level: `set -privilege advanced`
  - b. Verify if any FlexGroup volume is enabled with the qtree functionality.

For ONTAP 9.6 or later, use: `volume show -is-qtrees-caching-enabled true`

For ONTAP 9.5 or earlier, use: `volume show -is-flexgroup-qtrees-enabled true`

```
cluster1::*> volume show -is-flexgroup-qtrees-enabled true
Vserver   Volume      Aggregate   State      Type      Size
Available Used%
-----
-----
vs0       fg          -           online     RW        320MB
220.4MB  31%
```

c. Delete all of the non-default qtrees in each FlexGroup volume that are enabled with the qtree functionality:

`volume qtree delete -vserver svm_name -volume volume_name -qtree qtree_name`

If the qtree functionality is enabled because you modified the attributes of the default qtree and if you do not have any qtrees, you can skip this step.

```
cluster1::*> volume qtree delete -vserver vs0 -volume fg -qtree
qtree4
WARNING: Are you sure you want to delete qtree qtree4 in volume fg
vserver vs0? {y|n}: y
[Job 38] Job is queued: Delete qtree qtree4 in volume fg vserver vs0.
```

2. Disable the qtree functionality on each FlexGroup volume: `volume flexgroup qtree-disable -vserver svm_name -volume volume_name`

```
cluster1::*> volume flexgroup qtree-disable -vserver vs0 -volume fg
```

3. Identify and delete any Snapshot copies that are enabled with the qtree functionality.

a. Verify if any Snapshot copies are enabled with the qtree functionality: `volume snapshot show`

`-vserver vserver_name -volume volume_name -fields is-flexgroup-qtrees-enabled`

```
cluster1::*> volume snapshot show -vserver vs0 -volume fg -fields is-
flexgroup-qtrees-enabled
vserver volume snapshot is-flexgroup-qtrees-enabled
-----
-----
vs0       fg          fg_snap1 true
vs0       fg          daily.2017-09-27_0010 true
vs0       fg          daily.2017-09-28_0010 true
vs0       fg          snapmirror.0241f354-a865-11e7-a1c0-
00a098a71764_2147867740.2017-10-04_124524 true
```

b. Delete all of the Snapshot copies that are enabled with the qtree functionality: `volume snapshot`

```
delete -vserver svm_name -volume volume_name -snapshot snapshot_name -force true -ignore-owners true
```

The Snapshot copies that must be deleted include regular Snapshot copies and the Snapshot copies taken for SnapMirror relationships. If you have created any SnapMirror relationship for the FlexGroup volumes with a destination cluster that is running ONTAP 9.2 or earlier, you must delete all of the Snapshot copies that were taken when the source FlexGroup volume was enabled for the qtree functionality.

```
cluster1::> volume snapshot delete -vserver vs0 -volume fg -snapshot daily.2017-09-27_0010 -force true -ignore-owners true
```

## Related information

[FlexGroup volumes management](#)

## Identify and move SMB servers in workgroup mode

Before performing a revert, you must delete any SMB servers in workgroup mode or move them in to a domain. Workgroup mode is not supported on ONTAP versions prior to ONTAP 9.

1. Identify any SMB servers with a Authentication Style of workgroup: `vserver cifs show`
2. Move or delete the servers you identified:

If you are going to...	Then use this command....
Move the SMB server from the workgroup to an Active Directory domain:	<code>vserver cifs modify -vserver vserver_name -domain domain_name</code>
Delete the SMB server	<code>vserver cifs delete -vserver vserver_name</code>

3. If you deleted the SMB server, enter the username of the domain, then enter the user password.

## Related information

[SMB management](#)

## Verify deduplicated volumes have enough free space before reverting

Before reverting from any version of ONTAP 9, you must ensure that the volumes contain sufficient free space for the revert operation.

The volume must have enough space to accommodate the savings that were achieved through the inline detection of blocks of zeros. See the Knowledge Base article [How to see space savings from deduplication, compression, and compaction in ONTAP 9](#).

If you have enabled both deduplication and data compression on a volume that you want to revert, then you must revert data compression before reverting deduplication.

1. Use the volume efficiency show command with the -fields option to view the progress of the efficiency operations that are running on the volumes.

The following command displays the progress of efficiency operations: `volume efficiency show -fields vserver,volume,progress`

2. Use the volume efficiency stop command with the -all option to stop all active and queued deduplication operations.

The following command stops all active and queued deduplication operations on volume VolA: `volume efficiency stop -vserver vs1 -volume VolA -all`

3. Use the set -privilege advanced command to log in at the advanced privilege level.
4. Use the volume efficiency revert-to command with the -version option to downgrade the efficiency metadata of a volume to a specific version of ONTAP.

The following command reverts the efficiency metadata on volume VolA to ONTAP 9.x: `volume efficiency revert-to -vserver vs1 -volume VolA -version 9.x`



The volume efficiency revert-to command reverts volumes that are present on the node on which this command is executed. This command does not revert volumes across nodes.

5. Use the volume efficiency show command with the -op-status option to monitor the progress of the downgrade.

The following command monitors and displays the status of the downgrade: `volume efficiency show -vserver vs1 -op-status Downgrading`

6. If the revert does not succeed, use the volume efficiency show command with the -instance option to see why the revert failed.

The following command displays detailed information about all fields: `volume efficiency show -vserver vs1 -volume voll - instance`

7. After the revert operation is complete, return to the admin privilege level: `set -privilege admin`

## [Logical storage management](#)

### **Disable automatic unplanned switchover before reverting two-node and four-node MetroCluster configurations**

Before reverting a two-node or four-node MetroCluster configuration, you must disable automatic unplanned switchover (AUSO).

1. On both the clusters in MetroCluster, disable automatic unplanned switchover: `metrocluster modify -auto-switchover-failure-domain auso-disabled`

#### **Related information**

[MetroCluster management and disaster recovery](#)



## Prepare Snapshot copies before reverting

Before reverting to an earlier ONTAP release, you must disable all Snapshot copy policies and delete any Snapshot copies that were created after upgrading to the current release.

If you are reverting in a SnapMirror environment, you must first have deleted the following mirror relationships:

- All load-sharing mirror relationships
  - Any data protection mirror relationships that were created in ONTAP 8.3.x
  - All data protection mirror relationships if the cluster was re-created in ONTAP 8.3.x
1. Disable Snapshot copy policies for all data SVMs: `volume snapshot policy modify -vserver * -enabled false`
  2. Disable Snapshot copy policies for each node's aggregates:
    - a. Identify the node's aggregates by using the `run-nodenodenameaggr status` command.
    - b. Disable the Snapshot copy policy for each aggregate: `run -node nodename aggr options aggr_name nosnap on`
    - c. Repeat this step for each remaining node.
  3. Disable Snapshot copy policies for each node's root volume:
    - a. Identify the node's root volume by using the `run-nodenodenamevol status` command.

You identify the root volume by the word `root` in the Options column of the `vol status` command output.

```
vs1::> run -node node1 vol status
```

Volume State	Status	Options
vol0 online	raid_dp, flex 64-bit	root, nvfail=on

- b. Disable the Snapshot copy policy on the root volume: `run -node nodename vol options root_volume_name nosnap on`
  - c. Repeat this step for each remaining node.
4. Delete all Snapshot copies that were created after upgrading to the current release:
  - a. Set the privilege level to advanced: `set -privilege advanced`
  - b. Disable the snapshots: `snapshot policy modify -vserver * -enabled false`
  - c. Delete the node's newer-version Snapshot copies: `volume snapshot prepare-for-revert -node nodename`

This command deletes the newer-version Snapshot copies on each data volume, root aggregate, and root volume.

If any Snapshot copies cannot be deleted, the command fails and notifies you of any required actions you must take before the Snapshot copies can be deleted. You must complete the required

actions and then rerun the volume snapshot prepare-for-revert command before proceeding to the next step.

```
cluster1::*> volume snapshot prepare-for-revert -node node1
```

```
Warning: This command will delete all Snapshot copies that have  
the format used by the current version of ONTAP. It will fail if  
any Snapshot copy polices are enabled, or  
if any Snapshot copies have an owner. Continue? {y|n}: y
```

d. Verify that the Snapshot copies have been deleted: `volume snapshot show -node nodename`

```
If any newer-version Snapshot copies remain, force them to be deleted: volume snapshot  
delete {-fs-version 9.0 -node nodename -is-constituent true} -ignore  
-owners -force
```

e. Repeat this step c for each remaining node.

f. Return to the admin privilege level: `set -privilege admin`



You must perform these steps on both the clusters in MetroCluster configuration.

### Identify user accounts that use SHA-2 hash function

If you are reverting from ONTAP 9.1 or ONTAP 9.0 to ONTAP 8.3.x, SHA-2 account users can no longer be authenticated with their passwords. Before you revert, you should identify the user accounts that use the SHA-2 hash function, so that after reverting, you can have them reset their passwords to use the encryption type (MD5) that is supported by the release you revert to.

1. Change to the privilege setting to advanced: `set -privilege advanced`
2. Identify the user accounts that use the SHA-2 has function: `security login show -vserver * -username * -application * -authentication-method password -hash-function !md5`
3. Retain the command output for use after the revert.



During the revert, you will be prompted to run the advanced command `security login password-prepare-to-downgrade` to reset your own password to use the MD5 hash function. If your password is not encrypted with MD5, the command prompts you for a new password and encrypts it with MD5, enabling your credential to be authenticated after the revert.

### Check Autonomous Ransomware Protection licensing before reverting from ONTAP 9.11.1 or later

If you have configured Autonomous Ransomware Protection (ARP) and you revert from ONTAP 9.11.1 or later to ONTAP 9.10.1 or earlier, you might experience warning messages and limited ARP functionality.

In ONTAP 9.11.1, the Anti-ransomware license replaced the Multi-Tenant Key Management (MTKM) license. If your system has the Anti\_ransomware license but no MT\_EK\_MGMT license, you will see a warning during

revert that ARP cannot be enabled on new volumes upon revert.

The volumes with existing protection will continue to work normally after revert, and ARP status can be displayed using the ONTAP CLI. However, System Manager cannot show ARP status without the MTKM license.

Therefore, if you want ARP to continue after reverting to ONTAP 9.10.1, be sure the MTKM license is installed before reverting. [Learn about ARP licensing](#).

## Download and install the ONTAP software image

You must first download the ONTAP software from the NetApp Support site; then you can install it.

### Download the software image

To downgrade or revert from ONTAP 9.4 and later, you can copy the ONTAP software image from the NetApp Support Site to a local folder. For a downgrade or revert to ONTAP 9.3 or earlier, you must copy the ONTAP software image to an HTTP server or FTP server on your network.

You should note the following important information:

- Software images are specific to platform models.

You must obtain the correct image for your cluster. Software images, firmware version information, and the latest firmware for your platform model are available on the NetApp Support Site.

- Software images include the latest version of system firmware that was available when a given version of ONTAP was released.
- If you are downgrading a system with NetApp Volume Encryption from ONTAP 9.5 or later, you must download the ONTAP software image for non-restricted countries, which includes NetApp Volume Encryption.

If you use the ONTAP software image for restricted countries to downgrade or revert a system with NetApp Volume Encryption, the system panics and you lose access to your volumes.

1. Locate the target ONTAP software in the [Software Downloads](#) area of the NetApp Support Site.
2. Copy the software image.
  - For ONTAP 9.3 or earlier, copy the software image (for example, 93\_q\_image.tgz) from the NetApp Support Site to the directory on the HTTP server or FTP server from which the image will be served.
  - For ONTAP 9.4 or later, copy the software image (for example, 97\_q\_image.tgz) from the NetApp Support Site to the directory on the HTTP server or FTP server from which the image will be served or to a local folder.

### Install the software image

You must install the target software image on the cluster's nodes.

- If you are downgrading or reverting a system with NetApp Volume Encryption from ONTAP 9.5 or later, you must have downloaded the ONTAP software image for non-restricted countries, which includes NetApp Volume Encryption.

If you use the ONTAP software image for restricted countries to downgrade or revert a system with NetApp Volume Encryption, the system panics and you lose access to your volumes.

1. Set the privilege level to advanced, entering **y** when prompted to continue: `set -privilege advanced`

The advanced prompt (**\*>**) appears.

2. Install the software image on the nodes.

This command downloads and installs the software image on all of the nodes simultaneously. To download and install the image on each node one at a time, do not specify the `-background` parameter.

- If you are downgrading or reverting a non-MetroCluster configuration or a two-node MetroCluster configuration: `system node image update -node * -package location -replace -package true -setdefault true -background true`

This command uses an extended query to change the target software image, which is installed as the alternate image, to be the default image for the node.

- If you are downgrading or reverting a four or eight-node MetroCluster configuration, you must issue the following command on both clusters: `system node image update -node * -package location -replace-package true true -background true -setdefault false`

This command uses an extended query to change the target software image, which is installed as the alternate image on each node.

3. Enter **y** to continue when prompted.

4. Verify that the software image is downloaded and installed on each node: `system node image show-update-progress -node *`

This command displays the current status of the software image download and installation. You should continue to run this command until all nodes report a Run Status of Exited, and an Exit Status of Success.

The system node image update command can fail and display error or warning messages. After resolving any errors or warnings, you can run the command again.

This example shows a two-node cluster in which the software image is downloaded and installed successfully on both nodes:

```

cluster1::*> system node image show-update-progress -node *
There is no update/install in progress
Status of most recent operation:
    Run Status:      Exited
    Exit Status:     Success
    Phase:           Run Script
    Exit Message:    After a clean shutdown, image2 will be set as
the default boot image on node0.
There is no update/install in progress
Status of most recent operation:
    Run Status:      Exited
    Exit Status:     Success
    Phase:           Run Script
    Exit Message:    After a clean shutdown, image2 will be set as
the default boot image on node1.
2 entries were acted on.

```

## Revert an ONTAP cluster

To take the cluster offline to revert to an earlier ONTAP release, you must disable storage failover and the data LIFs, address reversion preconditions, revert the cluster and file system configurations on a node, and then repeat the process for each additional node in the cluster.

You must have completed the revert [verifications](#) and [pre-checks](#).

Reverting a cluster requires you to take the cluster offline for the duration of the reversion.

1. Set the privilege level from admin to advanced, entering **y** when prompted to continue: `set -privilege advanced`

The advanced prompt (`*>`) appears.

2. Verify that the target ONTAP software is installed: `system image show`

The following example shows that version 9.1 is installed as the alternate image on both nodes:

```

cluster1::*> system image show
          Is      Is      Install
Node      Image  Default Current Version  Date
-----  -
node0
  image1  true   true   9.2    MM/DD/YYYY TIME
  image2  false  false  9.1    MM/DD/YYYY TIME
node1
  image1  true   true   9.2    MM/DD/YYYY TIME
  image2  false  false  9.1    MM/DD/YYYY TIME
4 entries were displayed.

```

3. Disable all of the data LIFs in the cluster: `network interface modify {-role data} -status -admin down`
4. If the cluster consists of only two nodes, disable cluster HA: `cluster ha modify -configured false`
5. Disable storage failover for the nodes in the HA pair from either node: `storage failover modify -node nodename -enabled false`

You only need to disable storage failover once for the HA pair. When you disable storage failover for a node, storage failover is also disabled on the node's partner.

6. Log in to the node that you want to revert.

To revert a node, you must be logged in to the cluster through the node's node management LIF.

7. Set the node's target ONTAP software image to be the default image: `system image modify -node nodename -image target_image -isdefault true`
8. Verify that the target ONTAP software image is set as the default image for the node that you are reverting: `system image show`

The following example shows that version 9.1 is set as the default image on node0:

```

cluster1::*> system image show
          Is      Is      Install
Node      Image  Default Current Version  Date
-----  -
node0
  image1  false  true   9.2    MM/DD/YYYY TIME
  image2  true   false  9.1    MM/DD/YYYY TIME
node1
  image1  true   true   9.2    MM/DD/YYYY TIME
  image2  false  false  9.1    MM/DD/YYYY TIME
4 entries were displayed.

```

9. If the cluster consists of only two nodes, verify that the node does not hold epsilon:

- a. Check whether the node currently holds epsilon: `cluster show -node nodename`

The following example shows that the node holds epsilon:

```
cluster1::*> cluster show -node node1

      Node: node1
      UUID: 026efc12-ac1a-11e0-80ed-0f7eba8fc313
      Epsilon: true
      Eligibility: true
      Health: true
```

- b. If the node holds epsilon, mark epsilon as false on the node so that epsilon can be transferred to the node's partner: `cluster modify -node nodenameA -epsilon false`

- c. Transfer epsilon to the node's partner by marking epsilon true on the partner node: `cluster modify -node nodenameB -epsilon true`

10. Verify that the node is ready for reversion: `system node revert-to -node nodename -check -only true -version 9.x`

The check-only parameter identifies any preconditions that must be addressed before reverting, such as the following examples:

- Disabling storage failover
- Disabling the Snapshot policy
- Deleting Snapshot copies that were created after upgrading to the later version of ONTAP

11. Verify that all of the preconditions have been addressed: `system node revert-to -node nodename -check-only true -version 9.x`

12. Revert the cluster configuration of the node: `system node revert-to -node nodename -version 9.x`

The `-version` option refers to the target release. For example, if the software you installed and verified is ONTAP 9.1, the correct value of the `-version` option is 9.1.

The cluster configuration is reverted, and then you are logged out of the clustershell.

13. Log back in to the clustershell, and then switch to the nodeshell: `run -node nodename`

After logging on the clustershell again, it might take a few minutes before it is ready to accept the nodeshell command. So, if the command fails, wait a few minutes and try it again.

14. Revert the file system configuration of the node: `revert_to 9.x`

This command verifies that the node's file system configuration is ready to be reverted, and then reverts it. If any preconditions are identified, you must address them and then rerun the `revert_to` command.



Using a system console to monitor the revert process displays greater details than seen in nodeshell.

If AUTOBOOT is true, when the command finishes, the node will reboot to ONTAP.

If AUTOBOOT is false, when the command finishes the LOADER prompt is displayed. Enter `yes` to revert; then use `boot_ontap` to manually reboot the node.

- After the node has rebooted, confirm that the new software is running: `system node image show`

In the following example, image1 is the new ONTAP version and is set as the current version on node0:

```
cluster1::*> system node image show
```

Node	Image	Is Default	Is Current	Version	Install Date
node0					
	image1	true	true	X.X.X	MM/DD/YYYY TIME
	image2	false	false	Y.Y.Y	MM/DD/YYYY TIME
node1					
	image1	true	false	X.X.X	MM/DD/YYYY TIME
	image2	false	true	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

- Verify that the revert status is complete for each node: `system node upgrade-revert show -node nodename`

The status should be listed as complete.

- Repeat [step-5] through [step-17] on the other node in the HA pair.
- If the cluster consists of only two nodes, reenabling cluster HA: `cluster ha modify -configured true`
- Reenable storage failover on both nodes if it was previously disabled: `storage failover modify -node nodename -enabled true`
- Repeat [step-6] through [step-18] for each additional HA pair and both the clusters in MetroCluster Configuration.

## What should I do after reverting my cluster?

### Verify cluster and storage health after downgrade or revert

After you downgrade or revert a cluster, you should verify that the nodes are healthy and eligible to participate in the cluster, and that the cluster is in quorum. You should also verify the status of your disks, aggregates, and volumes.



## Verify cluster health

1. Verify that the nodes in the cluster are online and are eligible to participate in the cluster: `cluster show`

```
cluster1::> cluster show
Node           Health Eligibility
-----
node0          true  true
node1          true  true
```

If any node is unhealthy or ineligible, check EMS logs for errors and take corrective action.

2. Set the privilege level to advanced:

```
set -privilege advanced
```

Enter `y` to continue.

3. Verify the configuration details for each RDB process.

- The relational database epoch and database epochs should match for each node.
- The per-ring quorum master should be the same for all nodes.

Note that each ring might have a different quorum master.

To display this RDB process...	Enter this command...
Management application	<code>cluster ring show -unitname mgmt</code>
Volume location database	<code>cluster ring show -unitname vldb</code>
Virtual-Interface manager	<code>cluster ring show -unitname vifmgr</code>
SAN management daemon	<code>cluster ring show -unitname bcomd</code>

This example shows the volume location database process:

```
cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch   DB Epoch DB Trnxs Master  Online
-----
node0     vldb      154      154      14847   node0   master
node1     vldb      154      154      14847   node0   secondary
node2     vldb      154      154      14847   node0   secondary
node3     vldb      154      154      14847   node0   secondary
4 entries were displayed.
```

4. Return to the admin privilege level: `set -privilege admin`

- If you are operating in a SAN environment, verify that each node is in a SAN quorum: `event log show -severity informational -message-name scsiblade.*`

The most recent scsiblade event message for each node should indicate that the scsi-blade is in quorum.

```
cluster1::*> event log show -severity informational -message-name
scsiblade.*
Time                Node          Severity      Event
-----
MM/DD/YYYY TIME    node0         INFORMATIONAL scsiblade.in.quorum: The
scsi-blade ...
MM/DD/YYYY TIME    node1         INFORMATIONAL scsiblade.in.quorum: The
scsi-blade ...
```

## Related information

[System administration](#)

### Verify storage health

After you revert or downgrade a cluster, you should verify the status of your disks, aggregates, and volumes.

- Verify disk status:

To check for...	Do this...
Broken disks	<ol style="list-style-type: none"> <li>Display any broken disks: <code>storage disk show -state broken</code></li> <li>Remove or replace any broken disks.</li> </ol>
Disks undergoing maintenance or reconstruction	<ol style="list-style-type: none"> <li>Display any disks in maintenance, pending, or reconstructing states: <code>storage disk show -state maintenance pending reconstructing</code></li> <li>Wait for the maintenance or reconstruction operation to finish before proceeding.</li> </ol>

- Verify that all aggregates are online by displaying the state of physical and logical storage, including storage aggregates: `storage aggregate show -state !online`

This command displays the aggregates that are *not* online. All aggregates must be online before and after performing a major upgrade or reversion.

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

- Verify that all volumes are online by displaying any volumes that are *not* online: `volume show -state`

!online

All volumes must be online before and after performing a major upgrade or reversion.

```
cluster1::> volume show -state !online
There are no entries matching your query.
```

4. Verify that there are no inconsistent volumes: `volume show -is-inconsistent true`

See the Knowledge Base article [Volume Showing WAFL Inconsistent](#) on how to address the inconsistent volumes.

### Related information

[Disk and aggregate management](#)

### Enable automatic switchover for MetroCluster configurations

This topic provides information regarding the additional tasks that you must perform after the reversion of MetroCluster configurations.

1. Enable automatic unplanned switchover: `metrocluster modify -auto-switchover-failure -domain auto-on-cluster-disaster`
2. Validate the MetroCluster configuration: `metrocluster check run`

### Enable and revert LIFs to home ports after a revert

During a reboot, some LIFs might have been migrated to their assigned failover ports. After you revert a cluster, you must enable and revert any LIFs that are not on their home ports.

The network interface revert command reverts a LIF that is not currently on its home port back to its home port, provided that the home port is operational. A LIF's home port is specified when the LIF is created; you can determine the home port for a LIF by using the network interface show command.

1. Display the status of all LIFs: `network interface show`

This example displays the status of all LIFs for a storage virtual machine (SVM).

```

cluster1::> network interface show -vserver vs0
          Logical      Status      Network      Current
Current Is
Vserver   Interface  Admin/Oper  Address/Mask  Node      Port
Home
-----
vs0
          data001    down/down  192.0.2.120/24  node0     e0e
true
          data002    down/down  192.0.2.121/24  node0     e0f
true
          data003    down/down  192.0.2.122/24  node0     e2a
true
          data004    down/down  192.0.2.123/24  node0     e2b
true
          data005    down/down  192.0.2.124/24  node0     e0e
false
          data006    down/down  192.0.2.125/24  node0     e0f
false
          data007    down/down  192.0.2.126/24  node0     e2a
false
          data008    down/down  192.0.2.127/24  node0     e2b
false
8 entries were displayed.

```

If any LIFs appear with a Status Admin status of down or with an Is home status of false, continue with the next step.

2. Enable the data LIFs: `network interface modify {-role data} -status-admin up`

```

cluster1::> network interface modify {-role data} -status-admin up
8 entries were modified.

```

3. Revert LIFs to their home ports: `network interface revert *`

This command reverts all LIFs back to their home ports.

```

cluster1::> network interface revert *
8 entries were acted on.

```

4. Verify that all LIFs are in their home ports: `network interface show`

This example shows that all LIFs for SVM vs0 are on their home ports.

```

cluster1::> network interface show -vserver vs0
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper  Address/Mask  Node      Port
Home
-----
vs0
      data001      up/up      192.0.2.120/24  node0      e0e
true
      data002      up/up      192.0.2.121/24  node0      e0f
true
      data003      up/up      192.0.2.122/24  node0      e2a
true
      data004      up/up      192.0.2.123/24  node0      e2b
true
      data005      up/up      192.0.2.124/24  node1      e0e
true
      data006      up/up      192.0.2.125/24  node1      e0f
true
      data007      up/up      192.0.2.126/24  node1      e2a
true
      data008      up/up      192.0.2.127/24  node1      e2b
true
8 entries were displayed.

```

### Enable Snapshot copy policies after reverting

After reverting to an earlier version of ONTAP, you must enable Snapshot copy policies to start creating Snapshot copies again.

You are reenabling the Snapshot schedules that you disabled before you reverted to an earlier version of ONTAP.

1. Enable Snapshot copy policies for all data SVMs:

```
volume snapshot policy modify -vserver * -enabled true
```

```
snapshot policy modify pg-rpo-hourly -enable true
```

2. For each node, enable the Snapshot copy policy of the root volume by using the run-nodenodenamevol optionsroot\_vol\_namenosnap off command.

```
cluster1::> run -node node1 vol options vol0 nosnap off
```

## Verify client access (SMB and NFS)

For the configured protocols, test access from SMB and NFS clients to verify that the cluster is accessible.

## Verify IPv6 firewall entries

A reversion from any version of ONTAP 9 might result in missing default IPv6 firewall entries for some services in firewall policies. You need to verify that the required firewall entries have been restored to your system.

1. Verify that all firewall policies are correct by comparing them to the default policies: `system services firewall policy show`

The following example shows the default policies:

```
cluster1::*> system services firewall policy show
Policy           Service      Action IP-List
-----
cluster
    dns          allow  0.0.0.0/0
    http         allow  0.0.0.0/0
    https        allow  0.0.0.0/0
    ndmp         allow  0.0.0.0/0
    ntp          allow  0.0.0.0/0
    rsh          allow  0.0.0.0/0
    snmp         allow  0.0.0.0/0
    ssh          allow  0.0.0.0/0
    telnet       allow  0.0.0.0/0
data
    dns          allow  0.0.0.0/0, ::/0
    http         deny   0.0.0.0/0, ::/0
    https        deny   0.0.0.0/0, ::/0
    ndmp         allow  0.0.0.0/0, ::/0
    ntp          deny   0.0.0.0/0, ::/0
    rsh          deny   0.0.0.0/0, ::/0
.
.
.
```

2. Manually add any missing default IPv6 firewall entries by creating a new firewall policy: `system services firewall policy create`

```
cluster1::*> system services firewall policy create -policy newIPv6
-service ssh -action allow -ip-list ::/0
```

3. Apply the new policy to the LIF to allow access to a network service: `network interface modify`

```
cluster1::*> network interface modify -vserver VS1 -lif LIF1
-firewall-policy newIPv6
```

### Revert password hash function to the supported encryption type

If you reverted from ONTAP 9.1 or ONTAP 9.0 to ONTAP 8.3.x, SHA-2 account users can no longer be authenticated with their passwords. Passwords must be reset to use the MDS encryption type.

1. Set a temporary password for each SHA-2 user account that you [identified prior to reverting](#): `security login password -username user_name -vserver vserver_name`
2. Communicate the temporary password to the affected users and have them log in through a console or SSH session to change their passwords as prompted by the system.

### Considerations for whether to manually update the SP firmware

If the SP automatic update functionality is enabled (the default), downgrading or reverting to ONTAP 8.3.x does not require a manual SP firmware update. The SP firmware is automatically updated to the newest compatible version that is supported by the ONTAP version you reverted or downgraded to.

If the SP automatic update functionality is disabled (not recommended), after the ONTAP revert or downgrade process is complete, you must manually update the SP firmware to a version that is supported for the ONTAP version you reverted or downgraded to.

[NetApp BIOS/ONTAP Support Matrix](#)

[NetApp Downloads: System Firmware and Diagnostics](#)

### Change in user accounts that can access the Service Processor

If you created user accounts on ONTAP 9.8 or earlier, upgraded to ONTAP 9.9.1 or later (when the `-role` parameter is changed to `admin`), and then reverted back to ONTAP 9.8 or earlier, the `-role` parameter is restored to its original value. You should nonetheless verify that the modified values are acceptable.

During revert, if the role for an SP user has been deleted, the "rbac.spuser.role.notfound" EMS message will be logged.

For more information, see [Accounts that can access the SP](#).

# Cluster administration

## Cluster management with System Manager

### Administration overview with System Manager

System Manager is a graphical management interface that enables you to use a web browser to manage storage systems and storage objects (such as disks, volumes, and storage tiers) and perform common management tasks related to storage systems.

The procedures in this section help you manage your cluster with System Manager in ONTAP 9.7 and later releases.



- Beginning with ONTAP 9.8, System Manager is no longer available as an executable file and is included with ONTAP software as a web service, enabled by default, and accessible by using a browser.
- The name of System Manager has changed beginning with ONTAP 9.6. In ONTAP 9.5 and earlier it was called OnCommand System Manager. Beginning with ONTAP 9.6 and later, it is called System Manager.
- If you are using the classic System Manager (available only in ONTAP 9.7 and earlier), refer to [System Manager Classic \(ONTAP 9.0 to 9.7\)](#)

Using the System Manager Dashboard, you can view at-a-glance information about important alerts and notifications, the efficiency and capacity of storage tiers and volumes, the nodes that are available in a cluster, the status of the nodes in an HA pair, the most active applications and objects, and the performance metrics of a cluster or a node.

With System Manager you can perform many common tasks, such as the following:

- Create a cluster, configure a network, and set up support details for the cluster.
- Configure and manage storage objects, such as disks, local tiers, volumes, qtrees, and quotas.
- Configure protocols, such as SMB and NFS, and provision file sharing.
- Configure protocols such as FC, FCoE, NVMe, and iSCSI for block access.
- Create and configure network components, such as subnets, broadcast domains, data and management interfaces, and interface groups.
- Set up and manage mirroring and vaulting relationships.
- Perform cluster management, storage node management, and storage virtual machine (storage VM) management operations.
- Create and configure storage VMs, manage storage objects associated with storage VMs, and manage storage VM services.
- Monitor and manage high-availability (HA) configurations in a cluster.
- Configure service processors to remotely log in, manage, monitor, and administer the node, regardless of the state of the node.



## System Manager terminology

System Manager uses different terminology than the CLI for some ONTAP key functionality.

- **Local tier** – a set of physical solid-state drives or hard-disk drives you store your data on. You might know these as aggregates. In fact, if you use the ONTAP CLI, you will still see the term *aggregate* used to represent a local tier.
- **Cloud tier** – storage in the cloud used by ONTAP when you want to have some of your data off premises for one of several reasons. If you are thinking of the cloud part of a FabricPool, you've already figured it out. And if you are using a StorageGRID system, your cloud might not be off premises at all. (A cloud-like experience on premises is called a *private cloud*.)
- **Storage VM** – a virtual machine running within ONTAP that provides storage and data services to your clients. You might know this as an *SVM* or a *vserver*.
- **Network interface** - an address and properties assigned to a physical network port. You might know this as a *logical interface (LIF)*.
- **Pause** - an action that halts operations. Before ONTAP 9.8, you might have referred to *quiesce* in other versions of System Manager.

## Use System Manager to access a cluster

If you prefer to use a graphic interface instead of the command-line interface (CLI) for accessing and managing a cluster, you can do so by using System Manager, which is included with ONTAP as a web service, is enabled by default, and is accessible by using a browser.

### What you'll need

- You must have a cluster user account that is configured with the `admin` role and the `http` and `console` application types.
- You must have enabled cookies and site data in the browser.

### About this task

You can use a cluster management network interface (LIF) or node management network interface (LIF) to access System Manager. For uninterrupted access to System Manager, you should use a cluster management network interface (LIF).

### Steps

1. Point the web browser to the IP address of the cluster management network interface:
  - If you are using IPv4: `https://cluster-mgmt-LIF`
  - If you are using IPv6: `https://[cluster-mgmt-LIF]`



Only HTTPS is supported for browser access of System Manager.

If the cluster uses a self-signed digital certificate, the browser might display a warning indicating that the certificate is not trusted. You can either acknowledge the risk to continue the access or install a Certificate Authority (CA) signed digital certificate on the cluster for server authentication.

2. **Optional:** If you have configured an access banner by using the CLI, then read the message that is displayed in the **Warning** dialog box, and choose the required option to proceed.

This option is not supported on systems on which Security Assertion Markup Language (SAML) authentication is enabled.

- If you do not want to continue, click **Cancel**, and close the browser.
- If you want to continue, click **OK** to navigate to the System Manager login page.

3. Log in to System Manager by using your cluster administrator credentials.



Beginning with ONTAP 9.11.1, when you log in to System Manager, you can specify the locale. The locale specifies certain localization settings, such as language, currency, time and date format, and similar settings. For ONTAP 9.10.1 and earlier, the locale is detected from the browser. To change the locale, you have to change the locale of the browser.

### Related information

[Managing access to web services](#)

[Accessing a node's log, core dump, and MIB files by using a web browser](#)


## Enable new features by adding license keys

Some ONTAP features are enabled by license keys. You can add license keys using System Manager.

Beginning with ONTAP 9.10.1, you use System Manager to install a NetApp License File to enable multiple licensed features all at once. Using a NetApp License File simplifies license installation because you no longer have to add separate feature license keys. You download the NetApp License File from the NetApp Support Site.

If you already have license keys for some features and you are upgrading to ONTAP 9.10.1, you can continue to use those license keys.

### Steps

1. Click **Cluster > Settings**.
2. Under **License**, click .
3. Click **Browse** to locate and select the NetApp License File you downloaded.
4. If you have license keys you want to add, select **Use 28-character license keys** and enter the keys.

## View and submit support cases

Beginning with ONTAP 9.9.1, you can view support cases from Active IQ associated with the cluster. You can also copy cluster details that you need to submit a new support case on the NetApp Support Site.

Beginning with ONTAP 9.10.1, you can enable telemetry logging, which helps support personnel troubleshoot problems.



To receive alerts about firmware updates, you must be registered with Active IQ Unified Manager. Refer to [Active IQ Unified Manager documentation resources](#).

### Steps

1. In System Manager, select **Support**.

A list of open support cases associated with this cluster is displayed.

2. Click on the following links to perform procedures:
  - **Case Number**: See details about the case.
  - **Go to NetApp Support Site**: Navigate to the **My AutoSupport** page on the NetApp Support Site to view knowledge base articles or submit a new support case.
  - **View My Cases**: Navigate to the **My Cases** page on the NetApp Support Site.
  - **View Cluster Details**: View and copy information you will need when you submit a new case.

## Enable telemetry logging

Beginning with ONTAP 9.10.1, you can use System Manager to enable telemetry logging. When telemetry logging is allowed, messages that are logged by System Manager are given a specific telemetry identifier that indicates the exact process that triggered the message. All messages that are issued relating to that process have the same identifier, which consists of the name of the operational workflow and a number (for example "add-volume-1941290").

If you experience performance problems, you can enable telemetry logging, which allows support personnel to more easily identify the specific process for which a message was issued. When telemetry identifiers are added to the messages, the log file is only slightly enlarged.

### Steps

1. In System Manager, select **Cluster > Settings**.
2. In **UI Settings** section, click the check box for **Allow telemetry logging**.

## Monitor risks

Beginning with ONTAP 9.10.0, you can use System Manager to monitor the risks reported by Active IQ Digital Advisor. Beginning with ONTAP 9.10.1, you can use System Manager to also acknowledge the risks.

NetApp Active IQ Digital Advisor reports opportunities to reduce risk and improve the performance and efficiency of your storage environment. With System Manager, you can learn about risks reported by Active IQ and receive actionable intelligence that helps you administer storage and achieve higher availability, improved security, and better storage performance.

### Link to your Active IQ account

To receive information about risks from Active IQ, you should first link to your Active IQ account from System Manager.

### Steps

1. In System Manager, click **Cluster > Settings**.
2. Under **Active IQ Registration**, click **Register**.
3. Enter your credentials for Active IQ.
4. After your credentials are authenticated, click **Confirm to link Active IQ with System Manager**.

## View the number of risks

Beginning with ONTAP 9.10.0, you can view from the dashboard in System Manager the number of risks reported by Active IQ.

### Before you begin

You must establish a connection from System Manager to your Active IQ account. Refer to [Link to your Active IQ account](#).

### Steps

1. In System Manager, click **Dashboard**.
2. In the **Health** section, view the number of reported risks.



You can view more detailed information about each risk by clicking the message showing the number of risks. See [View details of risks](#).

## View details of risks

Beginning with ONTAP 9.10.0, you can view from System Manager how the risks reported by Active IQ are categorized by impact areas. You can also view detailed information about each reported risk, its potential impact on your system, and corrective actions you can take.

### Before you begin

You must establish a connection from System Manager to your Active IQ account. Refer to [Link to your Active IQ account](#).

### Steps

1. Click **Events > All Events**.
2. In the **Overview** section, under **Active IQ Suggestions**, view the number of risks in each impact area category. The risk categories include:
  - Performance & efficiency
  - Availability & protection
  - Capacity
  - Configuration
  - Security
3. Click on the **Active IQ Suggestions** tab to view information about each risk, including the following:
  - Level of impact to your System
  - Category of the risk
  - Nodes that are affected
  - Type of mitigation needed
  - Corrective actions you can take

## Acknowledge risks

Beginning with ONTAP 9.10.1, you can use System Manager to acknowledge any of the open risks.

### Steps

1. In System Manager, display the list of risks by performing the procedure in [View details of risks](#).
2. Click on the risk name of an open risk that you want to acknowledge.
3. Enter information into the following fields:
  - Reminder (date)
  - Justification
  - Comments
4. Click **Acknowledge**.



After you acknowledge a risk, it takes a few minutes for the change to be reflected in the list of Active IQ suggestions.

## Unacknowledge risks

Beginning with ONTAP 9.10.1, you can use System Manager to unacknowledge any risk that was previously acknowledged.

### Steps

1. In System Manager, display the list of risks by performing the procedure in [View details of risks](#).
2. Click on the risk name of an acknowledged risk that you want to unacknowledge.
3. Enter information into the following fields:
  - Justification
  - Comments
4. Click **Unacknowledge**.



After you unacknowledge a risk, it takes a few minutes for the change to be reflected in the list of Active IQ suggestions.

## Gain insights to help optimize your system

With System Manager, you can view insights that help you optimize your system.

### About this task

Beginning with ONTAP 9.11.0, you can view insights in System Manager that help you optimize the capacity and security compliance of your system.

Beginning with ONTAP 9.11.1, you can view additional insights that help you optimize the capacity, security compliance, and configuration of your system.





Based on best practices, these insights are displayed on one page from which you can initiate immediate actions to optimize your system.

### View optimization insights

#### Steps

1. In System Manager, click **Insights** in the left-hand navigation column.

The **Insights** page shows groups of insights. Each group of insights might contain one or more insights. The following groups are displayed:

- Needs your attention
  - Remediate risks
  - Optimize your storage
2. (Optional) Filter the insights that are displayed by clicking these buttons in the upper-right corner of the page:
-  Displays the security-related insights.
  -  Displays the capacity-related insights.
  -  Displays the configuration-related insights.
  -  Displays all of the insights.

## Respond to insights to optimize your system

In System Manager, you can respond to insights by either dismissing them, exploring different ways to remediate the problems, or initiating the process to fix the problems.

### Steps

1. In System Manager, click **Insights** in the left-hand navigation column.
2. Hover over an insight to reveal the buttons to perform the following actions:
  - **Dismiss**: Remove the insight from the view. To “undismiss” the insight, refer to [Customize the settings for insights](#).
  - **Explore**: Find out various ways to remediate the problem mentioned in the insight. This button appears only if there is more than one method of remediation.
  - **Fix**: Initiate the process of remediating the problem mentioned in the insight. You will be asked to confirm whether you want to take the action needed to apply the fix.




Some of these actions can be initiated from other pages in System Manager, but the **Insights** page helps you streamline your day-to-day tasks by allowing you to initiate these action from this one page.

## Customize the settings for insights

You can customize which insights you will notified about in System Manager.

### Steps

1. In System Manager, click **Insights** in the left-hand navigation column.
2. In the upper-right corner of the page, click , then select **Settings**.
3. On the **Settings** page, ensure there is a check in the check boxes next to the insights you want to be notified about. If you previously dismissed an insight, you can “undismiss” it by ensuring a check is in its check box.

4. Click **Save**.

### **Export the insights as a PDF file**

You can export all applicable insights as a PDF file.

#### **Steps**

1. In System Manager, click **Insights** in the left-hand navigation column.
2. In the upper-right corner of the page, click , then select **Export**.

### **View hardware configurations to determine problems**

With ONTAP 9.8 and later, you can use System Manager to view the configuration of hardware on your network and determine if problems might arise.

#### **Steps**

To view hardware configurations, perform the following steps:

1. In System Manager, select **Cluster > Hardware**.
2. Hover your mouse over components to view status and other details.

You can view various types of information:

- [Information about controllers](#)
- [Information about disk shelves](#)
- [Information about storage switches](#)

#### **Information about controllers**

You can view the following:

## Nodes

### Nodes:

- Front and rear views are displayed.
- Models with an internal disk shelf also show the disk layout in the front view.
- You can view the following platform models:

If your system is running...	Then you can use System Manager to view...
ONTAP 9.8	A220, A300, A400, A700, and C190 (Only a <i>preview</i> of this feature is available.)
ONTAP 9.9.1	A220, A250, A300, A320, A400, A700, A700s, A800, C190, and FAS500f
ONTAP 9.10.1	A220, A250, A300, A320, A400, A700, A700s, A800, A900, C190, and FAS500f.
ONTAP 9.11.1	A220, A250, A300, A320, A400, A700, A700s, A800, A900, C190, FAS2720, FAS2750, FAS500F, FAS8300, FAS8700, FAS9000, and FAS9500

## Ports

### Ports:

- Console ports are not shown.
- A port is red if it is down.
- The status of a port and other details are shown when you hover over the port.

### Notes:

- For ONTAP 9.10.1 and earlier, SAS ports are displayed in red when they are disabled.
- Beginning with 9.11.1, SAS ports are highlighted in red only if they are in an error state or if a cabled port that is being used goes offline. The ports are shown in white if they are offline and uncabled.

## FRUs

### FRUs:

Information about FRUs appears only when the state of a FRU is non-optimal.

- Failed PSUs in nodes or chassis.
- High temperatures detected in nodes.
- Failed fans on the nodes or chassis.

## Adapter cards

### Adapter cards:

- Cards with defined part number fields are shown in the slots if external cards have been inserted.



- Ports on cards are shown.
- Certain cards are shown with specific images of the cards. If the card is not in the list of supported part numbers, then a generic graphic is displayed.

## Information about disk shelves

You can view the following:

### Disk shelves

#### Disk shelves:

- Front and rear views are displayed.
- You can view the following disk shelf models:

If your system is running...	Then you can use System Manager to view...
ONTAP 9.8	DS4243, DS4486, DS212C, DS2246, DS224C, and NS224
ONTAP 9.9.1 and later	All non-EOS and non-EOA shelves

### Shelf ports

#### Shelf ports:

- Port status is displayed.
- Remote port information is shown if the port is connected.

### Shelf FRUs

#### Shelf FRUs:

- PSU failure information is shown.

## Information about storage switches

You can view the following:

## Storage switches

### Storage switches:

- The display shows switches that act as storage switches used to connect shelves to nodes.
- Beginning with 9.9.1, System Manager displays information about a switch that acts as both a storage switch and a cluster, which can also be shared between nodes of an HA pair.
- The following information is displayed:
  - Switch name
  - IP address
  - Serial number
  - SNMP version
  - System version
- You can view the following storage switch models:

If your system is running...	Then you can use System Manager to view...
ONTAP 9.8	Cisco Nexus 3232C Switch
ONTAP 9.9.1 and 9.10.1	Cisco Nexus 3232C Switch Cisco Nexus 9336C-FX2 Switch
ONTAP 9.11.1	Cisco Nexus 3232C Switch Cisco Nexus 9336C-FX2 Switch Mellanox SN2100 Switch

## Storage switch ports

### Storage switch ports

- The following information is displayed:
  - Identity name
  - Identity index
  - State
  - Remote connection
  - Other details


## Manage nodes

### Reboot, shut down, take over, and give back nodes

You should switch a node's workload to its HA partner (takeover) before rebooting or shutting down the node.

#### Steps

1. Click **Cluster > Overview**.

2. Under **Nodes**, click .
3. Click the node and select the desired action.

## Add nodes to cluster

You can increase the size and capabilities of your cluster by adding new nodes.

### Before you Start

You should have already cabled the new nodes to the cluster.

There are separate processes for working with System Manager in ONTAP 9.7 or ONTAP 9.8.

- [Adding nodes to a cluster with System Manager \(ONTAP 9.7\)](#)
- [Adding nodes to a cluster with System Manager \(ONTAP 9.8\)](#)

### Adding nodes to a cluster with System Manager (ONTAP 9.7)

#### Steps

1. Click **(Return to classic version)**.
2. Click **Configurations > Cluster Expansion**.

System Manager automatically discovers the new nodes.

3. Click **Switch to the new experience**.
4. Click **Cluster > Overview** to view the new nodes.

### Adding nodes to a cluster with System Manager (ONTAP 9.8)

#### Steps

1. Select **Cluster > Overview**.

The new controllers are shown as nodes connected to the cluster network but are not in the cluster.

2. Click **Add**.
  - The nodes are added into the cluster.
  - Storage is allocated implicitly.

## Cluster management with the CLI

### Administration overview with the CLI

You can administer ONTAP systems with the command-line interface (CLI). You can use the ONTAP management interfaces, access the cluster, manage nodes, and much more.

You should use these procedures under the following circumstances:

- You want to understand the range of ONTAP administrator capabilities.
- You want to use the CLI, not System Manager or an automated scripting tool.

### Related information

For details about CLI syntax and usage, see the [ONTAP 9 manual page reference](#) documentation.

## Cluster and SVM administrators

### Cluster and SVM administrators

Cluster administrators administer the entire cluster and the storage virtual machines (SVMs, formerly known as Vservers) it contains. SVM administrators administer only their own data SVMs.

Cluster administrators can administer the entire cluster and its resources. They can also set up data SVMs and delegate SVM administration to SVM administrators. The specific capabilities that cluster administrators have depend on their access-control roles. By default, a cluster administrator with the “admin” account name or role name has all capabilities for managing the cluster and SVMs.

SVM administrators can administer only their own SVM storage and network resources, such as volumes, protocols, LIFs, and services. The specific capabilities that SVM administrators have depend on the access-control roles that are assigned by cluster administrators.



The ONTAP command-line interface (CLI) continues to use the term *Vserver* in the output, and `vserver` as a command or parameter name has not changed.

### Manage access to System Manager

You can enable or disable a web browser’s access to System Manager. You can also view the System Manager log.

You can control a web browser’s access to System Manager by using `vserver services web modify -name sysmgr -vserver cluster_name -enabled [true|false]`.

System Manager logging is recorded in the `/mroot/etc/log/mlog/sysmgr.log` files of the node that hosts the cluster management LIF at the time System Manager is accessed. You can view the log files by using a browser. The System Manager log is also included in AutoSupport messages.

### What the cluster management server is

The cluster management server, also called an *adminSVM*, is a specialized storage virtual machine (SVM) implementation that presents the cluster as a single manageable entity. In addition to serving as the highest-level administrative domain, the cluster management server owns resources that do not logically belong with a data SVM.

The cluster management server is always available on the cluster. You can access the cluster management server through the console or cluster management LIF.

Upon failure of its home network port, the cluster management LIF automatically fails over to another node in the cluster. Depending on the connectivity characteristics of the management protocol you are using, you might or might not notice the failover. If you are using a connectionless protocol (for example, SNMP) or have a limited connection (for example, HTTP), you are not likely to notice the failover. However, if you are using a long-term connection (for example, SSH), then you will have to reconnect to the cluster management server after the failover.

When you create a cluster, all of the characteristics of the cluster management LIF are configured, including its IP address, netmask, gateway, and port.

Unlike a data SVM or node SVM, a cluster management server does not have a root volume or host user volumes (though it can host system volumes). Furthermore, a cluster management server can only have LIFs of the cluster management type.

If you run the `vserver show` command, the cluster management server appears in the output listing for that command.

## Types of SVMs

A cluster consists of four types of SVMs, which help in managing the cluster and its resources and data access to the clients and applications.

A cluster contains the following types of SVMs:

- Admin SVM

The cluster setup process automatically creates the admin SVM for the cluster. The admin SVM represents the cluster.

- Node SVM

A node SVM is created when the node joins the cluster, and the node SVM represents the individual nodes of the cluster.

- System SVM (advanced)

A system SVM is automatically created for cluster-level communications in an IPspace.

- Data SVM

A data SVM represents the data serving SVMs. After the cluster setup, a cluster administrator must create data SVMs and add volumes to these SVMs to facilitate data access from the cluster.

A cluster must have at least one data SVM to serve data to its clients.



Unless otherwise specified, the term SVM refers to a data (data-serving) SVM.

In the CLI, SVMs are displayed as Vservers.

## ONTAP management interface basics

### Access the cluster by using the CLI (cluster administrators only)

#### Access the cluster by using the serial port

You can access the cluster directly from a console that is attached to a node's serial port.

#### Steps

1. At the console, press Enter.

The system responds with the login prompt.

2. At the login prompt, do one of the following:

To access the cluster with...	Enter the following account name...
The default cluster account	<b>admin</b>
An alternative administrative user account	<i>username</i>

The system responds with the password prompt.

3. Enter the password for the admin or administrative user account, and then press Enter.

### Access the cluster by using SSH

You can issue SSH requests to the cluster to perform administrative tasks. SSH is enabled by default.

#### What you'll need

- You must have a user account that is configured to use `ssh` as an access method.

The `-application` parameter of the `security login` commands specifies the access method for a user account. The `security login` man pages contain additional information.

- If you use an Active Directory (AD) domain user account to access the cluster, an authentication tunnel for the cluster must have been set up through a CIFS-enabled storage virtual machine (SVM), and your AD domain user account must also have been added to the cluster with `ssh` as an access method and `domain` as the authentication method.
- If you use IPv6 connections, IPv6 must already be configured and enabled on the cluster, and firewall policies must already be configured with IPv6 addresses.

The `network options ipv6 show` command displays whether IPv6 is enabled. The `system services firewall policy show` command displays firewall policies.

#### About this task

- You must use an OpenSSH 5.7 or later client.
- Only the SSH v2 protocol is supported; SSH v1 is not supported.
- ONTAP supports a maximum of 64 concurrent SSH sessions per node.

If the cluster management LIF resides on the node, it shares this limit with the node management LIF.

If the rate of incoming connections is higher than 10 per second, the service is temporarily disabled for 60 seconds.

- ONTAP supports only the AES and 3DES encryption algorithms (also known as *ciphers*) for SSH.

AES is supported with 128, 192, and 256 bits in key length. 3DES is 56 bits in key length as in the original DES, but it is repeated three times.

- When FIPS mode is on, SSH clients should negotiate with Elliptic Curve Digital Signature Algorithm (ECDSA) public key algorithms for the connection to be successful.
- If you want to access the ONTAP CLI from a Windows host, you can use a third-party utility such as PuTTY.
- If you use a Windows AD user name to log in to ONTAP, you should use the same uppercase or lowercase letters that were used when the AD user name and domain name were created in ONTAP.

AD user names and domain names are not case-sensitive. However, ONTAP user names are case-sensitive. Case mismatch between the user name created in ONTAP and the user name created in AD results in a login failure.

- Beginning with ONTAP 9.3, you can enable SSH multifactor authentication for local administrator accounts.

When SSH multifactor authentication is enabled, users are authenticated by using a public key and a password.

- Beginning with ONTAP 9.4, you can enable SSH multifactor authentication for LDAP and NIS remote users.

## Steps

1. From an administration host, enter the `ssh` command in one of the following formats:

- `ssh username@hostname_or_IP [command]`
- `ssh -l username hostname_or_IP [command]`

If you are using an AD domain user account, you must specify *username* in the format of *domainname* \ *AD\_accountname* (with double backslashes after the domain name) or "*domainname* \ *AD\_accountname*" (enclosed in double quotation marks and with a single backslash after the domain name).

*hostname\_or\_IP* is the host name or the IP address of the cluster management LIF or a node management LIF. Using the cluster management LIF is recommended. You can use an IPv4 or IPv6 address.

*command* is not required for SSH-interactive sessions.

## Examples of SSH requests

The following examples show how the user account named "joe" can issue an SSH request to access a cluster whose cluster management LIF is 10.72.137.28:

```
$ ssh joe@10.72.137.28
Password:
cluster1::> cluster show
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.
```

```

$ ssh -l joe 10.72.137.28 cluster show
Password:
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.

```

The following examples show how the user account named “john” from the domain named “DOMAIN1” can issue an SSH request to access a cluster whose cluster management LIF is 10.72.137.28:

```

$ ssh DOMAIN1\john@10.72.137.28
Password:
cluster1::> cluster show
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.

```

```

$ ssh -l "DOMAIN1\john" 10.72.137.28 cluster show
Password:
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.

```

The following example shows how the user account named “joe” can issue an SSH MFA request to access a cluster whose cluster management LIF is 10.72.137.32:

```

$ ssh joe@10.72.137.32
Authenticated with partial success.
Password:
cluster1::> cluster show
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.

```

## Related information



### SSH login security

Beginning with ONTAP 9.5, you can view information about previous logins, unsuccessful attempts to log in, and changes to your privileges since your last successful login.

Security-related information is displayed when you successfully log in as an SSH admin user. You are alerted about the following conditions:

- The last time your account name was logged in.
- The number of unsuccessful login attempts since the last successful login.
- Whether the role has changed since the last login (for example, if the admin account's role changed from "admin" to "backup.")
- Whether the add, modify, or delete capabilities of the role were modified since the last login.



If any of the information displayed is suspicious, you should immediately contact your security department.

To obtain this information when you login, the following prerequisites must be met:

- Your SSH user account must be provisioned in ONTAP.
- Your SSH security login must be created.
- Your login attempt must be successful.

### Restrictions and other considerations for SSH login security

The following restrictions and considerations apply to SSH login security information:

- The information is available only for SSH-based logins.
- For group-based admin accounts, such as LDAP/NIS and AD accounts, users can view the SSH login information if the group of which they are a member is provisioned as an admin account in ONTAP.

However, alerts about changes to the role of the user account cannot be displayed for these users. Also, users belonging to an AD group that has been provisioned as an admin account in ONTAP cannot view the count of unsuccessful login attempts that occurred since the last time they logged in.

- The information maintained for a user is deleted when the user account is deleted from ONTAP.
- The information is not displayed for connections to applications other than SSH.

### Examples of SSH login security information

The following examples demonstrate the type of information displayed after you login.

- This message is displayed after each successful login:

```
Last Login : 7/19/2018 06:11:32
```

- These messages are displayed if there have been unsuccessful attempts to login since the last successful

login:

```
Last Login : 4/12/2018 08:21:26
Unsuccessful login attempts since last login - 5
```

- These messages are displayed if there have been unsuccessful attempts to login and your privileges were modified since the last successful login:

```
Last Login : 8/22/2018 20:08:21
Unsuccessful login attempts since last login - 3
Your privileges have changed since last login
```

### Enable Telnet or RSH access to the cluster

As a security best practice, Telnet and RSH are disabled in the predefined management firewall policy (`mgmt`). To enable the cluster to accept Telnet or RSH requests, you must create a new management firewall policy that has Telnet or RSH enabled, and then associate the new policy with the cluster management LIF.

#### About this task

ONTAP prevents you from changing predefined firewall policies, but you can create a new policy by cloning the predefined `mgmt` management firewall policy, and then enabling Telnet or RSH under the new policy. However, Telnet and RSH are not secure protocols, so you should consider using SSH to access the cluster. SSH provides a secure remote shell and interactive network session.

Perform the following steps to enable Telnet or RSH access to the clusters:

#### Steps

1. Enter the advanced privilege mode:  
**set advanced**
2. Enable a security protocol (RSH or Telnet):  
**security protocol modify -application *security\_protocol* -enabled true**
3. Create a new management firewall policy based on the `mgmt` management firewall policy:  
**system services firewall policy clone -policy *mgmt* -destination-policy *policy-name***
4. Enable Telnet or RSH in the new management firewall policy:  
**system services firewall policy create -policy *policy-name* -service *security\_protocol* -action allow -ip-list *ip\_address/netmask***  
To allow all IP addresses, you should specify `-ip-list 0.0.0.0/0`
5. Associate the new policy with the cluster management LIF:  
**network interface modify -vserver *cluster\_management\_LIF* -lif *cluster\_mgmt* -firewall-policy *policy-name***

## Access the cluster by using Telnet

You can issue Telnet requests to the cluster to perform administrative tasks. Telnet is disabled by default.

### What you'll need

The following conditions must be met before you can use Telnet to access the cluster:

- You must have a cluster local user account that is configured to use Telnet as an access method.

The `-application` parameter of the `security login` commands specifies the access method for a user account. For more information, see the `security login` man pages.

- Telnet must already be enabled in the management firewall policy that is used by the cluster or node management LIFs so that Telnet requests can go through the firewall.

By default, Telnet is disabled. The `system services firewall policy show` command with the `-service telnet` parameter displays whether Telnet has been enabled in a firewall policy. For more information, see the `system services firewall policy` man pages.

- If you use IPv6 connections, IPv6 must already be configured and enabled on the cluster, and firewall policies must already be configured with IPv6 addresses.

The `network options ipv6 show` command displays whether IPv6 is enabled. The `system services firewall policy show` command displays firewall policies.

### About this task

- Telnet is not a secure protocol.

You should consider using SSH to access the cluster. SSH provides a secure remote shell and interactive network session.

- ONTAP supports a maximum of 50 concurrent Telnet sessions per node.

If the cluster management LIF resides on the node, it shares this limit with the node management LIF.

If the rate of in-coming connections is higher than 10 per second, the service is temporarily disabled for 60 seconds.

- If you want to access the ONTAP CLI from a Windows host, you can use a third-party utility such as PuTTY.

### Steps

1. From an administration host, enter the following command:

```
telnet hostname_or_IP
```

*hostname\_or\_IP* is the host name or the IP address of the cluster management LIF or a node management LIF. Using the cluster management LIF is recommended. You can use an IPv4 or IPv6 address.

### Example of a Telnet request

The following example shows how the user named "joe", who has been set up with Telnet access, can issue a

Telnet request to access a cluster whose cluster management LIF is 10.72.137.28:

```
admin_host$ telnet 10.72.137.28
Data ONTAP
login: joe
Password:
cluster1::>
```

### Access the cluster by using RSH

You can issue RSH requests to the cluster to perform administrative tasks. RSH is not a secure protocol and is disabled by default.

### What you'll need

The following conditions must be met before you can use RSH to access the cluster:

- You must have a cluster local user account that is configured to use RSH as an access method.

The `-application` parameter of the `security login` commands specifies the access method for a user account. For more information, see the `security login` man pages.

- RSH must already be enabled in the management firewall policy that is used by the cluster or node management LIFs so that RSH requests can go through the firewall.

By default, RSH is disabled. The `system services firewall policy show` command with the `-service rsh` parameter displays whether RSH has been enabled in a firewall policy. For more information, see the `system services firewall policy` man pages.

- If you use IPv6 connections, IPv6 must already be configured and enabled on the cluster, and firewall policies must already be configured with IPv6 addresses.

The `network options ipv6 show` command displays whether IPv6 is enabled. The `system services firewall policy show` command displays firewall policies.

### About this task

- RSH is not a secure protocol.

You should consider using SSH to access the cluster. SSH provides a secure remote shell and interactive network session.

- ONTAP supports a maximum of 50 concurrent RSH sessions per node.

If the cluster management LIF resides on the node, it shares this limit with the node management LIF.

If the rate of in-coming connections is higher than 10 per second, the service is temporarily disabled for 60 seconds.

### Steps

1. From an administration host, enter the following command:

```
rsh hostname_or_IP -l username:passwordcommand
```

*hostname\_or\_IP* is the host name or the IP address of the cluster management LIF or a node management LIF. Using the cluster management LIF is recommended. You can use an IPv4 or IPv6 address.

*command* is the command you want to execute over RSH.

### Example of an RSH request

The following example shows how the user named “joe”, who has been set up with RSH access, can issue an RSH request to run the `cluster show` command:

```
admin_host$ rsh 10.72.137.28 -l joe:password cluster show
```

```
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.
```

```
admin_host$
```

## Use the ONTAP command-line interface

### Using the ONTAP command-line interface

The ONTAP command-line interface (CLI) provides a command-based view of the management interface. You enter commands at the storage system prompt, and command results are displayed in text.

The CLI command prompt is represented as `cluster_name::>`.

If you set the privilege level (that is, the `-privilege` parameter of the `set` command) to `advanced`, the prompt includes an asterisk (\*), for example:

```
cluster_name::*>
```

### About the different shells for CLI commands (cluster administrators only)

### About the different shells for CLI commands overview (cluster administrators only)

The cluster has three different shells for CLI commands, the *clustershell*, the *nodeshell*, and the *systemshell*. The shells are for different purposes, and they each have a different command set.

- The *clustershell* is the native shell that is started automatically when you log in to the cluster.

It provides all the commands you need to configure and manage the cluster. The *clustershell* CLI help (triggered by `?` at the *clustershell* prompt) displays available *clustershell* commands. The `man`

`command_name` command in the clustershell displays the man page for the specified clustershell command.

- The nodeshell is a special shell for commands that take effect only at the node level.

The nodeshell is accessible through the `system node run` command.

The nodeshell CLI help (triggered by `?` or `help` at the nodeshell prompt) displays available nodeshell commands. The `man command_name` command in the nodeshell displays the man page for the specified nodeshell command.

Many commonly used nodeshell commands and options are tunneled or aliased into the clustershell and can be executed also from the clustershell.

- The systemshell is a low-level shell that is used only for diagnostic and troubleshooting purposes.

The systemshell and the associated “diag” account are intended for low-level diagnostic purposes. Their access requires the diagnostic privilege level and is reserved only for technical support to perform troubleshooting tasks.

## Access of nodeshell commands and options in the clustershell

Nodeshell commands and options are accessible through the nodeshell:

```
system node run -node nodename
```

Many commonly used nodeshell commands and options are tunneled or aliased into the clustershell and can be executed also from the clustershell.

Nodeshell options that are supported in the clustershell can be accessed by using the `vserver options clustershell` command. To see these options, you can do one of the following:

- Query the clustershell CLI with `vserver options -vserver nodename_or_clustername -option-name?`
- Access the `vserver options` man page in the clustershell CLI with `man vserver options`

If you enter a nodeshell or legacy command or option in the clustershell, and the command or option has an equivalent clustershell command, ONTAP informs you of the clustershell command to use.

If you enter a nodeshell or legacy command or option that is not supported in the clustershell, ONTAP informs you of the “not supported” status for the command or option.

## Display available nodeshell commands

You can obtain a list of available nodeshell commands by using the CLI help from the nodeshell.

### Steps

1. To access the nodeshell, enter the following command at the clustershell’s system prompt:

```
system node run -node {nodename|local}
```

`local` is the node you used to access the cluster.



The `system node run` command has an alias command, `run`.

2. Enter the following command in the nodeshell to see the list of available nodeshell commands:

**[*commandname*] help**

*commandname* is the name of the command whose availability you want to display. If you do not include *commandname*, the CLI displays all available nodeshell commands.

You enter `exit` or type `Ctrl-d` to return to the clustershell CLI.

### Example of displaying available nodeshell commands

The following example accesses the nodeshell of a node named `node2` and displays information for the nodeshell command `environment`:

```
cluster1::> system node run -node node2
Type 'exit' or 'Ctrl-D' to return to the CLI

node2> environment help
Usage: environment status |
      [status] [shelf [<adapter>[.<shelf-number>]]] |
      [status] [shelf_log] |
      [status] [shelf_stats] |
      [status] [shelf_power_status] |
      [status] [chassis [all | list-sensors | Temperature | PSU 1 |
PSU 2 | Voltage | SYS FAN | NVRAM6-temperature-3 | NVRAM6-battery-3]]
```

### Methods of navigating CLI command directories

Commands in the CLI are organized into a hierarchy by command directories. You can run commands in the hierarchy either by entering the full command path or by navigating through the directory structure.

When using the CLI, you can access a command directory by typing the directory's name at the prompt and then pressing `Enter`. The directory name is then included in the prompt text to indicate that you are interacting with the appropriate command directory. To move deeper into the command hierarchy, you type the name of a command subdirectory followed by pressing `Enter`. The subdirectory name is then included in the prompt text and the context shifts to that subdirectory.

You can navigate through several command directories by entering the entire command. For example, you can display information about disk drives by entering the `storage disk show` command at the prompt. You can also run the command by navigating through one command directory at a time, as shown in the following example:

```
cluster1::> storage
cluster1::storage> disk
cluster1::storage disk> show
```

You can abbreviate commands by entering only the minimum number of letters in a command that makes the command unique to the current directory. For example, to abbreviate the command in the previous example, you can enter `st d sh`. You can also use the Tab key to expand abbreviated commands and to display a command's parameters, including default parameter values.

You can use the `top` command to go to the top level of the command hierarchy, and the `up` command or `..` command to go up one level in the command hierarchy.



Commands and command options preceded by an asterisk (\*) in the CLI can be executed only at the advanced privilege level or higher.

### Rules for specifying values in the CLI

Most commands include one or more required or optional parameters. Many parameters require you to specify a value for them. A few rules exist for specifying values in the CLI.

- A value can be a number, a Boolean specifier, a selection from an enumerated list of predefined values, or a text string.

Some parameters can accept a comma-separated list of two or more values. Comma-separated lists of values do not need to be in quotation marks (" "). Whenever you specify text, a space, or a query character (when not meant as a query or text starting with a less-than or greater-than symbol), you must enclose the entity in quotation marks.

- The CLI interprets a question mark (" ? ") as the command to display help information for a particular command.
- Some text that you enter in the CLI, such as command names, parameters, and certain values, is not case-sensitive.

For example, when you enter parameter values for the `vserver cifs` commands, capitalization is ignored. However, most parameter values, such as the names of nodes, storage virtual machines (SVMs), aggregates, volumes, and logical interfaces, are case-sensitive.

- If you want to clear the value of a parameter that takes a string or a list, you specify an empty set of quotation marks (" ") or a dash ("-").
- The hash sign (" # "), also known as the pound sign, indicates a comment for a command-line input; if used, it should appear after the last parameter in a command line.

The CLI ignores the text between " # " and the end of the line.

In the following example, an SVM is created with a text comment. The SVM is then modified to delete the comment:



```
cluster1::> vserver create -vserver vs0 -subtype default -rootvolume
root_vs0
-aggregate aggr1 -rootvolume-security-style unix -language C.UTF-8 -is
-repository false -ipSPACE ipSPACEA -comment "My SVM"
cluster1::> vserver modify -vserver vs0 -comment ""
```

In the following example, a command-line comment that uses the “#” sign indicates what the command does.

```
cluster1::> security login create -vserver vs0 -user-or-group-name new-
admin
-application ssh -authmethod password #This command creates a new user
account
```

### Methods of viewing command history and reissuing commands

Each CLI session keeps a history of all commands issued in it. You can view the command history of the session that you are currently in. You can also reissue commands.

To view the command history, you can use the `history` command.

To reissue a command, you can use the `redo` command with one of the following arguments:

- A string that matches part of a previous command

For example, if the only `volume` command you have run is `volume show`, you can use the `redo volume` command to reexecute the command.

- The numeric ID of a previous command, as listed by the `history` command

For example, you can use the `redo 4` command to reissue the fourth command in the history list.

- A negative offset from the end of the history list

For example, you can use the `redo -2` command to reissue the command that you ran two commands ago.

For example, to redo the command that is third from the end of the command history, you would enter the following command:

```
cluster1::> redo -3
```

### Keyboard shortcuts for editing CLI commands

The command at the current command prompt is the active command. Using keyboard shortcuts enables you to edit the active command quickly. These keyboard shortcuts are

similar to those of the UNIX tcsh shell and the Emacs editor.

The following table lists the keyboard shortcuts for editing CLI commands. “Ctrl-” indicates that you press and hold the Ctrl key while typing the character specified after it. “Esc-” indicates that you press and release the Esc key and then type the character specified after it.

If you want to...	Use the following keyboard shortcut...
Move the cursor back by one character	Ctrl-B
	Back arrow
Move the cursor forward by one character	Ctrl-F
	Forward arrow
Move the cursor back by one word	Esc-B
Move the cursor forward by one word	Esc-F
Move the cursor to the beginning of the line	Ctrl-A
Move the cursor to the end of the line	Ctrl-E
Remove the content of the command line from the beginning of the line to the cursor, and save it in the cut buffer. The cut buffer acts like temporary memory, similar to what is called a <i>clipboard</i> in some programs.	Ctrl-U
Remove the content of the command line from the cursor to the end of the line, and save it in the cut buffer	Ctrl-K
Remove the content of the command line from the cursor to the end of the following word, and save it in the cut buffer	Esc-D
Remove the word before the cursor, and save it in the cut buffer	Ctrl-W
Yank the content of the cut buffer, and push it into the command line at the cursor	Ctrl-Y
Delete the character before the cursor	Ctrl-H
	Backspace

If you want to...	Use the following keyboard shortcut...
Delete the character where the cursor is	Ctrl-D
Clear the line	Ctrl-C
Clear the screen	Ctrl-L
Replace the current content of the command line with the previous entry on the history list.	Ctrl-P
With each repetition of the keyboard shortcut, the history cursor moves to the previous entry.	Esc-P
	Up arrow
Replace the current content of the command line with the next entry on the history list. With each repetition of the keyboard shortcut, the history cursor moves to the next entry.	Ctrl-N
	Esc-N
	Down arrow
Expand a partially entered command or list valid input from the current editing position	Tab
	Ctrl-I
Display context-sensitive help	?
Escape the special mapping for the question mark (“?”) character. For instance, to enter a question mark into a command’s argument, press Esc and then the “?” character.	Esc-?
Start TTY output	Ctrl-Q
Stop TTY output	Ctrl-S

### Use of administrative privilege levels

ONTAP commands and parameters are defined at three privilege levels: *admin*, *advanced*, and *diagnostic*. The privilege levels reflect the skill levels required in performing the tasks.

- **admin**

Most commands and parameters are available at this level. They are used for common or routine tasks.

- **advanced**

Commands and parameters at this level are used infrequently, require advanced knowledge, and can

cause problems if used inappropriately.

You use advanced commands or parameters only with the advice of support personnel.

- **diagnostic**

Diagnostic commands and parameters are potentially disruptive. They are used only by support personnel to diagnose and fix problems.

### Set the privilege level in the CLI

You can set the privilege level in the CLI by using the `set` command. Changes to privilege level settings apply only to the session you are in. They are not persistent across sessions.

#### Steps

1. To set the privilege level in the CLI, use the `set` command with the `-privilege` parameter.

#### Example of setting the privilege level

The following example sets the privilege level to advanced and then to admin:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by technical support.
Do you wish to continue? (y or n): y
cluster1::*> set -privilege admin
```

### Set display preferences in the CLI

You can set display preferences for a CLI session by using the `set` command and `rows` command. The preferences you set apply only to the session you are in. They are not persistent across sessions.

#### About this task

You can set the following CLI display preferences:

- The privilege level of the command session
- Whether confirmations are issued for potentially disruptive commands
- Whether `show` commands display all fields
- The character or characters to use as the field separator
- The default unit when reporting data sizes
- The number of rows the screen displays in the current CLI session before the interface pauses output

If the preferred number of rows is not specified, it is automatically adjusted based on the actual height of the terminal. If the actual height is undefined, the default number of rows is 24.

- The default storage virtual machine (SVM) or node

- Whether a continuing command should stop if it encounters an error

## Steps

1. To set CLI display preferences, use the `set` command.

To set the number of rows the screen displays in the current CLI session, you can also use the `rows` command.

For more information, see the man pages for the `set` command and `rows` command.

## Example of setting display preferences in the CLI

The following example sets a comma to be the field separator, sets GB as the default data-size unit, and sets the number of rows to 50:

```
cluster1::> set -showseparator "," -units GB
cluster1::> rows 50
```

## Methods of using query operators

The management interface supports queries and UNIX-style patterns and wildcards to enable you to match multiple values in command-parameter arguments.

The following table describes the supported query operators:

Operator	Description
*	Wildcard that matches all entries.  For example, the command <code>volume show -volume *tmp*</code> displays a list of all volumes whose names include the string <code>tmp</code> .
!	NOT operator.  Indicates a value that is not to be matched; for example, <code>!vs0</code> indicates not to match the value <code>vs0</code> .
	OR operator.  Separates two values that are to be compared; for example, <code>vs0   vs2</code> matches either <code>vs0</code> or <code>vs2</code> . You can specify multiple OR statements; for example, <code>a   b*   *c*</code> matches the entry <code>a</code> , any entry that starts with <code>b</code> , and any entry that includes <code>c</code> .
..	Range operator.  For example, <code>5..10</code> matches any value from 5 to 10, inclusive.

Operator	Description
<	Less-than operator.  For example, <20 matches any value that is less than 20.
>	Greater-than operator.  For example, >5 matches any value that is greater than 5.
<=	Less-than-or-equal-to operator.  For example, ≤5 matches any value that is less than or equal to 5.
>=	Greater-than-or-equal-to operator.  For example, ≥5 matches any value that is greater than or equal to 5.
{query}	Extended query.  An extended query must be specified as the first argument after the command name, before any other parameters.  For example, the command <code>volume modify {-volume *tmp*} -state offline</code> sets offline all volumes whose names include the string <code>tmp</code> .

If you want to parse query characters as literals, you must enclose the characters in double quotes (for example, “^”, “.”, “\*”, or “\$”) for the correct results to be returned.

You can use multiple query operators in one command line. For example, the command `volume show -size >1GB -percent-used <50 -vserver !vs1` displays all volumes that are greater than 1 GB in size, less than 50% utilized, and not in the storage virtual machine (SVM) named “vs1”.

#### Methods of using extended queries

You can use extended queries to match and perform operations on objects that have specified values.

You specify extended queries by enclosing them within curly brackets ({}). An extended query must be specified as the first argument after the command name, before any other parameters. For example, to set offline all volumes whose names include the string `tmp`, you run the command in the following example:

```
cluster1::> volume modify {-volume *tmp*} -state offline
```

Extended queries are generally useful only with `modify` and `delete` commands. They have no meaning in `create` or `show` commands.

The combination of queries and modify operations is a useful tool. However, it can potentially cause confusion and errors if implemented incorrectly. For example, using the (advanced privilege) `system node image`

`modify` command to set a node's default software image automatically sets the other software image not to be the default. The command in the following example is effectively a null operation:

```
cluster1::*> system node image modify {-isdefault true} -isdefault false
```

This command sets the current default image as the non-default image, then sets the new default image (the previous non-default image) to the non-default image, resulting in the original default settings being retained. To perform the operation correctly, you can use the command as given in the following example:

```
cluster1::*> system node image modify {-iscurrent false} -isdefault true
```

### Methods of customizing `show` command output by using fields

When you use the `-instance` parameter with a `show` command to display details, the output can be lengthy and include more information than you need. The `-fields` parameter of a `show` command enables you to display only the information you specify.

For example, running `volume show -instance` is likely to result in several screens of information. You can use `volume show -fields fieldname[,fieldname...]` to customize the output so that it includes only the specified field or fields (in addition to the default fields that are always displayed.) You can use `-fields ?` to display valid fields for a `show` command.

The following example shows the output difference between the `-instance` parameter and the `-fields` parameter:

```

cluster1::> volume show -instance

                                Vserver Name: cluster1-1
                                Volume Name: vol0
                                Aggregate Name: aggr0
                                Volume Size: 348.3GB
                                Volume Data Set ID: -
                                Volume Master Data Set ID: -
                                Volume State: online
                                Volume Type: RW
                                Volume Style: flex
                                ...
                                Space Guarantee Style: volume
                                Space Guarantee in Effect: true
                                ...
Press <space> to page down, <return> for next line, or 'q' to quit...
...
cluster1::>

cluster1::> volume show -fields space-guarantee,space-guarantee-enabled

vserver  volume  space-guarantee  space-guarantee-enabled
-----  -
cluster1-1  vol0    volume          true
cluster1-2  vol0    volume          true
vs1        root_vol
          volume          true
vs2        new_vol
          volume          true
vs2        root_vol
          volume          true
...
cluster1::>

```

### About positional parameters

You can take advantage of the positional parameter functionality of the ONTAP CLI to increase efficiency in command input. You can query a command to identify parameters that are positional for the command.

### What a positional parameter is

- A positional parameter is a parameter that does not require you to specify the parameter name before specifying the parameter value.
- A positional parameter can be interspersed with nonpositional parameters in the command input, as long as it observes its relative sequence with other positional parameters in the same command, as indicated in



the ***command\_name*** ? output.

- A positional parameter can be a required or optional parameter for a command.
- A parameter can be positional for one command but nonpositional for another.



Using the positional parameter functionality in scripts is not recommended, especially when the positional parameters are optional for the command or have optional parameters listed before them.

### Identify a positional parameter

You can identify a positional parameter in the ***command\_name*** ? command output. A positional parameter has square brackets surrounding its parameter name, in one of the following formats:

- `[-parameter_name] parameter_value` shows a required parameter that is positional.
- `[[[-parameter_name] parameter_value]` shows an optional parameter that is positional.

For example, when displayed as the following in the ***command\_name*** ? output, the parameter is positional for the command it appears in:

- `[-lif] <lif-name>`
- `[[[-lif] <lif-name>]`

However, when displayed as the following, the parameter is nonpositional for the command it appears in:

- `-lif <lif-name>`
- `[-lif <lif-name>]`

### Examples of using positional parameters

In the following example, the ***volume create*** ? output shows that three parameters are positional for the command: `-volume`, `-aggregate`, and `-size`.

```

cluster1::> volume create ?
  -vserver <vserver name>           Vserver Name
  [-volume] <volume name>           Volume Name
  [-aggregate] <aggregate name>     Aggregate Name
  [[-size] {<integer>[KB|MB|GB|TB|PB]] Volume Size
  [ -state {online|restricted|offline|force-online|force-offline|mixed} ]
                                         Volume State (default: online)
  [ -type {RW|DP|DC} ]               Volume Type (default: RW)
  [ -policy <text> ]                 Export Policy
  [ -user <user name> ]              User ID
  ...
  [ -space-guarantee|-s {none|volume} ] Space Guarantee Style (default:
volume)
  [ -percent-snapshot-space <percent> ] Space Reserved for Snapshot
Copies
  ...

```

In the following example, the `volume create` command is specified without taking advantage of the positional parameter functionality:

```

cluster1::> volume create -vserver svml -volume vol1 -aggregate aggr1 -size 1g
-percent-snapshot-space 0

```

The following examples use the positional parameter functionality to increase the efficiency of the command input. The positional parameters are interspersed with nonpositional parameters in the `volume create` command, and the positional parameter values are specified without the parameter names. The positional parameters are specified in the same sequence indicated by the `volume create ?` output. That is, the value for `-volume` is specified before that of `-aggregate`, which is in turn specified before that of `-size`.

```

cluster1::> volume create vol2 aggr1 1g -vserver svml -percent-snapshot-space 0

```

```

cluster1::> volume create -vserver svml vol3 -snapshot-policy default aggr1
-nvfail off 1g -space-guarantee none

```

### Methods of accessing ONTAP man pages

ONTAP manual (man) pages explain how to use ONTAP commands. They are available at the command line and on the NetApp Support Site.

The `man command_name` command displays the manual page of the specified command. If you do not specify a command name, the manual page index is displayed. You can use the `man man` command to view information about the `man` command itself. You can exit a man page by entering `q`.

The [ONTAP 9 man pages](#) contains command references for the admin-level and advanced-level ONTAP commands.

## Manage CLI sessions (cluster administrators only)

### Manage records of CLI sessions

#### Manage records of CLI sessions overview

You can record a CLI session into a file with a specified name and size limit, then upload the file to an FTP or HTTP destination. You can also display or delete files in which you previously recorded CLI sessions.

A record of a CLI session ends when you stop the recording or end the CLI session, or when the file reaches the specified size limit. The default file size limit is 1 MB. The maximum file size limit is 2 GB.

Recording a CLI session is useful, for example, if you are troubleshooting an issue and want to save detailed information or if you want to create a permanent record of space usage at a specific point in time.

#### Record a CLI session

You can use the `system script start` and `system script stop` commands to record a CLI session.

#### Steps

1. To start recording the current CLI session into a file, use the `system script start` command.

For more information about using the `system script start` command, see the man page.

ONTAP starts recording your CLI session into the specified file.

2. Proceed with your CLI session.
3. To stop recording the session, use the `system script stop` command.

For more information about using the `system script stop` command, see the man page.

ONTAP stops recording your CLI session.

#### Commands for managing records of CLI sessions

You use the `system script` commands to manage records of CLI sessions.

If you want to...	Use this command...
Start recording the current CLI session in to a specified file	<code>system script start</code>
Stop recording the current CLI session	<code>system script stop</code>
Display information about records of CLI sessions	<code>system script show</code>

If you want to...	Use this command...
Upload a record of a CLI session to an FTP or HTTP destination	<code>system script upload</code>
Delete a record of a CLI session	<code>system script delete</code>

#### Related information

[ONTAP 9 Commands](#)

#### Commands for managing the automatic timeout period of CLI sessions

The timeout value specifies how long a CLI session remains idle before being automatically terminated. The CLI timeout value is cluster-wide. That is, every node in a cluster uses the same CLI timeout value.

By default, the automatic timeout period of CLI sessions is 30 minutes.

You use the `system timeout` commands to manage the automatic timeout period of CLI sessions.

If you want to...	Use this command...
Display the automatic timeout period for CLI sessions	<code>system timeout show</code>
Modify the automatic timeout period for CLI sessions	<code>system timeout modify</code>

#### Related information

[ONTAP 9 Commands](#)

## Using the ONTAP command-line interface

The ONTAP command-line interface (CLI) provides a command-based view of the management interface. You enter commands at the storage system prompt, and command results are displayed in text.

The CLI command prompt is represented as `cluster_name::>`.

If you set the privilege level (that is, the `-privilege` parameter of the `set` command) to `advanced`, the prompt includes an asterisk (\*), for example:

```
cluster_name::*>
```

#### About the different shells for CLI commands (cluster administrators only)

##### About the different shells for CLI commands overview (cluster administrators only)

The cluster has three different shells for CLI commands, the *clustershell*, the *nodeshell*, and the *systemshell*. The shells are for different purposes, and they each have a different

## command set.

- The clustershell is the native shell that is started automatically when you log in to the cluster.

It provides all the commands you need to configure and manage the cluster. The clustershell CLI help (triggered by `?` at the clustershell prompt) displays available clustershell commands. The `man command_name` command in the clustershell displays the man page for the specified clustershell command.

- The nodeshell is a special shell for commands that take effect only at the node level.

The nodeshell is accessible through the `system node run` command.

The nodeshell CLI help (triggered by `?` or `help` at the nodeshell prompt) displays available nodeshell commands. The `man command_name` command in the nodeshell displays the man page for the specified nodeshell command.

Many commonly used nodeshell commands and options are tunneled or aliased into the clustershell and can be executed also from the clustershell.

- The systemshell is a low-level shell that is used only for diagnostic and troubleshooting purposes.

The systemshell and the associated “diag” account are intended for low-level diagnostic purposes. Their access requires the diagnostic privilege level and is reserved only for technical support to perform troubleshooting tasks.

### Access of nodeshell commands and options in the clustershell

Nodeshell commands and options are accessible through the nodeshell:

```
system node run -node nodename
```

Many commonly used nodeshell commands and options are tunneled or aliased into the clustershell and can be executed also from the clustershell.

Nodeshell options that are supported in the clustershell can be accessed by using the `vserver options clustershell` command. To see these options, you can do one of the following:

- Query the clustershell CLI with `vserver options -vserver nodename_or_clustername -option-name?`
- Access the `vserver options` man page in the clustershell CLI with `man vserver options`

If you enter a nodeshell or legacy command or option in the clustershell, and the command or option has an equivalent clustershell command, ONTAP informs you of the clustershell command to use.

If you enter a nodeshell or legacy command or option that is not supported in the clustershell, ONTAP informs you of the “not supported” status for the command or option.

### Display available nodeshell commands

You can obtain a list of available nodeshell commands by using the CLI help from the nodeshell.

## Steps

1. To access the nodeshell, enter the following command at the clustershell's system prompt:

```
system node run -node {nodename|local}
```

`local` is the node you used to access the cluster.



The `system node run` command has an alias command, `run`.

2. Enter the following command in the nodeshell to see the list of available nodeshell commands:

```
[commandname] help
```

*commandname* is the name of the command whose availability you want to display. If you do not include *commandname*, the CLI displays all available nodeshell commands.

You enter `exit` or type `Ctrl-d` to return to the clustershell CLI.

## Example of displaying available nodeshell commands

The following example accesses the nodeshell of a node named `node2` and displays information for the nodeshell command `environment`:

```
cluster1::> system node run -node node2
Type 'exit' or 'Ctrl-D' to return to the CLI

node2> environment help
Usage: environment status |
      [status] [shelf [<adapter>[.<shelf-number>]]] |
      [status] [shelf_log] |
      [status] [shelf_stats] |
      [status] [shelf_power_status] |
      [status] [chassis [all | list-sensors | Temperature | PSU 1 |
      PSU 2 | Voltage | SYS FAN | NVRAM6-temperature-3 | NVRAM6-battery-3]]
```

## Methods of navigating CLI command directories

Commands in the CLI are organized into a hierarchy by command directories. You can run commands in the hierarchy either by entering the full command path or by navigating through the directory structure.

When using the CLI, you can access a command directory by typing the directory's name at the prompt and then pressing `Enter`. The directory name is then included in the prompt text to indicate that you are interacting with the appropriate command directory. To move deeper into the command hierarchy, you type the name of a command subdirectory followed by pressing `Enter`. The subdirectory name is then included in the prompt text and the context shifts to that subdirectory.

You can navigate through several command directories by entering the entire command. For example, you can display information about disk drives by entering the `storage disk show` command at the prompt. You can

also run the command by navigating through one command directory at a time, as shown in the following example:

```
cluster1::> storage
cluster1::storage> disk
cluster1::storage disk> show
```

You can abbreviate commands by entering only the minimum number of letters in a command that makes the command unique to the current directory. For example, to abbreviate the command in the previous example, you can enter `st d sh`. You can also use the Tab key to expand abbreviated commands and to display a command's parameters, including default parameter values.

You can use the `top` command to go to the top level of the command hierarchy, and the `up` command or `..` command to go up one level in the command hierarchy.



Commands and command options preceded by an asterisk (\*) in the CLI can be executed only at the advanced privilege level or higher.

### Rules for specifying values in the CLI

Most commands include one or more required or optional parameters. Many parameters require you to specify a value for them. A few rules exist for specifying values in the CLI.

- A value can be a number, a Boolean specifier, a selection from an enumerated list of predefined values, or a text string.

Some parameters can accept a comma-separated list of two or more values. Comma-separated lists of values do not need to be in quotation marks (" "). Whenever you specify text, a space, or a query character (when not meant as a query or text starting with a less-than or greater-than symbol), you must enclose the entity in quotation marks.

- The CLI interprets a question mark ("?") as the command to display help information for a particular command.
- Some text that you enter in the CLI, such as command names, parameters, and certain values, is not case-sensitive.

For example, when you enter parameter values for the `vserver cifs` commands, capitalization is ignored. However, most parameter values, such as the names of nodes, storage virtual machines (SVMs), aggregates, volumes, and logical interfaces, are case-sensitive.

- If you want to clear the value of a parameter that takes a string or a list, you specify an empty set of quotation marks ("") or a dash ("-").
- The hash sign ("#"), also known as the pound sign, indicates a comment for a command-line input; if used, it should appear after the last parameter in a command line.

The CLI ignores the text between "#" and the end of the line.

In the following example, an SVM is created with a text comment. The SVM is then modified to delete the comment:

```
cluster1::> vservice create -vservice vs0 -subtype default -rootvolume
root_vs0
-aggregate aggr1 -rootvolume-security-style unix -language C.UTF-8 -is
-repository false -ipstack ipstackA -comment "My SVM"
cluster1::> vservice modify -vservice vs0 -comment ""
```

In the following example, a command-line comment that uses the “#” sign indicates what the command does.

```
cluster1::> security login create -vservice vs0 -user-or-group-name new-
admin
-application ssh -authmethod password #This command creates a new user
account
```

### Methods of viewing command history and reissuing commands

Each CLI session keeps a history of all commands issued in it. You can view the command history of the session that you are currently in. You can also reissue commands.

To view the command history, you can use the `history` command.

To reissue a command, you can use the `redo` command with one of the following arguments:

- A string that matches part of a previous command

For example, if the only `volume` command you have run is `volume show`, you can use the `redo volume` command to reexecute the command.

- The numeric ID of a previous command, as listed by the `history` command

For example, you can use the `redo 4` command to reissue the fourth command in the history list.

- A negative offset from the end of the history list

For example, you can use the `redo -2` command to reissue the command that you ran two commands ago.

For example, to redo the command that is third from the end of the command history, you would enter the following command:

```
cluster1::> redo -3
```

### Keyboard shortcuts for editing CLI commands

The command at the current command prompt is the active command. Using keyboard shortcuts enables you to edit the active command quickly. These keyboard shortcuts are



similar to those of the UNIX tcsh shell and the Emacs editor.

The following table lists the keyboard shortcuts for editing CLI commands. “Ctrl-” indicates that you press and hold the Ctrl key while typing the character specified after it. “Esc-” indicates that you press and release the Esc key and then type the character specified after it.

If you want to...	Use the following keyboard shortcut...
Move the cursor back by one character	Ctrl-B
	Back arrow
Move the cursor forward by one character	Ctrl-F
	Forward arrow
Move the cursor back by one word	Esc-B
Move the cursor forward by one word	Esc-F
Move the cursor to the beginning of the line	Ctrl-A
Move the cursor to the end of the line	Ctrl-E
Remove the content of the command line from the beginning of the line to the cursor, and save it in the cut buffer. The cut buffer acts like temporary memory, similar to what is called a <i>clipboard</i> in some programs.	Ctrl-U
Remove the content of the command line from the cursor to the end of the line, and save it in the cut buffer	Ctrl-K
Remove the content of the command line from the cursor to the end of the following word, and save it in the cut buffer	Esc-D
Remove the word before the cursor, and save it in the cut buffer	Ctrl-W
Yank the content of the cut buffer, and push it into the command line at the cursor	Ctrl-Y
Delete the character before the cursor	Ctrl-H
	Backspace

If you want to...	Use the following keyboard shortcut...
Delete the character where the cursor is	Ctrl-D
Clear the line	Ctrl-C
Clear the screen	Ctrl-L
Replace the current content of the command line with the previous entry on the history list.	Ctrl-P
With each repetition of the keyboard shortcut, the history cursor moves to the previous entry.	Esc-P
	Up arrow
Replace the current content of the command line with the next entry on the history list. With each repetition of the keyboard shortcut, the history cursor moves to the next entry.	Ctrl-N
	Esc-N
	Down arrow
Expand a partially entered command or list valid input from the current editing position	Tab
	Ctrl-I
Display context-sensitive help	?
Escape the special mapping for the question mark (“?”) character. For instance, to enter a question mark into a command’s argument, press Esc and then the “?” character.	Esc-?
Start TTY output	Ctrl-Q
Stop TTY output	Ctrl-S

### Use of administrative privilege levels

ONTAP commands and parameters are defined at three privilege levels: *admin*, *advanced*, and *diagnostic*. The privilege levels reflect the skill levels required in performing the tasks.

- **admin**

Most commands and parameters are available at this level. They are used for common or routine tasks.

- **advanced**

Commands and parameters at this level are used infrequently, require advanced knowledge, and can cause problems if used inappropriately.

You use advanced commands or parameters only with the advice of support personnel.

- **diagnostic**

Diagnostic commands and parameters are potentially disruptive. They are used only by support personnel to diagnose and fix problems.

## Set the privilege level in the CLI

You can set the privilege level in the CLI by using the `set` command. Changes to privilege level settings apply only to the session you are in. They are not persistent across sessions.

### Steps

1. To set the privilege level in the CLI, use the `set` command with the `-privilege` parameter.

### Example of setting the privilege level

The following example sets the privilege level to advanced and then to admin:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by technical support.
Do you wish to continue? (y or n): y
cluster1::*> set -privilege admin
```

## Set display preferences in the CLI

You can set display preferences for a CLI session by using the `set` command and `rows` command. The preferences you set apply only to the session you are in. They are not persistent across sessions.

### About this task

You can set the following CLI display preferences:

- The privilege level of the command session
- Whether confirmations are issued for potentially disruptive commands
- Whether `show` commands display all fields
- The character or characters to use as the field separator
- The default unit when reporting data sizes
- The number of rows the screen displays in the current CLI session before the interface pauses output

If the preferred number of rows is not specified, it is automatically adjusted based on the actual height of the terminal. If the actual height is undefined, the default number of rows is 24.

- The default storage virtual machine (SVM) or node
- Whether a continuing command should stop if it encounters an error

## Steps

1. To set CLI display preferences, use the `set` command.

To set the number of rows the screen displays in the current CLI session, you can also use the `rows` command.

For more information, see the man pages for the `set` command and `rows` command.

## Example of setting display preferences in the CLI

The following example sets a comma to be the field separator, sets GB as the default data-size unit, and sets the number of rows to 50:

```
cluster1::> set -showseparator "," -units GB
cluster1::> rows 50
```

## Methods of using query operators

The management interface supports queries and UNIX-style patterns and wildcards to enable you to match multiple values in command-parameter arguments.

The following table describes the supported query operators:

Operator	Description
*	Wildcard that matches all entries.  For example, the command <code>volume show -volume *tmp*</code> displays a list of all volumes whose names include the string <code>tmp</code> .
!	NOT operator.  Indicates a value that is not to be matched; for example, <code>!vs0</code> indicates not to match the value <code>vs0</code> .
	OR operator.  Separates two values that are to be compared; for example, <code>vs0   vs2</code> matches either <code>vs0</code> or <code>vs2</code> . You can specify multiple OR statements; for example, <code>a   b*   *c*</code> matches the entry <code>a</code> , any entry that starts with <code>b</code> , and any entry that includes <code>c</code> .
..	Range operator.  For example, <code>5..10</code> matches any value from 5 to 10, inclusive.

Operator	Description
<	Less-than operator.  For example, <20 matches any value that is less than 20.
>	Greater-than operator.  For example, >5 matches any value that is greater than 5.
<=	Less-than-or-equal-to operator.  For example, ≤5 matches any value that is less than or equal to 5.
>=	Greater-than-or-equal-to operator.  For example, ≥5 matches any value that is greater than or equal to 5.
{query}	Extended query.  An extended query must be specified as the first argument after the command name, before any other parameters.  For example, the command <code>volume modify {-volume *tmp*} -state offline</code> sets offline all volumes whose names include the string <code>tmp</code> .

If you want to parse query characters as literals, you must enclose the characters in double quotes (for example, “^”, “.”, “\*”, or “\$”) for the correct results to be returned.

You can use multiple query operators in one command line. For example, the command `volume show -size >1GB -percent-used <50 -vserver !vs1` displays all volumes that are greater than 1 GB in size, less than 50% utilized, and not in the storage virtual machine (SVM) named “vs1”.

### Methods of using extended queries

You can use extended queries to match and perform operations on objects that have specified values.

You specify extended queries by enclosing them within curly brackets ({}). An extended query must be specified as the first argument after the command name, before any other parameters. For example, to set offline all volumes whose names include the string `tmp`, you run the command in the following example:

```
cluster1::> volume modify {-volume *tmp*} -state offline
```

Extended queries are generally useful only with `modify` and `delete` commands. They have no meaning in `create` or `show` commands.

The combination of queries and modify operations is a useful tool. However, it can potentially cause confusion and errors if implemented incorrectly. For example, using the (advanced privilege) `system node image`

`modify` command to set a node's default software image automatically sets the other software image not to be the default. The command in the following example is effectively a null operation:

```
cluster1::*> system node image modify {-isdefault true} -isdefault false
```

This command sets the current default image as the non-default image, then sets the new default image (the previous non-default image) to the non-default image, resulting in the original default settings being retained. To perform the operation correctly, you can use the command as given in the following example:

```
cluster1::*> system node image modify {-iscurrent false} -isdefault true
```

### Methods of customizing show command output by using fields

When you use the `-instance` parameter with a `show` command to display details, the output can be lengthy and include more information than you need. The `-fields` parameter of a `show` command enables you to display only the information you specify.

For example, running `volume show -instance` is likely to result in several screens of information. You can use `volume show -fields fieldname [, fieldname...]` to customize the output so that it includes only the specified field or fields (in addition to the default fields that are always displayed.) You can use `-fields ?` to display valid fields for a `show` command.

The following example shows the output difference between the `-instance` parameter and the `-fields` parameter:

```

cluster1::> volume show -instance

                                Vserver Name: cluster1-1
                                Volume Name: vol0
                                Aggregate Name: aggr0
                                Volume Size: 348.3GB
                                Volume Data Set ID: -
                                Volume Master Data Set ID: -
                                Volume State: online
                                Volume Type: RW
                                Volume Style: flex
                                ...
                                Space Guarantee Style: volume
                                Space Guarantee in Effect: true
                                ...
Press <space> to page down, <return> for next line, or 'q' to quit...
...
cluster1::>

cluster1::> volume show -fields space-guarantee,space-guarantee-enabled

vserver  volume  space-guarantee  space-guarantee-enabled
-----  -
cluster1-1  vol0    volume          true
cluster1-2  vol0    volume          true
vs1        root_vol
          volume          true
vs2        new_vol
          volume          true
vs2        root_vol
          volume          true
...
cluster1::>

```

### About positional parameters

You can take advantage of the positional parameter functionality of the ONTAP CLI to increase efficiency in command input. You can query a command to identify parameters that are positional for the command.

#### What a positional parameter is

- A positional parameter is a parameter that does not require you to specify the parameter name before specifying the parameter value.
- A positional parameter can be interspersed with nonpositional parameters in the command input, as long as it observes its relative sequence with other positional parameters in the same command, as indicated in

the ***command\_name*** ? output.

- A positional parameter can be a required or optional parameter for a command.
- A parameter can be positional for one command but nonpositional for another.



Using the positional parameter functionality in scripts is not recommended, especially when the positional parameters are optional for the command or have optional parameters listed before them.

### Identify a positional parameter

You can identify a positional parameter in the ***command\_name*** ? command output. A positional parameter has square brackets surrounding its parameter name, in one of the following formats:

- `[-parameter_name] parameter_value` shows a required parameter that is positional.
- `[[[-parameter_name] parameter_value]]` shows an optional parameter that is positional.

For example, when displayed as the following in the ***command\_name*** ? output, the parameter is positional for the command it appears in:

- `[-lif] <lif-name>`
- `[[[-lif] <lif-name>]]`

However, when displayed as the following, the parameter is nonpositional for the command it appears in:

- `-lif <lif-name>`
- `[-lif <lif-name>]`

### Examples of using positional parameters

In the following example, the ***volume create*** ? output shows that three parameters are positional for the command: `-volume`, `-aggregate`, and `-size`.



```

cluster1::> volume create ?
  -vserver <vserver name>           Vserver Name
  [-volume] <volume name>          Volume Name
  [-aggregate] <aggregate name>    Aggregate Name
  [[-size] {<integer>[KB|MB|GB|TB|PB]]] Volume Size
  [ -state {online|restricted|offline|force-online|force-offline|mixed} ]
                                         Volume State (default: online)
  [ -type {RW|DP|DC} ]              Volume Type (default: RW)
  [ -policy <text> ]                Export Policy
  [ -user <user name> ]             User ID
  ...
  [ -space-guarantee|-s {none|volume} ] Space Guarantee Style (default:
volume)
  [ -percent-snapshot-space <percent> ] Space Reserved for Snapshot
Copies
  ...

```

In the following example, the `volume create` command is specified without taking advantage of the positional parameter functionality:

```

cluster1::> volume create -vserver svml -volume vol1 -aggregate aggr1 -size 1g
-percent-snapshot-space 0

```

The following examples use the positional parameter functionality to increase the efficiency of the command input. The positional parameters are interspersed with nonpositional parameters in the `volume create` command, and the positional parameter values are specified without the parameter names. The positional parameters are specified in the same sequence indicated by the `volume create ?` output. That is, the value for `-volume` is specified before that of `-aggregate`, which is in turn specified before that of `-size`.

```

cluster1::> volume create vol2 aggr1 1g -vserver svml -percent-snapshot-space 0

```

```

cluster1::> volume create -vserver svml vol3 -snapshot-policy default aggr1
-nvfail off 1g -space-guarantee none

```

## Methods of accessing ONTAP man pages

ONTAP manual (man) pages explain how to use ONTAP commands. They are available at the command line and on the NetApp Support Site.

The `man command_name` command displays the manual page of the specified command. If you do not specify a command name, the manual page index is displayed. You can use the `man man` command to view information about the `man` command itself. You can exit a man page by entering `q`.

The [ONTAP 9 man pages](#) contains command references for the admin-level and advanced-level ONTAP commands.

## Cluster management basics (cluster administrators only)

### Display information about the nodes in a cluster

You can display node names, whether the nodes are healthy, and whether they are eligible to participate in the cluster. At the advanced privilege level, you can also display whether a node holds epsilon.

#### Steps

1. To display information about the nodes in a cluster, use the `cluster show` command.

If you want the output to show whether a node holds epsilon, run the command at the advanced privilege level.

### Examples of displaying the nodes in a cluster

The following example displays information about all nodes in a four-node cluster:

```
cluster1::> cluster show
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
node3                true   true
node4                true   true
```

The following example displays detailed information about the node named “node1” at the advanced privilege level:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> cluster show -node node1

    Node: node1
Node UUID: a67f9f34-9d8f-11da-b484-000423b6f094
    Epsilon: false
Eligibility: true
    Health: true
```

### Display cluster attributes

You can display a cluster’s unique identifier (UUID), name, serial number, location, and contact information.

## Steps

1. To display a cluster's attributes, use the `cluster identity show` command.

### Example of displaying cluster attributes

The following example displays the name, serial number, location, and contact information of a cluster.

```
cluster1::> cluster identity show

      Cluster UUID: 1cd8a442-86d1-11e0-ae1c-123478563412
      Cluster Name: cluster1
Cluster Serial Number: 1-80-123456
      Cluster Location: Sunnyvale
      Cluster Contact: jsmith@example.com
```

## Modify cluster attributes

You can modify a cluster's attributes, such as the cluster name, location, and contact information as needed.

### About this task

You cannot change a cluster's UUID, which is set when the cluster is created.

## Steps

1. To modify cluster attributes, use the `cluster identity modify` command.

The `-name` parameter specifies the name of the cluster. The `cluster identity modify` man page describes the rules for specifying the cluster's name.

The `-location` parameter specifies the location for the cluster.

The `-contact` parameter specifies the contact information such as a name or e-mail address.

### Example of renaming a cluster

The following command renames the current cluster ("cluster1") to "cluster2":

```
cluster1::> cluster identity modify -name cluster2
```

## Display the status of cluster replication rings

You can display the status of cluster replication rings to help you diagnose cluster-wide problems. If your cluster is experiencing problems, support personnel might ask you to perform this task to assist with troubleshooting efforts.

## Steps

1. To display the status of cluster replication rings, use the `cluster ring show` command at the advanced privilege level.

## Example of displaying cluster ring-replication status

The following example displays the status of the VLDB replication ring on a node named node0:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you wish to continue? (y or n): y

cluster1::*> cluster ring show -node node0 -unitname vldb
      Node: node0
    Unit Name: vldb
      Status: master
      Epoch: 5
  Master Node: node0
    Local Node: node0
      DB Epoch: 5
DB Transaction: 56
  Number Online: 4
      RDB UUID: e492d2c1-fc50-11e1-bae3-123478563412
```

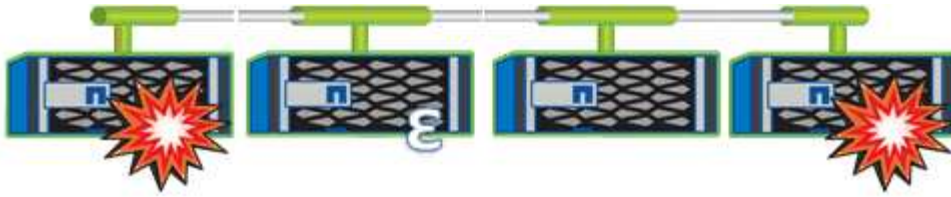
## About quorum and epsilon

Quorum and epsilon are important measures of cluster health and function that together indicate how clusters address potential communications and connectivity challenges.

*Quorum* is a precondition for a fully functioning cluster. When a cluster is in quorum, a simple majority of nodes are healthy and can communicate with each other. When quorum is lost, the cluster loses the ability to accomplish normal cluster operations. Only one collection of nodes can have quorum at any one time because all of the nodes collectively share a single view of the data. Therefore, if two non-communicating nodes are permitted to modify the data in divergent ways, it is no longer possible to reconcile the data into a single data view.

Each node in the cluster participates in a voting protocol that elects one node *master*; each remaining node is a *secondary*. The master node is responsible for synchronizing information across the cluster. When quorum is formed, it is maintained by continual voting. If the master node goes offline and the cluster is still in quorum, a new master is elected by the nodes that remain online.

Because there is the possibility of a tie in a cluster that has an even number of nodes, one node has an extra fractional voting weight called *epsilon*. If the connectivity between two equal portions of a large cluster fails, the group of nodes containing epsilon maintains quorum, assuming that all of the nodes are healthy. For example, the following illustration shows a four-node cluster in which two of the nodes have failed. However, because one of the surviving nodes holds epsilon, the cluster remains in quorum even though there is not a simple majority of healthy nodes.



Epsilon is automatically assigned to the first node when the cluster is created. If the node that holds epsilon becomes unhealthy, takes over its high-availability partner, or is taken over by its high-availability partner, then epsilon is automatically reassigned to a healthy node in a different HA pair.

Taking a node offline can affect the ability of the cluster to remain in quorum. Therefore, ONTAP issues a warning message if you attempt an operation that will either take the cluster out of quorum or else put it one outage away from a loss of quorum. You can disable the quorum warning messages by using the `cluster quorum-service options modify` command at the advanced privilege level.

In general, assuming reliable connectivity among the nodes of the cluster, a larger cluster is more stable than a smaller cluster. The quorum requirement of a simple majority of half the nodes plus epsilon is easier to maintain in a cluster of 24 nodes than in a cluster of two nodes.

A two-node cluster presents some unique challenges for maintaining quorum. Two-node clusters use *cluster HA*, in which neither node holds epsilon; instead, both nodes are continuously polled to ensure that if one node fails, the other has full read-write access to data, as well as access to logical interfaces and management functions.

### What system volumes are

System volumes are FlexVol volumes that contain special metadata, such as metadata for file services audit logs. These volumes are visible in the cluster so that you can fully account for storage use in your cluster.

System volumes are owned by the cluster management server (also called the admin SVM), and they are created automatically when file services auditing is enabled.

You can view system volumes by using the `volume show` command, but most other volume operations are not permitted. For example, you cannot modify a system volume by using the `volume modify` command.

This example shows four system volumes on the admin SVM, which were automatically created when file services auditing was enabled for a data SVM in the cluster:

```

cluster1::> volume show -vserver cluster1
Vserver      Volume                Aggregate      State      Type      Size  Available
Used%
-----
-----
cluster1 MDV_aud_1d0131843d4811e296fc123478563412
          aggr0                online      RW          2GB      1.90GB
5%
cluster1 MDV_aud_8be27f813d7311e296fc123478563412
          root_vs0              online      RW          2GB      1.90GB
5%
cluster1 MDV_aud_9dc4ad503d7311e296fc123478563412
          aggr1                online      RW          2GB      1.90GB
5%
cluster1 MDV_aud_a4b887ac3d7311e296fc123478563412
          aggr2                online      RW          2GB      1.90GB
5%
4 entries were displayed.

```

## Manage nodes

### Display node attributes

You can display the attributes of one or more nodes in the cluster, for example, the name, owner, location, model number, serial number, how long the node has been running, health state, and eligibility to participate in a cluster.

### Steps

1. To display the attributes of a specified node or about all nodes in a cluster, use the `system node show` command.

### Example of displaying information about a node

The following example displays detailed information about node1:

```
cluster1::> system node show -node node1
                Node: node1
                Owner: Eng IT
                Location: Lab 5
                Model: model_number
Serial Number: 12345678
                Asset Tag: -
                Uptime: 23 days 04:42
NVRAM System ID: 118051205
                System ID: 0118051205
                Vendor: NetApp
                Health: true
                Eligibility: true
Differentiated Services: false
                All-Flash Optimized: true
                Capacity Optimized: false
                QLC Optimized: false
                All-Flash Select Optimized: false
SAS2/SAS3 Mixed Stack Support: none
```

## Modify node attributes

You can modify the attributes of a node as required. The attributes that you can modify include the node's owner information, location information, asset tag, and eligibility to participate in the cluster.

### About this task

A node's eligibility to participate in the cluster can be modified at the advanced privilege level by using the `-eligibility` parameter of the `system node modify` or `cluster modify` command. If you set a node's eligibility to `false`, the node becomes inactive in the cluster.



You cannot modify node eligibility locally. It must be modified from a different node. Node eligibility also cannot be modified with a cluster HA configuration.



You should avoid setting a node's eligibility to `false`, except for situations such as restoring the node configuration or prolonged node maintenance. SAN and NAS data access to the node might be impacted when the node is ineligible.

### Steps

1. Use the `system node modify` command to modify a node's attributes.

### Example of modifying node attributes

The following command modifies the attributes of the "node1" node. The node's owner is set to "Joe Smith" and its asset tag is set to "js1234":

```
cluster1::> system node modify -node node1 -owner "Joe Smith" -assettag
js1234
```

## Rename a node

You can change a node's name as required.

### Steps

1. To rename a node, use the `system node rename` command.

The `-newname` parameter specifies the new name for the node. The `system node rename` man page describes the rules for specifying the node name.

If you want to rename multiple nodes in the cluster, you must run the command for each node individually.



Node name cannot be "all" because "all" is a system reserved name.

### Example of renaming a node

The following command renames node "node1" to "node1a":

```
cluster1::> system node rename -node node1 -newname node1a
```

## Add nodes to the cluster

After a cluster is created, you can expand it by adding nodes to it. You add only one node at a time.

### What you'll need

- If you are adding nodes to a multiple-node cluster, more than half of the existing nodes in the cluster must be healthy (indicated by `cluster show`).
- If you are adding nodes to a two-node switchless cluster, you must have installed and configured the cluster management and interconnect switches before adding additional nodes.

The switchless cluster functionality is supported only in a two-node cluster.

When a cluster contains or grows to more than two nodes, cluster HA is not required and is disabled automatically.

- If you are adding a second node to a single-node cluster, the second node must have been installed, and the cluster network must have been configured.
- If the cluster has the SP automatic configuration enabled, the subnet specified for the SP to use must have available resources for the joining node.

A node that joins the cluster uses the specified subnet to perform automatic configuration for the SP.

- You must have gathered the following information for the new node's node management LIF:
  - Port



- IP address
- Netmask
- Default gateway

### About this task

Nodes must be in even numbers so that they can form HA pairs. After you start to add a node to the cluster, you must complete the process. The node must be part of the cluster before you can start to add another node.

### Steps

1. Power on the node that you want to add to the cluster.

The node boots, and the Node Setup wizard starts on the console.

```
Welcome to node setup.
```

```
You can enter the following commands at any time:
```

```
"help" or "?" - if you want to have a question clarified,
```

```
"back" - if you want to change previously answered questions, and
```

```
"exit" or "quit" - if you want to quit the setup wizard.
```

```
Any changes you made before quitting will be saved.
```

```
To accept a default or omit a question, do not enter a value.
```

```
Enter the node management interface port [e0c]:
```

2. Exit the Node Setup wizard: `exit`

The Node Setup wizard exits, and a login prompt appears, warning that you have not completed the setup tasks.

3. Log in to the admin account by using the `admin` user name.
4. Start the Cluster Setup wizard:

```
cluster setup
```

```
::> cluster setup
```

Welcome to the cluster setup wizard.

You can enter the following commands at any time:

```
"help" or "?" - if you want to have a question clarified,  
"back" - if you want to change previously answered questions, and  
"exit" or "quit" - if you want to quit the cluster setup wizard.  
Any changes you made before quitting will be saved.
```

You can return to cluster setup at any time by typing "cluster setup".  
To accept a default or omit a question, do not enter a value....

Use your web browser to complete cluster setup by accessing  
<https://10.63.11.29>

Otherwise, press Enter to complete cluster setup using the  
command line interface:



For more information on setting up a cluster using the setup GUI, see the [System Manager online help](#).

5. Press Enter to use the CLI to complete this task. When prompted to create a new cluster or join an existing one, enter **join**.

```
Do you want to create a new cluster or join an existing cluster?  
{create, join}:  
join
```

6. Follow the prompts to set up the node and join it to the cluster:
  - To accept the default value for a prompt, press Enter.
  - To enter your own value for a prompt, enter the value, and then press Enter.
7. Repeat the preceding steps for each additional node that you want to add.

### After you finish

After adding nodes to the cluster, you should enable storage failover for each HA pair.

### Remove nodes from the cluster

You can remove unwanted nodes from a cluster, one node at a time. After you remove a node, you must also remove its failover partner. If you are removing a node, then its data becomes inaccessible or erased.

### Before you begin

The following conditions must be satisfied before removing nodes from the cluster:

- More than half of the nodes in the cluster must be healthy.
- All of the data on the node that you want to remove must have been evacuated.
  - This might include [purging data from an encrypted volume](#).
- All volumes have been [moved](#) or [deleted](#) from aggregates owned by the node.
- All aggregates have been [deleted](#) from the node.
- If the node owns Federal Information Processing Standards (FIPS) disks or self-encrypting disks (SEDs), [disk encryption has been removed](#) by returning the disks to unprotected mode.
  - You might also want to [sanitize FIPS drives or SEDs](#).
- Data LIFs have been [deleted](#) or [relocated](#) from the node.
- Cluster management LIFs have been [relocated](#) from the node and the home ports changed.
- All intercluster LIFs have been [removed](#).
  - When you remove intercluster LIFs a warning is displayed that can be ignored.
- Storage failover has been [disabled](#) for the node.
- All LIF failover rules have been [modified](#) to remove ports on the node.
- All VLANs on the node have been [deleted](#).

It is recommended that you issue an AutoSupport message to notify NetApp technical support that node removal is underway.

**Note:** You must not perform operations such as `cluster remove-node`, `cluster unjoin`, and `node rename` when an automated ONTAP upgrade is in progress.

### About this task

If you are running a mixed-version cluster, you can remove the last low-version node by using one of the advanced privilege commands beginning with ONTAP 9.3:

- ONTAP 9.3: `cluster unjoin -skip-last-low-version-node-check`
- ONTAP 9.4 and later: `cluster remove-node -skip-last-low-version-node-check`

**Note:** All system and user data, from all disks that are connected to the node, must be made inaccessible to users before removing a node from the cluster. If a node was incorrectly unjoined from a cluster, contact NetApp Support for assistance with options for recovery.

### Steps

1. Change the privilege level to advanced:

```
set -privilege advanced
```

2. If the node you want to remove is the current master node, then enable another node in the cluster to be elected as the master node by changing the master node's cluster eligibility to `false`:

```
cluster modify -eligibility false
```

The master node is the node that holds processes such as "mgmt", "vldb", "vifmgr", "bcomd", and "crs". The `cluster ring show advanced` command shows the current master node.

```
cluster::*> cluster modify -node nodel -eligibility false
```

3. Remove the node from the cluster:

For this ONTAP version...	Use this command...
ONTAP 9.3	<code>cluster unjoin</code>
ONTAP 9.4 and later	<code>cluster remove-node</code>

If you have a mixed version cluster and you are removing the last lower version node, use the `-skip -last-low-version-node-check` parameter with these commands.

The system informs you of the following:

- You must also remove the node's failover partner from the cluster.
- After the node is removed and before it can rejoin a cluster, you must use boot menu option (4) Clean configuration and initialize all disks or option (9) Configure Advanced Drive Partitioning to erase the node's configuration and initialize all disks.

A failure message is generated if you have conditions that you must address before removing the node. For example, the message might indicate that the node has shared resources that you must remove or that the node is in a cluster HA configuration or storage failover configuration that you must disable.

If the node is the quorum master, the cluster will briefly lose and then return to quorum. This quorum loss is temporary and does not affect any data operations.

4. If a failure message indicates error conditions, address those conditions and rerun the `cluster remove-node` or `cluster unjoin` command.

The node is automatically rebooted after it is successfully removed from the cluster.

5. If you are repurposing the node, erase the node configuration and initialize all disks:
- a. During the boot process, press Ctrl-C to display the boot menu when prompted to do so.
  - b. Select the boot menu option **(4) Clean configuration and initialize all disks**.

6. Return to admin privilege level:

```
set -privilege admin
```

7. Repeat the preceding steps to remove the failover partner from the cluster.

### After you finish

If you removed nodes to have a single-node cluster, you should modify the cluster ports to serve data traffic by modifying the cluster ports to be data ports, and then creating data LIFs on the data ports.

### Access a node's log, core dump, and MIB files by using a web browser

The Service Processor Infrastructure (`spl`) web service is enabled by default to enable a

web browser to access the log, core dump, and MIB files of a node in the cluster. The files remain accessible even when the node is down, provided that the node is taken over by its partner.

### What you'll need

- The cluster management LIF must be up.

You can use the management LIF of the cluster or a node to access the `spi` web service. However, using the cluster management LIF is recommended.

The `network interface show` command displays the status of all LIFs in the cluster.

- If your user account does not have the “admin” role (which has access to the `spi` web service by default), your access-control role must be granted access to the `spi` web service.

The `vserver services web access show` command shows what roles are granted access to which web services.

- If you are not using the “admin” user account (which includes the `http` access method by default), your user account must be set up with the `http` access method.

The `security login show` command shows user accounts' access and login methods and their access-control roles.

- If you want to use HTTPS for secure web access, SSL must be enabled and a digital certificate must be installed.

The `system services web show` command displays the configuration of the web protocol engine at the cluster level.

### About this task

The `spi` web service is enabled by default, and the service can be disabled manually (`vserver services web modify -vserver * -name spi -enabled false`).

The “admin” role is granted access to the `spi` web service by default, and the access can be disabled manually (`services web access delete -vserver cluster_name -name spi -role admin`).

### Steps

1. Point the web browser to the `spi` web service URL in one of the following formats:

- `http://cluster-mgmt-LIF/spi/`
- `https://cluster-mgmt-LIF/spi/`

`cluster-mgmt-LIF` is the IP address of the cluster management LIF.

2. When prompted by the browser, enter your user account and password.

After your account is authenticated, the browser displays links to the `/mroot/etc/log/`, `/mroot/etc/crash/`, and `/mroot/etc/mib/` directories of each node in the cluster.

## Access the system console of a node

If a node is hanging at the boot menu or the boot environment prompt, you can access it only through the system console (also called the *serial console*). You can access the system console of a node from an SSH connection to the node's SP or to the cluster.

### About this task

Both the SP and ONTAP offer commands that enable you to access the system console. However, from the SP, you can access only the system console of its own node. From the cluster, you can access the system console of any node in the cluster.

### Steps

1. Access the system console of a node:

If you are in the...	Enter this command...
SP CLI of the node	<code>system console</code>
ONTAP CLI	<code>system node run-console</code>

2. Log in to the system console when you are prompted to do so.
3. To exit the system console, press Ctrl-D.

### Examples of accessing the system console

The following example shows the result of entering the `system console` command at the "SP node2" prompt. The system console indicates that node2 is hanging at the boot environment prompt. The `boot_ontap` command is entered at the console to boot the node to ONTAP. Ctrl-D is then pressed to exit the console and return to the SP.

```
SP node2> system console
Type Ctrl-D to exit.

LOADER>
LOADER> boot_ontap
...
*****
*                                     *
* Press Ctrl-C for Boot Menu.      *
*                                     *
*****
...
```

(Ctrl-D is pressed to exit the system console.)

```
Connection to 123.12.123.12 closed.  
SP node2>
```

The following example shows the result of entering the `system node run-console` command from ONTAP to access the system console of node2, which is hanging at the boot environment prompt. The `boot_ontap` command is entered at the console to boot node2 to ONTAP. Ctrl-D is then pressed to exit the console and return to ONTAP.

```
cluster1::> system node run-console -node node2  
Pressing Ctrl-D will end this session and any further sessions you might  
open on top of this session.  
Type Ctrl-D to exit.  
  
LOADER>  
LOADER> boot_ontap  
  
...  
*****  
*                                     *  
* Press Ctrl-C for Boot Menu. *  
*                                     *  
*****  
  
...
```

(Ctrl-D is pressed to exit the system console.)

```
Connection to 123.12.123.12 closed.  
cluster1::>
```

## Rules governing node root volumes and root aggregates

### Rules governing node root volumes and root aggregates overview

A node's root volume contains special directories and files for that node. The root aggregate contains the root volume. A few rules govern a node's root volume and root aggregate.

A node's root volume is a FlexVol volume that is installed at the factory or by setup software. It is reserved for system files, log files, and core files. The directory name is `/mroot`, which is accessible only through the systemshell by technical support. The minimum size for a node's root volume depends on the platform model.

- The following rules govern the node's root volume:
  - Unless technical support instructs you to do so, do not modify the configuration or content of the root volume.
  - Do not store user data in the root volume.

Storing user data in the root volume increases the storage giveback time between nodes in an HA pair.

- You can move the root volume to another aggregate.

#### [Relocate root volumes to new aggregates](#)

- The root aggregate is dedicated to the node's root volume only.

ONTAP prevents you from creating other volumes in the root aggregate.

## NetApp Hardware Universe

### Free up space on a node's root volume

A warning message appears when a node's root volume has become full or almost full. The node cannot operate properly when its root volume is full. You can free up space on a node's root volume by deleting core dump files, packet trace files, and root volume Snapshot copies.

#### Steps

1. Display the node's core dump files and their names by using the `system node coredump show` command.
2. Delete unwanted core dump files from the node by using the `system node coredump delete` command.
3. Access the nodeshell:

```
system node run -node nodename
```

*nodename* is the name of the node whose root volume space you want to free up.

4. Switch to the nodeshell advanced privilege level from the nodeshell:

```
priv set advanced
```

5. Display and delete the node's packet trace files through the nodeshell:
  - a. Display all files in the node's root volume:

```
ls /etc
```

- b. If any packet trace files (`*.trc`) are in the node's root volume, delete them individually:

```
rm /etc/log/packet_traces/file_name.trc
```

6. Identify and delete the node's root volume Snapshot copies through the nodeshell:
  - a. Identify the root volume name:

```
vol status
```

The root volume is indicated by the word "root" in the "Options" column of the `vol status` command output.



In the following example, the root volume is `vol10`:

```
node1*> vol status

          Volume State           Status           Options
          vol10 online          raid_dp, flex  root, nvfail=on
                               64-bit
```

b. Display root volume Snapshot copies:

```
snap list root_vol_name
```

c. Delete unwanted root volume Snapshot copies:

```
snap delete root_vol_name snapshot_name
```

7. Exit the nodeshell and return to the clustershell:

```
exit
```

### Relocate root volumes to new aggregates

The root replacement procedure migrates the current root aggregate to another set of disks without disruption.

#### About this task

Storage failover must be enabled to relocate root volumes. You can use the `storage failover modify -node nodename -enable true` command to enable failover.

You can change the location of the root volume to a new aggregate in the following scenarios:

- When the root aggregates are not on the disk you prefer
- When you want to rearrange the disks connected to the node
- When you are performing a shelf replacement of the EOS disk shelves

#### Steps

1. Set the privilege level to advanced:

```
set privilege advanced
```

2. Relocate the root aggregate:

```
system node migrate-root -node nodename -disklist disklist -raid-type raid-type
```

- **-node**

Specifies the node that owns the root aggregate that you want to migrate.

- **-disklist**

Specifies the list of disks on which the new root aggregate will be created. All disks must be spares and owned by the same node. The minimum number of disks required is dependent on the RAID type.

- **-raid-type**

Specifies the RAID type of the root aggregate. The default value is `raid-dp`.

3. Monitor the progress of the job:

```
job show -id jobid -instance
```

## Results

If all of the pre-checks are successful, the command starts a root volume replacement job and exits. Expect the node to restart.

## Start or stop a node

### Start or stop a node overview

You might need to start or stop a node for maintenance or troubleshooting reasons. You can do so from the ONTAP CLI, the boot environment prompt, or the SP CLI.

Using the SP CLI command `system power off` or `system power cycle` to turn off or power-cycle a node might cause an improper shutdown of the node (also called a *dirty shutdown*) and is not a substitute for a graceful shutdown using the ONTAP `system node halt` command.

### Reboot a node at the system prompt

You can reboot a node in normal mode from the system prompt. A node is configured to boot from the boot device, such as a PC CompactFlash card.

## Steps

1. If the cluster contains four or more nodes, verify that the node to be rebooted does not hold epsilon:
  - a. Set the privilege level to advanced:

```
set -privilege advanced
```

- b. Determine which node holds epsilon:

```
cluster show
```

The following example shows that “node1” holds epsilon:

```
cluster1::*> cluster show
Node                Health  Eligibility  Epsilon
-----
node1                true   true         true
node2                true   true         false
node3                true   true         false
node4                true   true         false
4 entries were displayed.
```

c. If the node to be rebooted holds epsilon, then remove epsilon from the node:

```
cluster modify -node node_name -epsilon false
```

d. Assign epsilon to a different node that will remain up:

```
cluster modify -node node_name -epsilon true
```

e. Return to the admin privilege level:

```
set -privilege admin
```

2. Use the `system node reboot` command to reboot the node.

If you do not specify the `-skip-lif-migration` parameter, the command attempts to migrate data and cluster management LIFs synchronously to another node prior to the reboot. If the LIF migration fails or times out, the rebooting process is aborted, and ONTAP displays an error to indicate the LIF migration failure.

```
cluster1::> system node reboot -node node1 -reason "software upgrade"
```

The node begins the reboot process. The ONTAP login prompt appears, indicating that the reboot process is complete.

### Boot ONTAP at the boot environment prompt

You can boot the current release or the backup release of ONTAP when you are at the boot environment prompt of a node.

#### Steps

1. Access the boot environment prompt from the storage system prompt by using the `system node halt` command.

The storage system console displays the boot environment prompt.

2. At the boot environment prompt, enter one of the following commands:

To boot...	Enter...
The current release of ONTAP	boot_ontap
The ONTAP primary image from the boot device	boot_primary
The ONTAP backup image from the boot device	boot_backup

If you are unsure about which image to use, you should use `boot_ontap` in the first instance.

### Shut down a node

You can shut down a node if it becomes unresponsive or if support personnel direct you to do so as part of troubleshooting efforts.

#### Steps

1. If the cluster contains four or more nodes, verify that the node to be shut down does not hold epsilon:

- a. Set the privilege level to advanced:

```
set -privilege advanced
```

- b. Determine which node holds epsilon:

```
cluster show
```

The following example shows that “node1” holds epsilon:

```
cluster1::*> cluster show
Node                Health  Eligibility  Epsilon
-----
node1                true    true         true
node2                true    true         false
node3                true    true         false
node4                true    true         false
4 entries were displayed.
```

- c. If the node to be shut down holds epsilon, then remove epsilon from the node:

```
cluster modify -node node_name -epsilon false
```

- d. Assign epsilon to a different node that will remain up:

```
cluster modify -node node_name -epsilon true
```

- e. Return to the admin privilege level:

```
set -privilege admin
```

2. Use the `system node halt` command to shut down the node.

If you do not specify the `-skip-lif-migration` parameter, the command attempts to migrate data and cluster management LIFs synchronously to another node prior to the shutdown. If the LIF migration fails or times out, the shutdown process is aborted, and ONTAP displays an error to indicate the LIF migration failure.

You can manually trigger a core dump with the shutdown by using both the `-dump` parameter.

The following example shuts down the node named “node1” for hardware maintenance:

```
cluster1::> system node halt -node node1 -reason 'hardware maintenance'
```

## Manage a node by using the boot menu

You can use the boot menu to correct configuration problems on a node, reset the admin password, initialize disks, reset the node configuration, and restore the node configuration information back to the boot device.



If an HA pair is using [encrypting SAS or NVMe drives \(SED, NSE, FIPS\)](#), you must follow the instructions in the topic [Returning a FIPS drive or SED to unprotected mode](#) for all drives within the HA pair prior to initializing the system (boot options 4 or 9). Failure to do this may result in future data loss if the drives are repurposed.

### Steps

1. Reboot the node to access the boot menu by using the `system node reboot` command at the system prompt.

The node begins the reboot process.

2. During the reboot process, press Ctrl-C to display the boot menu when prompted to do so.


The node displays the following options for the boot menu:

```
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning
Selection (1-9)?
```



Boot menu option (2) Boot without `/etc/rc` is obsolete and takes no effect on the system.

3. Select one of the following options by entering the corresponding number:

To...	Select...
Continue to boot the node in normal mode	1) Normal Boot
Change the password of the node, which is also the "admin" account password	3) Change Password
Initialize the node's disks and create a root volume for the node	<p>4) Clean configuration and initialize all disks</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-left: 20px;">  <p>This menu option erases all data on the disks of the node and resets your node configuration to the factory default settings.</p> </div> <p>Only select this menu item after the node has been removed from a cluster (unjoined) and is not joined to another cluster.</p> <p>For a node with internal or external disk shelves, the root volume on the internal disks is initialized. If there are no internal disk shelves, then the root volume on the external disks is initialized.</p> <p>For a system running FlexArray Virtualization with internal or external disk shelves, the array LUNs are not initialized. Any native disks on either internal or external shelves are initialized.</p> <p>For a system running FlexArray Virtualization with only array LUNS and no internal or external disk shelves, the root volume on the storage array LUNS are initialized, see <a href="#">Installing FlexArray</a>.</p> <p>If the node you want to initialize has disks that are partitioned for root-data partitioning, the disks must be unpartitioned before the node can be initialized, see <b>9) Configure Advanced Drive Partitioning</b> and <a href="#">Disks and aggregates management</a>.</p>
Perform aggregate and disk maintenance operations and obtain detailed aggregate and disk information.	<p>5) Maintenance mode boot</p> <p>You exit Maintenance mode by using the <code>halt</code> command.</p>
Restore the configuration information from the node's root volume to the boot device, such as a PC CompactFlash card	<p>6) Update flash from backup config</p> <p>ONTAP stores some node configuration information on the boot device. When the node reboots, the information on the boot device is automatically backed up onto the node's root volume. If the boot device becomes corrupted or needs to be replaced, you must use this menu option to restore the configuration information from the node's root volume back to the boot device.</p>

To...	Select...
Install new software on the node	<p>7) Install new software first</p> <p>If the ONTAP software on the boot device does not include support for the storage array that you want to use for the root volume, you can use this menu option to obtain a version of the software that supports your storage array and install it on the node.</p> <p>This menu option is only for installing a newer version of ONTAP software on a node that has no root volume installed. Do <i>not</i> use this menu option to upgrade ONTAP.</p>
Reboot the node	8) Reboot node
Unpartition all disks and remove their ownership information or clean the configuration and initialize the system with whole or partitioned disks	<p>9) Configure Advanced Drive Partitioning</p> <p>Beginning with ONTAP 9.2, the Advanced Drive Partitioning option provides additional management features for disks that are configured for root-data or root-data-data partitioning. The following options are available from Boot Option 9:</p> <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;"> <p>(9a) Unpartition all disks and remove their ownership information.</p> <p>(9b) Clean configuration and initialize system with partitioned disks.</p> <p>(9c) Clean configuration and initialize system with whole disks.</p> <p>(9d) Reboot the node.</p> <p>(9e) Return to main boot menu.</p> </div>

## Manage a node remotely using the SP/BMC

### Manage a node remotely using the SP/BMC overview

You can manage a node remotely using an onboard controller, called a Service Processor (SP) or Baseboard Management Controller (BMC). This remote management controller is included in all current platform models. The controller stays operational regardless of the operating state of the node.

The following platforms support BMC instead of SP:

- FAS 8700
- FAS 8300
- FAS27x0
- AFF A800

- AFF A700s
- AFF A400
- AFF A320
- AFF A220
- AFF C190

## About the SP

The Service Processor (SP) is a remote management device that enables you to access, monitor, and troubleshoot a node remotely.

The key capabilities of the SP include the following:

- The SP enables you to access a node remotely to diagnose, shut down, power-cycle, or reboot the node, regardless of the state of the node controller.

The SP is powered by a standby voltage, which is available as long as the node has input power from at least one of its power supplies.

You can log in to the SP by using a Secure Shell client application from an administration host. You can then use the SP CLI to monitor and troubleshoot the node remotely. In addition, you can use the SP to access the serial console and run ONTAP commands remotely.

You can access the SP from the serial console or access the serial console from the SP. The SP enables you to open both an SP CLI session and a separate console session simultaneously.

For instance, when a temperature sensor becomes critically high or low, ONTAP triggers the SP to shut down the motherboard gracefully. The serial console becomes unresponsive, but you can still press Ctrl-G on the console to access the SP CLI. You can then use the `system power on` or `system power cycle` command from the SP to power on or power-cycle the node.

- The SP monitors environmental sensors and logs events to help you take timely and effective service actions.

The SP monitors environmental sensors such as the node temperatures, voltages, currents, and fan speeds. When an environmental sensor has reached an abnormal condition, the SP logs the abnormal readings, notifies ONTAP of the issue, and sends alerts and “down system” notifications as necessary through an AutoSupport message, regardless of whether the node can send AutoSupport messages.

The SP also logs events such as boot progress, Field Replaceable Unit (FRU) changes, events generated by ONTAP, and SP command history. You can manually invoke an AutoSupport message to include the SP log files that are collected from a specified node.

Other than generating these messages on behalf of a node that is down and attaching additional diagnostic information to AutoSupport messages, the SP has no effect on the AutoSupport functionality. The AutoSupport configuration settings and message content behavior are inherited from ONTAP.



The SP does not rely on the `-transport` parameter setting of the `system node autosupport modify` command to send notifications. The SP only uses the Simple Mail Transport Protocol (SMTP) and requires its host's AutoSupport configuration to include mail host information.



If SNMP is enabled, the SP generates SNMP traps to configured trap hosts for all “down system” events.

- The SP has a nonvolatile memory buffer that stores up to 4,000 events in a system event log (SEL) to help you diagnose issues.

The SEL stores each audit log entry as an audit event. It is stored in onboard flash memory on the SP. The event list from the SEL is automatically sent by the SP to specified recipients through an AutoSupport message.

The SEL contains the following information:

- Hardware events detected by the SP—for example, sensor status about power supplies, voltage, or other components
  - Errors detected by the SP—for example, a communication error, a fan failure, or a memory or CPU error
  - Critical software events sent to the SP by the node—for example, a panic, a communication failure, a boot failure, or a user-triggered “down system” as a result of issuing the SP `system reset` or `system power cycle` command
- The SP monitors the serial console regardless of whether administrators are logged in or connected to the console.

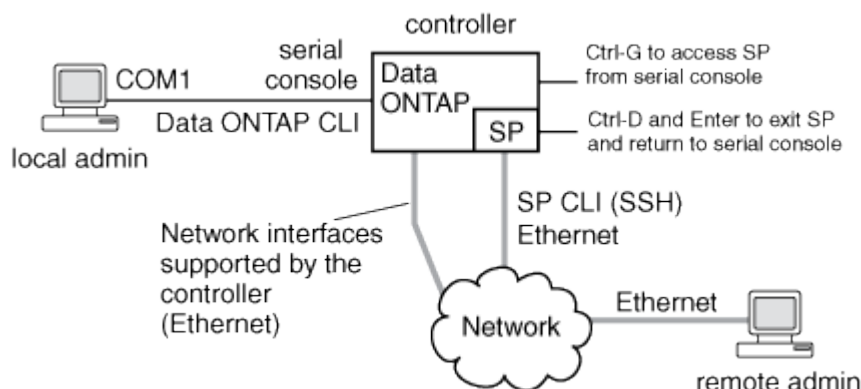
When messages are sent to the console, the SP stores them in the console log. The console log persists as long as the SP has power from either of the node power supplies. Because the SP operates with standby power, it remains available even when the node is power-cycled or turned off.

- Hardware-assisted takeover is available if the SP is configured.
- The SP API service enables ONTAP to communicate with the SP over the network.

The service enhances ONTAP management of the SP by supporting network-based functionality such as using the network interface for the SP firmware update, enabling a node to access another node’s SP functionality or system console, and uploading the SP log from another node.

You can modify the configuration of the SP API service by changing the port the service uses, renewing the SSL and SSH certificates that are used by the service for internal communication, or disabling the service entirely.

The following diagram illustrates access to ONTAP and the SP of a node. The SP interface is accessed through the Ethernet port (indicated by a wrench icon on the rear of the chassis):



## What the Baseboard Management Controller does

Beginning with ONTAP 9.1, on certain hardware platforms, software is customized to support a new onboard controller in called the Baseboard Management Controller (BMC). The BMC has command-line interface (CLI) commands you can use to manage the device remotely.

The BMC works similarly to the Service Processor (SP) and uses many of the same commands. The BMC allows you to do the following:

- Configure the BMC network settings.
- Access a node remotely and perform node management tasks such as diagnose, shut down, power-cycle, or reboot the node.

There are some differences between the SP and BMC:

- The BMC completely controls the environmental monitoring of power supply elements, cooling elements, temperature sensors, voltage sensors, and current sensors. The BMC reports sensor information to ONTAP through IPMI.
- Some of the high-availability (HA) and storage commands are different.
- The BMC does not send AutoSupport messages.

Automatic firmware updates are also available when running ONTAP 9.2 GA or later with the following requirements:

- BMC firmware revision 1.15 or later must be installed.



A manual update is required to upgrade BMC firmware from 1.12 to 1.15 or later.

- BMC automatically reboots after a firmware update is completed.



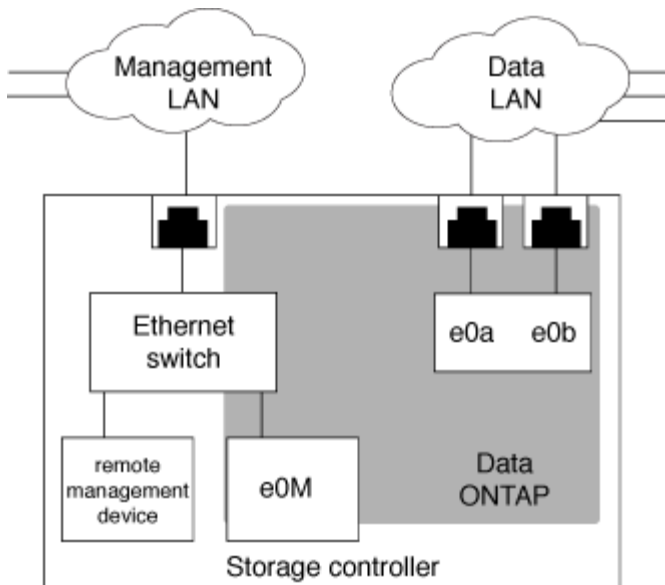
Node operations are not impacted during a BMC reboot.

## Configure the SP/BMC network

### Isolate management network traffic

It is a best practice to configure SP/BMC and the e0M management interface on a subnet dedicated to management traffic. Running data traffic over the management network can cause performance degradation and routing problems.

The management Ethernet port on most storage controllers (indicated by a wrench icon on the rear of the chassis) is connected to an internal Ethernet switch. The internal switch provides connectivity to SP/BMC and to the e0M management interface, which you can use to access the storage system via TCP/IP protocols like Telnet, SSH, and SNMP.



If you plan to use both the remote management device and e0M, you must configure them on the same IP subnet. Since these are low-bandwidth interfaces, the best practice is to configure SP/BMC and e0M on a subnet dedicated to management traffic.

If you cannot isolate management traffic, or if your dedicated management network is unusually large, you should try to keep the volume of network traffic as low as possible. Excessive ingress broadcast or multicast traffic may degrade SP/BMC performance.



Some storage controllers, such as the AFF A800, have two external ports, one for BMC and the other for e0M. For these controllers, there is no requirement to configure BMC and e0M on the same IP subnet.

### Considerations for the SP/BMC network configuration

You can enable cluster-level, automatic network configuration for the SP (recommended). You can also leave the SP automatic network configuration disabled (the default) and manage the SP network configuration manually at the node level. A few considerations exist for each case.



This topic applies to both the SP and the BMC.

The SP automatic network configuration enables the SP to use address resources (including the IP address, subnet mask, and gateway address) from the specified subnet to set up its network automatically. With the SP automatic network configuration, you do not need to manually assign IP addresses for the SP of each node. By default, the SP automatic network configuration is disabled; this is because enabling the configuration requires that the subnet to be used for the configuration be defined in the cluster first.

If you enable the SP automatic network configuration, the following scenarios and considerations apply:

- If the SP has never been configured, the SP network is configured automatically based on the subnet specified for the SP automatic network configuration.
- If the SP was previously configured manually, or if the existing SP network configuration is based on a different subnet, the SP network of all nodes in the cluster are reconfigured based on the subnet that you specify in the SP automatic network configuration.

The reconfiguration could result in the SP being assigned a different address, which might have an impact on your DNS configuration and its ability to resolve SP host names. As a result, you might need to update your DNS configuration.

- A node that joins the cluster uses the specified subnet to configure its SP network automatically.
- The `system service-processor network modify` command does not enable you to change the SP IP address.

When the SP automatic network configuration is enabled, the command only allows you to enable or disable the SP network interface.

- If the SP automatic network configuration was previously enabled, disabling the SP network interface results in the assigned address resource being released and returned to the subnet.
- If you disable the SP network interface and then reenabling it, the SP might be reconfigured with a different address.

If the SP automatic network configuration is disabled (the default), the following scenarios and considerations apply:

- If the SP has never been configured, SP IPv4 network configuration defaults to using IPv4 DHCP, and IPv6 is disabled.

A node that joins the cluster also uses IPv4 DHCP for its SP network configuration by default.

- The `system service-processor network modify` command enables you to configure a node's SP IP address.

A warning message appears when you attempt to manually configure the SP network with addresses that are allocated to a subnet. Ignoring the warning and proceeding with the manual address assignment might result in a scenario with duplicate addresses.

If the SP automatic network configuration is disabled after having been enabled previously, the following scenarios and considerations apply:

- If the SP automatic network configuration has the IPv4 address family disabled, the SP IPv4 network defaults to using DHCP, and the `system service-processor network modify` command enables you to modify the SP IPv4 configuration for individual nodes.
- If the SP automatic network configuration has the IPv6 address family disabled, the SP IPv6 network is also disabled, and the `system service-processor network modify` command enables you to enable and modify the SP IPv6 configuration for individual nodes.

### Enable the SP/BMC automatic network configuration

Enabling the SP to use automatic network configuration is preferred over manually configuring the SP network. Because the SP automatic network configuration is cluster wide, you do not need to manually manage the SP network for individual nodes.



This task applies to both the SP and the BMC.

- The subnet you want to use for the SP automatic network configuration must already be defined in the cluster and must have no resource conflicts with the SP network interface.

The `network subnet show` command displays subnet information for the cluster.

The parameter that forces subnet association (the `-force-update-lif-associations` parameter of the `network subnet` commands) is supported only on network LIFs and not on the SP network interface.

- If you want to use IPv6 connections for the SP, IPv6 must already be configured and enabled for ONTAP.

The `network options ipv6 show` command displays the current state of IPv6 settings for ONTAP.

## Steps

1. Specify the IPv4 or IPv6 address family and name for the subnet that you want the SP to use by using the `system service-processor network auto-configuration enable` command.
2. Display the SP automatic network configuration by using the `system service-processor network auto-configuration show` command.
3. If you subsequently want to disable or reenab the SP IPv4 or IPv6 network interface for all nodes that are in quorum, use the `system service-processor network modify` command with the `-address -family [IPv4|IPv6]` and `-enable [true|false]` parameters.

When the SP automatic network configuration is enabled, you cannot modify the SP IP address for a node that is in quorum. You can only enable or disable the SP IPv4 or IPv6 network interface.

If a node is out of quorum, you can modify the node's SP network configuration, including the SP IP address, by running `system service-processor network modify` from the node and confirming that you want to override the SP automatic network configuration for the node. However, when the node joins the quorum, the SP automatic reconfiguration takes place for the node based on the specified subnet.

## Configure the SP/BMC network manually

If you do not have automatic network configuration set up for the SP, you must manually configure a node's SP network for the SP to be accessible by using an IP address.

### What you'll need

If you want to use IPv6 connections for the SP, IPv6 must already be configured and enabled for ONTAP. The `network options ipv6` commands manage IPv6 settings for ONTAP.



This task applies to both the SP and the BMC.

You can configure the SP to use IPv4, IPv6, or both. The SP IPv4 configuration supports static and DHCP addressing, and the SP IPv6 configuration supports static addressing only.

If the SP automatic network configuration has been set up, you do not need to manually configure the SP network for individual nodes, and the `system service-processor network modify` command allows you to only enable or disable the SP network interface.

## Steps

1. Configure the SP network for a node by using the `system service-processor network modify` command.
  - The `-address-family` parameter specifies whether the IPv4 or IPv6 configuration of the SP is to be modified.

- The `-enable` parameter enables the network interface of the specified IP address family.
- The `-dhcp` parameter specifies whether to use the network configuration from the DHCP server or the network address that you provide.

You can enable DHCP (by setting `-dhcp` to `v4`) only if you are using IPv4. You cannot enable DHCP for IPv6 configurations.

- The `-ip-address` parameter specifies the public IP address for the SP.

A warning message appears when you attempt to manually configure the SP network with addresses that are allocated to a subnet. Ignoring the warning and proceeding with the manual address assignment might result in a duplicate address assignment.

- The `-netmask` parameter specifies the netmask for the SP (if using IPv4.)
- The `-prefix-length` parameter specifies the network prefix-length of the subnet mask for the SP (if using IPv6.)
- The `-gateway` parameter specifies the gateway IP address for the SP.

2. Configure the SP network for the remaining nodes in the cluster by repeating the step 1.
3. Display the SP network configuration and verify the SP setup status by using the `system service-processor network show` command with the `-instance` or `-field setup-status` parameters.

The SP setup status for a node can be one of the following:

- `not-setup` — Not configured
- `succeeded` — Configuration succeeded
- `in-progress` — Configuration in progress
- `failed` — Configuration failed

### Example of configuring the SP network

The following example configures the SP of a node to use IPv4, enables the SP, and displays the SP network configuration to verify the settings:

```

cluster1::> system service-processor network modify -node local
-address-family IPv4 -enable true -ip-address 192.168.123.98
-netmask 255.255.255.0 -gateway 192.168.123.1

cluster1::> system service-processor network show -instance -node local

                Node: node1
            Address Type: IPv4
    Interface Enabled: true
        Type of Device: SP
                Status: online
            Link Status: up
            DHCP Status: none
            IP Address: 192.168.123.98
            MAC Address: ab:cd:ef:fe:ed:02
            Netmask: 255.255.255.0
Prefix Length of Subnet Mask: -
    Router Assigned IP Address: -
        Link Local IP Address: -
            Gateway IP Address: 192.168.123.1
            Time Last Updated: Thu Apr 10 17:02:13 UTC 2014
            Subnet Name: -
Enable IPv6 Router Assigned Address: -
            SP Network Setup Status: succeeded
            SP Network Setup Failure Reason: -

1 entries were displayed.

cluster1::>

```

## Modify the SP API service configuration

The SP API is a secure network API that enables ONTAP to communicate with the SP over the network. You can change the port used by the SP API service, renew the certificates the service uses for internal communication, or disable the service entirely. You need to modify the configuration only in rare situations.

### About this task

- The SP API service uses port 50000 by default.

You can change the port value if, for example, you are in a network setting where port 50000 is used for communication by another networking application, or you want to differentiate between traffic from other applications and traffic generated by the SP API service.

- The SSL and SSH certificates used by the SP API service are internal to the cluster and not distributed externally.

In the unlikely event that the certificates are compromised, you can renew them.

- The SP API service is enabled by default.

You only need to disable the SP API service in rare situations, such as in a private LAN where the SP is not configured or used and you want to disable the service.

If the SP API service is disabled, the API does not accept any incoming connections. In addition, functionality such as network-based SP firmware updates and network-based SP “down system” log collection becomes unavailable. The system switches to using the serial interface.

## Steps

1. Switch to the advanced privilege level by using the `set -privilege advanced` command.
2. Modify the SP API service configuration:

If you want to...	Use the following command...
Change the port used by the SP API service	<code>system service-processor api-service modify with the -port {49152..65535} parameter</code>
Renew the SSL and SSH certificates used by the SP API service for internal communication	<ul style="list-style-type: none"> <li>• For ONTAP 9.5 or later use <code>system service-processor api-service renew-internal-certificate</code></li> <li>• For ONTAP 9.4 and earlier use <code>system service-processor api-service renew-certificates</code></li> </ul> <p>If no parameter is specified, only the host certificates (including the client and server certificates) are renewed.</p> <p>If the <code>-renew-all true</code> parameter is specified, both the host certificates and the root CA certificate are renewed.</p>
comm	
Disable or reenables the SP API service	<code>system service-processor api-service modify with the -is-enabled {true false} parameter</code>

3. Display the SP API service configuration by using the `system service-processor api-service show` command.

## Methods of managing SP/BMC firmware updates

ONTAP includes an SP firmware image that is called the *baseline image*. If a new version of the SP firmware becomes subsequently available, you have the option to download it



and update the SP firmware to the downloaded version without upgrading the ONTAP version.



This topic applies to both the SP and the BMC.

ONTAP offers the following methods for managing SP firmware updates:

- The SP automatic update functionality is enabled by default, allowing the SP firmware to be automatically updated in the following scenarios:
  - When you upgrade to a new version of ONTAP

The ONTAP upgrade process automatically includes the SP firmware update, provided that the SP firmware version bundled with ONTAP is newer than the SP version running on the node.



ONTAP detects a failed SP automatic update and triggers a corrective action to retry the SP automatic update up to three times. If all three retries fail, see the Knowledge Base article [xref:./system-admin/ Health Monitor SPAutoUpgradeFailedMajorAlert SP upgrade fails - AutoSupport Message](#).

- When you download a version of the SP firmware from the NetApp Support Site and the downloaded version is newer than the one that the SP is currently running
- When you downgrade or revert to an earlier version of ONTAP

The SP firmware is automatically updated to the newest compatible version that is supported by the ONTAP version you reverted or downgraded to. A manual SP firmware update is not required.

You have the option to disable the SP automatic update functionality by using the `system service-processor image modify` command. However, it is recommended that you leave the functionality enabled. Disabling the functionality can result in suboptimal or nonqualified combinations between the ONTAP image and the SP firmware image.

- ONTAP enables you to trigger an SP update manually and specify how the update should take place by using the `system service-processor image update` command.

You can specify the following options:

- The SP firmware package to use (`-package`)

You can update the SP firmware to a downloaded package by specifying the package file name. The `advance system image package show` command displays all package files (including the files for the SP firmware package) that are available on a node.

- Whether to use the baseline SP firmware package for the SP update (`-baseline`)

You can update the SP firmware to the baseline version that is bundled with the currently running version of ONTAP.



If you use some of the more advanced update options or parameters, the BMC's configuration settings may be temporarily cleared. After reboot, it can take up to 10 minutes for ONTAP to restore the BMC configuration.

- ONTAP enables you to display the status for the latest SP firmware update triggered from ONTAP by using the `system service-processor image update-progress show` command.

Any existing connection to the SP is terminated when the SP firmware is being updated. This is the case whether the SP firmware update is automatically or manually triggered.

#### Related information

[NetApp Downloads: System Firmware and Diagnostics](#)

#### When the SP/BMC uses the network interface for firmware updates

An SP firmware update that is triggered from ONTAP with the SP running version 1.5, 2.5, 3.1, or later supports using an IP-based file transfer mechanism over the SP network interface.



This topic applies to both the SP and the BMC.

An SP firmware update over the network interface is faster than an update over the serial interface. It reduces the maintenance window during which the SP firmware is being updated, and it is also nondisruptive to ONTAP operation. The SP versions that support this capability are included with ONTAP. They are also available on the NetApp Support Site and can be installed on controllers that are running a compatible version of ONTAP.

When you are running SP version 1.5, 2.5, 3.1, or later, the following firmware upgrade behaviors apply:

- An SP firmware update that is *automatically* triggered by ONTAP defaults to using the network interface for the update; however, the SP automatic update switches to using the serial interface for the firmware update if one of the following conditions occurs:
  - The SP network interface is not configured or not available.
  - The IP-based file transfer fails.
  - The SP API service is disabled.

Regardless of the SP version you are running, an SP firmware update triggered from the SP CLI always uses the SP network interface for the update.

#### Related information

[NetApp Downloads: System Firmware and Diagnostics](#)

#### Access the SP/BMC

#### Accounts that can access the SP

When you try to access the SP, you are prompted for credential. Cluster user accounts that are created with the `service-processor` application type have access to the SP CLI on any node of the cluster. SP user accounts are managed from ONTAP and authenticated by password. Beginning with ONTAP 9.9.1, SP user accounts must have the `admin` role.

User accounts for accessing the SP are managed from ONTAP instead of the SP CLI. A cluster user account can access the SP if it is created with the `-application` parameter of the `security login create` command set to `service-processor` and the `-authmethod` parameter set to `password`. The SP supports

only password authentication.

You must specify the `-role` parameter when creating an SP user account.

- In ONTAP 9.9.1 and later releases, you must specify `admin` for the `-role` parameter, and any modifications to an account require the `admin` role. Other roles are no longer permitted for security reasons.
  - If you are upgrading to ONTAP 9.9.1 or later releases, see [Change in user accounts that can access the Service Processor](#).
  - If you are reverting to ONTAP 9.8 or earlier releases, see [Verify user accounts that can access the Service Processor](#).
- In ONTAP 9.8 and earlier releases, any role can access the SP, but `admin` is recommended.

By default, the cluster user account named “admin” includes the `service-processor` application type and has access to the SP.

ONTAP prevents you from creating user accounts with names that are reserved for the system (such as “root” and “naroot”). You cannot use a system-reserved name to access the cluster or the SP.

You can display current SP user accounts by using the `-application service-processor` parameter of the `security login show` command.

## Access the SP/BMC from an administration host

You can log in to the SP of a node from an administration host to perform node management tasks remotely.

### What you'll need

The following conditions must be met:

- The administration host you use to access the SP must support SSHv2.
- Your user account must already be set up for accessing the SP.

To access the SP, your user account must have been created with the `-application` parameter of the `security login create` command set to `service-processor` and the `-authmethod` parameter set to `password`.



This task applies to both the SP and the BMC.

If the SP is configured to use an IPv4 or IPv6 address, and if five SSH login attempts from a host fail consecutively within 10 minutes, the SP rejects SSH login requests and suspends the communication with the IP address of the host for 15 minutes. The communication resumes after 15 minutes, and you can try to log in to the SP again.

ONTAP prevents you from creating or using system-reserved names (such as “root” and “naroot”) to access the cluster or the SP.

### Steps

1. From the administration host, log in to the SP:

```
ssh username@SP_IP_address
```

2. When you are prompted, enter the password for username.

The SP prompt appears, indicating that you have access to the SP CLI.

### Examples of SP access from an administration host

The following example shows how to log in to the SP with a user account `joe`, which has been set up to access the SP.

```
[admin_host]$ ssh joe@192.168.123.98
joe@192.168.123.98's password:
SP>
```

The following examples show how to use the IPv6 global address or IPv6 router-advertised address to log in to the SP on a node that has SSH set up for IPv6 and the SP configured for IPv6.

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202::1234
joe@fd22:8b1e:b255:202::1234's password:
SP>
```

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b
joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b's password:
SP>
```

### Access the SP/BMC from the system console

You can access the SP from the system console (also called *serial console*) to perform monitoring or troubleshooting tasks.

#### About this task

This task applies to both the SP and the BMC.

#### Steps

1. Access the SP CLI from the system console by pressing Ctrl-G at the prompt.
2. Log in to the SP CLI when you are prompted.

The SP prompt appears, indicating that you have access to the SP CLI.

3. Exit the SP CLI and return to the system console by pressing Ctrl-D, and then press Enter.

### Example of accessing the SP CLI from the system console

The following example shows the result of pressing Ctrl-G from the system console to access the SP CLI. The `help system power` command is entered at the SP prompt, followed by pressing Ctrl-D and then Enter to return to the system console.

```
cluster1::>
```

(Press Ctrl-G to access the SP CLI.)

```
Switching console to Service Processor
Service Processor Login:
Password:
SP>
SP> help system power
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status
SP>
```

(Press Ctrl-D and then Enter to return to the system console.)

```
cluster1::>
```

### Relationship among the SP CLI, SP console, and system console sessions

You can open an SP CLI session to manage a node remotely and open a separate SP console session to access the console of the node. The SP console session mirrors output displayed in a concurrent system console session. The SP and the system console have independent shell environments with independent login authentication.

Understanding how the SP CLI, SP console, and system console sessions are related helps you manage a node remotely. The following describes the relationship among the sessions:

- Only one administrator can log in to the SP CLI session at a time; however, the SP enables you to open both an SP CLI session and a separate SP console session simultaneously.

The SP CLI is indicated with the SP prompt (`SP>`). From an SP CLI session, you can use the SP `system console` command to initiate an SP console session. At the same time, you can start a separate SP CLI session through SSH. If you press Ctrl-D to exit from the SP console session, you automatically return to the SP CLI session. If an SP CLI session already exists, a message asks you whether to terminate the existing SP CLI session. If you enter “y”, the existing SP CLI session is terminated, enabling you to return from the SP console to the SP CLI. This action is recorded in the SP event log.

In an ONTAP CLI session that is connected through SSH, you can switch to the system console of a node by running the ONTAP `system node run-console` command from another node.

- For security reasons, the SP CLI session and the system console session have independent login authentication.

When you initiate an SP console session from the SP CLI (by using the SP `system console` command), you are prompted for the system console credential. When you access the SP CLI from a system console

session (by pressing Ctrl-G), you are prompted for the SP CLI credential.

- The SP console session and the system console session have independent shell environments.

The SP console session mirrors output that is displayed in a concurrent system console session. However, the concurrent system console session does not mirror the SP console session.

The SP console session does not mirror output of concurrent SSH sessions.

## Manage the IP addresses that can access the SP

By default, the SP accepts SSH connection requests from administration hosts of any IP addresses. You can configure the SP to accept SSH connection requests from only the administration hosts that have the IP addresses you specify. The changes you make apply to SSH access to the SP of any nodes in the cluster.

### Steps

1. Grant SP access to only the IP addresses you specify by using the `system service-processor ssh add-allowed-addresses` command with the `-allowed-addresses` parameter.

- The value of the `-allowed-addresses` parameter must be specified in the format of `address/netmask`, and multiple `address/netmask` pairs must be separated by commas, for example, `10.98.150.10/24, fd20:8b1e:b255:c09b::/64`.

Setting the `-allowed-addresses` parameter to `0.0.0.0/0, ::/0` enables all IP addresses to access the SP (the default).

- When you change the default by limiting SP access to only the IP addresses you specify, ONTAP prompts you to confirm that you want the specified IP addresses to replace the “allow all” default setting (`0.0.0.0/0, ::/0`).
- The `system service-processor ssh show` command displays the IP addresses that can access the SP.

2. If you want to block a specified IP address from accessing the SP, use the `system service-processor ssh remove-allowed-addresses` command with the `-allowed-addresses` parameter.

If you block all IP addresses from accessing the SP, the SP becomes inaccessible from any administration hosts.

## Examples of managing the IP addresses that can access the SP

The following examples show the default setting for SSH access to the SP, change the default by limiting SP access to only the specified IP addresses, remove the specified IP addresses from the access list, and then restore SP access for all IP addresses:

```

cluster1::> system service-processor ssh show
  Allowed Addresses: 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: The default "allow all" setting (0.0.0.0/0, ::/0) will be
replaced
      with your changes. Do you want to continue? {y|n}: y

cluster1::> system service-processor ssh show
  Allowed Addresses: 192.168.1.202/24, 192.168.10.201/24

cluster1::> system service-processor ssh remove-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: If all IP addresses are removed from the allowed address list,
all IP
      addresses will be denied access. To restore the "allow all"
default,
      use the "system service-processor ssh add-allowed-addresses
      -allowed-addresses 0.0.0.0/0, ::/0" command. Do you want to
continue?
      {y|n}: y

cluster1::> system service-processor ssh show
  Allowed Addresses: -

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh show
  Allowed Addresses: 0.0.0.0/0, ::/0

```

### Use online help at the SP/BMC CLI

The online help displays the SP/BMC CLI commands and options.

### About this task

This task applies to both the SP and the BMC.

### Steps

1. To display help information for the SP/BMC commands, enter the following:

To access SP help...	To access BMC help...
Type <code>help</code> at the SP prompt.	Type <code>system</code> at the BMC prompt.

The following example shows the SP CLI online help.

```
SP> help
date - print date and time
exit - exit from the SP command line interface
events - print system events and event information
help - print command help
priv - show and set user mode
sp - commands to control the SP
system - commands to control the system
version - print SP version
```

The following example shows the BMC CLI online help.

```
BMC> system
system acp - acp related commands
system battery - battery related commands
system console - connect to the system console
system core - dump the system core and reset
system cpld - cpld commands
system log - print system console logs
system power - commands controlling system power
system reset - reset the system using the selected firmware
system sensors - print environmental sensors status
system service-event - print service-event status
system fru - fru related commands
system watchdog - system watchdog commands

BMC>
```

2. To display help information for the option of an SP/BMC command, enter `help` before or after the SP/BMC command.

The following example shows the SP CLI online help for the SP `events` command.



```

SP> help events
events all - print all system events
events info - print system event log information
events newest - print newest system events
events oldest - print oldest system events
events search - search for and print system events

```

The following example shows the BMC CLI online help for the BMC `system power` command.

```

BMC> system power help
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status

BMC>

```


#### Commands for managing a node remotely

You can manage a node remotely by accessing its SP and running SP CLI commands to perform node-management tasks. For several commonly performed remote node-management tasks, you can also use ONTAP commands from another node in the cluster. Some SP commands are platform-specific and might not be available on your platform.

If you want to...	Use this SP command...	Use this BMC command...	Or this ONTAP command ...
Display available SP commands or subcommands of a specified SP command	<code>help [command]</code>		
Display the current privilege level for the SP CLI	<code>priv show</code>		
Set the privilege level to access the specified mode for the SP CLI	<code>priv set {admin   advanced   diag}</code>		
Display system date and time	<code>date</code>		<code>date</code>

If you want to...	Use this SP command...	Use this BMC command...	Or this ONTAP command ...
Display events that are logged by the SP	<code>events {all   info   newest number   oldest number   search keyword}</code>		
Display SP status and network configuration information	<code>sp status [-v   -d]</code>  The <code>-v</code> option displays SP statistics in verbose form. The <code>-d</code> option adds the SP debug log to the display.	<code>bmc status [-v   -d]</code>  The <code>-v</code> option displays SP statistics in verbose form. The <code>-d</code> option adds the SP debug log to the display.	<code>system service-processor show</code>
Display the length of time the SP has been up and the average number of jobs in the run queue over the last 1, 5, and 15 minutes	<code>sp uptime</code>	<code>bmc uptime</code>	
Display system console logs	<code>system log</code>		
Display the SP log archives or the files in an archive	<code>sp log history show [-archive {latest   all   archive-name}] [-dump {all   file-name}]</code>	<code>bmc log history show [-archive {latest   all   archive-name}] [-dump {all   file-name}]</code>	
Display the power status for the controller of a node	<code>system power status</code>		<code>system node power show</code>
Display battery information	<code>system battery show</code>		
Display ACP information or the status for expander sensors	<code>system acp [show   sensors show]</code>		
List all system FRUs and their IDs	<code>system fru list</code>		
Display product information for the specified FRU	<code>system fru show fru_id</code>		

If you want to...	Use this SP command...	Use this BMC command...	Or this ONTAP command ...
Display the FRU data history log	<code>system fru log show</code> (advanced privilege level)		
Display the status for the environmental sensors, including their states and current values	<code>system sensors</code> or <code>system sensors show</code>		<code>system node environment sensors show</code>
Display the status and details for the specified sensor	<code>system sensors get sensor_name</code>  You can obtain <code>sensor_name</code> by using the <code>system sensors</code> or the <code>system sensors show</code> command.		
Display the SP firmware version information	<code>version</code>		<code>system service-processor image show</code>
Display the SP command history	<code>sp log audit</code> (advanced privilege level)	<code>bmc log audit</code>	
Display the SP debug information	<code>sp log debug</code> (advanced privilege level)	<code>bmc log debug</code> (advanced privilege level)	
Display the SP messages file	<code>sp log messages</code> (advanced privilege level)	<code>bmc log messages</code> (advanced privilege level)	
Display the settings for collecting system forensics on a watchdog reset event, display system forensics information collected during a watchdog reset event, or clear the collected system forensics information	<code>system forensics [show   log dump   log clear]</code>		
Log in to the system console	<code>system console</code>		<code>system node run-console</code>
	You should press Ctrl-D to exit the system console session.		

If you want to...	Use this SP command...	Use this BMC command...	Or this ONTAP command ...
Turn the node on or off, or perform a power-cycle (turning the power off and then back on)	<code>system power on</code>		<code>system node power on</code> (advanced privilege level)
	<code>system power off</code>		
	<code>system power cycle</code>		
	<p>The standby power stays on to keep the SP running without interruption. During the power-cycle, a brief pause occurs before power is turned back on.</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;">  <p>Using these commands to turn off or power-cycle the node might cause an improper shutdown of the node (also called a <i>dirty shutdown</i>) and is not a substitute for a graceful shutdown using the ONTAP <code>system node halt</code> command.</p> </div>		
Create a core dump and reset the node	<code>system core [-f]</code>  The <code>-f</code> option forces the creation of a core dump and the reset of the node.		<code>system node coredump trigger</code>  (advanced privilege level)
Reboot the node with an optionally specified BIOS firmware image (primary, backup, or current) to recover from issues such as a corrupted image of the node's boot device	<code>system reset {primary   backup   current}</code>		<code>system node reset</code> with the <code>-firmware {primary   backup   current}</code> parameter (advanced privilege level)  <code>system node reset</code>
	<div style="border: 1px solid gray; padding: 5px; margin: 10px 0;">  <p>This operation causes a dirty shutdown of the node.</p> </div> <p>If no BIOS firmware image is specified, the current image is used for the reboot. The SP stays operational as long as the input power to the node is not interrupted.</p>		

If you want to...	Use this SP command...	Use this BMC command...	Or this ONTAP command ...
Display the status of battery firmware automatic update, or enable or disable battery firmware automatic update upon next SP boot	<pre>system battery auto_update [status   enable   disable]</pre> <p>(advanced privilege level)</p>		
Compare the current battery firmware image against a specified firmware image	<pre>system battery verify [image_URL]</pre> <p>(advanced privilege level)</p> <p>If <code>image_URL</code> is not specified, the default battery firmware image is used for comparison.</p>		
Update the battery firmware from the image at the specified location	<pre>system battery flash image_URL</pre> <p>(advanced privilege level)</p> <p>You use this command if the automatic battery firmware upgrade process has failed for some reason.</p>		
Update the SP firmware by using the image at the specified location	<pre>sp update image_URL</pre> <p><code>image_URL</code> must not exceed 200 characters.</p>	<pre>bmc update image_URL</pre> <p><code>image_URL</code> must not exceed 200 characters.</p>	<pre>system service-processor image update</pre>
Reboot the SP	<pre>sp reboot</pre>		<pre>system service-processor reboot-sp</pre>
Erase the NVRAM flash content	<pre>system nvram flash clear (advanced privilege level)</pre> <p>This command cannot be initiated when the controller power is off (<code>system power off</code>).</p>		
Exit the SP CLI	<pre>exit</pre>		

## About the threshold-based SP sensor readings and status values of the system sensors command output

Threshold-based sensors take periodic readings of a variety of system components. The SP compares the reading of a threshold-based sensor against its preset threshold limits that define a component's acceptable operating conditions.

Based on the sensor reading, the SP displays the sensor state to help you monitor the condition of the component.

Examples of threshold-based sensors include sensors for the system temperatures, voltages, currents, and fan speeds. The specific list of threshold-based sensors depends on the platform.

Threshold-based sensors have the following thresholds, displayed in the output of the SP `system sensors` command:

- Lower critical (LCR)
- Lower noncritical (LNC)
- Upper noncritical (UNC)
- Upper critical (UCR)

A sensor reading between LNC and LCR or between UNC and UCR means that the component is showing signs of a problem and a system failure might occur as a result. Therefore, you should plan for component service soon.

A sensor reading below LCR or above UCR means that the component is malfunctioning and a system failure is about to occur. Therefore, the component requires immediate attention.

The following diagram illustrates the severity ranges that are specified by the thresholds:



You can find the reading of a threshold-based sensor under the `Current` column in the `system sensors` command output. The `system sensors get sensor_name` command displays additional details for the specified sensor. As the reading of a threshold-based sensor crosses the noncritical and critical threshold ranges, the sensor reports a problem of increasing severity. When the reading exceeds a threshold limit, the sensor's status in the `system sensors` command output changes from `ok` to `nc` (noncritical) or `cr` (critical) depending on the exceeded threshold, and an event message is logged in the SEL event log.

Some threshold-based sensors do not have all four threshold levels. For those sensors, the missing thresholds show `na` as their limits in the `system sensors` command output, indicating that the particular sensor has no limit or severity concern for the given threshold and the SP does not monitor the sensor for that threshold.

### Example of the system sensors command output

The following example shows some of the information displayed by the `system sensors` command in the SP CLI:

```
SP nodel> system sensors
```

Sensor Name	Current	Unit	Status	LCR	LNC
UNC	UCR				
CPU0_Temp_Margin	-55.000	degrees C	ok	na	na
-5.000	0.000				
CPU1_Temp_Margin	-56.000	degrees C	ok	na	na
-5.000	0.000				
In_Flow_Temp	32.000	degrees C	ok	0.000	10.000
42.000	52.000				
Out_Flow_Temp	38.000	degrees C	ok	0.000	10.000
59.000	68.000				
CPU1_Error	0x0	discrete	0x0180	na	na
na	na				
CPU1_Therm_Trip	0x0	discrete	0x0180	na	na
na	na				
CPU1_Hot	0x0	discrete	0x0180	na	na
na	na				
IO_Mid1_Temp	30.000	degrees C	ok	0.000	10.000
55.000	64.000				
IO_Mid2_Temp	30.000	degrees C	ok	0.000	10.000
55.000	64.000				
CPU_VTT	1.106	Volts	ok	1.028	1.048
1.154	1.174				
CPU0_VCC	1.154	Volts	ok	0.834	0.844
1.348	1.368				
3.3V	3.323	Volts	ok	3.053	3.116
3.466	3.546				
5V	5.002	Volts	ok	4.368	4.465
5.490	5.636				
STBY_1.8V	1.794	Volts	ok	1.678	1.707
1.892	1.911				
...					

### Example of the system sensors sensor\_name command output for a threshold-based sensor

The following example shows the result of entering `system sensors get sensor_name` in the SP CLI for the threshold-based sensor 5V:

```

SP node1> system sensors get 5V

Locating sensor record...
Sensor ID           : 5V (0x13)
Entity ID          : 7.97
Sensor Type (Analog) : Voltage
Sensor Reading     : 5.002 (+/- 0) Volts
Status             : ok
Lower Non-Recoverable : na
Lower Critical     : 4.246
Lower Non-Critical  : 4.490
Upper Non-Critical  : 5.490
Upper Critical     : 5.758
Upper Non-Recoverable : na
Assertion Events   :
Assertions Enabled  : lnc- lcr- ucr+
Deassertions Enabled : lnc- lcr- ucr+

```

#### About the discrete SP sensor status values of the system sensors command output

Discrete sensors do not have thresholds. Their readings, displayed under the `Current` column in the SP CLI `system sensors` command output, do not carry actual meanings and thus are ignored by the SP. The `Status` column in the `system sensors` command output displays the status values of discrete sensors in hexadecimal format.

Examples of discrete sensors include sensors for the fan, power supply unit (PSU) fault, and system fault. The specific list of discrete sensors depends on the platform.

You can use the SP CLI `system sensors get sensor_name` command for help with interpreting the status values for most discrete sensors. The following examples show the results of entering `system sensors get sensor_name` for the discrete sensors `CPU0_Error` and `IO_Slot1_Present`:

```

SP node1> system sensors get CPU0_Error
Locating sensor record...
Sensor ID           : CPU0_Error (0x67)
Entity ID          : 7.97
Sensor Type (Discrete): Temperature
States Asserted    : Digital State
                   [State Deasserted]

```



```

SP node1> system sensors get IO_Slot1_Present
Locating sensor record...
Sensor ID           : IO_Slot1_Present (0x74)
Entity ID          : 11.97
Sensor Type (Discrete): Add-in Card
States Asserted    : Availability State
                   [Device Present]

```

Although the `system sensors get sensor_name` command displays the status information for most discrete sensors, it does not provide status information for the `System_FW_Status`, `System_Watchdog`, `PSU1_Input_Type`, and `PSU2_Input_Type` discrete sensors. You can use the following information to interpret these sensors' status values.

### System\_FW\_Status

The `System_FW_Status` sensor's condition appears in the form of `0xAABB`. You can combine the information of `AA` and `BB` to determine the condition of the sensor.

`AA` can have one of the following values:

Values	Condition of the sensor
01	System firmware error
02	System firmware hang
04	System firmware progress

`BB` can have one of the following values:

Values	Condition of the sensor
00	System software has properly shut down
01	Memory initialization in progress
02	NVMEM initialization in progress (when NVMEM is present)
04	Restoring memory controller hub (MCH) values (when NVMEM is present)
05	User has entered Setup
13	Booting the operating system or LOADER

Values	Condition of the sensor
1F	BIOS is starting up
20	LOADER is running
21	LOADER is programming the primary BIOS firmware. You must not power down the system.
22	LOADER is programming the alternate BIOS firmware. You must not power down the system.
2F	ONTAP is running
60	SP has powered off the system
61	SP has powered on the system
62	SP has reset the system
63	SP watchdog power cycle
64	SP watchdog cold reset

For instance, the System\_FW\_Status sensor status 0x042F means "system firmware progress (04), ONTAP is running (2F)."

### System\_Watchdog

The System\_Watchdog sensor can have one of the following conditions:

- **0x0080**

The state of this sensor has not changed

Values	Condition of the sensor
0x0081	Timer interrupt
0x0180	Timer expired
0x0280	Hard reset
0x0480	Power down
0x0880	Power cycle

For instance, the System\_Watchdog sensor status 0x0880 means a watchdog timeout occurs and causes a system power cycle.

### PSU1\_Input\_Type and PSU2\_Input\_Type

For direct current (DC) power supplies, the PSU1\_Input\_Type and PSU2\_Input\_Type sensors do not apply. For alternating current (AC) power supplies, the sensors' status can have one of the following values:

Values	Condition of the sensor
0x01 xx	220V PSU type
0x02 xx	110V PSU type

For instance, the PSU1\_Input\_Type sensor status 0x0280 means that the sensor reports that the PSU type is 110V.

### Commands for managing the SP from ONTAP

ONTAP provides commands for managing the SP, including the SP network configuration, SP firmware image, SSH access to the SP, and general SP administration.

### Commands for managing the SP network configuration


If you want to...	Run this ONTAP command...
Enable the SP automatic network configuration for the SP to use the IPv4 or IPv6 address family of the specified subnet	<code>system service-processor network auto-configuration enable</code>
Disable the SP automatic network configuration for the IPv4 or IPv6 address family of the subnet specified for the SP	<code>system service-processor network auto-configuration disable</code>
Display the SP automatic network configuration	<code>system service-processor network auto-configuration show</code>

If you want to...	Run this ONTAP command...
<p>Manually configure the SP network for a node, including the following:</p> <ul style="list-style-type: none"> <li>• The IP address family (IPv4 or IPv6)</li> <li>• Whether the network interface of the specified IP address family should be enabled</li> <li>• If you are using IPv4, whether to use the network configuration from the DHCP server or the network address that you specify</li> <li>• The public IP address for the SP</li> <li>• The netmask for the SP (if using IPv4)</li> <li>• The network prefix-length of the subnet mask for the SP (if using IPv6)</li> <li>• The gateway IP address for the SP</li> </ul>	<pre>system service-processor network modify</pre>
<p>Display the SP network configuration, including the following:</p> <ul style="list-style-type: none"> <li>• The configured address family (IPv4 or IPv6) and whether it is enabled</li> <li>• The remote management device type</li> <li>• The current SP status and link status</li> <li>• Network configuration, such as IP address, MAC address, netmask, prefix-length of subnet mask, router-assigned IP address, link local IP address, and gateway IP address</li> <li>• The time the SP was last updated</li> <li>• The name of the subnet used for SP automatic configuration</li> <li>• Whether the IPv6 router-assigned IP address is enabled</li> <li>• SP network setup status</li> <li>• Reason for the SP network setup failure</li> </ul>	<pre>system service-processor network show</pre> <p>Displaying complete SP network details requires the <code>-instance</code> parameter.</p>
<p>Modify the SP API service configuration, including the following:</p> <ul style="list-style-type: none"> <li>• Changing the port used by the SP API service</li> <li>• Enabling or disabling the SP API service</li> </ul>	<pre>system service-processor api-service modify</pre> <p>(advanced privilege level)</p>

If you want to...	Run this ONTAP command...
Display the SP API service configuration	<pre>system service-processor api-service show</pre> <p>(advanced privilege level)</p>
Renew the SSL and SSH certificates used by the SP API service for internal communication	<ul style="list-style-type: none"> <li>• For ONTAP 9.5 or later: <pre>system service-processor api-service renew-internal-certificates</pre></li> <li>• For ONTAP 9.4 or earlier: <pre>system service-processor api-service renew-certificates</pre></li> </ul> <p>(advanced privilege level)</p>

### Commands for managing the SP firmware image

If you want to...	Run this ONTAP command...
Display the details of the currently installed SP firmware image, including the following: <ul style="list-style-type: none"> <li>• The remote management device type</li> <li>• The image (primary or backup) that the SP is booted from, its status, and firmware version</li> <li>• Whether the firmware automatic update is enabled and the last update status</li> </ul>	<pre>system service-processor image show</pre> <p>The <code>-is-current</code> parameter indicates the image (primary or backup) that the SP is currently booted from, not if the installed firmware version is most current.</p>
Enable or disable the SP automatic firmware update	<pre>system service-processor image modify</pre> <p>By default, the SP firmware is automatically updated with the update of ONTAP or when a new version of the SP firmware is manually downloaded. Disabling the automatic update is not recommended because doing so can result in suboptimal or nonqualified combinations between the ONTAP image and the SP firmware image.</p>

If you want to...	Run this ONTAP command...
Manually download an SP firmware image on a node	<pre>system node image get</pre> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;">  <p>Before you run the <code>system node image</code> commands, you must set the privilege level to advanced (<code>set -privilege advanced</code>), entering <b>y</b> when prompted to continue.</p> </div> <p>The SP firmware image is packaged with ONTAP. You do not need to download the SP firmware manually, unless you want to use an SP firmware version that is different from the one packaged with ONTAP.</p>
Display the status for the latest SP firmware update triggered from ONTAP, including the following information: <ul style="list-style-type: none"> <li>• The start and end time for the latest SP firmware update</li> <li>• Whether an update is in progress and the percentage that is complete</li> </ul>	<pre>system service-processor image update-progress show</pre>

### Commands for managing SSH access to the SP

If you want to...	Run this ONTAP command...
Grant SP access to only the specified IP addresses	<pre>system service-processor ssh add-allowed-addresses</pre>
Block the specified IP addresses from accessing the SP	<pre>system service-processor ssh remove-allowed-addresses</pre>
Display the IP addresses that can access the SP	<pre>system service-processor ssh show</pre>

### Commands for general SP administration

If you want to...	Run this ONTAP command...
Display general SP information, including the following: <ul style="list-style-type: none"> <li>• The remote management device type</li> <li>• The current SP status</li> <li>• Whether the SP network is configured</li> <li>• Network information, such as the public IP address and the MAC address</li> <li>• The SP firmware version and Intelligent Platform Management Interface (IPMI) version</li> <li>• Whether the SP firmware automatic update is enabled</li> </ul>	<pre>system service-processor show</pre> Displaying complete SP information requires the <code>-instance</code> parameter.
Reboot the SP on a node	<pre>system service-processor reboot-sp</pre>
Generate and send an AutoSupport message that includes the SP log files collected from a specified node	<pre>system node autosupport invoke-splog</pre>
Display the allocation map of the collected SP log files in the cluster, including the sequence numbers for the SP log files that reside in each collecting node	<pre>system service-processor log show-allocations</pre>

### Related information

[ONTAP 9 Commands](#)

### ONTAP commands for BMC management

These ONTAP commands are supported on the Baseboard Management Controller (BMC).

The BMC uses some of the same commands as the Service Processor (SP). The following SP commands are supported on the BMC.

If you want to...	Use this command
Display the BMC information	<b>system service-processor show</b>
Display/modify the BMC network configuration	<b>system service-processor network show/modify</b>
Reset the BMC	<b>system service-processor reboot-sp</b>

If you want to...	Use this command
Display/modify the details of the currently installed BMC firmware image	<code>system service-processor image show/modify</code>
Update BMC firmware	<code>system service-processor image update</code>
Display the status for the latest BMC firmware update	<code>system service-processor image update-progress show</code>
Enable the automatic network configuration for the BMC to use an IPv4 or IPv6 address on the specified subnet	<code>system service-processor network auto-configuration enable</code>
Disable the automatic network configuration for an IPv4 or IPv6 address on the subnet specified for the BMC	<code>system service-processor network auto-configuration disable</code>
Display the BMC automatic network configuration	<code>system service-processor network auto-configuration show</code>

For commands that are not supported by the BMC firmware, the following error message is returned.

```

::> Error: Command not supported on this platform.

```

### BMC CLI commands

You can log into the BMC using SSH. The following commands are supported from the BMC command line.

Command	Function
<code>system</code>	Display a list of all commands.
<code>system console</code>	Connect to the system's console. Use <code>Ctrl+D</code> to exit the session.
<code>system core</code>	Dump the system core and reset.
<code>system power cycle</code>	Power the system off, then on.
<code>system power off</code>	Power the system off.
<code>system power on</code>	Power the system on.



Command	Function
system power status	Print system power status.
system reset	Reset the system.
system log	Print system console logs
system fru show [id]	Dump all/selected field replaceable unit (FRU) info.

## Manage audit logging for management activities

### How ONTAP implements audit logging

Management activities recorded in the audit log are included in standard AutoSupport reports, and certain logging activities are included in EMS messages. You can also forward the audit log to destinations that you specify, and you can display audit log files by using the CLI or a web browser.

Beginning with ONTAP 9.11.1, you can display audit log contents using System Manager.

ONTAP logs management activities that are performed on the cluster, for example, what request was issued, the user who triggered the request, the user's access method, and the time of the request.

The management activities can be one of the following types:

- SET requests, which typically apply to non-display commands or operations
  - These requests are issued when you run a `create`, `modify`, or `delete` command, for instance.
  - Set requests are logged by default.
- GET requests, which retrieve information and display it in the management interface
  - These requests are issued when you run a `show` command, for instance.
  - GET requests are not logged by default, but you can control whether GET requests sent from the ONTAP CLI (`-cliget`) or from the ONTAP APIs (`-ontapiget`) are logged in the file.

ONTAP records management activities in the `/mroot/etc/log/mlog/audit.log` file of a node. Commands from the three shells for CLI commands—the clustershell, the nodeshell, and the non-interactive systemshell (interactive systemshell commands are not logged)—as well as API commands are logged here. Audit logs include timestamps to show whether all nodes in a cluster are time synchronized.

The `audit.log` file is sent by the AutoSupport tool to the specified recipients. You can also forward the content securely to external destinations that you specify; for example, a Splunk or a syslog server.

The `audit.log` file is rotated daily. The rotation also occurs when it reaches 100 MB in size, and the previous 48 copies are preserved (with a maximum total of 49 files). When the audit file performs its daily rotation, no EMS message is generated. If the audit file rotates because its file size limit is exceeded, an EMS message is generated.

## Changes to audit logging in ONTAP 9

Beginning with ONTAP 9, the `command-history.log` file is replaced by `audit.log`, and the `mgwd.log` file no longer contains audit information. If you are upgrading to ONTAP 9, you should review any scripts or tools that refer to the legacy files and their contents.

After upgrade to ONTAP 9, existing `command-history.log` files are preserved. They are rotated out (deleted) as new `audit.log` files are rotated in (created).

Tools and scripts that check the `command-history.log` file might continue to work, because a soft link from `command-history.log` to `audit.log` is created at upgrade. However, tools and scripts that check the `mgwd.log` file will fail, because that file no longer contains audit information.

In addition, audit logs in ONTAP 9 and later no longer include the following entries because they are not considered useful and cause unnecessary logging activity:

- Internal commands run by ONTAP (that is, where `username=root`)
- Command aliases (separately from the command they point to)

Beginning with ONTAP 9, you can transmit the audit logs securely to external destinations using the TCP and TLS protocols.

### Display audit log contents

You can display the contents of the cluster's `/mroot/etc/log/mlog/audit.log` files by using the ONTAP CLI, System Manager, or a web browser.

The cluster's log file entries include the following:

#### Time

The log entry timestamp.

#### Application

The application used to connect to the cluster. Examples of possible values are `internal`, `console`, `ssh`, `http`, `ontapi`, `snmp`, `rsh`, `telnet`, and `service-processor`.

#### User

The username of the remote user.

#### State

The current state of the audit request, which could be `success`, `pending`, or `error`.

#### Message

An optional field that might contain error or additional information about the status of a command.

#### Session ID

The session ID on which the request is received. Each SSH *session* is assigned a session ID, while each HTTP, ONTAPI, or SNMP *request* is assigned a unique session ID.

## Storage VM

The SVM through which the user connected.

## Scope

Displays `svm` when the request is on a data storage VM; otherwise displays `cluster`.

## Command ID

The ID for each command received on a CLI session. This enables you to correlate a request and response. ZAPI, HTTP, and SNMP requests do not have command IDs.

You can display the cluster's log entries from the ONTAP CLI, from a web browser, and beginning with ONTAP 9.11.1, from System Manager.

### System Manager

- To display the inventory, select **Events & Jobs > Audit Logs**. Each column has controls to filter, sort, search, show, and inventory categories. The inventory details can be downloaded as an Excel workbook.
- To set filters, click the **Filter** button on the upper right side, then select the desired fields. You can also view all the commands executed in the session in which a failure occurred by clicking on the Session ID link.

### CLI

To display audit entries merged from multiple nodes in the cluster, enter:

```
security audit log show [parameters]
```

You can use the `security audit log show` command to display audit entries for individual nodes or merged from multiple nodes in the cluster. You can also display the content of the `/mroot/etc/log/mlog` directory on a single node by using a web browser. See the man page for details.

### Web browser

You can display the content of the `/mroot/etc/log/mlog` directory on a single node by using a web browser. [Learn about how to access a node's log, core dump, and MIB files by using a web browser.](#)

## Manage audit GET request settings

While SET requests are logged by default, GET requests are not. However, you can control whether GET requests sent from ONTAP HTML (`-httpget`), the ONTAP CLI (`-cliget`), or from the ONTAP APIs (`-ontapiget`) are logged in the file.

You can modify audit logging settings from the ONTAP CLI, and beginning with ONTAP 9.11.1, from System Manager.

## System Manager

1. Select **Events & Jobs > Audit Logs**.
2. Click  in the upper-right corner, then choose the requests to add or remove.

## CLI

- To specify that GET requests from the ONTAP CLI or APIs should be recorded in the audit log (the audit.log file), in addition to default set requests, enter:  

```
security audit modify [-cliget {on|off}][-httpget {on|off}][-ontapiget {on|off}]
```
- To display the current settings, enter:  

```
security audit show
```

See the man pages for details.

## Manage audit log destinations

You can forward the audit log to a maximum of 10 destinations. For example, you can forward the log to a Splunk or syslog server for monitoring, analysis, or backup purposes.

### About this task

To configure forwarding, you must provide the IP address of the syslog or Splunk host, its port number, a transmission protocol, and the syslog facility to use for the forwarded logs. [Learn about syslog facilities.](#)

You can select one of the following transmission values:

### UDP Unencrypted

User Datagram Protocol with no security (default)

### TCP Unencrypted

Transmission Control Protocol with no security




### TCP Encrypted

Transmission Control Protocol with Transport Layer Security (TLS)

A **Verify server** option is available when the TCP Encrypted protocol is selected.

You can forward audit logs from the ONTAP CLI, and beginning with ONTAP 9.11.1, from System Manager.

## System Manager

- To display audit log destinations, select **Cluster >Settings**. A count of log destinations is shown in the **Notification Management** tile. Click  to show details.
- To add, modify, or delete audit log destinations, select **Events & Jobs > Audit Logs**, then click **Manage Audit Destinations** in the upper right of the screen. Click  **Add**, or click  in the **Host Address** column to edit or delete entries.

## CLI

1. For each destination that you want to forward the audit log to, specify the destination IP address or host name and any security options.

```
cluster1::> cluster log-forwarding create -destination
192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 514 -protocol tcp-encrypted -facility user
```

- If the `cluster log-forwarding create` command cannot ping the destination host to verify connectivity, the command fails with an error. Although not recommended, using the `-force` parameter with the command bypasses the connectivity verification.
  - When you set the `-verify-server` parameter to `true`, the identity of the log forwarding destination is verified by validating its certificate. You can set the value to `true` only when you select the `tcp-encrypted` value in the `-protocol` field.
2. Verify that the destination records are correct by using the `cluster log-forwarding show` command.

```
cluster1::> cluster log-forwarding show

Destination Host          Port    Protocol          Verify Syslog
-----
192.168.123.96           514    udp-unencrypted  false  user
192.168.123.98           514    tcp-encrypted   true   user
2 entries were displayed.
```

See the man pages for details.

## Manage the cluster time (cluster administrators only)

Problems can occur when the cluster time is inaccurate. Although ONTAP enables you to manually set the time zone, date, and time on the cluster, you should configure the

## Network Time Protocol (NTP) servers to synchronize the cluster time.

Beginning with ONTAP 9.5, you can configure your NTP server with symmetric authentication.

NTP is always enabled. However, configuration is still required for the cluster to synchronize with an external time source. ONTAP enables you to manage the cluster's NTP configuration in the following ways:

- You can associate a maximum of 10 external NTP servers with the cluster (`cluster time-service ntp server create`).
  - For redundancy and quality of time service, you should associate at least three external NTP servers with the cluster.
  - You can specify an NTP server by using its IPv4 or IPv6 address or fully qualified host name.
  - You can manually specify the NTP version (v3 or v4) to use.

By default, ONTAP automatically selects the NTP version that is supported for a given external NTP server.

If the NTP version you specify is not supported for the NTP server, time exchange cannot take place.

- At the advanced privilege level, you can specify an external NTP server that is associated with the cluster to be the primary time source for correcting and adjusting the cluster time.
- You can display the NTP servers that are associated with the cluster (`cluster time-service ntp server show`).
- You can modify the cluster's NTP configuration (`cluster time-service ntp server modify`).
- You can disassociate the cluster from an external NTP server (`cluster time-service ntp server delete`).
- At the advanced privilege level, you can reset the configuration by clearing all external NTP servers' association with the cluster (`cluster time-service ntp server reset`).

A node that joins a cluster automatically adopts the NTP configuration of the cluster.

In addition to using NTP, ONTAP also enables you to manually manage the cluster time. This capability is helpful when you need to correct erroneous time (for example, a node's time has become significantly incorrect after a reboot). In that case, you can specify an approximate time for the cluster until NTP can synchronize with an external time server. The time you manually set takes effect across all nodes in the cluster.

You can manually manage the cluster time in the following ways:

- You can set or modify the time zone, date, and time on the cluster (`cluster date modify`).
- You can display the current time zone, date, and time settings of the cluster (`cluster date show`).



Job schedules do not adjust to manual cluster date and time changes. These jobs are scheduled to run based on the current cluster time when the job was created or when the job most recently ran. Therefore, if you manually change the cluster date or time, you must use the `job show` and `job history show` commands to verify that all scheduled jobs are queued and completed according to your requirements.


## Commands for managing the cluster time

You use the `cluster time-service ntp server` commands to manage the NTP servers for the cluster. You use the `cluster date` commands to manage the cluster time manually.

Beginning with ONTAP 9.5, you can configure your NTP server with symmetric authentication.

The following commands enable you to manage the NTP servers for the cluster:

If you want to...	Use this command...
Associate the cluster with an external NTP server without symmetric authentication	<pre>cluster time-service ntp server create -server server_name</pre>
Associate the cluster with an external NTP server with symmetric authentication Available in ONTAP 9.5 or later	<pre>cluster time-service ntp server create -server server_ip_address -key-id key_id</pre> <p> The <code>key_id</code> must refer to an existing shared key configured with 'cluster time-service ntp key'.</p>
Enable symmetric authentication for an existing NTP server An existing NTP server can be modified to enable authentication by adding the required key-id. Available in ONTAP 9.5 or later	<pre>cluster time-service ntp server modify -server server_name -key-id key_id</pre>
Disable symmetric authentication	<pre>cluster time-service ntp server modify -server server_name -authentication disabled</pre>
Configure a shared NTP key	<pre>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</pre> <p> Shared keys are referred to by an ID. The ID, its type, and value must be identical on both the node and the NTP server</p>
Display information about the NTP servers that are associated with the cluster	<pre>cluster time-service ntp server show</pre>
Modify the configuration of an external NTP server that is associated with the cluster	<pre>cluster time-service ntp server modify</pre>

If you want to...	Use this command...
Dissociate an NTP server from the cluster	<code>cluster time-service ntp server delete</code>
Reset the configuration by clearing all external NTP servers' association with the cluster	<code>cluster time-service ntp server reset</code>  This command requires the advanced privilege level.

The following commands enable you to manage the cluster time manually:

If you want to...	Use this command...
Set or modify the time zone, date, and time	<code>cluster date modify</code>
Display the time zone, date, and time settings for the cluster	<code>cluster date show</code>

#### Related information

[ONTAP 9 Commands](#)

## Manage the banner and MOTD

### Manage the banner and MOTD overview

ONTAP enables you to configure a login banner or a message of the day (MOTD) to communicate administrative information to CLI users of the cluster or storage virtual machine (SVM).

A banner is displayed in a console session (for cluster access only) or an SSH session (for cluster or SVM access) before a user is prompted for authentication such as a password. For example, you can use the banner to display a warning message such as the following to someone who attempts to log in to the system:

```
$ ssh admin@cluster1-01
```

```
This system is for authorized users only. Your IP Address has been logged.
```

```
Password:
```

An MOTD is displayed in a console session (for cluster access only) or an SSH session (for cluster or SVM access) after a user is authenticated but before the clustershell prompt appears. For example, you can use the MOTD to display a welcome or informational message such as the following that only authenticated users will see:



```
$ ssh admin@cluster1-01
```

```
Password:
```

```
Greetings. This system is running ONTAP 9.0.  
Your user name is 'admin'. Your last login was Wed Apr 08 16:46:53 2015  
from 10.72.137.28.
```

You can create or modify the content of the banner or MOTD by using the `security login banner modify` or `security login motd modify` command, respectively, in the following ways:

- You can use the CLI interactively or noninteractively to specify the text to use for the banner or MOTD.

The interactive mode, launched when the command is used without the `-message` or `-uri` parameter, enables you to use newlines (also known as end of lines) in the message.

The noninteractive mode, which uses the `-message` parameter to specify the message string, does not support newlines.

- You can upload content from an FTP or HTTP location to use for the banner or MOTD.
- You can configure the MOTD to display dynamic content.

Examples of what you can configure the MOTD to display dynamically include the following:

- Cluster name, node name, or SVM name
- Cluster date and time
- Name of the user logging in
- Last login for the user on any node in the cluster
- Login device name or IP address
- Operating system name
- Software release version
- Effective cluster version string

The `security login motd modify` man page describes the escape sequences that you can use to enable the MOTD to display dynamically generated content.

The banner does not support dynamic content.

You can manage the banner and MOTD at the cluster or SVM level:

- The following facts apply to the banner:
  - The banner configured for the cluster is also used for all SVMs that do not have a banner message defined.
  - An SVM-level banner can be configured for each SVM.

If a cluster-level banner has been configured, it is overridden by the SVM-level banner for the given SVM.

- The following facts apply to the MOTD:
  - By default, the MOTD configured for the cluster is also enabled for all SVMs.
  - Additionally, an SVM-level MOTD can be configured for each SVM.

In this case, users logging in to the SVM will see two MOTDs, one defined at the cluster level and the other at the SVM level.

- The cluster-level MOTD can be enabled or disabled on a per-SVM basis by the cluster administrator.

If the cluster administrator disables the cluster-level MOTD for an SVM, a user logging in to the SVM does not see the cluster-level MOTD.

## Create a banner

You can create a banner to display a message to someone who attempts to access the cluster or SVM. The banner is displayed in a console session (for cluster access only) or an SSH session (for cluster or SVM access) before a user is prompted for authentication.

### Steps

1. Use the `security login banner modify` command to create a banner for the cluster or SVM:

If you want to...	Then...
Specify a message that is a single line	Use the <code>-message "text"</code> parameter to specify the text.
Include newlines (also known as end of lines) in the message	Use the command without the <code>-message</code> or <code>-uri</code> parameter to launch the interactive mode for editing the banner.
Upload content from a location to use for the banner	Use the <code>-uri</code> parameter to specify the content's FTP or HTTP location.

The maximum size for a banner is 2,048 bytes, including newlines.

A banner created by using the `-uri` parameter is static. It is not automatically refreshed to reflect subsequent changes of the source content.

The banner created for the cluster is displayed also for all SVMs that do not have an existing banner. Any subsequently created banner for an SVM overrides the cluster-level banner for that SVM. Specifying the `-message` parameter with a hyphen within double quotes ("`-`") for the SVM resets the SVM to use the cluster-level banner.

2. Verify that the banner has been created by displaying it with the `security login banner show` command.

Specifying the `-message` parameter with an empty string ("`''`") displays banners that have no content.

Specifying the `-message` parameter with "`-`" displays all (admin or data) SVMs that do not have a banner configured.

## Examples of creating banners

The following example uses the noninteractive mode to create a banner for the "cluster1" cluster:

```
cluster1::> security login banner modify -message "Authorized users only!"  
  
cluster1::>
```

The following example uses the interactive mode to create a banner for the "svm1" SVM:

```
cluster1::> security login banner modify -vserver svm1  
  
Enter the message of the day for Vserver "svm1".  
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to  
abort.  
0          1          2          3          4          5          6          7  
8  
12345678901234567890123456789012345678901234567890123456789012345678901234  
567890  
The svm1 SVM is reserved for authorized users only!  
  
cluster1::>
```

The following example displays the banners that have been created:

```
cluster1::> security login banner show  
Vserver: cluster1  
Message  
-----  
---  
Authorized users only!  
  
Vserver: svm1  
Message  
-----  
---  
The svm1 SVM is reserved for authorized users only!  
  
2 entries were displayed.  
  
cluster1::>
```

## Related information

[Managing the banner](#)

## Managing the banner

You can manage the banner at the cluster or SVM level. The banner configured for the cluster is also used for all SVMs that do not have a banner message defined. A subsequently created banner for an SVM overrides the cluster banner for that SVM.

### Choices

- Manage the banner at the cluster level:

If you want to...	Then...
Create a banner to display for all CLI login sessions	Set a cluster-level banner:  <pre>security login banner modify -vserver cluster_name { [-message "text"]   [ -uri ftp_or_http_addr] }</pre>
Remove the banner for all (cluster and SVM) logins	Set the banner to an empty string (""):  <pre>security login banner modify -vserver * -message ""</pre>
Override a banner created by an SVM administrator	Modify the SVM banner message:  <pre>security login banner modify -vserver svm_name { [-message "text"]   [ ftp_or_http_addr] }</pre>

- Manage the banner at the SVM level:

Specifying `-vserver svm_name` is not required in the SVM context.

If you want to...	Then...
Override the banner supplied by the cluster administrator with a different banner for the SVM	Create a banner for the SVM:  <pre>security login banner modify -vserver svm_name { [-message "text"]   [ ftp_or_http_addr] }</pre>
Suppress the banner supplied by the cluster administrator so that no banner is displayed for the SVM	Set the SVM banner to an empty string for the SVM:  <pre>security login banner modify -vserver svm_name -message ""</pre>
Use the cluster-level banner when the SVM currently uses an SVM-level banner	Set the SVM banner to "-":  <pre>security login banner modify -vserver svm_name -message "-"</pre>

## Create an MOTD

You can create a message of the day (MOTD) to communicate information to authenticated CLI users. The MOTD is displayed in a console session (for cluster access only) or an SSH session (for cluster or SVM access) after a user is authenticated but before the clustershell prompt appears.

### Steps

1. Use the `security login motd modify` command to create an MOTD for the cluster or SVM:

If you want to...	Then...
Specify a message that is a single line	Use the <code>-message "text"</code> parameter to specify the text.
Include newlines (also known as end of lines)	Use the command without the <code>-message</code> or <code>-uri</code> parameter to launch the interactive mode for editing the MOTD.
Upload content from a location to use for the MOTD	Use the <code>-uri</code> parameter to specify the content's FTP or HTTP location.

The maximum size for an MOTD is 2,048 bytes, including newlines.

The `security login motd modify man` page describes the escape sequences that you can use to enable the MOTD to display dynamically generated content.

An MOTD created by using the `-uri` parameter is static. It is not automatically refreshed to reflect subsequent changes of the source content.

An MOTD created for the cluster is displayed also for all SVM logins by default, along with an SVM-level MOTD that you can create separately for a given SVM. Setting the `-is-cluster-message-enabled` parameter to `false` for an SVM prevents the cluster-level MOTD from being displayed for that SVM.

2. Verify that the MOTD has been created by displaying it with the `security login motd show` command.

Specifying the `-message` parameter with an empty string (`""`) displays MOTDs that are not configured or have no content.

See the [security login motd modify](#) command man page for a list of parameters to use to enable the MOTD to display dynamically generated content. Be sure to check the man page specific to your ONTAP version.

### Examples of creating MOTDs

The following example uses the noninteractive mode to create an MOTD for the "cluster1" cluster:

```
cluster1::> security login motd modify -message "Greetings!"
```

The following example uses the interactive mode to create an MOTD for the "svm1" SVM that uses escape

sequences to display dynamically generated content:

```
cluster1::> security login motd modify -vserver svml

Enter the message of the day for Vserver "svml".
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to
abort.
0          1          2          3          4          5          6          7
8
12345678901234567890123456789012345678901234567890123456789012345678901234
567890
Welcome to the \n SVM.  Your user ID is '\N'. Your last successful login
was \L.
```

The following example displays the MOTDs that have been created:

```
cluster1::> security login motd show
Vserver: cluster1
Is the Cluster MOTD Displayed?: true
Message
-----
---
Greetings!

Vserver: svml
Is the Cluster MOTD Displayed?: true
Message
-----
---
Welcome to the \n SVM.  Your user ID is '\N'. Your last successful login
was \L.

2 entries were displayed.
```

## Manage the MOTD

You can manage the message of the day (MOTD) at the cluster or SVM level. By default, the MOTD configured for the cluster is also enabled for all SVMs. Additionally, an SVM-level MOTD can be configured for each SVM. The cluster-level MOTD can be enabled or disabled for each SVM by the cluster administrator.

### Choices

- Manage the MOTD at the cluster level:

If you want to...	Then...
Create an MOTD for all logins when there is no existing MOTD	Set a cluster-level MOTD:  <pre>security login motd modify -vserver cluster_name { [-message "text"]   [- uri ftp_or_http_addr] }</pre>
Change the MOTD for all logins when no SVM-level MOTDs are configured	Modify the cluster-level MOTD:  <pre>security login motd modify -vserver cluster_name { [-message "text"] }   [-uri ftp_or_http_addr] }</pre>
Remove the MOTD for all logins when no SVM-level MOTDs are configured	Set the cluster-level MOTD to an empty string (""): <pre>security login motd modify -vserver cluster_name -message ""</pre>
Have every SVM display the cluster-level MOTD instead of using the SVM-level MOTD	Set a cluster-level MOTD, then set all SVM-level MOTDs to an empty string with the cluster-level MOTD enabled: <ol style="list-style-type: none"> <li><pre>security login motd modify -vserver cluster_name { [-message "text"]   [-uri ftp_or_http_addr] }</pre></li> <li><pre>security login motd modify { -vserver !"cluster_name" } -message "" -is-cluster-message-enabled true</pre></li> </ol>
Have an MOTD displayed for only selected SVMs, and use no cluster-level MOTD	Set the cluster-level MOTD to an empty string, then set SVM-level MOTDs for selected SVMs: <ol style="list-style-type: none"> <li><pre>security login motd modify -vserver cluster_name -message ""</pre></li> <li><pre>security login motd modify -vserver svm_name { [-message "text"]   [- uri ftp_or_http_addr] }</pre></li> </ol> <p>You can repeat this step for each SVM as needed.</p>

If you want to...	Then...
Use the same SVM-level MOTD for all (data and admin) SVMs	Set the cluster and all SVMs to use the same MOTD: <pre data-bbox="841 268 1463 365">security login motd modify -vserver * { [-message "text"]   [-uri ftp_or_http_addr] }</pre> <div data-bbox="873 485 927 541" style="border: 1px solid gray; border-radius: 50%; width: 30px; height: 30px; display: flex; align-items: center; justify-content: center; margin: 10px 0;">i</div> <p data-bbox="987 415 1458 615">If you use the interactive mode, the CLI prompts you to enter the MOTD individually for the cluster and each SVM. You can paste the same MOTD into each instance when you are prompted to.</p>
Have a cluster-level MOTD optionally available to all SVMs, but do not want the MOTD displayed for cluster logins	Set a cluster-level MOTD, but disable its display for the cluster: <pre data-bbox="841 787 1463 919">security login motd modify -vserver cluster_name { [-message "text"]   [-uri ftp_or_http_addr] } -is-cluster -message-enabled false</pre>
Remove all MOTDs at the cluster and SVM levels when only some SVMs have both cluster-level and SVM-level MOTDs	Set the cluster and all SVMs to use an empty string for the MOTD: <pre data-bbox="841 1081 1463 1138">security login motd modify -vserver * -message ""</pre>
Modify the MOTD only for the SVMs that have a non-empty string, when other SVMs use an empty string, and when a different MOTD is used at the cluster level	Use extended queries to modify the MOTD selectively: <pre data-bbox="841 1302 1463 1434">security login motd modify { -vserver !"cluster_name" -message !"" } { [-message "text"]   [-uri ftp_or_http_addr] }</pre>
Display all MOTDs that contain specific text (for example, “January” followed by “2015”) anywhere in a single or multiline message, even if the text is split across different lines	Use a query to display MOTDs: <pre data-bbox="841 1564 1398 1621">security login motd show -message *"January"*"2015"*</pre>
Interactively create an MOTD that includes multiple and consecutive newlines (also known as end of lines, or EOLs)	In the interactive mode, press the space bar followed by Enter to create a blank line without terminating the input for the MOTD.

- Manage the MOTD at the SVM level:

Specifying `-vserver svm_name` is not required in the SVM context.



If you want to...	Then...
Use a different SVM-level MOTD, when the SVM already has an existing SVM-level MOTD	Modify the SVM-level MOTD:  <pre>security login motd modify -vserver svm_name { [-message "text"]   [-uri ftp_or_http_addr] }</pre>
Use only the cluster-level MOTD for the SVM, when the SVM already has an SVM-level MOTD	Set the SVM-level MOTD to an empty string, then have the cluster administrator enable the cluster-level MOTD for the SVM:  <ol style="list-style-type: none"> <li>1. <code>security login motd modify -vserver svm_name -message ""</code></li> <li>2. (For the cluster administrator) <code>security login motd modify -vserver svm_name -is-cluster-message-enabled true</code></li> </ol>
Not have the SVM display any MOTD, when both the cluster-level and SVM-level MOTDs are currently displayed for the SVM	Set the SVM-level MOTD to an empty string, then have the cluster administrator disable the cluster-level MOTD for the SVM:  <ol style="list-style-type: none"> <li>1. <code>security login motd modify -vserver svm_name -message ""</code></li> <li>2. (For the cluster administrator) <code>security login motd modify -vserver svm_name -is-cluster-message-enabled false</code></li> </ol>

## Manage licenses (cluster administrators only)

### Manage licenses overview (cluster administrators only)

A license is a record of one or more software entitlements. In ONTAP 8.2 through ONTAP 9.9.1, license keys are delivered as 28-character strings, and there is one key per ONTAP feature. A new license key format called a NetApp License File (NLF) was introduced in ONTAP 9.2 for cluster-wide features only, such as FabricPool.

Beginning with ONTAP 9.10.1, all license are delivered as NLFs. NLF licenses can enable one or more ONTAP features, depending on your purchase. You can retrieve NLF licenses from the NetApp Support Site by searching for the system (controller) serial number.

You can find licenses for your initial or add-on software orders at the NetApp Support Site under **My Support > Software Licenses** (login required). For more information on license replacements, see the Knowledge Base article [Post motherboard replacement process to update licensing on a AFF/FAS system](#).

ONTAP enables you to manage feature licenses in the following ways:

- Display information about installed licenses (`system license show`)

- Display the packages that require licenses and their current license status on the cluster (`system license status show`)
- Delete a license from the cluster or a node whose serial number you specify (`system license delete`)
- Display or remove expired or unused licenses (`system license clean-up`)

ONTAP enables you to monitor feature usage and license entitlement risk in the following ways:

- Display a summary of feature usage in the cluster on a per-node basis (`system feature-usage show-summary`)

The summary includes counter information such as the number of weeks a feature was in use and the last date and time the feature was used.

- Display feature usage status in the cluster on a per-node and per-week basis (`system feature-usage show-history`)

The feature usage status can be `not-used`, `configured`, or `in-use`. If the usage information is not available, the status shows `not-available`.

- Display the status of license entitlement risk for each license package (`system license entitlement-risk show`)

The risk status can be `low`, `medium`, `high`, `unlicensed`, or `unknown`. The risk status is also included in the AutoSupport message. License entitlement risk does not apply to the base license package.

The license entitlement risk is evaluated by using a number of factors, which might include but are not limited to the following:

- Each package's licensing state
  - The type of each license, its expiry status, and the uniformity of the licenses across the cluster
  - Usage for the features associated with the license package
- If the evaluation process determines that the cluster has a license entitlement risk, the command output also suggests a corrective action.



Note: ONTAP 9.10.1 also supports 28-character license keys using System Manager or the CLI. However, if an NLF license is installed for a feature, you cannot install a 28-character license key over the NLF license for the same feature. For information about installing NLFs or license keys using System Manager, see “Enable new features.”

### Related information

[What are Data ONTAP 8.2 and 8.3 licensing overview and references?](#)

[How to verify Data ONTAP Software Entitlements and related License Keys using the Support Site](#)

[FAQ: Licensing updates in Data ONTAP 9.2](#)

[NetApp: Data ONTAP Entitlement Risk Status](#)

### License types and licensed method

Understanding license types and the licensed method helps you manage the licenses in a

cluster.

### License types

A package can have one or more of the following license types installed in the cluster. The `system license show` command displays the installed license type or types for a package.

- Standard license (`license`)

A standard license is a node-locked license. It is issued for a node with a specific system serial number (also known as a *controller serial number*). A standard license is valid only for the node that has the matching serial number.

Installing a standard, node-locked license entitles a node to the licensed functionality. For the cluster to use licensed functionality, at least one node must be licensed for the functionality. It might be out of compliance to use licensed functionality on a node that does not have an entitlement for the functionality.

- Site license (`site`)

A site license is not tied to a specific system serial number. When you install a site license, all nodes in the cluster are entitled to the licensed functionality. The `system license show` command displays site licenses under the cluster serial number.

If your cluster has a site license and you remove a node from the cluster, the node does not carry the site license with it, and it is no longer entitled to the licensed functionality. If you add a node to a cluster that has a site license, the node is automatically entitled to the functionality granted by the site license.

- Evaluation license (`demo`)

An evaluation license is a temporary license that expires after a certain period of time (indicated by the `system license show` command). It enables you to try certain software functionality without purchasing an entitlement. It is a cluster-wide license, and it is not tied to a specific serial number of a node.

If your cluster has an evaluation license for a package and you remove a node from the cluster, the node does not carry the evaluation license with it.

### Licensed method

It is possible to install both a cluster-wide license (the `site` or `demo` type) and a node-locked license (the `license` type) for a package. Therefore, an installed package can have multiple license types in the cluster. However, to the cluster, there is only one *licensed method* for a package. The `licensed method` field of the `system license status show` command displays the entitlement that is being used for a package. The command determines the licensed method as follows:

- If a package has only one license type installed in the cluster, the installed license type is the licensed method.
- If a package does not have any licenses installed in the cluster, the licensed method is `none`.
- If a package has multiple license types installed in the cluster, the licensed method is determined in the following priority order of the license type--`site`, `license`, and `demo`.

For example:


- If you have a site license, a standard license, and an evaluation license for a package, the licensed


method for the package in the cluster is `site`.

- If you have a standard license and an evaluation license for a package, the licensed method for the package in the cluster is `license`.
- If you have only an evaluation license for a package, the licensed method for the package in the cluster is `demo`.

## Commands for managing licenses

You use the `system license` commands to manage feature licenses for the cluster. You use the `system feature-usage` commands to monitor feature usage.

If you want to...	Use this command...
Add one or more licenses	<code>system license add</code>
Display information about installed licenses, for example: <ul style="list-style-type: none"><li>• License package name and description</li><li>• License type (<code>site</code>, <code>license</code>, or <code>demo</code>)</li><li>• Expiration date, if applicable</li><li>• The cluster or nodes that a package is licensed for</li><li>• Whether the license was installed prior to Data ONTAP 8.2 (<code>legacy</code>)</li><li>• Customer ID</li></ul>	<code>system license show</code>   Some information is displayed only when you use the <code>-instance</code> parameter.
Display all packages that require licenses and their current license status, including the following: <ul style="list-style-type: none"><li>• The package name</li><li>• The licensed method</li><li>• The expiration date, if applicable</li></ul>	<code>system license status show</code>
Delete the license of a package from the cluster or a node whose serial number you specify	<code>system license delete</code>
Display or remove expired or unused licenses	<code>system license clean-up</code>
Display summary of feature usage in the cluster on a per-node basis	<code>system feature-usage show-summary</code>
Display feature usage status in the cluster on a per-node and per-week basis	<code>system feature-usage show-history</code>

If you want to...	Use this command...
Display the status of license entitlement risk for each license package	<pre>system license entitlement-risk show</pre> <div style="display: flex; align-items: center; margin-top: 10px;">  <p>Some information is displayed only when you use the <code>-detail</code> and <code>-instance</code> parameters.</p> </div>

#### Related information

[ONTAP 9 Commands](#)

## Manage jobs and schedules

### Job categories

There are three categories of jobs that you can manage: server-affiliated, cluster-affiliated, and private.

A job can be in any of the following categories:

- **Server-Affiliated jobs**

These jobs are queued by the management framework to a specific node to be run.

- **Cluster-Affiliated jobs**

These jobs are queued by the management framework to any node in the cluster to be run.

- **Private jobs**

These jobs are specific to a node and do not use the replicated database (RDB) or any other cluster mechanism. The commands that manage private jobs require the advanced privilege level or higher.

### Commands for managing jobs

Jobs are placed into a job queue and run in the background when resources are available. If a job is consuming too many cluster resources, you can stop it or pause it until there is less demand on the cluster. You can also monitor and restart jobs.

When you enter a command that invokes a job, typically, the command informs you that the job has been queued and then returns to the CLI command prompt. However, some commands instead report job progress and do not return to the CLI command prompt until the job has been completed. In these cases, you can press Ctrl-C to move the job to the background.

If you want to...	Use this command...
Display information about all jobs	<code>job show</code>
Display information about jobs on a per-node basis	<code>job show bynode</code>

<b>If you want to...</b>	<b>Use this command...</b>
Display information about cluster-affiliated jobs	<code>job show-cluster</code>
Display information about completed jobs	<code>job show-completed</code>
Display information about job history	<code>job history show</code>  Up to 25,000 job records are stored for each node in the cluster. Consequently, attempting to display the full job history could take a long time. To avoid potentially long wait times, you should display jobs by node, storage virtual machine (SVM), or record ID.
Display the list of private jobs	<code>job private show</code> (advanced privilege level)
Display information about completed private jobs	<code>job private show-completed</code> (advanced privilege level)
Display information about the initialization state for job managers	<code>job initstate show</code> (advanced privilege level)
Monitor the progress of a job	<code>job watch-progress</code>
Monitor the progress of a private job	<code>job private watch-progress</code> (advanced privilege level)
Pause a job	<code>job pause</code>
Pause a private job	<code>job private pause</code> (advanced privilege level)
Resume a paused job	<code>job resume</code>
Resume a paused private job	<code>job private resume</code> (advanced privilege level)
Stop a job	<code>job stop</code>
Stop a private job	<code>job private stop</code> (advanced privilege level)
Delete a job	<code>job delete</code>
Delete a private job	<code>job private delete</code> (advanced privilege level)

If you want to...	Use this command...
Disassociate a cluster-affiliated job with an unavailable node that owns it, so that another node can take ownership of that job	<code>job unclaim</code> (advanced privilege level)



You can use the `event log show` command to determine the outcome of a completed job.

### Related information

[ONTAP 9 Commands](#)

### Commands for managing job schedules

Many tasks—for instance, volume Snapshot copies—can be configured to run on specified schedules. Schedules that run at specific times are called *cron* schedules (similar to UNIX `cron` schedules). Schedules that run at intervals are called *interval* schedules. You use the `job schedule` commands to manage job schedules.

Job schedules do not adjust to manual changes to the cluster date and time. These jobs are scheduled to run based on the current cluster time when the job was created or when the job most recently ran. Therefore, if you manually change the cluster date or time, you should use the `job show` and `job history show` commands to verify that all scheduled jobs are queued and completed according to your requirements.

If the cluster is part of a MetroCluster configuration, then the job schedules on both clusters must be identical. Therefore, if you create, modify, or delete a job schedule, you must perform the same operation on the remote cluster.

If you want to...	Use this command...
Display information about all schedules	<code>job schedule show</code>
Display the list of jobs by schedule	<code>job schedule show-jobs</code>
Display information about cron schedules	<code>job schedule cron show</code>
Display information about interval schedules	<code>job schedule interval show</code>
Create a cron schedule <sup>1</sup>	<code>job schedule cron create</code>
Create an interval schedule	<code>job schedule interval create</code>  You must specify at least one of the following parameters: <code>-days</code> , <code>-hours</code> , <code>-minutes</code> , or <code>-seconds</code> .
Modify a cron schedule	<code>job schedule cron modify</code>

If you want to...	Use this command...
Modify an interval schedule	<code>job schedule interval modify</code>
Delete a schedule	<code>job schedule delete</code>
Delete a cron schedule	<code>job schedule cron delete</code>
Delete an interval schedule	<code>job schedule interval delete</code>

<sup>1</sup>Beginning with ONTAP 9.10.1, when you create a job schedule by using the `job schedule cron create` command, you can include the Vserver for your job schedule.

### Related information

[ONTAP 9 Commands](#)

## Back up and restore cluster configurations (cluster administrators only)

### What configuration backup files are

Configuration backup files are archive files (.7z) that contain information for all configurable options that are necessary for the cluster, and the nodes within it, to operate properly.

These files store the local configuration of each node, plus the cluster-wide replicated configuration. You use configuration backup files to back up and restore the configuration of your cluster.

There are two types of configuration backup files:

- **Node configuration backup file**

Each healthy node in the cluster includes a node configuration backup file, which contains all of the configuration information and metadata necessary for the node to operate healthy in the cluster.

- **Cluster configuration backup file**

These files include an archive of all of the node configuration backup files in the cluster, plus the replicated cluster configuration information (the replicated database, or RDB file). Cluster configuration backup files enable you to restore the configuration of the entire cluster, or of any node in the cluster. The cluster configuration backup schedules create these files automatically and store them on several nodes in the cluster.



Configuration backup files contain configuration information only. They do not include any user data. For information about restoring user data, see [Data Protection](#).

### Manage configuration backups



## How the node and cluster configurations are backed up automatically

Three separate schedules automatically create cluster and node configuration backup files and replicate them among the nodes in the cluster.

The configuration backup files are automatically created according to the following schedules:

- Every 8 hours
- Daily
- Weekly


At each of these times, a node configuration backup file is created on each healthy node in the cluster. All of these node configuration backup files are then collected in a single cluster configuration backup file along with the replicated cluster configuration and saved on one or more nodes in the cluster.


For single-node clusters (including Data ONTAP Edge systems), you can specify the configuration backup destination during software setup. After setup, those settings can be modified using ONTAP commands.

### Commands for managing configuration backup schedules

You can use the `system configuration backup settings` commands to manage configuration backup schedules.

These commands are available at the advanced privilege level.


If you want to...	Use this command...
<p>Change the settings for a configuration backup schedule:</p> <ul style="list-style-type: none"><li>• Specify a remote URL (HTTP, HTTPS, FTP, FTPS, or TFTP ) where the configuration backup files will be uploaded in addition to the default locations in the cluster</li><li>• Specify a user name to be used to log in to the remote URL</li><li>• Set the number of backups to keep for each configuration backup schedule</li></ul>	<pre>system configuration backup settings modify</pre> <p>When you use HTTPS in the remote URL, use the <code>-validate-certification</code> option to enable or disable digital certificate validation. Certificate validation is disabled by default.</p> <div data-bbox="850 1331 1446 1541"><p>The web server to which you are uploading the configuration backup file must have PUT operations enabled for HTTP and POST operations enabled for HTTPS. For more information, see your web server's documentation.</p></div>
<p>Set the password to be used to log in to the remote URL</p>	<pre>system configuration backup settings set-password</pre>


If you want to...	Use this command...
View the settings for the configuration backup schedule	<pre>system configuration backup settings show</pre> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  You set the <code>-instance</code> parameter to view the user name and the number of backups to keep for each schedule. </div>

### Commands for managing configuration backup files

You use the `system configuration backup` commands to manage cluster and node configuration backup files.

These commands are available at the advanced privilege level.

If you want to...	Use this command...
Create a new node or cluster configuration backup file	<pre>system configuration backup create</pre>
Copy a configuration backup file from a node to another node in the cluster	<pre>system configuration backup copy</pre>
Upload a configuration backup file from a node in the cluster to a remote URL (FTP, HTTP, HTTPS, TFTP, or FTPS)	<pre>system configuration backup upload</pre> <p>When you use HTTPS in the remote URL, use the <code>-validate-certification</code> option to enable or disable digital certificate validation. Certificate validation is disabled by default.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  The web server to which you are uploading the configuration backup file must have PUT operations enabled for HTTP and POST operations enabled for HTTPS. Some web servers might require the installation of an additional module. For more information, see your web server's documentation. Supported URL formats vary by ONTAP release. See the command line help for your ONTAP version. </div>
Download a configuration backup file from a remote URL to a node in the cluster, and, if specified, validate the digital certificate	<pre>system configuration backup download</pre> <p>When you use HTTPS in the remote URL, use the <code>-validate-certification</code> option to enable or disable digital certificate validation. Certificate validation is disabled by default.</p>

If you want to...	Use this command...
Rename a configuration backup file on a node in the cluster	<code>system configuration backup rename</code>
View the node and cluster configuration backup files for one or more nodes in the cluster	<code>system configuration backup show</code>
Delete a configuration backup file on a node	<code>system configuration backup delete</code> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-left: 20px;">  <p>This command deletes the configuration backup file on the specified node only. If the configuration backup file also exists on other nodes in the cluster, it remains on those nodes.</p> </div>

## Recovering a node configuration

### Find a configuration backup file to use for recovering a node

You use a configuration backup file located at a remote URL or on a node in the cluster to recover a node configuration.

### About this task

You can use either a cluster or node configuration backup file to restore a node configuration.

### Step

1. Make the configuration backup file available to the node for which you need to restore the configuration.

If the configuration backup file is located...	Then...
At a remote URL	Use the <code>system configuration backup download</code> command at the advanced privilege level to download it to the recovering node.
On a node in the cluster	<ol style="list-style-type: none"> <li>a. Use the <code>system configuration backup show</code> command at the advanced privilege level to view the list of configuration backup files available in the cluster that contains the recovering node's configuration.</li> <li>b. If the configuration backup file you identify does not exist on the recovering node, then use the <code>system configuration backup copy</code> command to copy it to the recovering node.</li> </ol>

If you previously re-created the cluster, you should choose a configuration backup file that was created after the cluster recreation. If you must use a configuration backup file that was created prior to the cluster recreation, then after recovering the node, you must re-create the cluster again.

## Restore the node configuration using a configuration backup file

You restore the node configuration using the configuration backup file that you identified and made available to the recovering node.

### About this task

You should only perform this task to recover from a disaster that resulted in the loss of the node's local configuration files.

### Steps

1. Change to the advanced privilege level:

```
set -privilege advanced
```

2. If the node is healthy, then at the advanced privilege level of a different node, use the `cluster modify` command with the `-node` and `-eligibility` parameters to mark it ineligible and isolate it from the cluster.

If the node is not healthy, then you should skip this step.

This example modifies node2 to be ineligible to participate in the cluster so that its configuration can be restored:

```
cluster1::*> cluster modify -node node2 -eligibility false
```

1. Use the `system configuration recovery node restore` command at the advanced privilege level to restore the node's configuration from a configuration backup file.

If the node lost its identity, including its name, then you should use the `-nodename-in-backup` parameter to specify the node name in the configuration backup file.

This example restores the node's configuration using one of the configuration backup files stored on the node:

```
cluster1::*> system configuration recovery node restore -backup  
cluster1.8hour.2011-02-22.18_15_00.7z
```

```
Warning: This command overwrites local configuration files with  
files contained in the specified backup file. Use this  
command only to recover from a disaster that resulted  
in the loss of the local configuration files.  
The node will reboot after restoring the local configuration.  
Do you want to continue? {y|n}: y
```

The configuration is restored, and the node reboots.

1. If you marked the node ineligible, then use the `system configuration recovery cluster sync` command to mark the node as eligible and synchronize it with the cluster.
2. If you are operating in a SAN environment, use the `system node reboot` command to reboot the node and reestablish SAN quorum.

### After you finish

If you previously re-created the cluster, and if you are restoring the node configuration by using a configuration

backup file that was created prior to that cluster re-creation, then you must re-create the cluster again.

## Recover a cluster configuration

### Find a configuration to use for recovering a cluster

You use the configuration from either a node in the cluster or a cluster configuration backup file to recover a cluster.

#### Steps

1. Choose a type of configuration to recover the cluster.

- A node in the cluster

If the cluster consists of more than one node, and one of the nodes has a cluster configuration from when the cluster was in the desired configuration, then you can recover the cluster using the configuration stored on that node.

In most cases, the node containing the replication ring with the most recent transaction ID is the best node to use for restoring the cluster configuration. The `cluster ring show` command at the advanced privilege level enables you to view a list of the replicated rings available on each node in the cluster.

- A cluster configuration backup file

If you cannot identify a node with the correct cluster configuration, or if the cluster consists of a single node, then you can use a cluster configuration backup file to recover the cluster.

If you are recovering the cluster from a configuration backup file, any configuration changes made since the backup was taken will be lost. You must resolve any discrepancies between the configuration backup file and the present configuration after recovery. See Knowledge Base article [ONTAP Configuration Backup Resolution Guide](#) for troubleshooting guidance.

2. If you chose to use a cluster configuration backup file, then make the file available to the node you plan to use to recover the cluster.

If the configuration backup file is located...	Then...
At a remote URL	Use the <code>system configuration backup download</code> command at the advanced privilege level to download it to the recovering node.
On a node in the cluster	<ol style="list-style-type: none"><li>a. Use the <code>system configuration backup show</code> command at the advanced privilege level to find a cluster configuration backup file that was created when the cluster was in the desired configuration.</li><li>b. If the cluster configuration backup file is not located on the node you plan to use to recover the cluster, then use the <code>system configuration backup copy</code> command to copy it to the recovering node.</li></ol>

## Restore a cluster configuration from an existing configuration

To restore a cluster configuration from an existing configuration after a cluster failure, you re-create the cluster using the cluster configuration that you chose and made available to the recovering node, and then rejoin each additional node to the new cluster.

### About this task

You should only perform this task to recover from a disaster that resulted in the loss of the cluster's configuration.



If you are re-creating the cluster from a configuration backup file, you must contact technical support to resolve any discrepancies between the configuration backup file and the configuration present in the cluster.

If you are recovering the cluster from a configuration backup file, any configuration changes made since the backup was taken will be lost. You must resolve any discrepancies between the configuration backup file and the present configuration after recovery. See the Knowledge Base article [ONTAP Configuration Backup Resolution Guide for troubleshooting guidance](#).

### Steps

1. Disable storage failover for each HA pair:

```
storage failover modify -node node_name -enabled false
```

You only need to disable storage failover once for each HA pair. When you disable storage failover for a node, storage failover is also disabled on the node's partner.

2. Halt each node except for the recovering node:

```
system node halt -node node_name -reason "text"
```

```
cluster1::*> system node halt -node node0 -reason "recovering cluster"  
Warning: Are you sure you want to halt the node? {y|n}: y
```

3. Set the privilege level to advanced:

```
set -privilege advanced
```

4. On the recovering node, use the **system configuration recovery cluster recreate** command to re-create the cluster.

This example re-creates the cluster using the configuration information stored on the recovering node:

```
cluster1::*> configuration recovery cluster recreate -from node
```

```
Warning: This command will destroy your existing cluster. It will
        rebuild a new single-node cluster consisting of this node
        and its current configuration. This feature should only be
        used to recover from a disaster. Do not perform any other
        recovery operations while this operation is in progress.
Do you want to continue? {y|n}: y
```

A new cluster is created on the recovering node.

5. If you are re-creating the cluster from a configuration backup file, verify that the cluster recovery is still in progress:

```
system configuration recovery cluster show
```

You do not need to verify the cluster recovery state if you are re-creating the cluster from a healthy node.

```
cluster1::*> system configuration recovery cluster show
Recovery Status: in-progress
Is Recovery Status Persisted: false
```

6. Boot each node that needs to be rejoined to the re-created cluster.

You must reboot the nodes one at a time.

7. For each node that needs to be joined to the re-created cluster, do the following:

- a. From a healthy node on the re-created cluster, rejoin the target node:

```
system configuration recovery cluster rejoin -node node_name
```

This example rejoins the “node2” target node to the re-created cluster:

```
cluster1::*> system configuration recovery cluster rejoin -node node2

Warning: This command will rejoin node "node2" into the local
        cluster, potentially overwriting critical cluster
        configuration files. This command should only be used
        to recover from a disaster. Do not perform any other
        recovery operations while this operation is in progress.
        This command will cause node "node2" to reboot.
Do you want to continue? {y|n}: y
```

The target node reboots and then joins the cluster.

- b. Verify that the target node is healthy and has formed quorum with the rest of the nodes in the cluster:

```
cluster show -eligibility true
```

The target node must rejoin the re-created cluster before you can rejoin another node.

```
cluster1::*> cluster show -eligibility true
Node                Health  Eligibility  Epsilon
-----
node0                true    true         false
node1                true    true         false
2 entries were displayed.
```

8. If you re-created the cluster from a configuration backup file, set the recovery status to be complete:

```
system configuration recovery cluster modify -recovery-status complete
```

9. Return to the admin privilege level:

```
set -privilege admin
```

10. If the cluster consists of only two nodes, use the **cluster ha modify** command to reenables cluster HA.

11. Use the **storage failover modify** command to reenables storage failover for each HA pair.

#### After you finish

If the cluster has SnapMirror peer relationships, then you also need to re-create those relationships. For more information, see [Data Protection](#).

#### Synchronize a node with the cluster

If cluster-wide quorum exists, but one or more nodes are out of sync with the cluster, then you must synchronize the node to restore the replicated database (RDB) on the node and bring it into quorum.

#### Step

1. From a healthy node, use the `system configuration recovery cluster sync` command at the advanced privilege level to synchronize the node that is out of sync with the cluster configuration.

This example synchronizes a node (*node2*) with the rest of the cluster:



```
cluster1::*> system configuration recovery cluster sync -node node2
```

```
Warning: This command will synchronize node "node2" with the cluster
configuration, potentially overwriting critical cluster
configuration files on the node. This feature should only be
used to recover from a disaster. Do not perform any other
recovery operations while this operation is in progress. This
command will cause all the cluster applications on node
"node2" to restart, interrupting administrative CLI and Web
interface on that node.
```

```
Do you want to continue? {y|n}: y
```

```
All cluster applications on node "node2" will be restarted. Verify that
the cluster applications go online.
```

## Result

The RDB is replicated to the node, and the node becomes eligible to participate in the cluster.

## Manage core dumps (cluster administrators only)

When a node panics, a core dump occurs and the system creates a core dump file that technical support can use to troubleshoot the problem. You can configure or display core dump attributes. You can also save, display, segment, upload, or delete a core dump file.

You can manage core dumps in the following ways:

- Configuring core dumps and displaying the configuration settings
- Displaying basic information, the status, and attributes of core dumps

Core dump files and reports are stored in the `/mroot/etc/crash/` directory of a node. You can display the directory content by using the `system node coredump` commands or a web browser.

- Saving the core dump content and uploading the saved file to a specified location or to technical support

ONTAP prevents you from initiating the saving of a core dump file during a takeover, an aggregate relocation, or a giveback.

- Deleting core dump files that are no longer needed




AFF A220, AFF A800, FAS2720, FAS2750, and later systems store core dumps on their boot device. When NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) is enabled on these systems, the core dump is also encrypted.

## Commands for managing core dumps

You use the `system node coredump config` commands to manage the configuration of core dumps, the `system node coredump` commands to manage the core dump files, and the `system node coredump reports` commands to manage application

## core reports.

If you want to...	Use this command...
Configure core dumps	<code>system node coredump config modify</code>
Display the configuration settings for core dumps	<code>system node coredump config show</code>
Display basic information about core dumps	<code>system node coredump show</code>
Manually trigger a core dump when you reboot a node	<code>system node reboot</code> with both the <code>-dump</code> and <code>-skip-lif-migration</code> parameters
Manually trigger a core dump when you shut down a node	<code>system node halt</code> with both the <code>-dump</code> and <code>-skip-lif-migration</code> parameters
Save a specified core dump	<code>system node coredump save</code>
Save all unsaved core dumps that are on a specified node	<code>system node coredump save-all</code>
Generate and send an AutoSupport message with a core dump file you specify	<code>system node autosupport invoke-core-upload</code>   The <code>-uri</code> optional parameter specifies an alternate destination for the AutoSupport message.
Display status information about core dumps	<code>system node coredump status</code>
Delete a specified core dump	<code>system node coredump delete</code>
Delete all unsaved core dumps or all saved core files on a node	<code>system node coredump delete-all</code>
Display application core dump reports	<code>system node coredump reports show</code>
Delete an application core dump report	<code>system node coredump reports delete</code>

### Related information

[ONTAP 9 Commands](#)

## Monitor a storage system

## Use AutoSupport and Active IQ Digital Advisor

The AutoSupport component of ONTAP collects telemetry and sends it for analysis. Active IQ Digital Advisor analyzes the data from AutoSupport and provides proactive care and optimization. Using artificial intelligence, Active IQ can identify potential problems and help you resolve them before they impact your business.

Active IQ enables you to optimize your data infrastructure across your global hybrid cloud by delivering actionable predictive analytics and proactive support through a cloud-based portal and mobile app. Data-driven insights and recommendations from Active IQ are available to all NetApp customers with an active SupportEdge contract (features vary by product and support tier).

Here are some things you can do with Active IQ:

- Plan upgrades. Active IQ identifies issues in your environment that can be resolved by upgrading to a newer version of ONTAP and the Upgrade Advisor component helps you plan for a successful upgrade.
- View system wellness. Your Active IQ dashboard reports any issues with wellness and helps you correct those issues. Monitor system capacity to make sure you never run out of storage space. View support cases for your system.
- Manage performance. Active IQ shows system performance over a longer period than you can see in System Manager. Identify configuration and system issues that are impacting your performance.
- Maximize efficiency. View storage efficiency metrics and identify ways to store more data in less space.
- View inventory and configuration. Active IQ displays complete inventory and software and hardware configuration information. See when service contracts are expiring and renew them to ensure you remain supported.

### Related information

[NetApp Documentation: Active IQ Digital Advisor](#)

[Launch Active IQ](#)

[SupportEdge Services](#)

## Manage AutoSupport settings with System Manager

You can use System Manager to view and edit the settings for your AutoSupport account.

You can perform the following procedures:

- [View AutoSupport settings](#)
- [Generate and send AutoSupport data](#)
- [Test the connection to AutoSupport](#)
- [Enable or disable AutoSupport](#)
- [Suppress the generation of support cases](#)
- [Resume the generation of support cases](#)
- [Edit AutoSupport settings](#)

## View AutoSupport settings


You can use System Manager to view the settings for your AutoSupport account.

### Steps

1. In System Manager, click **Cluster > Settings**.

In the **AutoSupport** section, the following information is displayed:

- Status
- Transport protocol
- Proxy server
- From email address


2. In the **AutoSupport** section, click , then click **More Options**.

Additional information is displayed about the AutoSupport connection and email settings. Also, the transfer history of messages is listed.

## Generate and send AutoSupport data

In System Manager, you can initiate the generation of AutoSupport messages and choose from which cluster node or nodes the data is collected.

### Steps

1. In System Manager, click **Cluster > Settings**.
2. In the **AutoSupport** section, click , then click **Generate and Send**.
3. Enter a subject.
4. Click the check box under **Collect Data From** to specify the nodes from which to collect the data.

## Test the connection to AutoSupport

From System Manager, you can send a test message to verify the connection to AutoSupport.



### Steps

1. In System Manager, click **Cluster > Settings**.
2. In the **AutoSupport** section, click , then click **Test Connectivity**.
3. Enter a subject for the message.

## Enable or disable AutoSupport

In System Manager, you can disable the ability of AutoSupport to monitor the health of your storage system and send you notification messages. You can enable AutoSupport again after it has been disabled.

### Steps

1. Click **Cluster > Settings**.
2. In the **AutoSupport** section, click , then click **Disable**.
3. If want to enable AutoSupport again, in the **AutoSupport** section, click , then click **Enable**.

## Suppress the generation of support cases


Beginning with ONTAP 9.10.1, you can use System Manager to send a request to AutoSupport to suppress the generation of support cases.

### About this task

To suppress the generation of support cases, you specify the nodes and number of hours for which you want the suppression to occur.

Suppressing support cases can be especially helpful if you do not want AutoSupport to create automated cases while you are performing maintenance on your systems.


### Steps

1. Click **Cluster > Settings**.
2. In the **AutoSupport** section, click , then click **Suppress Support Case Generation**.
3. Enter the number of hours that you want the suppression to occur.
4. Select the nodes for which you want the suppression to occur.

## Resume the generation of support cases

Beginning with ONTAP 9.10.1, you can use System Manager to resume the generation of support cases from AutoSupport if it has been suppressed.



### Steps

1. Click **Cluster > Settings**.
2. In the **AutoSupport** section, click , then click **Resume Support Case Generation**.
3. Select the nodes for which you want the generation to resume.

## Edit AutoSupport settings

You can use System Manager to modify the connection and email settings for your AutoSupport account.

### Steps

1. Click **Cluster > Settings**.
2. In the **AutoSupport** section, click , then click **More Options**.
3. In the **Connections** section or the **Email** section, click  **Edit** to modify the setting for either section.

## Manage AutoSupport with the CLI

### Manage AutoSupport overview

AutoSupport is a mechanism that proactively monitors the health of your system and automatically sends messages to NetApp technical support, your internal support organization, and a support partner. Although AutoSupport messages to technical support are enabled by default, you must set the correct options and have a valid mail host to have messages sent to your internal support organization.

Only the cluster administrator can perform AutoSupport management. The storage virtual machine (SVM) administrator has no access to AutoSupport.

AutoSupport is enabled by default when you configure your storage system for the first time. AutoSupport begins sending messages to technical support 24 hours after AutoSupport is enabled. You can shorten the 24-hour period by upgrading or reverting the system, modifying the AutoSupport configuration, or changing the system time to be something other than a 24-hour period.



You can disable AutoSupport at any time, but you should leave it enabled. Enabling AutoSupport can significantly help speed problem determination and resolution should a problem occur on your storage system. By default, the system collects AutoSupport information and stores it locally, even if you disable AutoSupport.

For more information about AutoSupport, see the NetApp Support Site.

### Related information

- [NetApp Support](#)
- [Learn more about the AutoSupport commands in the ONTAP CLI](#)

### When and where AutoSupport messages are sent

AutoSupport sends messages to different recipients, depending on the type of message. Learning when and where AutoSupport sends messages can help you understand messages that you receive through email or view on the Active IQ (formerly known as My AutoSupport) web site.

Unless specified otherwise, settings in the following tables are parameters of the `system node autosupport modify` command.

### Event-triggered messages

When events occur on the system that require corrective action, AutoSupport automatically sends an event-triggered message.

When the message is sent	Where the message is sent
AutoSupport responds to a trigger event in the EMS	Addresses specified in <code>-to</code> and <code>-noteto</code> . (Only critical, service-affecting events are sent.)  Addresses specified in <code>-partner-address</code>  Technical support, if <code>-support</code> is set to <code>enable</code>

### Scheduled messages

AutoSupport automatically sends several messages on a regular schedule.

When the message is sent	Where the message is sent
Daily (by default, sent between 12:00 a.m. and 1:00 a.m. as a log message)	Addresses specified in <code>-partner-address</code>  Technical support, if <code>-support</code> is set to <code>enable</code>

When the message is sent	Where the message is sent
Daily (by default, sent between 12:00 a.m. and 1:00 a.m. as a performance message), if the <code>-perf</code> parameter is set to <code>true</code>	Addresses specified in <code>-partner-address`</code>  Technical support, if <code>-support</code> is set to <code>enable</code>
Weekly (by default, sent Sunday between 12:00 a.m. and 1:00 a.m.)	Addresses specified in <code>-partner-address</code>  Technical support, if <code>-support</code> is set to <code>enable</code>

## Manually triggered messages

You can manually initiate or resend an AutoSupport message.

When the message is sent	Where the message is sent
You manually initiate a message using the <code>system node autosupport invoke</code> command	If a URI is specified using the <code>-uri</code> parameter in the <code>system node autosupport invoke</code> command, the message is sent to that URI.  If <code>-uri</code> is omitted, the message is sent to the addresses specified in <code>-to</code> and <code>-partner-address</code> . The message is also sent to technical support if <code>-support</code> is set to <code>enable</code> .
You manually initiate a message using the <code>system node autosupport invoke-core-upload</code> command	If a URI is specified using the <code>-uri</code> parameter in the <code>system node autosupport invoke-core-upload</code> command, the message is sent to that URI, and the core dump file is uploaded to the URI.  If <code>-uri</code> is omitted in the <code>system node autosupport invoke-core-upload</code> command, the message is sent to technical support, and the core dump file is uploaded to the technical support site.  Both scenarios require that <code>-support</code> is set to <code>enable</code> and <code>-transport</code> is set to <code>https</code> or <code>http</code> .  Due to the large size of core dump files, the message is not sent to the addresses specified in the <code>-to</code> and <code>-partner-addresses</code> parameters.

When the message is sent	Where the message is sent
You manually initiate a message using the <code>system node autosupport invoke-performance-archive</code> command	<p>If a URI is specified using the <code>-uri</code> parameter in the <code>system node autosupport invoke-performance-archive</code> command, the message is sent to that URI, and the performance archive file is uploaded to the URI.</p> <p>If <code>-uri</code> is omitted in the <code>system node autosupport invoke-performance-archive</code>, the message is sent to technical support, and the performance archive file is uploaded to the technical support site.</p> <p>Both scenarios require that <code>-support</code> is set to <code>enable</code> and <code>-transport</code> is set to <code>https</code> or <code>http</code>.</p> <p>Due to the large size of performance archive files, the message is not sent to the addresses specified in the <code>-to</code> and <code>-partner-addresses</code> parameters.</p>
You manually resend a past message using the <code>system node autosupport history retransmit</code> command	Only to the URI that you specify in the <code>-uri</code> parameter of the <code>system node autosupport history retransmit</code> command

### Messages triggered by technical support

Technical support can request messages from AutoSupport using the AutoSupport OnDemand feature.

When the message is sent	Where the message is sent
When AutoSupport obtains delivery instructions to generate new AutoSupport messages	<p>Addresses specified in <code>-partner-address</code></p> <p>Technical support, if <code>-support</code> is set to <code>enable</code> and <code>-transport</code> is set to <code>https</code></p>
When AutoSupport obtains delivery instructions to resend past AutoSupport messages	Technical support, if <code>-support</code> is set to <code>enable</code> and <code>-transport</code> is set to <code>https</code>
When AutoSupport obtains delivery instructions to generate new AutoSupport messages that upload core dump or performance archive files	Technical support, if <code>-support</code> is set to <code>enable</code> and <code>-transport</code> is set to <code>https</code> . The core dump or performance archive file is uploaded to the technical support site.

### How AutoSupport creates and sends event-triggered messages

AutoSupport creates event-triggered AutoSupport messages when the EMS processes a trigger event. An event-triggered AutoSupport message alerts recipients to problems that require corrective action and contains only information that is relevant to the problem. You



can customize what content to include and who receives the messages.

AutoSupport uses the following process to create and send event-triggered AutoSupport messages:

1. When the EMS processes a trigger event, EMS sends AutoSupport a request.

A trigger event is an EMS event with an AutoSupport destination and a name that begins with a `callhome.` prefix.

2. AutoSupport creates an event-triggered AutoSupport message.

AutoSupport collects basic and troubleshooting information from subsystems that are associated with the trigger to create a message that includes only information that is relevant to the trigger event.

A default set of subsystems is associated with each trigger. However, you can choose to associate additional subsystems with a trigger by using the `system node autosupport trigger modify` command.

3. AutoSupport sends the event-triggered AutoSupport message to the recipients defined by the `system node autosupport modify` command with the `-to`, `-noteto`, `-partner-address`, and `-support` parameters.

You can enable and disable delivery of AutoSupport messages for specific triggers by using the `system node autosupport trigger modify` command with the `-to` and `-noteto` parameters.

### Example of data sent for a specific event

The `storage shelf PSU failed` EMS event triggers a message that contains basic data from the Mandatory, Log Files, Storage, RAID, HA, Platform, and Networking subsystems and troubleshooting data from the Mandatory, Log Files, and Storage subsystems.

You decide that you want to include data about NFS in any AutoSupport messages sent in response to a future `storage shelf PSU failed` event. You enter the following command to enable troubleshooting-level data for NFS for the `callhome.shlf.ps.fault` event:

```
cluster1::\>
system node autosupport trigger modify -node node1 -autosupport
-message shlf.ps.fault -troubleshooting-additional nfs
```

Note that the `callhome.` prefix is dropped from the `callhome.shlf.ps.fault` event when you use the `system node autosupport trigger` commands, or when referenced by AutoSupport and EMS events in the CLI.

### Types of AutoSupport messages and their content

AutoSupport messages contain status information about supported subsystems. Learning what AutoSupport messages contain can help you interpret or respond to messages that you receive in email or view on the Active IQ (formerly known as My AutoSupport) web site.

Type of message	Type of data the message contains
Event-triggered	Files containing context-sensitive data about the specific subsystem where the event occurred
Daily	Log files
Performance	Performance data sampled during the previous 24 hours
Weekly	Configuration and status data
Triggered by the <code>system node autosupport invoke</code> command	<p>Depends on the value specified in the <code>-type</code> parameter:</p> <ul style="list-style-type: none"> <li>• <code>test</code> sends a user-triggered message with some basic data.</li> </ul> <p>This message also triggers an automated email response from technical support to any specified email addresses, using the <code>-to</code> option, so that you can confirm that AutoSupport messages are being received.</p> <ul style="list-style-type: none"> <li>• <code>performance</code> sends performance data.</li> <li>• <code>all</code> sends a user-triggered message with a complete set of data similar to the weekly message, including troubleshooting data from each subsystem.</li> </ul> <p>Technical support typically requests this message.</p>
Triggered by the <code>system node autosupport invoke-core-upload</code> command	Core dump files for a node
Triggered by the <code>system node autosupport invoke-performance-archive</code> command	Performance archive files for a specified period of time

Type of message	Type of data the message contains
Triggered by AutoSupport OnDemand	<p>AutoSupport OnDemand can request new messages or past messages:</p> <ul style="list-style-type: none"> <li>• New messages, depending on the type of AutoSupport collection, can be <code>test</code>, <code>all</code>, or <code>performance</code>.</li> <li>• Past messages depend on the type of message that is resent.</li> </ul> <p>AutoSupport OnDemand can request new messages that upload the following files to the NetApp Support Site at <a href="https://mysupport.netapp.com">mysupport.netapp.com</a>:</p> <ul style="list-style-type: none"> <li>• Core dump</li> <li>• Performance archive</li> </ul>

### What AutoSupport subsystems are

Each subsystem provides basic and troubleshooting information that AutoSupport uses for its messages. Each subsystem is also associated with trigger events that allow AutoSupport to collect from subsystems only information that is relevant to the trigger event.

AutoSupport collects context-sensitive content. You can view information about subsystems and trigger events by using the `system node autosupport trigger show` command.

### AutoSupport size and time budgets

AutoSupport collects information, organized by subsystem, and enforces a size and time budget on content for each subsystem. As storage systems grow, AutoSupport budgets provide control over the AutoSupport payload, which in turn provides scalable delivery of AutoSupport data.

AutoSupport stops collecting information and truncates the AutoSupport content if the subsystem content exceeds its size or time budget. If the content cannot be truncated easily (for example, binary files), AutoSupport omits the content.

You should modify the default size and time budgets only if asked to do so by NetApp Support. You can also review the default size and time budgets of the subsystems by using the `autosupport manifest show` command.

### Files sent in event-triggered AutoSupport messages

Event-triggered AutoSupport messages only contain basic and troubleshooting information from subsystems that are associated with the event that caused AutoSupport to generate the message. The specific data helps NetApp support and support partners troubleshoot the problem.

AutoSupport uses the following criteria to control content in event-triggered AutoSupport messages:

- Which subsystems are included

Data is grouped into subsystems, including common subsystems, such as Log Files, and specific subsystems, such as RAID. Each event triggers a message that contains only the data from specific subsystems.

- The detail level of each included subsystem

Data for each included subsystem is provided at a basic or troubleshooting level.

You can view all possible events and determine which subsystems are included in messages about each event using the `system node autosupport trigger show` command with the `-instance` parameter.

In addition to the subsystems that are included by default for each event, you can add additional subsystems at either a basic or a troubleshooting level using the `system node autosupport trigger modify` command.

### Log files sent in AutoSupport messages

AutoSupport messages can contain several key log files that enable technical support staff to review recent system activity.

All types of AutoSupport messages might include the following log files when the Log Files subsystem is enabled:

Log file	Amount of data included from the file
<ul style="list-style-type: none"><li>• Log files from the <code>/mroot/etc/log/mlog/</code> directory</li><li>• The MESSAGES log file</li></ul>	<p>Only new lines added to the logs since the last AutoSupport message up to a specified maximum. This ensures that AutoSupport messages have unique, relevant—not overlapping—data.</p> <p>(Log files from partners are the exception; for partners, the maximum allowed data is included.)</p>
<ul style="list-style-type: none"><li>• Log files from the <code>/mroot/etc/log/shelflog/</code> directory</li><li>• Log files from the <code>/mroot/etc/log/acp/</code> directory</li><li>• Event Management System (EMS) log data</li></ul>	<p>The most recent lines of data up to a specified maximum.</p>

The content of AutoSupport messages can change between releases of ONTAP.

### Files sent in weekly AutoSupport messages

Weekly AutoSupport messages contain additional configuration and status data that is useful to track changes in your system over time.

The following information is sent in weekly AutoSupport messages:

- Basic information about every subsystem
- Contents of selected `/mroot/etc` directory files
- Log files
- Output of commands that provide system information
- Additional information, including replicated database (RDB) information, service statistics, and more

#### How AutoSupport OnDemand obtains delivery instructions from technical support

AutoSupport OnDemand periodically communicates with technical support to obtain delivery instructions for sending, resending, and declining AutoSupport messages as well as uploading large files to the NetApp support site. AutoSupport OnDemand enables AutoSupport messages to be sent on-demand instead of waiting for the weekly AutoSupport job to run.

AutoSupport OnDemand consists of the following components:

- AutoSupport OnDemand client that runs on each node
- AutoSupport OnDemand service that resides in technical support

The AutoSupport OnDemand client periodically polls the AutoSupport OnDemand service to obtain delivery instructions from technical support. For example, technical support can use the AutoSupport OnDemand service to request that a new AutoSupport message be generated. When the AutoSupport OnDemand client polls the AutoSupport OnDemand service, the client obtains the delivery instructions and sends the new AutoSupport message on-demand as requested.

AutoSupport OnDemand is enabled by default. However, AutoSupport OnDemand relies on some AutoSupport settings to continue communicating with technical support. AutoSupport OnDemand automatically communicates with technical support when the following requirements are met:

- AutoSupport is enabled.
- AutoSupport is configured to send messages to technical support.
- AutoSupport is configured to use the HTTPS transport protocol.

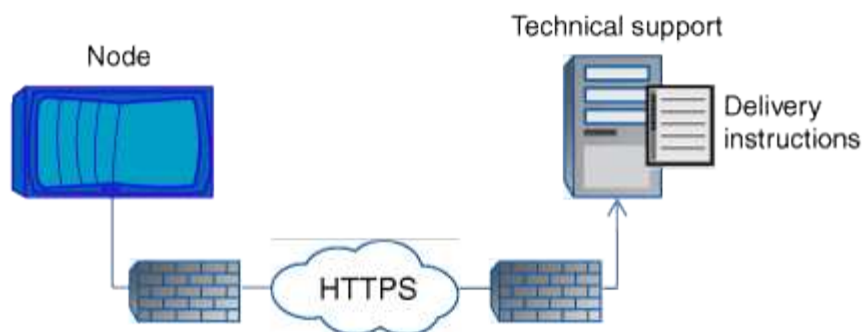
The AutoSupport OnDemand client sends HTTPS requests to the same technical support location to which AutoSupport messages are sent. The AutoSupport OnDemand client does not accept incoming connections.



AutoSupport OnDemand uses the “autosupport” user account to communicate with technical support. ONTAP prevents you from deleting this account.

If you want to disable AutoSupport OnDemand, but keep AutoSupport enabled, use the command: `system node autosupport modify -ondemand-state disable`.

The following illustration shows how AutoSupport OnDemand sends HTTPS requests to technical support to obtain delivery instructions.



The delivery instructions can include requests for AutoSupport to do the following:

- Generate new AutoSupport messages.

Technical support might request new AutoSupport messages to help triage issues.

- Generate new AutoSupport messages that upload core dump files or performance archive files to the NetApp support site.

Technical support might request core dump or performance archive files to help triage issues.

- Retransmit previously generated AutoSupport messages.

This request automatically happens if a message was not received due to a delivery failure.

- Disable delivery of AutoSupport messages for specific trigger events.

Technical support might disable delivery of data that is not used.

### Structure of AutoSupport messages sent by email

When an AutoSupport message is sent by email, the message has a standard subject, a brief body, and a large attachment in 7z file format that contains the data.



If AutoSupport is configured to hide private data, certain information, such as the hostname, is omitted or masked in the header, subject, body, and attachments.

### Subject

The subject line of messages sent by the AutoSupport mechanism contains a text string that identifies the reason for the notification. The format of the subject line is as follows:

HA Group Notification from *System\_Name* (*Message*) *Severity*

- *System\_Name* is either the hostname or the system ID, depending on the AutoSupport configuration

### Body

The body of the AutoSupport message contains the following information:

- Date and timestamp of the message
- Version of ONTAP on the node that generated the message

- System ID, serial number, and hostname of the node that generated the message
- AutoSupport sequence number
- SNMP contact name and location, if specified
- System ID and hostname of the HA partner node

### Attached files

The key information in an AutoSupport message is contained in files that are compressed into a 7z file called `body.7z` and attached to the message.

The files contained in the attachment are specific to the type of AutoSupport message.

### AutoSupport severity types

AutoSupport messages have severity types that help you understand the purpose of each message—for example, to draw immediate attention to an emergency problem, or only to provide information.

Messages have one of the following severities:

- **Alert:** Alert messages indicate that a next-higher level event might occur if you do not take some action.  
You must take an action against alert messages within 24 hours.
- **Emergency:** Emergency messages are displayed when a disruption has occurred.  
You must take an action against emergency messages immediately.
- **Error:** Error conditions indicate what might happen if you ignore.
- **Notice:** Normal but significant condition.
- **Info:** Informational message provides details about the issue, which you can ignore.
- **Debug:** Debug-level messages provide instructions you should perform.

If your internal support organization receives AutoSupport messages through email, the severity appears in the subject line of the email message.

### Requirements for using AutoSupport

You should use HTTPS for delivery of AutoSupport messages to provide the best security and to support all of the latest AutoSupport features. Although AutoSupport supports HTTP and SMTP for delivery of AutoSupport messages, HTTPS is recommended.

### Supported protocols

All of these protocols run on IPv4 or IPv6, based on the address family to which the name resolves.

Protocol and port	Description
HTTPS on port 443	<p>This is the default protocol. You should use this whenever possible.</p> <p>This protocol supports AutoSupport OnDemand and uploads of large files.</p> <p>The certificate from the remote server is validated against the root certificate, unless you disable validation.</p> <p>The delivery uses an HTTP PUT request. With PUT, if the request fails during transmission, the request restarts where it stopped. If the server receiving the request does not support PUT, the delivery uses an HTTP POST request.</p>
HTTP on port 80	<p>This protocol is preferred over SMTP.</p> <p>This protocol supports uploads of large files, but not AutoSupport OnDemand.</p> <p>The delivery uses an HTTP PUT request. With PUT, if the request fails during transmission, the request restarts where it stopped. If the server receiving the request does not support PUT, the delivery uses an HTTP POST request.</p>
SMTP on port 25 or another port	<p>You should use this protocol only if the network connection does not allow HTTPS or HTTP.</p> <p>The default port value is 25, but you can configure AutoSupport to use a different port.</p> <p>Keep the following limitations in mind when using SMTP:</p> <ul style="list-style-type: none"> <li>• AutoSupport OnDemand and uploads of large files are not supported.</li> <li>• Data is not encrypted.</li> </ul> <p>SMTP sends data in clear text, making text in the AutoSupport message easy to intercept and read.</p> <ul style="list-style-type: none"> <li>• Limitations on message length and line length can be introduced.</li> </ul>

If you configure AutoSupport with specific email addresses for your internal support organization, or a support partner organization, those messages are always sent by SMTP.

For example, if you use the recommended protocol to send messages to technical support and you also want to send messages to your internal support organization, your messages will be transported using both HTTPS



and SMTP, respectively.

AutoSupport limits the maximum file size for each protocol. The default setting for HTTP and HTTPS transfers is 25 MB. The default setting for SMTP transfers is 5 MB. If the size of the AutoSupport message exceeds the configured limit, AutoSupport delivers as much of the message as possible. You can edit the maximum size by modifying AutoSupport configuration. See the `system node autosupport modify` man page for more information.



AutoSupport automatically overrides the maximum file size limit for the HTTPS and HTTP protocols when you generate and send AutoSupport messages that upload core dump or performance archive files to the NetApp support site or a specified URI. The automatic override applies only when you upload files by using the `system node autosupport invoke-core-upload` or the `system node autosupport invoke-performance-archive` commands.

## Configuration requirements

Depending on your network configuration, use of HTTP or HTTPS protocols may require additional configuration of a proxy URL. If you use HTTP or HTTPS to send AutoSupport messages to technical support and you have a proxy, you must identify the URL for that proxy. If the proxy uses a port other than the default port, which is 3128, you can specify the port for that proxy. You can also specify a user name and password for proxy authentication.

If you use SMTP to send AutoSupport messages either to your internal support organization or to technical support, you must configure an external mail server. The storage system does not function as a mail server; it requires an external mail server at your site to send mail. The mail server must be a host that listens on the SMTP port (25) or another port, and it must be configured to send and receive 8-bit Multipurpose Internet Mail Extensions (MIME) encoding. Example mail hosts include a UNIX host running an SMTP server such as the sendmail program and a Windows server running the Microsoft Exchange server. You can have one or more mail hosts.

### Set up AutoSupport

You can control whether and how AutoSupport information is sent to technical support and your internal support organization, and then test that the configuration is correct.

### About this task

In ONTAP 9.5 and later releases, you can enable AutoSupport and modify its configuration on all nodes of the cluster simultaneously. When a new node joins the cluster, the node inherits the AutoSupport cluster configuration automatically. You do not have to update the configuration on each node separately.



Beginning with ONTAP 9.5, the scope of the `system node autosupport modify` command is cluster-wide. The AutoSupport configuration is modified on all nodes in the cluster, even when the `-node` option is specified. The option is ignored, but it has been retained for CLI backward compatibility.

In ONTAP 9.4 and earlier releases, the scope of the "system node autosupport modify" command is specific to the node. The AutoSupport configuration should be modified on each node in your cluster.

By default, AutoSupport is enabled on each node to send messages to technical support by using the HTTPS transport protocol.

## Steps

1. Ensure that AutoSupport is enabled:

```
system node autosupport modify -state enable
```

2. If you want technical support to receive AutoSupport messages, use the following command:

```
system node autosupport modify -support enable
```

You must enable this option if you want to enable AutoSupport to work with AutoSupport OnDemand or if you want to upload large files, such as core dump and performance archive files, to technical support or a specified URL.

3. If technical support is enabled to receive AutoSupport messages, specify which transport protocol to use for the messages.

You can choose from the following options:

If you want to...	Then set the following parameters of the <code>system node autosupport modify</code> command...
Use the default HTTPS protocol	<ol style="list-style-type: none"><li>a. Set <code>-transport</code> to <code>https</code>.</li><li>b. If you use a proxy, set <code>-proxy-url</code> to the URL of your proxy. This configuration supports communication with AutoSupport OnDemand and uploads of large files.</li></ol>
Use HTTP that is preferred over SMTP	<ol style="list-style-type: none"><li>a. Set <code>-transport</code> to <code>http</code>.</li><li>b. If you use a proxy, set <code>-proxy-url</code> to the URL of your proxy. This configuration supports uploads of large files, but not AutoSupport OnDemand.</li></ol>
Use SMTP	Set <code>-transport</code> to <code>smtp</code> .  This configuration does not support AutoSupport OnDemand or uploads of large files.

4. If you want your internal support organization or a support partner to receive AutoSupport messages, perform the following actions:
  - a. Identify the recipients in your organization by setting the following parameters of the `system node autosupport modify` command:

Set this parameter...	To this...
-----------------------	------------

<code>-to</code>	Up to five comma-separated individual email addresses or distribution lists in your internal support organization that will receive key AutoSupport messages
<code>-noteto</code>	Up to five comma-separated individual email addresses or distribution lists in your internal support organization that will receive a shortened version of key AutoSupport messages designed for cell phones and other mobile devices
<code>-partner-address</code>	Up to five comma-separated individual email addresses or distribution lists in your support partner organization that will receive all AutoSupport messages

- b. Check that addresses are correctly configured by listing the destinations using the `system node autosupport destinations show` command.
5. If you are sending messages to your internal support organization or you chose SMTP transport for messages to technical support, configure SMTP by setting the following parameters of the `system node autosupport modify` command:
  - Set `-mail-hosts` to one or more mail hosts, separated by commas.  
  
You can set a maximum of five.  
  
You can configure a port value for each mail host by specifying a colon and port number after the mail host name: for example, `mymailhost.example.com:5678`, where 5678 is the port for the mail host.
  - Set `-from` to the email address that sends the AutoSupport message.
6. Configure DNS.
7. (Optional) Add command options if you want to change specific settings:

<b>If you want to do this...</b>	<b>Then set the following parameters of the <code>system node autosupport modify</code> command...</b>
Hide private data by removing, masking, or encoding sensitive data in the messages	Set <code>-remove-private-data</code> to <code>true</code> . If you change from <code>false</code> to <code>true</code> , all AutoSupport history and all associated files are deleted.
Stop sending performance data in periodic AutoSupport messages	Set <code>-perf</code> to <code>false</code> .

8. Check the overall configuration by using the `system node autosupport show` command with the `-node` parameter.
9. Verify the AutoSupport operation by using the `system node autosupport check show` command.

If any problems are reported, use the `system node autosupport check show-details` command to view more information.

10. Test that AutoSupport messages are being sent and received:

- a. Use the `system node autosupport invoke` command with the `-type` parameter set to `test`.

```
cluster1::> system node autosupport invoke -type test -node node1
```

- b. Confirm that NetApp is receiving your AutoSupport messages:

```
system node autosupport history show -node local
```

The status of the latest outgoing AutoSupport message should eventually change to `sent-successful` for all appropriate protocol destinations.

- c. (Optional) Confirm that the AutoSupport message is being sent to your internal support organization or to your support partner by checking the email of any address that you configured for the `-to`, `-noteto`, or `-partner-address` parameters of the `system node autosupport modify` command.

### Upload core dump files

When a core dump file is saved, an event message is generated. If the AutoSupport service is enabled and configured to send messages to NetApp support, an AutoSupport message is transmitted, and an automated email acknowledgement is sent to you.

### What you'll need

- You must have set up AutoSupport with the following settings:
  - AutoSupport is enabled on the node.
  - AutoSupport is configured to send messages to technical support.
  - AutoSupport is configured to use the HTTP or HTTPS transport protocol.

The SMTP transport protocol is not supported when sending messages that include large files, such as core dump files.

### About this task

You can also upload the core dump file through the AutoSupport service over HTTPS by using the `system node autosupport invoke-core-upload` command, if requested by NetApp support.

### [How to upload a file to NetApp](#)

### Steps

1. View the core dump files for a node by using the `system node coredump show` command.

In the following example, core dump files are displayed for the local node:

```
cluster1::> system node coredump show -node local
Node:Type Core Name Saved Panic Time
-----
node:kernel
core.4073000068.2013-09-11.15_05_01.nz true 9/11/2013 15:05:01
```

2. Generate an AutoSupport message and upload a core dump file by using the `system node autosupport invoke-core-upload` command.

In the following example, an AutoSupport message is generated and sent to the default location, which is technical support, and the core dump file is uploaded to the default location, which is the NetApp support site:

```
cluster1::> system node autosupport invoke-core-upload -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

In the following example, an AutoSupport message is generated and sent to the location specified in the URI, and the core dump file is uploaded to the URI:

```
cluster1::> system node autosupport invoke-core-upload -uri
https://files.company.com -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

### Upload performance archive files

You can generate and send an AutoSupport message that contains a performance archive. By default, NetApp technical support receives the AutoSupport message, and the performance archive is uploaded to the NetApp support site. You can specify an alternate destination for the message and upload.

#### What you'll need

- You must have set up AutoSupport with the following settings:
  - AutoSupport is enabled on the node.
  - AutoSupport is configured to send messages to technical support.
  - AutoSupport is configured to use the HTTP or HTTPS transport protocol.

The SMTP transport protocol is not supported when sending messages that include large files, such as performance archive files.

#### About this task

You must specify a start date for the performance archive data that you want to upload. Most storage systems retain performance archives for two weeks, enabling you to specify a start date up to two weeks ago. For example, if today is January 15, you can specify a start date of January 2.

## Step

1. Generate an AutoSupport message and upload the performance archive file by using the `system node autosupport invoke-performance-archive` command.

In the following example, 4 hours of performance archive files from January 12, 2015 are added to an AutoSupport message and uploaded to the default location, which is the NetApp support site:

```
cluster1::> system node autosupport invoke-performance-archive -node
local -start-date 1/12/2015 13:42:09 -duration 4h
```

In the following example, 4 hours of performance archive files from January 12, 2015 are added to an AutoSupport message and uploaded to the location specified by the URI:

```
cluster1::> system node autosupport invoke-performance-archive -node
local -start-date 1/12/2015 13:42:09 -duration 4h -uri
https://files.company.com
```

## Get AutoSupport message descriptions

The descriptions of the AutoSupport messages that you receive are available through the ONTAP Syslog Translator.

### Steps

1. Go to the [Syslog Translator](#).
2. In the **Release** field, enter the the version of ONTAP you are using. In the **Search String** field, enter "callhome". Select **Translate**.
3. The Syslog Translator will alphabetically list all events that match the message string you entered.

## Commands for managing AutoSupport

You use the `system node autosupport` commands to change or view AutoSupport configuration, display information about previous AutoSupport messages, and send, resend or cancel an AutoSupport message.

## Configure AutoSupport

If you want to...	Use this command...
Control whether any AutoSupport messages are sent	<code>system node autosupport modify with the -state parameter</code>
Control whether AutoSupport messages are sent to technical support	<code>system node autosupport modify with the -support parameter</code>

If you want to...	Use this command...
Set up AutoSupport or modify the configuration of AutoSupport	<code>system node autosupport modify</code>
Enable and disable AutoSupport messages to your internal support organization for individual trigger events, and specify additional subsystem reports to include in messages sent in response to individual trigger events	<code>system node autosupport trigger modify</code>



### Display information about the AutoSupport configuration

If you want to...	Use this command...
Display the AutoSupport configuration	<code>system node autosupport show</code> with the <code>-node</code> parameter
View a summary of all addresses and URLs that receive AutoSupport messages	<code>system node autosupport destinations show</code>
Display which AutoSupport messages are sent to your internal support organization for individual trigger events	<code>system node autosupport trigger show</code>
Display status of AutoSupport configuration as well as delivery to various destinations	<code>system node autosupport check show</code>
Display detailed status of AutoSupport configuration as well as delivery to various destinations	<code>system node autosupport check show-details</code>

### Display information about past AutoSupport messages

If you want to...	Use this command...
Display information about one or more of the 50 most recent AutoSupport messages	<code>system node autosupport history show</code>
Display information about recent AutoSupport messages generated to upload core dump or performance archive files to the technical support site or a specified URI	<code>system node autosupport history show-upload-details</code>
View the information in the AutoSupport messages including the name and size of each file collected for the message along with any errors	<code>system node autosupport manifest show</code>

## Send, resend, or cancel AutoSupport messages

If you want to...	Use this command...
<p>Retransmit a locally stored AutoSupport message, identified by its AutoSupport sequence number</p> <p> If you retransmit an AutoSupport message, and if support already received that message, the support system will not create a duplicate case. If, on the other hand, support did not receive that message, then the AutoSupport system will analyze the message and create a case, if necessary.</p>	<pre>system node autosupport history retransmit</pre>
<p>Generate and send an AutoSupport message—for example, for testing purposes</p>	<pre>system node autosupport invoke</pre> <p> Use the <code>-force</code> parameter to send a message even if AutoSupport is disabled. Use the <code>-uri</code> parameter to send the message to the destination you specify instead of the configured destination.</p>
<p>Cancel an AutoSupport message</p>	<pre>system node autosupport history cancel</pre>

### Related information

[ONTAP 9 Commands](#)

### Information included in the AutoSupport manifest

The AutoSupport manifest provides you with a detailed view of the files collected for each AutoSupport message. The AutoSupport manifest also includes information about collection errors when AutoSupport cannot collect the files it needs.

The AutoSupport manifest includes the following information:

- Sequence number of the AutoSupport message
- Which files AutoSupport included in the AutoSupport message
- Size of each file, in bytes
- Status of the AutoSupport manifest collection
- Error description, if AutoSupport failed to collect one or more files

You can view the AutoSupport manifest by using the `system node autosupport manifest show` command.

The AutoSupport manifest is included with every AutoSupport message and presented in XML format, which



means that you can either use a generic XML viewer to read it or view it using the Active IQ (formerly known as My AutoSupport) portal.

### AutoSupport case suppression during scheduled maintenance windows

AutoSupport case suppression enables you to stop unnecessary cases from being created by AutoSupport messages that are triggered during scheduled maintenance windows.

To suppress AutoSupport cases, you must manually invoke an AutoSupport message with a specially formatted text string: `MAINT=xh`. `x` is the duration of the maintenance window in units of hours.

### Related information

[How to suppress automatic case creation during scheduled maintenance windows](#)

### Troubleshoot AutoSupport

#### Troubleshoot AutoSupport when messages are not received

If the system does not send the AutoSupport message, you can determine whether that is because AutoSupport cannot generate the message or cannot deliver the message.

#### Steps

1. Check delivery status of the messages by using the `system node autosupport history show` command.
2. Read the status.

This status	Means
initializing	The collection process is starting. If this state is temporary, all is well. However, if this state persists, there is an issue.
collection-failed	AutoSupport cannot create the AutoSupport content in the spool directory. You can view what AutoSupport is trying to collect by entering the <code>system node autosupport history show -detail</code> command.
collection-in-progress	AutoSupport is collecting AutoSupport content. You can view what AutoSupport is collecting by entering the <code>system node autosupport manifest show</code> command.
queued	AutoSupport messages are queued for delivery, but not yet delivered.
transmitting	AutoSupport is currently delivering messages.
sent-successful	AutoSupport successfully delivered the message. You can find out where AutoSupport delivered the message by entering the <code>system node autosupport history show -delivery</code> command.

This status	Means
ignore	AutoSupport has no destinations for the message. You can view the delivery details by entering the <code>system node autosupport history show -delivery</code> command.
re-queued	AutoSupport tried to deliver messages, but the attempt failed. As a result, AutoSupport placed the messages back in the delivery queue for another attempt. You can view the error by entering the <code>system node autosupport history show</code> command.
transmission-failed	AutoSupport failed to deliver the message the specified number of times and stopped trying to deliver the message. You can view the error by entering the <code>system node autosupport history show</code> command.
ondemand-ignore	The AutoSupport message was processed successfully, but the AutoSupport OnDemand service chose to ignore it.

3. Perform one of the following actions:

For this status	Do this
initializing or collection-failed	Contact NetApp Support, because AutoSupport cannot generate the message. Mention the following Knowledge Base article:  <a href="#">AutoSupport is failing to deliver: status is stuck in initializing</a>
ignore, re-queued, or transmission failed	Check that destinations are correctly configured for SMTP, HTTP, or HTTPS because AutoSupport cannot deliver the message.

### Troubleshoot AutoSupport message delivery over HTTP or HTTPS

If the system does not send the expected AutoSupport message and you are using HTTP or HTTPS, or the Automatic Update feature is not working, you can check a number of settings to resolve the problem.

#### What you'll need

You should have confirmed basic network connectivity and DNS lookup:

- Your node management LIF must be up for operational and administrative status.
- You must be able to ping a functioning host on the same subnet from the cluster management LIF (not a LIF on any of the nodes).
- You must be able to ping a functioning host outside the subnet from the cluster management LIF.
- You must be able to ping a functioning host outside the subnet from the cluster management LIF using the name of the host (not the IP address).

## About this task

These steps are for cases when you have determined that AutoSupport can generate the message, but cannot deliver the message over HTTP or HTTPS.

If you encounter errors or cannot complete a step in this procedure, determine and address the problem before proceeding to the next step.

## Steps

1. Display the detailed status of the AutoSupport subsystem:

```
system node autosupport check show-details
```

This includes verifying connectivity to AutoSupport destinations by sending test messages and providing a list of possible errors in your AutoSupport configuration settings.

2. Verify the status of the node management LIF:

```
network interface show -home-node local -role node-mgmt -fields  
vserver, lif, status-oper, status-admin, address, role
```

The `status-oper` and `status-admin` fields should return “up”.

3. Record the SVM name, the LIF name, and the LIF IP address for later use.
4. Ensure that DNS is enabled and configured correctly:

```
vserver services name-service dns show
```

5. Address any errors returned by the AutoSupport message:

```
system node autosupport history show -node * -fields node, seq-  
num, destination, last-update, status, error
```

For assistance troubleshooting any returned errors, see the [ONTAP AutoSupport \(Transport HTTPS and HTTP\) Resolution Guide](#).

6. Confirm that the cluster can access both the servers it needs and the Internet successfully:

a. `network traceroute -lif node-management_LIF -destination DNS server`

b. `network traceroute -lif node_management_LIF -destination support.netapp.com`



The address `support.netapp.com` itself does not respond to ping/traceroute, but the per-hop information is valuable.

c. `system node autosupport show -fields proxy-url`

d. `network traceroute -node node_management_LIF -destination proxy_url`

If any of these routes are not functioning, try the same route from a functioning host on the same subnet as the cluster, using the “traceroute” or “tracert” utility found on most third-party network clients. This assists you in determining whether the issue is in your network configuration or your cluster configuration.

7. If you are using HTTPS for your AutoSupport transport protocol, ensure that HTTPS traffic can exit your network:

- a. Configure a web client on the same subnet as the cluster management LIF.

Ensure that all configuration parameters are the same values as for the AutoSupport configuration, including using the same proxy server, user name, password, and port.

- b. Access `https://support.netapp.com` with the web client.

The access should be successful. If not, ensure that all firewalls are configured correctly to allow HTTPS and DNS traffic, and that the proxy server is configured correctly. For more information on configuring static name resolution for `support.netapp.com`, see the Knowledge Base article [How would a HOST entry be added in ONTAP for support.netapp.com?](#)

8. Beginning with ONTAP 9.10.1, if you enabled the Automatic Update feature, ensure you have HTTPS connectivity to the following additional URLs:

- `https://support-sg-emea.netapp.com`
- `https://support-sg-naeast.netapp.com`
- `https://support-sg-nawest.netapp.com`

### Troubleshoot AutoSupport message delivery over SMTP

If the system cannot deliver AutoSupport messages over SMTP, you can check a number of settings to resolve the problem.

#### What you'll need

You should have confirmed basic network connectivity and DNS lookup:

- Your node management LIF must be up for operational and administrative status.
- You must be able to ping a functioning host on the same subnet from the cluster management LIF (not a LIF on any of the nodes).
- You must be able to ping a functioning host outside the subnet from the cluster management LIF.
- You must be able to ping a functioning host outside the subnet from the cluster management LIF using the name of the host (not the IP address).

#### About this task

These steps are for cases when you have determined that AutoSupport can generate the message, but cannot deliver the message over SMTP.

If you encounter errors or cannot complete a step in this procedure, determine and address the problem before proceeding to the next step.

All commands are entered at the ONTAP command-line interface, unless otherwise specified.

#### Steps

1. Verify the status of the node management LIF:

```
network interface show -home-node local -role node-mgmt -fields  
vserver,lif,status-oper,status-admin,address,role
```

The `status-oper` and `status-admin` fields should return `up`.

2. Record the SVM name, the LIF name, and the LIF IP address for later use.
3. Ensure that DNS is enabled and configured correctly:

```
vserver services name-service dns show
```

4. Display all of the servers configured to be used by AutoSupport:

```
system node autosupport show -fields mail-hosts
```

Record all server names displayed.

5. For each server displayed by the previous step, and `support.netapp.com`, ensure that the server or URL can be reached by the node:

```
network traceroute -node local -destination server_name
```

If any of these routes is not functioning, try the same route from a functioning host on the same subnet as the cluster, using the “traceroute” or “tracert” utility found on most third-party network clients. This assists you in determining whether the issue is in your network configuration or your cluster configuration.

6. Log in to the host designated as the mail host, and ensure that it can serve SMTP requests:

```
netstat -aAn|grep 25
```

25 is the listener SMTP port number.

A message similar to the following text is displayed:

```
ff64878c tcp          0          0 *.25      *.*      LISTEN.
```

7. From some other host, open a Telnet session with the SMTP port of the mail host:

```
telnet mailhost 25
```

A message similar to the following text is displayed:

```
220 filer.yourco.com Sendmail 4.1/SMI-4.1 ready at Thu, 30 Nov 2014  
10:49:04 PST
```

8. At the telnet prompt, ensure that a message can be relayed from your mail host:

```
HELO domain_name
```

```
MAIL FROM: your_email_address
```

```
RCPT TO: autosupport@netapp.com
```

`domain_name` is the domain name of your network.

If an error is returned saying that relaying is denied, relaying is not enabled on the mail host. Contact your

system administrator.

9. At the telnet prompt, send a test message:

**DATA**

**SUBJECT: TESTING**

**THIS IS A TEST**

.



Ensure that you enter the last period (.) on a line by itself. The period indicates to the mail host that the message is complete.

If an error is returned, your mail host is not configured correctly. Contact your system administrator.

10. From the ONTAP command-line interface, send an AutoSupport test message to a trusted email address that you have access to:

```
system node autosupport invoke -node local -type test
```

11. Find the sequence number of the attempt:

```
system node autosupport history show -node local -destination smtp
```

Find the sequence number for your attempt based on the timestamp. It is probably the most recent attempt.

12. Display the error for your test message attempt:

```
system node autosupport history show -node local -seq-num seq_num -fields error
```

If the error displayed is `Login denied`, your SMTP server is not accepting send requests from the cluster management LIF. If you do not want to change to using HTTPS as your transport protocol, contact your site network administrator to configure the SMTP gateways to address this issue.

If this test succeeds but the same message sent to `mailto:autosupport@netapp.com` does not, ensure that SMTP relay is enabled on all of your SMTP mail hosts, or use HTTPS as a transport protocol.

If even the message to the locally administered email account does not succeed, confirm that your SMTP servers are configured to forward attachments with both of these characteristics:

- The “7z” suffix
- The “application/x-7x-compressed” MIME type.

## Troubleshoot the AutoSupport subsystem

The `system node check show` commands can be used to verify and troubleshoot any issues related to the AutoSupport configuration and delivery.

### Step

1. Use the following commands to display the status of the AutoSupport subsystem.

Use this command...	To do this...
<code>system node autosupport check show</code>	Display overall status of the AutoSupport subsystem, such as the status of AutoSupport HTTP or HTTPS destination, AutoSupport SMTP destinations, AutoSupport OnDemand Server, and AutoSupport configuration
<code>system node autosupport check show-details</code>	Display detailed status of the AutoSupport subsystem, such as detailed descriptions of errors and the corrective actions

## Monitor the health of your system

### Monitor the health of your system overview

Health monitors proactively monitor certain critical conditions in your cluster and raise alerts if they detect a fault or risk. If there are active alerts, the system health status reports a degraded status for the cluster. The alerts include the information that you need to respond to degraded system health.

If the status is degraded, you can view details about the problem, including the probable cause and recommended recovery actions. After you resolve the problem, the system health status automatically returns to OK.

The system health status reflects multiple separate health monitors. A degraded status in an individual health monitor causes a degraded status for the overall system health.

For details on how ONTAP supports cluster switches for system health monitoring in your cluster, you can refer to the *Hardware Universe*.

### [Supported switches in the Hardware Universe](#)

For details on the causes of Cluster Switch Health Monitor (CSHM) AutoSupport messages, and the necessary actions required to resolve these alerts, you can refer to the Knowledgebase article.

### [AutoSupport Message: Health Monitor Process CSHM](#)

### How health monitoring works

Individual health monitors have a set of policies that trigger alerts when certain conditions occur. Understanding how health monitoring works can help you respond to problems and control future alerts.

Health monitoring consists of the following components:

- Individual health monitors for specific subsystems, each of which has its own health status

For example, the Storage subsystem has a node connectivity health monitor.

- An overall system health monitor that consolidates the health status of the individual health monitors

A degraded status in any single subsystem results in a degraded status for the entire system. If no subsystems have alerts, the overall system status is OK.

Each health monitor is made up of the following key elements:

- Alerts that the health monitor can potentially raise

Each alert has a definition, which includes details such as the severity of the alert and its probable cause.

- Health policies that identify when each alert is triggered

Each health policy has a rule expression, which is the exact condition or change that triggers the alert.

A health monitor continuously monitors and validates the resources in its subsystem for condition or state changes. When a condition or state change matches a rule expression in a health policy, the health monitor raises an alert. An alert causes the subsystem's health status and the overall system health status to become degraded.

### **Ways to respond to system health alerts**

When a system health alert occurs, you can acknowledge it, learn more about it, repair the underlying condition, and prevent it from occurring again.

When a health monitor raises an alert, you can respond in any of the following ways:

- Get information about the alert, which includes the affected resource, alert severity, probable cause, possible effect, and corrective actions.
- Get detailed information about the alert, such as the time when the alert was raised and whether anyone else has acknowledged the alert already.
- Get health-related information about the state of the affected resource or subsystem, such as a specific shelf or disk.
- Acknowledge the alert to indicate that someone is working on the problem, and identify yourself as the "Acknowledger."
- Resolve the problem by taking the corrective actions provided in the alert, such as fixing cabling to resolve a connectivity problem.
- Delete the alert, if the system did not automatically clear it.
- Suppress an alert to prevent it from affecting the health status of a subsystem.

Suppressing is useful when you understand a problem. After you suppress an alert, it can still occur, but the subsystem health displays as "ok-with-suppressed." when the suppressed alert occurs.

### **System health alert customization**

You can control which alerts a health monitor generates by enabling and disabling the system health policies that define when alerts are triggered. This enables you to customize the health monitoring system for your particular environment.

You can learn the name of a policy either by displaying detailed information about a generated alert or by displaying policy definitions for a specific health monitor, node, or alert ID.



Disabling health policies is different from suppressing alerts. When you suppress an alert, it does not affect the subsystem's health status, but the alert can still occur.

If you disable a policy, the condition or state that is defined in its policy rule expression no longer triggers an alert.

### **Example of an alert that you want to disable**

For example, suppose an alert occurs that is not useful to you. You use the `system health alert show -instance` command to obtain the Policy ID for the alert. You use the policy ID in the `system health policy definition show` command to view information about the policy. After reviewing the rule expression and other information about the policy, you decide to disable the policy. You use the `system health policy definition modify` command to disable the policy.

### **How health alerts trigger AutoSupport messages and events**

System health alerts trigger AutoSupport messages and events in the Event Management System (EMS), enabling you to monitor the health of the system using AutoSupport messages and the EMS in addition to using the health monitoring system directly.

Your system sends an AutoSupport message within five minutes of an alert. The AutoSupport message includes all alerts generated since the previous AutoSupport message, except for alerts that duplicate an alert for the same resource and probable cause within the previous week.


Some alerts do not trigger AutoSupport messages. An alert does not trigger an AutoSupport message if its health policy disables the sending of AutoSupport messages. For example, a health policy might disable AutoSupport messages by default because AutoSupport already generates a message when the problem occurs. You can configure policies to not trigger AutoSupport messages by using the `system health policy definition modify` command.

You can view a list of all of the alert-triggered AutoSupport messages sent in the previous week using the `system health autosupport trigger history show` command.

Alerts also trigger the generation of events to the EMS. An event is generated each time an alert is created and each time an alert is cleared.

### **Available cluster health monitors**

There are several health monitors that monitor different parts of a cluster. Health monitors help you to recover from errors within ONTAP systems by detecting events, sending alerts to you, and deleting events as they clear.

Health monitor name (identifier)	Subsystem name (identifier)	Purpose
Cluster switch(cluster-switch)	Switch (Switch-Health)	<p>Monitors cluster network switches and management network switches for temperature, utilization, interface configuration, redundancy (cluster network switches only), and fan and power supply operation. The cluster switch health monitor communicates with switches through SNMP. SNMPv2c is the default setting.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>Beginning with ONTAP 9.2, this monitor can detect and report when a cluster switch has rebooted since the last polling period.</p> </div>
MetroCluster Fabric	Switch	Monitors the MetroCluster configuration back-end fabric topology and detects misconfigurations such as incorrect cabling and zoning, and ISL failures.
MetroCluster Health	Interconnect, RAID, and storage	Monitors FC-VI adapters, FC initiator adapters, left-behind aggregates and disks, and inter-cluster ports
Node connectivity(node-connect)	CIFS nondisruptive operations (CIFS-NDO)	Monitors SMB connections for nondisruptive operations to Hyper-V applications.
	Storage (SAS-connect)	Monitors shelves, disks, and adapters at the node level for appropriate paths and connections.
System	not applicable	Aggregates information from other health monitors.
System connectivity (system-connect)	Storage (SAS-connect)	Monitors shelves at the cluster level for appropriate paths to two HA clustered nodes.

## Receive system health alerts automatically

You can manually view system health alerts by using the `system health alert show` command. However, you should subscribe to specific Event Management System (EMS) messages to automatically receive notifications when a health monitor generates an alert.

### About this task

The following procedure shows you how to set up notifications for all `hm.alert.raised` messages and all `hm.alert.cleared` messages.

All `hm.alert.raised` messages and all `hm.alert.cleared` messages include an SNMP trap. The names of the SNMP traps are `HealthMonitorAlertRaised` and `HealthMonitorAlertCleared`. For information about SNMP traps, see the *Network Management Guide*.

### Steps

1. Use the `event destination create` command to define the destination to which you want to send the EMS messages.

```
cluster1::> event destination create -name health_alerts -mail
admin@example.com
```

2. Use the `event route add-destinations` command to route the `hm.alert.raised` message and the `hm.alert.cleared` message to a destination.

```
cluster1::> event route add-destinations -messagename hm.alert*
-destinations health_alerts
```

### Related information

[Network management](#)

### Respond to degraded system health

When your system's health status is degraded, you can show alerts, read about the probable cause and corrective actions, show information about the degraded subsystem, and resolve the problem. Suppressed alerts are also shown so that you can modify them and see whether they have been acknowledged.

### About this task

You can discover that an alert was generated by viewing an AutoSupport message or an EMS event, or by using the `system health` commands.

### Steps

1. Use the `system health alert show` command to view the alerts that are compromising the system's health.
2. Read the alert's probable cause, possible effect, and corrective actions to determine whether you can resolve the problem or need more information.

3. If you need more information, use the `system health alert show -instance` command to view additional information available for the alert.
4. Use the `system health alert modify` command with the `-acknowledge` parameter to indicate that you are working on a specific alert.
5. Take corrective action to resolve the problem as described by the `Corrective Actions` field in the alert.

The corrective actions might include rebooting the system.

When the problem is resolved, the alert is automatically cleared. If the subsystem has no other alerts, the health of the subsystem changes to `OK`. If the health of all subsystems is `OK`, the overall system health status changes to `OK`.

6. Use the `system health status show` command to confirm that the system health status is `OK`.

If the system health status is not `OK`, repeat this procedure.

#### Example of responding to degraded system health

By reviewing a specific example of degraded system health caused by a shelf that lacks two paths to a node, you can see what the CLI displays when you respond to an alert.

After starting ONTAP, you check the system health and you discover that the status is degraded:

```
cluster1::>system health status show
Status
-----
degraded
```

You show alerts to find out where the problem is, and see that shelf 2 does not have two paths to node1:

```
cluster1::>system health alert show
      Node: node1
      Resource: Shelf ID 2
      Severity: Major
      Indication Time: Mon Nov 10 16:48:12 2013
      Probable Cause: Disk shelf 2 does not have two paths to controller
                     node1.
      Possible Effect: Access to disk shelf 2 via controller node1 will be
                     lost with a single hardware component failure (e.g.
                     cable, HBA, or IOM failure).
      Corrective Actions: 1. Halt controller node1 and all controllers attached
                          to disk shelf 2.
                          2. Connect disk shelf 2 to controller node1 via two
                          paths following the rules in the Universal SAS and ACP Cabling Guide.
                          3. Reboot the halted controllers.
                          4. Contact support personnel if the alert persists.
```

You display details about the alert to get more information, including the alert ID:

```

cluster1::>system health alert show -monitor node-connect -alert-id
DualPathToDiskShelf_Alert -instance
    Node: node1
    Monitor: node-connect
    Alert ID: DualPathToDiskShelf_Alert
Alerting Resource: 50:05:0c:c1:02:00:0f:02
    Subsystem: SAS-connect
    Indication Time: Mon Mar 21 10:26:38 2011
Perceived Severity: Major
    Probable Cause: Connection_establishment_error
    Description: Disk shelf 2 does not have two paths to controller
node1.
    Corrective Actions: 1. Halt controller node1 and all controllers
attached to disk shelf 2.
                        2. Connect disk shelf 2 to controller node1 via
two paths following the rules in the Universal SAS and ACP Cabling Guide.
                        3. Reboot the halted controllers.
                        4. Contact support personnel if the alert
persists.
    Possible Effect: Access to disk shelf 2 via controller node1 will
be lost with a single
hardware component failure (e.g. cable, HBA, or IOM failure).
    Acknowledge: false
    Suppress: false
    Policy: DualPathToDiskShelf_Policy
    Acknowledger: -
    Suppressor: -
Additional Information: Shelf uuid: 50:05:0c:c1:02:00:0f:02
                        Shelf id: 2
                        Shelf Name: 4d.shelf2
                        Number of Paths: 1
                        Number of Disks: 6
                        Adapter connected to IOMA:
                        Adapter connected to IOMB: 4d
Alerting Resource Name: Shelf ID 2

```

You acknowledge the alert to indicate that you are working on it.

```

cluster1::>system health alert modify -node node1 -alert-id
DualPathToDiskShelf_Alert -acknowledge true

```

You fix the cabling between shelf 2 and node1, and then reboot the system. Then you check system health again, and see that the status is OK:

```
cluster1::>system health status show
Status
-----
OK
```

### Configure discovery of cluster and management network switches

The cluster switch health monitor automatically attempts to discover your cluster and management network switches using the Cisco Discovery Protocol (CDP). You must configure the health monitor if it cannot automatically discover a switch or if you do not want to use CDP for automatic discovery.

#### About this task

The `system cluster-switch show` command lists the switches that the health monitor discovered. If you do not see a switch that you expected to see in that list, then the health monitor cannot automatically discover it.

#### Steps

1. If you want to use CDP for automatic discovery, do the following; otherwise, go to step 2:

- a. Ensure that the Cisco Discovery Protocol (CDP) is enabled on your switches.

Refer to your switch documentation for instructions.

- b. Run the following command on each node in the cluster to verify whether CDP is enabled or disabled:

```
run -node node_name -command options cdpd.enable
```

If CDP is enabled, go to step d. If CDP is disabled, go to step c.

- c. Run the following command to enable CDP:

```
run -node node_name -command options cdpd.enable on
```

Wait five minutes before you go to the next step.

- d. Use the `system cluster-switch show` command to verify whether ONTAP can now automatically discover the switches.

2. If the health monitor cannot automatically discover a switch, use the `system cluster-switch create` command to configure discovery of the switch:

```
cluster1::> system cluster-switch create -device switch1 -address
192.0.2.250 -snmp-version SNMPv2c -community cshml! -model NX5020 -type
cluster-network
```

Wait five minutes before you go to the next step.

3. Use the `system cluster-switch show` command to verify that ONTAP can discover the switch for which you added information.

## After you finish

Verify that the health monitor can monitor your switches.

### Verify the monitoring of cluster and management network switches

The cluster switch health monitor automatically attempts to monitor the switches that it discovers; however, monitoring might not happen automatically if the switches are not configured correctly. You should verify that the health monitor is properly configured to monitor your switches.

### Steps

1. To identify the switches that the cluster switch health monitor discovered, enter the following command:

#### ONTAP 9.8 and later

```
system switch ethernet show
```

#### ONTAP 9.7 and earlier

```
system cluster-switch show
```

If the `Model` column displays the value `OTHER`, then ONTAP cannot monitor the switch. ONTAP sets the value to `OTHER` if a switch that it automatically discovers is not supported for health monitoring.



If a switch does not display in the command output, you must configure discovery of the switch.

2. Upgrade to the latest supported switch software and reference the configuration file (RCF) from the NetApp Support Site.

#### [NetApp Support Downloads page](#)

The community string in the switch's RCF must match the community string that the health monitor is configured to use. By default, the health monitor uses the community string `cshml!`.



At this time, the health monitor only supports SNMPv2.

If you need to change information about a switch that the cluster monitors, you can modify the community string that the health monitor uses by using the following command:

#### ONTAP 9.8 and later

```
system switch ethernet modify
```

#### ONTAP 9.7 and earlier

```
system cluster-switch modify
```

3. Verify that the switch's management port is connected to the management network.

This connection is required to perform SNMP queries.



## Commands for monitoring the health of your system

You can use the `system health` commands to display information about the health of system resources, to respond to alerts, and to configure future alerts. Using the CLI commands enables you to view in-depth information about how health monitoring is configured. The man pages for the commands contain more information.

### Display the status of system health

If you want to...	Use this command...
Display the health status of the system, which reflects the overall status of individual health monitors	<code>system health status show</code>
Display the health status of subsystems for which health monitoring is available	<code>system health subsystem show</code>

### Display the status of node connectivity

If you want to...	Use this command...
Display details about connectivity from the node to the storage shelf, including port information, HBA port speed, I/O throughput, and the rate of I/O operations per second	<code>storage shelf show -connectivity</code> Use the <code>-instance</code> parameter to display detailed information about each shelf.
Display information about drives and array LUNs, including the usable space, shelf and bay numbers, and owning node name	<code>storage disk show</code> Use the <code>-instance</code> parameter to display detailed information about each drive.
Display detailed information about storage shelf ports, including port type, speed, and status	<code>storage port show</code> Use the <code>-instance</code> parameter to display detailed information about each adapter.

### Manage the discovery of cluster, storage, and management network switches

If you want to...	Use this command.. (ONTAP 9.8 and later)	Use this command.. (ONTAP 9.7 and earlier)
Display the switches that the cluster monitors	<code>system switch ethernet show</code>	<code>system cluster-switch show</code>

If you want to...	Use this command.. (ONTAP 9.8 and later)	Use this command.. (ONTAP 9.7 and earlier)
<p>Display the switches that the cluster currently monitors, including switches that you deleted (shown in the Reason column in the command output), and configuration information that you need for network access to the cluster and management network switches.</p> <p>This command is available at the advanced privilege level.</p>	<pre>system switch ethernet show-all</pre>	<pre>system cluster-switch show-all</pre>
<p>Configure discovery of an undiscovered switch</p>	<pre>system switch ethernet create</pre>	<pre>system cluster-switch create</pre>
<p>Modify information about a switch that the cluster monitors (for example, device name, IP address, SNMP version, and community string)</p>	<pre>system switch ethernet modify</pre>	<pre>system cluster-switch modify</pre>
<p>Disable monitoring of a switch</p>	<pre>system switch ethernet modify -disable-monitoring</pre>	<pre>system cluster-switch modify -disable-monitoring</pre>
<p>Disable discovery and monitoring of a switch and delete switch configuration information</p>	<pre>system switch ethernet delete</pre>	<pre>system cluster-switch delete</pre>
<p>Permanently remove the switch configuration information which is stored in the database (doing so reenables automatic discovery of the switch)</p>	<pre>system switch ethernet delete -force</pre>	<pre>system cluster-switch delete -force</pre>
<p>Enable automatic logging to send with AutoSupport messages.</p>	<pre>system switch ethernet log</pre>	<pre>system cluster-switch log</pre>

### Respond to generated alerts



If you want to...	Use this command...
<p>Display information about generated alerts, such as the resource and node where the alert was triggered, and the alert's severity and probable cause</p>	<pre>system health alert show</pre>


If you want to...	Use this command...
Display information about each generated alert	<code>system health alert show -instance</code>
Indicate that someone is working on an alert	<code>system health alert modify</code>
Acknowledge an alert	<code>system health alert modify -acknowledge</code>
Suppress a subsequent alert so that it does not affect the health status of a subsystem	<code>system health alert modify -suppress</code>
Delete an alert that was not automatically cleared	<code>system health alert delete</code>
Display information about the AutoSupport messages that alerts triggered within the last week, for example, to determine whether an alert triggered an AutoSupport message	<code>system health autosupport trigger history show</code>

### Configure future alerts

If you want to...	Use this command...
Enable or disable the policy that controls whether a specific resource state raises a specific alert	<code>system health policy definition modify</code>

### Display information about how health monitoring is configured

If you want to...	Use this command...
Display information about health monitors, such as their nodes, names, subsystems, and status	<code>system health config show</code> <div style="display: flex; align-items: center; margin-top: 10px;">  <p>Use the <code>-instance</code> parameter to display detailed information about each health monitor.</p> </div>
Display information about the alerts that a health monitor can potentially generate	<code>system health alert definition show</code> <div style="display: flex; align-items: center; margin-top: 10px;">  <p>Use the <code>-instance</code> parameter to display detailed information about each alert definition.</p> </div>

If you want to...	Use this command...
Display information about health monitor policies, which determine when alerts are raised	<pre>system health policy definition show</pre> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  <p>Use the <code>-instance</code> parameter to display detailed information about each policy. Use other parameters to filter the list of alerts—for example, by policy status (enabled or not), health monitor, alert, and so on.</p> </div>

## Display environmental information

Sensors help you monitor the environmental components of your system. The information you can display about environmental sensors include their type, name, state, value, and threshold warnings.

### Step

1. To display information about environmental sensors, use the `system node environment sensors show` command.

## Manage access to web services

### Manage access to web services overview

A web service is an application that users can access by using HTTP or HTTPS. The cluster administrator can set up the web protocol engine, configure SSL, enable a web service, and enable users of a role to access a web service.

Beginning with ONTAP 9.6, the following web services are supported:

- Service Processor Infrastructure (`spi`)

This service makes a node's log, core dump, and MIB files available for HTTP or HTTPS access through the cluster management LIF or a node management LIF. The default setting is `enabled`.

Upon a request to access a node's log files or core dump files, the `spi` web service automatically creates a mount point from a node to another node's root volume where the files reside. You do not need to manually create the mount point.

- ONTAP APIs (`ontapi`)

This service enables you to run ONTAP APIs to execute administrative functions with a remote program. The default setting is `enabled`.

This service might be required for some external management tools. For example, if you use System Manager, you should leave this service enabled.

- Data ONTAP Discovery (`disco`)

This service enables off-box management applications to discover the cluster in the network. The default setting is `enabled`.

- Support Diagnostics (`supdiag`)

This service controls access to a privileged environment on the system to assist problem analysis and resolution. The default setting is `disabled`. You should enable this service only when directed by technical support.

- System Manager (`sysmgr`)

This service controls the availability of System Manager, which is included with ONTAP. The default setting is `enabled`. This service is supported only on the cluster.

- Firmware Baseboard Management Controller (BMC) Update (`FW_BMC`)

This service enables you to download BMC firmware files. The default setting is `enabled`.

- ONTAP Documentation (`docs`)

This service provides access to the ONTAP documentation. The default setting is `enabled`.

- ONTAP RESTful APIs (`docs_api`)

This service provides access to the ONTAP RESTful API documentation. The default setting is `enabled`.

- File Upload and Download (`fud`)

This service offers file upload and download. The default setting is `enabled`.

- ONTAP Messaging (`ontapmsg`)

This service supports a publish and subscribe interface allowing you to subscribe to events. The default setting is `enabled`.

- ONTAP Portal (`portal`)

This service implements the gateway into a virtual server. The default setting is `enabled`.

- ONTAP Restful Interface (`rest`)

This service supports a RESTful interface that is used to remotely manage all elements of the cluster infrastructure. The default setting is `enabled`.

- Security Assertion Markup Language (SAML) Service Provider Support (`saml`)

This service provides resources to support the SAML service provider. The default setting is `enabled`.

- SAML Service Provider (`saml-sp`)

This service offers services such as SP metadata and the assertion consumer service to the service provider. The default setting is `enabled`.

Beginning with ONTAP 9.7, the following additional services are supported:

- Configuration Backup Files (`backups`)

This service enables you to download configuration backup files. The default setting is `enabled`.

- ONTAP Security (`security`)

This service supports CSRF token management for enhanced authentication. The default setting is `enabled`.

## Manage the web protocol engine

You can configure the web protocol engine on the cluster to control whether web access is allowed and what SSL versions can be used. You can also display the configuration settings for the web protocol engine.

You can manage the web protocol engine at the cluster level in the following ways:

- You can specify whether remote clients can use HTTP or HTTPS to access web service content by using the `system services web modify` command with the `-external` parameter.
- You can specify whether SSLv3 should be used for secure web access by using the `security config modify` command with the `-supported-protocol` parameter. By default, SSLv3 is disabled. Transport Layer Security 1.0 (TLSv1.0) is enabled and it can be disabled if needed.
- You can enable Federal Information Processing Standard (FIPS) 140-2 compliance mode for cluster-wide control plane web service interfaces.



By default, FIPS 140-2 compliance mode is disabled.

- **When FIPS 140-2 compliance mode is disabled**

You can enable FIPS 140-2 compliance mode by setting the `is-fips-enabled` parameter to `true` for the `security config modify` command, and then using the `security config show` command to confirm the online status.

- **When FIPS 140-2 compliance mode is enabled**

- Beginning in ONTAP 9.11.1, TLSv1, TLSv1.1 and SSLv3 are disabled, and only TLSv1.2 and TLSv1.3 remain enabled. It affects other systems and communications that are internal and external to ONTAP 9. If you enable FIPS 140-2 compliance mode and then subsequently disable, TLSv1, TLSv1.1, and SSLv3 remain disabled. Either TLSv1.2 or TLSv1.3 will remain enabled depending on the previous configuration.
- For versions of ONTAP prior to 9.11.1, both TLSv1 and SSLv3 are disabled and only TLSv1.1 and TLSv1.2 remain enabled. ONTAP prevents you from enabling both TLSv1 and SSLv3 when FIPS 140-2 compliance mode is enabled. If you enable FIPS 140-2 compliance mode and then subsequently disable it, TLSv1 and SSLv3 remain disabled, but either TLSv1.2 or both TLSv1.1 and TLSv1.2 are enabled depending on the previous configuration.

- You can display the configuration of cluster-wide security by using the `system security config show` command.

If the firewall is enabled, the firewall policy for the logical interface (LIF) to be used for web services must be

set up to allow HTTP or HTTPS access.

If you use HTTPS for web service access, SSL for the cluster or storage virtual machine (SVM) that offers the web service must also be enabled, and you must provide a digital certificate for the cluster or SVM.

In MetroCluster configurations, the setting changes you make for the web protocol engine on a cluster are not replicated on the partner cluster.

## Commands for managing the web protocol engine

You use the `system services web` commands to manage the web protocol engine. You use the `system services firewall policy create` and `network interface modify` commands to allow web access requests to go through the firewall.

If you want to...	Use this command...
Configure the web protocol engine at the cluster level: <ul style="list-style-type: none"><li>• Enable or disable the web protocol engine for the cluster</li><li>• Enable or disable SSLv3 for the cluster</li><li>• Enable or disable FIPS 140-2 compliance for secure web services (HTTPS)</li></ul>	<code>system services web modify</code>
Display the configuration of the web protocol engine at the cluster level, determine whether the web protocols are functional throughout the cluster, and display whether FIPS 140-2 compliance is enabled and online	<code>system services web show</code>
Display the configuration of the web protocol engine at the node level and the activity of web service handling for the nodes in the cluster	<code>system services web node show</code>
Create a firewall policy or add HTTP or HTTPS protocol service to an existing firewall policy to allow web access requests to go through firewall	<code>system services firewall policy create</code> Setting the <code>-service</code> parameter to <code>http</code> or <code>https</code> enables web access requests to go through firewall.
Associate a firewall policy with a LIF	<code>network interface modify</code> You can use the <code>-firewall-policy</code> parameter to modify the firewall policy of a LIF.

## Configure SAML authentication for web services

### Configure SAML authentication

Beginning with ONTAP 9.3, you can configure Security Assertion Markup Language (SAML) authentication for web services. When SAML authentication is configured and

enabled, users are authenticated by an external Identity Provider (IdP) instead of the directory service providers such as Active Directory and LDAP.

### What you'll need

- You must have configured the IdP for SAML authentication.
- You must have the IdP URI.

### About this task

- SAML authentication applies only to the `http` and `ontapi` applications.

The `http` and `ontapi` applications are used by the following web services: Service Processor Infrastructure, ONTAP APIs, or System Manager.

- SAML authentication is applicable only for accessing the admin SVM.

### Steps

1. Create a SAML configuration so that ONTAP can access the IdP metadata:

```
security saml-sp create -idp-uri idp_uri -sp-host ontap_host_name
```

`idp_uri` is the FTP or HTTP address of the IdP host from where the IdP metadata can be downloaded.

`ontap_host_name` is the host name or IP address of the SAML service provider host, which in this case is the ONTAP system. By default, the IP address of the cluster-management LIF is used.

You can optionally provide the ONTAP server certificate information. By default, the ONTAP web server certificate information is used.

```
cluster_12::> security saml-sp create -idp-uri
https://scspr0235321001.gdl.englab.netapp.com/idp/shibboleth -verify
-metadata-server false
```

```
Warning: This restarts the web server. Any HTTP/S connections that are
active
```

```
will be disrupted.
```

```
Do you want to continue? {y|n}: y
```

```
[Job 179] Job succeeded: Access the SAML SP metadata using the URL:
https://10.63.56.150/saml-sp/Metadata
```

```
Configure the IdP and Data ONTAP users for the same directory server
domain to ensure that users are the same for different authentication
methods. See the "security login show" command for the Data ONTAP user
configuration.
```

The URL to access the ONTAP host metadata is displayed.

2. From the IdP host, configure the IdP with the ONTAP host metadata.

For more information about configuring the IdP, see the IdP documentation.



### 3. Enable SAML configuration:

```
security saml-sp modify -is-enabled true
```

Any existing user that accesses the `http` or `ontapi` application is automatically configured for SAML authentication.

### 4. If you want to create users for the `http` or `ontapi` application after SAML is configured, specify SAML as the authentication method for the new users.

#### a. Create a login method for new users with SAML authentication:

+

```
security login create -user-or-group-name user_name -application [http |  
ontapi] -authentication-method saml -vserver svm_name
```

```
cluster_12::> security login create -user-or-group-name admin1  
-application http -authentication-method saml -vserver cluster_12
```

#### b. Verify that the user entry is created:

```
security login show
```

```
cluster_12::> security login show  
  
Vserver: cluster_12  
  
Second  
User/Group          Authentication      Acct  
Authentication  
Name                Application Method      Role Name      Locked  
Method  
-----  
-----  
admin               console      password      admin          no      none  
admin               http         password      admin          no      none  
admin               http         saml          admin          -      none  
admin               ontapi      password      admin          no      none  
admin               ontapi      saml          admin          -      none  
admin               service-processor  
                    password      admin          no      none  
admin               ssh         password      admin          no      none  
admin1              http         password      backup         no      none  
**admin1           http         saml          backup         -  
none**
```

## Related information

### Disable SAML authentication

You can disable SAML authentication when you want to stop authenticating web users by using an external Identity Provider (IdP). When SAML authentication is disabled, the configured directory service providers such as Active Directory and LDAP are used for authentication.

#### What you'll need

You must be logged in from the console.

#### Steps

1. Disable SAML authentication:

```
security saml-sp modify -is-enabled false
```

2. If you no longer want to use SAML authentication or if you want to modify the IdP, delete the SAML configuration:

```
security saml-sp delete
```

### Troubleshoot issues with SAML configuration

If configuring Security Assertion Markup Language (SAML) authentication fails, you can manually repair each node on which the SAML configuration failed and recover from the failure. During the repair process, the web server is restarted and any active HTTP connections or HTTPS connections are disrupted.

#### About this task

When you configure SAML authentication, ONTAP applies SAML configuration on a per-node basis. When you enable SAML authentication, ONTAP automatically tries to repair each node if there are configuration issues. If there are issues with SAML configuration on any node, you can disable SAML authentication and then reenabling SAML authentication. There can be situations when SAML configuration fails to apply on one or more nodes even after you reenabling SAML authentication. You can identify the node on which SAML configuration has failed and then manually repair that node.

#### Steps

1. Log in to the advanced privilege level:

```
set -privilege advanced
```

2. Identify the node on which SAML configuration failed:

```
security saml-sp status show -instance
```

```

cluster_12::*> security saml-sp status show -instance

                Node: node1
                Update Status: config-success
                Database Epoch: 9
                Database Transaction Count: 997
                Error Text:
SAML Service Provider Enabled: false
                ID of SAML Config Job: 179

                Node: node2
                Update Status: config-failed
                Database Epoch: 9
                Database Transaction Count: 997
                Error Text: SAML job failed, Reason: Internal error.
Failed to receive the SAML IDP Metadata file.
SAML Service Provider Enabled: false
                ID of SAML Config Job: 180
2 entries were displayed.

```

3. Repair the SAML configuration on the failed node:

**security saml-sp repair -node *node\_name***

```

cluster_12::*> security saml-sp repair -node node2

Warning: This restarts the web server. Any HTTP/S connections that are
active
        will be disrupted.
Do you want to continue? {y|n}: y
[Job 181] Job is running.
[Job 181] Job success.

```

The web server is restarted and any active HTTP connections or HTTPS connections are disrupted.

4. Verify that SAML is successfully configured on all of the nodes:

**security saml-sp status show -instance**

```

cluster_12::*> security saml-sp status show -instance

                Node: node1
                Update Status: config-success
                Database Epoch: 9
                Database Transaction Count: 997
                Error Text:
SAML Service Provider Enabled: false
                ID of SAML Config Job: 179

                Node: node2
                Update Status: **config-success**
                Database Epoch: 9
                Database Transaction Count: 997
                Error Text:
SAML Service Provider Enabled: false
                ID of SAML Config Job: 180
2 entries were displayed.

```

## Manage web services

### Manage web services overview

You can enable or disable a web service for the cluster or a storage virtual machine (SVM), display the settings for web services, and control whether users of a role can access a web service.

You can manage web services for the cluster or an SVM in the following ways:

- Enabling or disabling a specific web service
- Specifying whether access to a web service is restricted to only encrypted HTTP (SSL)
- Displaying the availability of web services
- Allowing or disallowing users of a role to access a web service
- Displaying the roles that are permitted to access a web service

For a user to access a web service, all of the following conditions must be met:

- The user must be authenticated.

For instance, a web service might prompt for a user name and password. The user's response must match a valid account.

- The user must be set up with the correct access method.

Authentication only succeeds for users with the correct access method for the given web service. For the ONTAP API web service (`ontapi`), users must have the `ontapi` access method. For all other web services, users must have the `http` access method.



You use the `security login` commands to manage users' access methods and authentication methods.

- The web service must be configured to allow the user's access-control role.



You use the `vserver services web access` commands to control a role's access to a web service.

If a firewall is enabled, the firewall policy for the LIF to be used for web services must be set up to allow HTTP or HTTPS.

If you use HTTPS for web service access, SSL for the cluster or SVM that offers the web service must also be enabled, and you must provide a digital certificate for the cluster or SVM.

### Commands for managing web services

You use the `vserver services web` commands to manage the availability of web services for the cluster or a storage virtual machine (SVM). You use the `vserver services web access` commands to control a role's access to a web service.

If you want to...	Use this command...
Configure a web service for the cluster or anSVM: <ul style="list-style-type: none"> <li>• Enable or disable a web service</li> <li>• Specify whether only HTTPS can be used for accessing a web service</li> </ul>	<code>vserver services web modify</code>
Display the configuration and availability of web services for the cluster or anSVM	<code>vserver services web show</code>
Authorize a role to access a web service on the cluster or anSVM	<code>vserver services web access create</code>
Display the roles that are authorized to access web services on the cluster or anSVM	<code>vserver services web access show</code>
Prevent a role from accessing a web service on the cluster or anSVM	<code>vserver services web access delete</code>

### Related information

[ONTAP 9 Commands](#)

### Commands for managing mount points on the nodes

The `spi` web service automatically creates a mount point from one node to another node's root volume upon a request to access the node's log files or core files. Although you do not need to manually manage mount points, you can do so by using the `system`

node root-mount commands.

If you want to...	Use this command...
Manually create a mount point from one node to another node's root volume	<code>system node root-mount create</code> Only a single mount point can exist from one node to another.
Display existing mount points on the nodes in the cluster, including the time a mount point was created and its current state	<code>system node root-mount show</code>
Delete a mount point from one node to another node's root volume and force connections to the mount point to close	<code>system node root-mount delete</code>

### Related information

[ONTAP 9 Commands](#)

### Manage SSL

The SSL protocol improves the security of web access by using a digital certificate to establish an encrypted connection between a web server and a browser.

You can manage SSL for the cluster or a storage virtual machine (SVM) in the following ways:

- Enabling SSL
- Generating and installing a digital certificate and associating it with the cluster or SVM
- Displaying the SSL configuration to see whether SSL has been enabled, and, if available, the SSL certificate name
- Setting up firewall policies for the cluster or SVM, so that web access requests can go through
- Defining which SSL versions can be used
- Restricting access to only HTTPS requests for a web service

### Commands for managing SSL

You use the `security ssl` commands to manage the SSL protocol for the cluster or a storage virtual machine (SVM).

If you want to...	Use this command...
Enable SSL for the cluster or SVM, and associate a digital certificate with it	<code>security ssl modify</code>
Display the SSL configuration and certificate name for the cluster or SVM	<code>security ssl show</code>

## Configure access to web services

Configuring access to web services allows authorized users to use HTTP or HTTPS to access the service content on the cluster or a storage virtual machine (SVM).

### Steps

1. If a firewall is enabled, ensure that HTTP or HTTPS access is set up in the firewall policy for the LIF that will be used for web services:



You can check whether a firewall is enabled by using the `system services firewall show` command.

- a. To verify that HTTP or HTTPS is set up in the firewall policy, use the `system services firewall policy show` command.

You set the `-service` parameter of the `system services firewall policy create` command to `http` or `https` to enable the policy to support web access.

- b. To verify that the firewall policy supporting HTTP or HTTPS is associated with the LIF that provides web services, use the `network interface show` command with the `-firewall-policy` parameter.

You use the `network interface modify` command with the `-firewall-policy` parameter to put the firewall policy into effect for a LIF.

2. To configure the cluster-level web protocol engine and make web service content accessible, use the `system services web modify` command.
3. If you plan to use secure web services (HTTPS), enable SSL and provide digital certificate information for the cluster or SVM by using the `security ssl modify` command.
4. To enable a web service for the cluster or SVM, use the `vserver services web modify` command.

You must repeat this step for each service that you want to enable for the cluster or SVM.

5. To authorize a role to access web services on the cluster or SVM, use the `vserver services web access create` command.

The role that you grant access must already exist. You can display existing roles by using the `security login role show` command or create new roles by using the `security login role create` command.

6. For a role that has been authorized to access a web service, ensure that its users are also configured with the correct access method by checking the output of the `security login show` command.

To access the ONTAP API web service (`ontapi`), a user must be configured with the `ontapi` access method. To access all other web services, a user must be configured with the `http` access method.






You use the `security login create` command to add an access method for a user.



## Troubleshoot web service access problems



Configuration errors cause web service access problems to occur. You can address the errors by ensuring that the LIF, firewall policy, web protocol engine, web services, digital certificates, and user access authorization are all configured correctly.

The following table helps you identify and address web service configuration errors:



This access problem...	Occurs because of this configuration error...	To address the error...
<p>Your web browser returns an unable to connect or failure to establish a connection error when you try to access a web service.</p>	<p>Your LIF might be configured incorrectly.</p>	<p>Ensure that you can ping the LIF that provides the web service.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;"> <p> You use the <code>network ping</code> command to ping a LIF. For information about network configuration, see the <i>Network Management Guide</i>.</p> </div>
	<p>Your firewall might be configured incorrectly.</p>	<p>Ensure that a firewall policy is set up to support HTTP or HTTPS and that the policy is assigned to the LIF that provides the web service.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;"> <p> You use the <code>system services firewall policy</code> commands to manage firewall policies. You use the <code>network interface modify</code> command with the <code>-firewall -policy</code> parameter to associate a policy with a LIF.</p> </div>
	<p>Your web protocol engine might be disabled.</p>	<p>Ensure that the web protocol engine is enabled so that web services are accessible.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;"> <p> You use the <code>system services web</code> commands to manage the web protocol engine for the cluster.</p> </div>

This access problem...	Occurs because of this configuration error...	To address the error...
<p>Your web browser returns a <code>not found</code> error when you try to access a web service.</p>	<p>The web service might be disabled.</p>	<p>Ensure that each web service that you want to allow access to is enabled individually.</p> <div data-bbox="1166 325 1490 556" style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> You use the <code>vserver services web modify</code> command to enable a web service for access.</p> </div>
<p>The web browser fails to log in to a web service with a user's account name and password.</p>	<p>The user cannot be authenticated, the access method is not correct, or the user is not authorized to access the web service.</p>	<p>Ensure that the user account exists and is configured with the correct access method and authentication method. Also, ensure that the user's role is authorized to access the web service.</p> <div data-bbox="1166 840 1490 1617" style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> You use the <code>security login</code> commands to manage user accounts and their access methods and authentication methods. Accessing the ONTAP API web service requires the <code>ontapi access</code> method. Accessing all other web services requires the <code>http access</code> method. You use the <code>vserver services web access</code> commands to manage a role's access to a web service.</p> </div>

This access problem...	Occurs because of this configuration error...	To address the error...
<p>You connect to your web service with HTTPS, and your web browser indicates that your connection is interrupted.</p>	<p>You might not have SSL enabled on the cluster or storage virtual machine (SVM) that provides the web service.</p>	<p>Ensure that the cluster or SVM has SSL enabled and that the digital certificate is valid.</p> <p> You use the <code>security ssl</code> commands to manage SSL configuration for HTTP servers and the <code>security certificate show</code> command to display digital certificate information.</p>
<p>You connect to your web service with HTTPS, and your web browser indicates that the connection is untrusted.</p>	<p>You might be using a self-signed digital certificate.</p>	<p>Ensure that the digital certificate associated with the cluster or SVM is signed by a trusted CA.</p> <p> You use the <code>security certificate generate-csr</code> command to generate a digital certificate signing request and the <code>security certificate install</code> command to install a CA-signed digital certificate. You use the <code>security ssl</code> commands to manage the SSL configuration for the cluster or SVM that provides the web service.</p>

## Verify the identity of remote servers using certificates

### Verify the identity of remote servers using certificates overview

ONTAP supports security certificate features to verify the identity of remote servers.

ONTAP software enables secure connections using these digital certificate features and protocols:

- Online Certificate Status Protocol (OCSP) validates the status of digital certificate requests from ONTAP services using SSL and Transport Layer Security (TLS) connections. This feature is disabled by default.
- A default set of trusted root certificates is included with ONTAP software.
- Key Management Interoperability Protocol (KMIP) certificates enable mutual authentication of a cluster and a KMIP server.

### Verify digital certificates are valid using OCSP

Beginning with ONTAP 9.2, Online Certificate Status Protocol (OCSP) enables ONTAP applications that use Transport Layer Security (TLS) communications to receive digital certificate status when OCSP is enabled. You can enable or disable OCSP certificate status checks for specific applications at any time. By default, OCSP certificate status checking is disabled.

#### What you'll need

These commands must be performed at the advanced privilege level.

#### About this task

OCSP supports the following applications:

- AutoSupport
- Event Management System (EMS)
- LDAP over TLS
- Key Management Interoperability Protocol (KMIP)
- Audit Logging
- FabricPool

#### Steps

1. Set the privilege level to advanced: `set -privilege advanced`.
2. To enable or disable OCSP certificate status checks for specific ONTAP applications, use the appropriate command.

If you want OCSP certificate status checks for some applications to be...	Use the command...
Enabled	<code>security config ocsp enable -app app name</code>
Disabled	<code>security config ocsp disable -app app name</code>

The following command enables OCSP support for AutoSupport and EMS.

```
cluster::*> security config ocsf enable -app asup,ems
```

When OCSP is enabled, the application receives one of the following responses:

- Good - the certificate is valid and communication proceeds.
- Revoked - the certificate is permanently deemed as not trustworthy by its issuing Certificate Authority and communication fails to proceed.
- Unknown - the server does not have any status information about the certificate and communication fails to proceed.
- OCSP server information is missing in the certificate - the server acts as if OCSP is disabled and continues with TLS communication, but no status check occurs.
- No response from OCSP server - the application fails to proceed.

3. To enable or disable OCSP certificate status checks for all applications using TLS communications, use the appropriate command.

<b>If you want OCSP certificate status checks for all applications to be...</b>	<b>Use the command...</b>
Enabled	<pre>security config ocsf enable  -app all</pre>
Disabled	<pre>security config ocsf disable  -app all</pre>

When enabled, all applications receive a signed response signifying that the specified certificate is good, revoked, or unknown. In the case of a revoked certificate, the application will fail to proceed. If the application fails to receive a response from the OCSP server or if the server is unreachable, the application will fail to proceed.

4. Use the `security config ocsf show` command to display all the applications that support OCSP and their support status.

```

cluster::*> security config oosp show
  Application                               OCSP Enabled?
  -----
  autosupport                               false
  audit_log                                 false
  fabricpool                                false
  ems                                        false
  kmip                                       false
  ldap_ad                                   true
  ldap_nis_namemap                          true

  7 entries were displayed.

```

### View default certificates for TLS-based applications

Beginning with ONTAP 9.2, ONTAP provides a default set of trusted root certificates for ONTAP applications using Transport Layer Security (TLS).

#### What you'll need

The default certificates are installed only on the admin SVM during its creation, or during an upgrade to ONTAP 9.2.

#### About this task

The current applications that act as a client and require certificate validation are AutoSupport, EMS, LDAP, Audit Logging, FabricPool, and KMIP.

When certificates expire, an EMS message is invoked that requests the user to delete the certificates. The default certificates can only be deleted at the advanced privilege level.



Deleting the default certificates may result in some ONTAP applications not functioning as expected (for example, AutoSupport and Audit Logging).

#### Step

1. You can view the default certificates that are installed on the admin SVM by using the security certificate show command:

```
security certificate show -vserver -type server-ca
```

```

fas2552-2n-abc-3::*> security certificate show -vserver fas2552-2n-abc-3
-type server-ca
Vserver      Serial Number  Common Name                                     Type
-----
fas2552-2n-abc-3
              01              AAACertificateServices
server-ca
Certificate Authority: AAA Certificate Services
Expiration Date: Sun Dec 31 18:59:59 2028

```

## Mutually authenticating the cluster and a KMIP server

### Mutually authenticating the cluster and a KMIP server overview

Mutually authenticating the cluster and an external key manager such as a Key Management Interoperability Protocol (KMIP) server enables the key manager to communicate with the cluster by using KMIP over SSL. You do so when an application or certain functionality (for example, the Storage Encryption functionality) requires secure keys to provide secure data access.

### Generate a certificate signing request for the cluster

You can use the security certificate `generate-csr` command to generate a certificate signing request (CSR). After processing your request, the certificate authority (CA) sends you the signed digital certificate.

### What you'll need

You must be a cluster administrator or SVM administrator to perform this task.

### Steps

1. Generate a CSR:

```

security certificate generate-csr -common-name FQDN_or_common_name -size
512|1024|1536|2048 -country country -state state -locality locality
-organization organization -unit unit -email-addr email_of_contact -hash
-function SHA1|SHA256|MD5

```

For complete command syntax, see the man pages.

The following command creates a CSR with a 2,048-bit private key generated by the SHA256 hashing function for use by the Software group in the IT department of a company whose custom common name is `server1.companyname.com`, located in Sunnyvale, California, USA. The email address of the SVM contact administrator is `web@example.com`. The system displays the CSR and the private key in the output.

```

cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California -
locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGx1LmNvbTELMakGA1UEBhMCMVVMx
CTAHBgNVBAgTADAEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAStADEPMA0G
CSqGSIB3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApTlnzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfVtwDJbmXuj6U3alwoUsb13wfEvQnHVFNCi
2ninsJ8CAwEAAaAAMA0GCSqGSIB3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
Private Key :
24 | Administrator Authentication and RBAC Power Guide
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApTlnzSxOcxixqImRRGZCR7tVmTYyqPSuTvfVtwDJb
mXuj6U3alwoUsb13wfEvQnHVFNCi2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQli
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgpV+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsferNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----
Note: Please keep a copy of your certificate request and private key
for future reference.

```

2. Copy the certificate request from the CSR output, and then send it in electronic form (such as email) to a trusted third-party CA for signing.

After processing your request, the CA sends you the signed digital certificate. You should keep a copy of the private key and the CA-signed digital certificate.

### Install a CA-signed server certificate for the cluster

To enable an SSL server to authenticate the cluster or storage virtual machine (SVM) as an SSL client, you install a digital certificate with the client type on the cluster or SVM. Then you provide the client-ca certificate to the SSL server administrator for installation on the server.

### What you'll need

You must have already installed the root certificate of the SSL server on the cluster or SVM with the `server-ca` certificate type.

### Steps

1. To use a self-signed digital certificate for client authentication, use the `security certificate create`



command with the `type client` parameter.

2. To use a CA-signed digital certificate for client authentication, complete the following steps:
  - a. Generate a digital certificate signing request (CSR) by using the security certificate `generate-csr` command.

ONTAP displays the CSR output, which includes a certificate request and private key, and reminds you to copy the output to a file for future reference.

- b. Send the certificate request from the CSR output in an electronic form (such as email) to a trusted CA for signing.

You should keep a copy of the private key and the CA-signed certificate for future reference.

After processing your request, the CA sends you the signed digital certificate.

- c. Install the CA-signed certificate by using the `security certificate install` command with the `-type client` parameter.
    - d. Enter the certificate and the private key when you are prompted, and then press **Enter**.
    - e. Enter any additional root or intermediate certificates when you are prompted, and then press **Enter**.

You install an intermediate certificate on the cluster or SVM if a certificate chain that begins at the trusted root CA, and ends with the SSL certificate issued to you, is missing the intermediate certificates. An intermediate certificate is a subordinate certificate issued by the trusted root specifically to issue end-entity server certificates. The result is a certificate chain that begins at the trusted root CA, goes through the intermediate certificate, and ends with the SSL certificate issued to you.

3. Provide the `client-ca` certificate of the cluster or SVM to the administrator of the SSL server for installation on the server.

The `security certificate show` command with the `-instance` and `-type client-ca` parameters displays the `client-ca` certificate information.

#### Install a CA-signed client certificate for the KMIP server

The certificate subtype of Key Management Interoperability Protocol (KMIP) (the `-subtype kmip-cert` parameter), along with the `client` and `server-ca` types, specifies that the certificate is used for mutually authenticating the cluster and an external key manager, such as a KMIP server.

#### About this task

Install a KMIP certificate to authenticate a KMIP server as an SSL server to the cluster.

#### Steps

1. Use the `security certificate install` command with the `-type server-ca` and `-subtype kmip-cert` parameters to install a KMIP certificate for the KMIP server.
2. When you are prompted, enter the certificate, and then press **Enter**.

ONTAP reminds you to keep a copy of the certificate for future reference.

```

cluster1::> security certificate install -type server-ca -subtype kmip-
cert
-vserver cluster1

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/Er4wDQYJKoZIhvcNAQEFBQAwXzELMAkG
2JhucwNhkcV8sEVAbkSdjbCxlRhLQ2pRdKkkirWmnWXbj9T/UWZYB2oK0z5XqcJ
2HUw19JlYD1n1khVdWk/kfVIC0dpImmClr7JyDiGSnoscx1IaU5rfGW/D/xwzoiQ
...
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for future
reference.

cluster1::>

```

## Disk and tier (aggregate) management

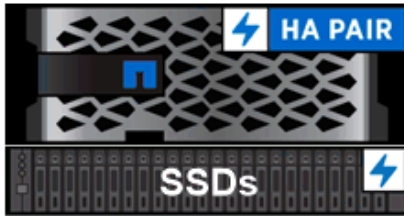
### Disks and local tiers (aggregates) overview

You can manage ONTAP physical storage using System Manager and the CLI. You can create, expand, and manage local tiers (aggregates), work with Flash Pool local tiers (aggregates), manage disks, and manage RAID policies.

### What local tiers (aggregates) are

*Local tiers* (also called *aggregates*) are containers for the disks managed by a node. You can use local tiers to isolate workloads with different performance demands, to tier data with different access patterns, or to segregate data for regulatory purposes.

- For business-critical applications that need the lowest possible latency and the highest possible performance, you might create a local tier consisting entirely of SSDs.
- To tier data with different access patterns, you can create a *hybrid local tier*, deploying flash as high-performance cache for a working data set, while using lower-cost HDDs or object storage for less frequently accessed data.
  - A *Flash Pool* consists of both SSDs and HDDs.
  - A *FabricPool* consists of an all-SSD local tier with an attached object store.
- If you need to segregate archived data from active data for regulatory purposes, you can use a local tier consisting of capacity HDDs, or a combination of performance and capacity HDDs.



Datacenter



Cloud

*You can use a FabricPool to tier data with different access patterns, deploying SSDs for frequently accessed “hot” data and object storage for rarely accessed “cold” data.*

### Working with local tiers (aggregates)

You can perform the following tasks:

- [Manage local tiers \(aggregates\)](#)
- [Manage disks](#)
- [Manage RAID configurations](#)
- [Manage Flash Pool tiers](#)

You perform these tasks if the following are true:

- You do not want to use an automated scripting tool.
- You want to use best practices, not explore every available option.
- You have a MetroCluster configuration and you are following the procedures in the [MetroCluster](#) documentation for initial configuration and guidelines for local tiers (aggregates) and disk management.

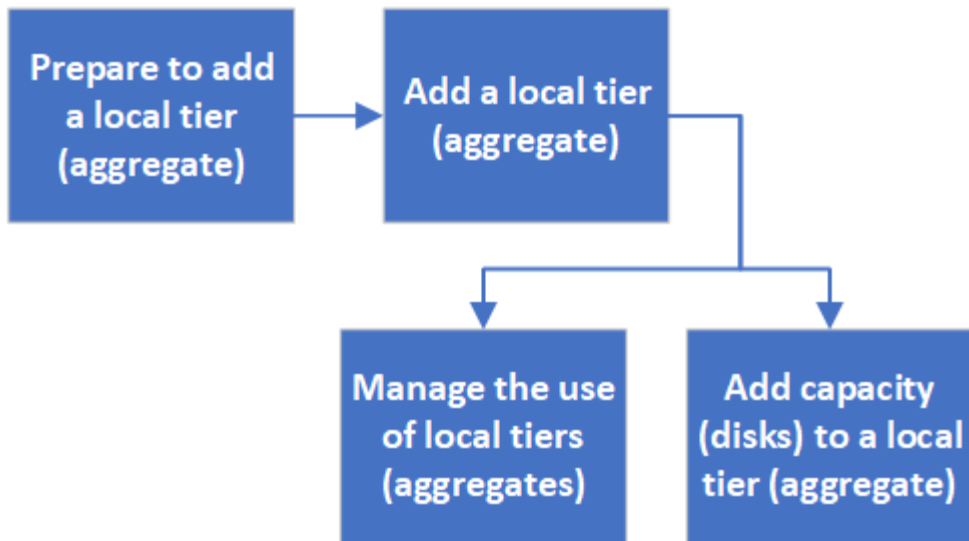
### Related information

- [Manage FabricPool cloud tiers](#)

## Manage local tiers (aggregates)

### Manage local tiers (aggregates)

You can add local tiers (aggregates), manage their usage, and add capacity (disks) to them using System Manager or the CLI.



You can perform the following tasks:

- **Prepare to add a local tier (aggregate)**

Before you add a local tier, you can learn about RAID groups and RAID protection levels and policies for local tiers. You can learn about mirrored and unmirrored local tiers and how to quickly zero drives before provisioning them. You also perform a manual assignment of disk ownership before provisioning a local tier.

- **Add (create) a local tier (aggregate)**

To add a local tier, you follow a specific workflow. You determine the number of disks or disk partitions that you need for the local tier and decide which method to use to create the local tier. You can add local tiers automatically by letting ONTAP assign the configuration, or you can manually specify the configuration.

- **Manage the use of local tiers (aggregates)**

For existing local tiers, you can rename them, set their media costs, or determine their drive and RAID group information. You can modify the RAID configuration of a local tier and assign local tiers to storage VMs (SVMs).

You can modify the RAID configuration of a local tier and assign local tiers to storage VMs (SVMs). You can determine which volumes reside on a local tier and how much space they use on a local tier. You can control how much space that volumes can use. You can relocate local tier ownership with an HA pair. You can also delete a local tier.

- **Add capacity (disks) to a local tier (aggregate)**

Using different methods, you follow a specific workflow to add capacity. You can add disks to a local tier and add drives to a node or shelf. If needed, you can correct misaligned spare partitions.

## Prepare to add a local tier (aggregate)

### Prepare to add a local tier (aggregate)

Before you add a local tier, you should understand the following topics:

- Learn about RAID groups, RAID protection levels, and RAID policies for local tiers.

- [Local tiers \(aggregates\) and RAID groups](#)
- Learn about mirrored and unmirrored local tiers and how to quickly zero drives before provisioning them.
  - [Mirrored and unmirrored local tiers \(aggregates\)](#)
  - [Fast zeroing of drives](#)
- Perform a manual assignment of disk ownership before provisioning a local tier.
  - [Manually assign disk ownership](#)

### Local tiers (aggregates) and RAID groups

Modern RAID technologies protect against disk failure by rebuilding a failed disk's data on a spare disk. The system compares index information on a "parity disk" with data on the remaining healthy disks to reconstruct the missing data, all without downtime or a significant performance cost.

A local tier (aggregate) consists of one or more *RAID groups*. The *RAID type* of the local tier determines the number of parity disks in the RAID group and the number of simultaneous disk failures that the RAID configuration protects against.

The default RAID type, RAID-DP (RAID-double parity), requires two parity disks per RAID group and protects against data loss in the event of two disks failing at the same time. For RAID-DP, the recommended RAID group size is between 12 and 20 HDDs and between 20 and 28 SSDs.

You can spread out the overhead cost of parity disks by creating RAID groups at the higher end of the sizing recommendation. This is especially the case for SSDs, which are much more reliable than capacity drives. For local tiers that use HDDs, you should balance the need to maximize disk storage against countervailing factors like the longer rebuild time required for larger RAID groups.

### Mirrored and unmirrored local tiers (aggregates)

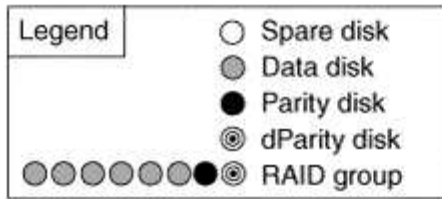
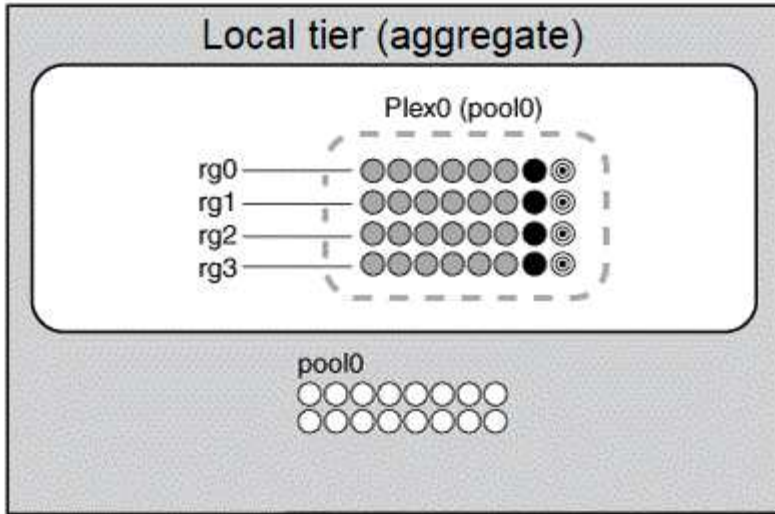
ONTAP has an optional feature called *SyncMirror* which you can use to synchronously mirror local tier (aggregate) data in copies, or *plexes*, stored in different RAID groups. Plexes ensure against data loss if more disks fail than the RAID type protects against, or if there is a loss of connectivity to RAID group disks.

When you create a local tier with System Manager or using the CLI, you can specify that the local tier is mirrored or unmirrored.

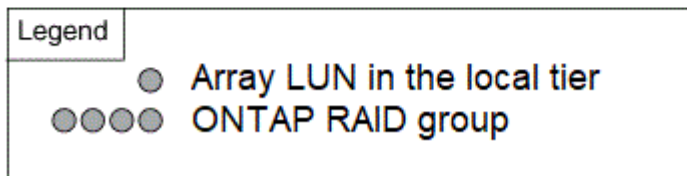
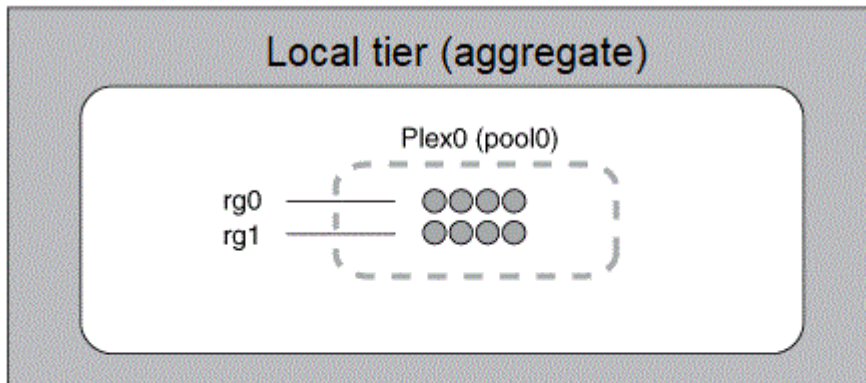
### How unmirrored local tiers (aggregates) work

If you do not specify that the local tiers are mirrored, then they are created as unmirrored local tiers (aggregates). Unmirrored local tiers have only one *plex* (a copy of their data), which contains all of the RAID groups belonging to that local tier.

The following diagram shows an unmirrored local tier composed of disks, with its one plex. The local tier has four RAID groups: rg0, rg1, rg2, and rg3. Each RAID group has six data disks, one parity disk, and one dparity (double parity) disk. All disks used by the local tier come from the same pool, "pool0".



The following diagram shows an unmirrored local tier with array LUNs, with its one plex. It has two RAID groups, rg0 and rg1. All array LUNs used by the local tier come from the same pool, "pool0".



### How mirrored local tiers (aggregates) work

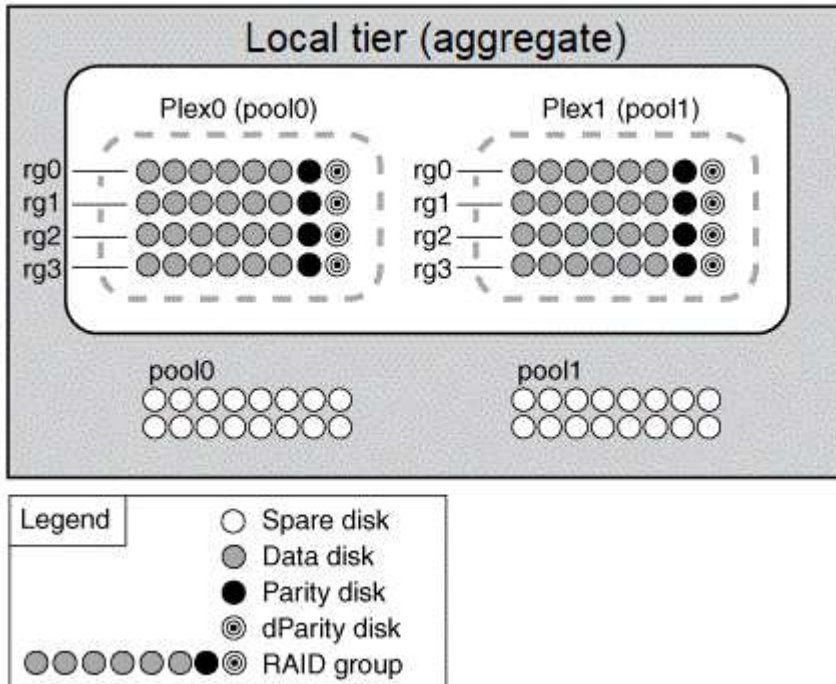
Mirrored aggregates have two *plexes* (copies of their data), which use the SyncMirror functionality to duplicate the data to provide redundancy.

When you create a local tier, you can specify that it is a mirrored local tier. Also, you can add a second plex to an existing unmirrored local tier to make it a mirrored tier. Using SyncMirror functionality, ONTAP copies the data in the original plex (plex0) to the new plex (plex1). The plexes are physically separated (each plex has its own RAID groups and its own pool), and the plexes are updated simultaneously.

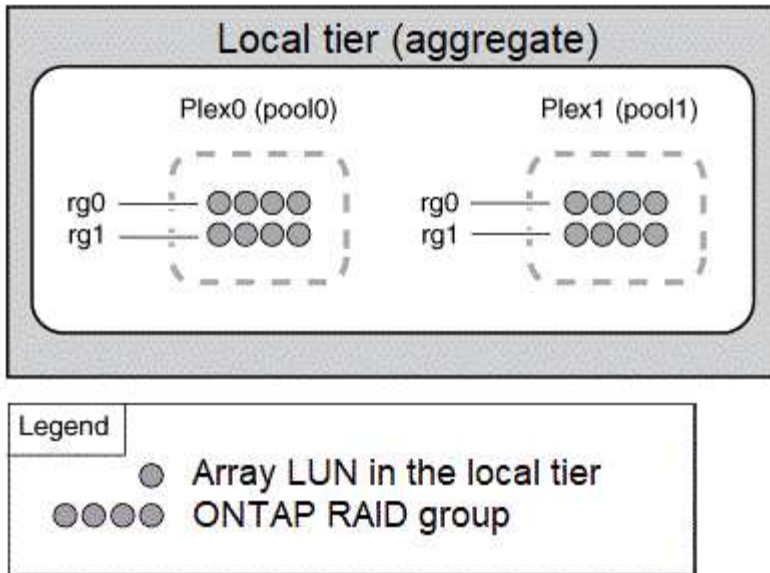
This configuration provides added protection against data loss if more disks fail than the RAID level of the aggregate protects against or if there is a loss of connectivity, because the unaffected plex continues to serve data while you fix the cause of the failure. After the plex that had a problem is fixed, the two plexes resynchronize and reestablish the mirror relationship.

The disks and array LUNs on the system are divided into two pools: “pool0” and “pool1”. Plex0 gets its storage from pool0 and plex1 gets its storage from pool1.

The following diagram shows a local tier composed of disks with the SyncMirror functionality enabled and implemented. A second plex has been created for the local tier, “plex1”. The data in plex1 is a copy of the data in plex0, and the RAID groups are also identical. The 32 spare disks are allocated to pool0 or pool1 using 16 disks for each pool.



The following diagram shows an local tier composed of array LUNs with the SyncMirror functionality enabled and implemented. A second plex has been created for the local tier, “plex1”. Plex1 is a copy of plex0, and the RAID groups are also identical.



### Fast zeroing of drives

Beginning with ONTAP 9.4, you can automatically and quickly zero drives (both SSDs and HDDs) before provisioning without experiencing long wait times.

For systems that are freshly installed with ONTAP 9.4 or later or systems that are reinitialized with ONTAP 9.4 or later, drive zeroing takes place automatically and is completed in seconds.

If you need to manually zero a drive, you can use one of the following methods:



## CLI command

### Use a CLI command to fast-zero drives

#### About this task

Admin privileges are required to use this command.

#### Steps

1. Enter the CLI command:

```
storage disk zerospares
```

## Boot menu options

### Select options from the boot menu to fast-zero drives

#### About this task

- The fast zeroing enhancement does not support systems upgraded from a release earlier than ONTAP 9.4.
- If any node on the cluster contains a local tier (aggregate) with fast-zeroed drives, then you cannot revert the cluster to ONTAP 9.2 or earlier.

#### Steps

1. From the boot menu, select one of the following options:
  - (4) Clean configuration and initialize all disks
  - (9a) Unpartition all disks and remove their ownership information
  - (9b) Clean configuration and initialize node with whole disks

## Manually assign disk ownership

Disks must be owned by a node before they can be used in a local tier (aggregate).

If your cluster is not configured to use automatic disk ownership assignment, you must assign ownership manually.

You cannot reassign ownership of a disk that is in use in a local tier.

#### Steps

1. Using the CLI, display all unowned disks:

```
storage disk show -container-type unassigned
```

2. Assign each disk:

```
storage disk assign -disk disk_name -owner owner_name
```

You can use the wildcard character to assign more than one disk at once. If you are reassigning a spare disk that is already owned by a different node, you must use the “-force” option.

## **Add (create) a local tier (aggregate)**

### **Add a local tier (create an aggregate)**

To add a local tier (create an aggregate), you follow a specific workflow. You determine the number of disks or disk partitions that you need for the local tier and decide which method to use to create the local tier. You can add local tiers automatically by letting ONTAP assign the configuration, or you can manually specify the configuration.

- [Workflow to add a local tier \(aggregate\)](#)
- [Determine the number of disks or disk partitions required for a local tier \(aggregate\)](#)
- [Decide which local tier \(aggregate\) creation method to use](#)
- [Add local tiers \(aggregates\) automatically](#)
- [Add local tiers \(aggregates\) manually](#)

### **Workflow to add a local tier (aggregate)**

Creating local tiers (aggregates) provides storage to volumes on your system.

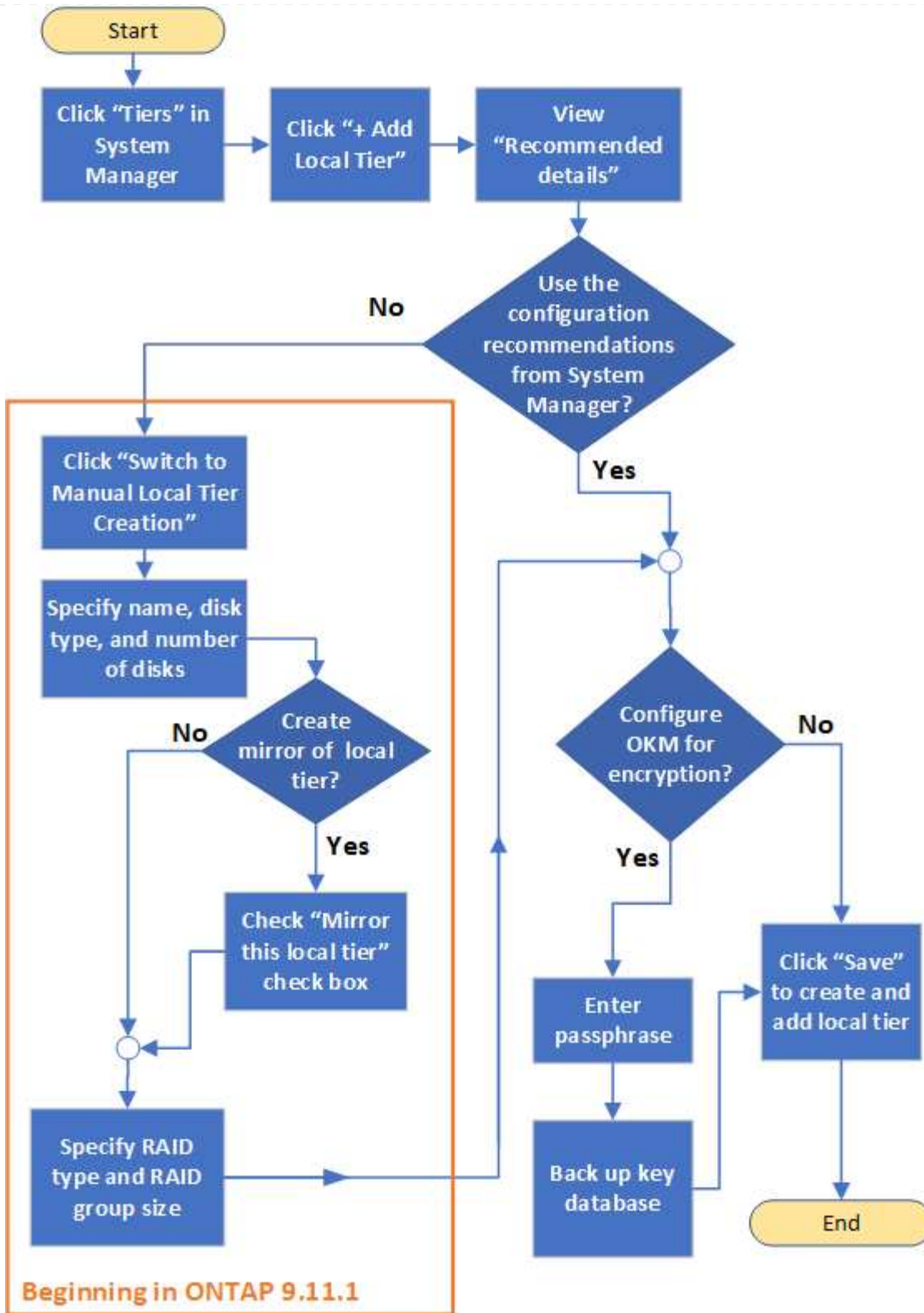
The workflow for creating local tiers (aggregates) is specific to the interface you use—System Manager or the CLI:

## **System Manager workflow**

### **Use System Manager to add (create) a local tier**

System Manager creates local tiers based on recommended best practices for configuring local tiers.

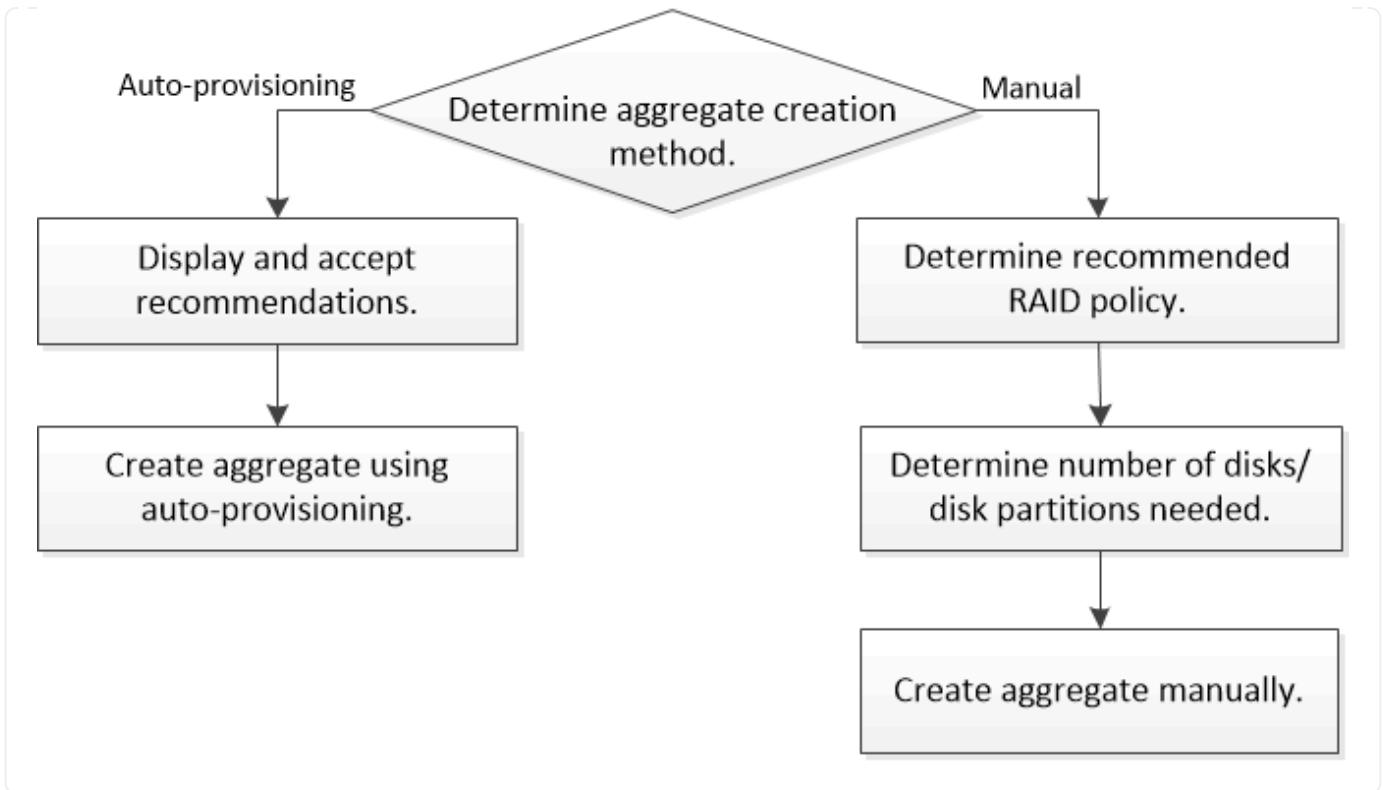
Beginning with ONTAP 9.11.1, you can decide to configure local tiers manually if you want a different configuration than the one recommended during the automatic process to add a local tier.



### CLI workflow

#### Use the CLI to add (create) an aggregate

Beginning with ONTAP 9.2, ONTAP can provide recommended configurations when you create aggregates (auto-provisioning). If the recommended configurations, based on best practices, are appropriate in your environment, you can accept them to create the aggregates. Otherwise, you can create aggregates manually.



**Determine the number of disks or disk partitions required for a local tier (aggregate)**

You must have enough disks or disk partitions in your local tier (aggregate) to meet system and business requirements. You should also have the recommended number of hot spare disks or hot spare disk partitions to minimize the potential of data loss.

Root-data partitioning is enabled by default on certain configurations. Systems with root-data partitioning enabled use disk partitions to create local tiers. Systems that do not have root-data partitioning enabled use unpartitioned disks.

You must have enough disks or disk partitions to meet the minimum number required for your RAID policy and enough to meet your minimum capacity requirements.



In ONTAP, the usable space of the drive is less than the physical capacity of the drive. You can find the usable space of a specific drive and the minimum number of disks or disk partitions required for each RAID policy in the [Hardware Universe](#).

**Determine usable space of a specific disk**


The procedure you follow depends on the interface you use—System Manager or the CLI:

## System Manager

### Use System Manager to determine usable space of disks

Perform the following steps to view the usable size of a disk:

#### Steps

1. Go to **Storage > Tiers**
2. Click  next to the name of the local tier.
3. Select the **Disk Information** tab.

#### CLI

### Use the CLI to determine usable space of disks

Perform the following step to view the usable size of a disk:

#### Step

1. Display spare disk information:

```
storage aggregate show-spare-disks
```

In addition to the number of disks or disk partitions necessary to create your RAID group and meet your capacity requirements, you should also have the minimum number of hot spare disks or hot spare disk partitions recommended for your aggregate:

- For all flash aggregates, you should have a minimum of one hot spare disk or disk partition.



The AFF C190 defaults to no spare drive. This exception is fully supported.

- For non-flash homogenous aggregates, you should have a minimum of two hot spare disks or disk partitions.
- For SSD storage pools, you should have a minimum of one hot spare disk for each HA pair.
- For Flash Pool aggregates, you should have a minimum of two spare disks for each HA pair. You can find more information on the supported RAID policies for Flash Pool aggregates in the [Hardware Universe](#).
- To support the use of the Maintenance Center and to avoid issues caused by multiple concurrent disk failures, you should have a minimum of four hot spares in multi-disk carriers.

#### Related information

[NetApp Hardware Universe](#)

[NetApp Technical Report 3838: Storage Subsystem Configuration Guide](#)

#### Decide which method to use to create local tiers (aggregates)

Although ONTAP provides best-practice recommendations for adding local tiers automatically (creating aggregates with auto-provisioning), you must determine whether the recommended configurations are supported in your environment. If they are not, you must make decisions about RAID policy and disk configuration and then create the local

tiers manually.

When a local tier is created automatically, ONTAP analyzes available spare disks in the cluster and generates a recommendation about how spare disks should be used to add local tiers according to best practices. ONTAP displays the recommended configurations. You can accept the recommendations or add the local tiers manually.

### Before you can accept ONTAP recommendations

If any of the following disk conditions are present, they must be addressed before accepting the recommendations from ONTAP:

- Missing disks
- Fluctuation in spare disk numbers
- Unassigned disks
- Non-zeroed spares
- Disks undergoing maintenance testing

The `storage aggregate auto-provision man` page contains more information about these requirements.

### When you must use the manual method

In many cases, the recommended layout of the local tier will be optimal for your environment. However, if your cluster is running ONTAP 9.1 or earlier, or your environment includes the following configurations, you must create the local tier using the manual method.



Beginning with ONTAP 9.11.1, you can manually add local tiers with System Manager.

- Aggregates using third-party array LUNs
- Virtual disks with Cloud Volumes ONTAP or ONTAP Select
- MetroCluster system
- SyncMirror
- MSATA disks
- FlashPool tiers (aggregates)
- Multiple disk types or sizes are connected to the node

### Select the method to create local tiers (aggregates)

Choose which method you want to use:

- [Add \(create\) local tiers \(aggregates\) automatically](#)
- [Add \(create\) local tiers \(aggregates\) manually](#)

### Related information

[ONTAP 9 commands](#)

**Add local tiers automatically (create aggregates with auto-provisioning)**

If the best-practice recommendation that ONTAP provides for automatically adding a local tier (creating an aggregate with auto-provisioning) is appropriate in your environment, you can accept the recommendation and let ONTAP add the local tier.

The process you follow depends on the interface that you use—System Manager or the CLI.



## System Manager

### Use System Manager to automatically add a local tier

#### Steps

1. In System Manager, click **Storage > Tiers**.
2. From the **Tiers** page, click [+ Add Local Tier](#) to create a new local tier:

The **Add Local Tier** page shows the recommended number of local tiers that can be created on the nodes and the usable storage available.

3. Click **Recommended details** to view the configuration recommended by System Manager.

System Manager displays the following information beginning with ONTAP 9.8:

- **Local tier name** (you can edit the local tier name beginning with ONTAP 9.10.1)
- **Node name**
- **Usable size**
- **Type of storage**

Beginning with ONTAP 9.10.1, additional information is displayed:

- **Disks:** showing the number, size, and type of the disks
- **Layout:** showing the RAID group layout, including which disks are parity or data and which slots are unused.
- **Spare disks:** showing the node name, the number and size of spare disks, and the type of storage.

4. Perform one of the following steps:

If you want to...	Then do this...
Accept the recommendations from System Manager.	Proceed to <a href="#">the step for configuring the Onboard Key Manager for encryption</a> .
Manually configure the local tiers and <b>not</b> use the recommendations from System Manager.	Proceed to <a href="#">Add a local tier (create aggregate) manually</a> : <ul style="list-style-type: none"><li>• For ONTAP 9.10.1 and earlier, follow the steps to use the CLI.</li><li>• Beginning with ONTAP 9.11.1, follow the steps to use System Manager.</li></ul>

5. (Optional): If the Onboard Key Manager has been installed, you can configure it for encryption. Check the **Configure Onboard Key Manager for encryption** check box.
  - a. Enter a passphrase.
  - b. Enter the passphrase again to confirm it.
  - c. Save the passphrase for future use in case the system needs to be recovered.
  - d. Back up the key database for future use.

6. Click **Save** to create the local tier and add it to your storage solution.

## CLI

### Use the CLI to create an aggregate with auto-provisioning

You run the `storage aggregate auto-provision` command to generate aggregate layout recommendations. You can then create aggregates after reviewing and approving ONTAP recommendations.

#### What you'll need

ONTAP 9.2 or later must be running on your cluster.

#### About this task

The default summary generated with the `storage aggregate auto-provision` command lists the recommended aggregates to be created, including names and usable size. You can view the list and determine whether you want to create the recommended aggregates when prompted.

You can also display a detailed summary by using the `-verbose` option, which displays the following reports:

- Per node summary of new aggregates to create, discovered spares, and remaining spare disks and partitions after aggregate creation
- New data aggregates to create with counts of disks and partitions to be used
- RAID group layout showing how spare disks and partitions will be used in new data aggregates to be created
- Details about spare disks and partitions remaining after aggregate creation

If you are familiar with the auto-provision method and your environment is correctly prepared, you can use the `-skip-confirmation` option to create the recommended aggregate without display and confirmation. The `storage aggregate auto-provision` command is not affected by the CLI session `-confirmations` setting.

The `storage aggregate auto-provision` man page contains more information about the aggregate layout recommendations.

#### Steps

1. Run the `storage aggregate auto-provision` command with the desired display options.
  - no options: Display standard summary
  - `-verbose` option: Display detailed summary
  - `-skip-confirmation` option: Create recommended aggregates without display or confirmation
2. Perform one of the following steps:

If you want to...	Then do this...
-------------------	-----------------

<p>Accept the recommendations from ONTAP.</p>	<p>Review the display of recommended aggregates, and then respond to the prompt to create the recommended aggregates.</p> <pre data-bbox="654 205 1458 464"> Do you want to create recommended aggregates? {y n}:y  Info: Creating node1_SSD_1 ...       Creating node2_SSD_1 ... </pre>
<p>Manually configure the local tiers and <b>not</b> use the recommendations from ONTAP.</p>	<p>Proceed to <a href="#">Add a local tier (create aggregate) manually</a>.</p>

**Related information**

[ONTAP 9 Commands](#)

**Add local tiers (create aggregates) manually**

If you do not want to add a local tier (create a aggregate) using the best-practice recommendations from ONTAP, you can perform the process manually.

The process you follow depends on the interface that you use—System Manager or the CLI.

## System Manager

### Use System Manager to add a local tier manually

Beginning with ONTAP 9.11.1, if you do not want to use the configuration recommended by System Manager to create a local tier, you can specify the configuration you want.

#### Steps

1. In System Manager, click **Storage > Tiers**.
2. From the **Tiers** page, click **+ Add Local Tier** to create a new local tier:

The **Add Local Tier** page shows the recommended number of local tiers that can be created on the nodes and the usable storage available.

3. When System Manager displays the storage recommendation for the local tier, click **Switch to Manual Local Tier Creation** in the **Spare Disks** section.

The **Add Local Tier** page displays fields that you use to configure the local tier.

4. In the first section of the **Add Local Tier** page, complete the following:
  - a. Enter the name of the local tier.
  - b. (Optional): Check the **Mirror this local tier** check box if you want to mirror the local tier.
  - c. Select a disk type.
  - d. Select the number of disks.
5. In the **RAID Configuration** section, complete the following:
  - a. Select the RAID type.
  - b. Select the RAID group size.
  - c. Click RAID allocation to view how the disks are allocated in the group.
6. (Optional): If the Onboard Key Manager has been installed, you can configure it for encryption in the **Encryption** section of the page. Check the **Configure Onboard Key Manager for encryption** check box.
  - a. Enter a passphrase.
  - b. Enter the passphrase again to confirm it.
  - c. Save the passphrase for future use in case the system needs to be recovered.
  - d. Back up the key database for future use.
7. Click **Save** to create the local tier and add it to your storage solution.

#### CLI

### Use the CLI to create an aggregate manually

Before you create aggregates manually, you should review disk configuration options and simulate creation.

Then you can issue the `storage aggregate create` command and verify the results.

#### What you'll need

You must have determined the number of disks and the number of hot spare disks you need in the

aggregate.

### About this task

If root-data-data partitioning is enabled and you have 24 solid-state drives (SSDs) or fewer in your configuration, it is recommended that your data partitions be assigned to different nodes.

The procedure for creating aggregates on systems with root-data partitioning and root-data-data partitioning enabled is the same as the procedure for creating aggregates on systems using unpartitioned disks. If root-data partitioning is enabled on your system, you should use the number of disk partitions for the `-diskcount` option. For root-data-data partitioning, the `-diskcount` option specifies the count of disks to use.



When creating multiple aggregates for use with FlexGroups, aggregates should be as close in size as possible.

The `storage aggregate create man` page contains more information about aggregate creation options and requirements.

### Steps

1. View the list of spare disk partitions to verify that you have enough to create your aggregate:

```
storage aggregate show-spare-disks -original-owner node_name
```

Data partitions are displayed under `Local Data Usable`. A root partition cannot be used as a spare.

2. Simulate the creation of the aggregate:

```
storage aggregate create -aggregate aggregate_name -node node_name  
-raidtype raid_dp -diskcount number_of_disks_or_partitions -simulate true
```

3. If any warnings are displayed from the simulated command, adjust the command and repeat the simulation.
4. Create the aggregate:

```
storage aggregate create -aggregate aggr_name -node node_name -raidtype  
raid_dp -diskcount number_of_disks_or_partitions
```

5. Display the aggregate to verify that it was created:

```
storage aggregate show-status aggregate_name
```

### Related information

[ONTAP 9 commands](#)

### Manage the use of local tiers (aggregates)

#### Manage the use of local tiers (aggregates)

After you have created local tiers (aggregates), you can manage how they are used.

You can perform the following tasks:

- [Rename a local tier \(aggregate\)](#)
- [Set the media cost of a local tier \(aggregate\)](#)
- [Determine drive and RAID group information for a local tier \(aggregate\)](#)
- [Assign local tiers \(aggregates\) to storage VMs \(SVMs\)](#)
- [Determine which volumes reside on a local tier \(aggregate\)](#)
- [Determine and control a volume's space usages in a local tier \(aggregate\)](#)
- [Determine space usage in a local tier \(aggregate\)](#)
- [Relocate local tier \(aggregate\) ownership within an HA pair](#)
- [Delete a local tier \(aggregate\)](#)

### Rename a local tier (aggregate)


You can rename a local tier (aggregate). The method you follow depends on the interface you use—System Manager or the CLI:

#### System Manager

##### Use System Manager to rename a local tier (aggregate)

Beginning with ONTAP 9.10.1, you can modify the name of a local tier (aggregate).

#### Steps

1. In System Manager, click **Storage > Tiers**.
2. Click  next to the name of the local tier.
3. Select **Rename**.
4. Specify a new name for the local tier.

#### CLI

##### Use the CLI to rename a local tier (aggregate)

#### Step

1. Using the CLI, rename the local tier (aggregate):

```
storage aggregate rename -aggregate aggr-name -newname aggr-new-name
```

The following example renames an aggregate named “aggr5” as “sales-aggr”:

```
> storage aggregate rename -aggregate aggr5 -newname sales-aggr
```

### Set media cost of a local tier (aggregate)

Beginning with ONTAP 9.11.1, you can use System Manager to set the media cost of a local tier (aggregate).

## Steps

1. In System Manager, click **Storage > Tiers**, then click **Set Media Cost** in the desired local tier (aggregate) tiles.
2. Select **active and inactive tiers** to enable comparison.
3. Enter a currency type and amount.

When you enter or change the media cost, the change is made in all media types.

## Determine drive and RAID group information for a local tier (aggregate)

Some local tier (aggregate) administration tasks require that you know what types of drives compose the local tier, their size, checksum, and status, whether they are shared with other local tiers, and the size and composition of the RAID groups.

## Step

1. Show the drives for the aggregate, by RAID group:

```
storage aggregate show-status aggr_name
```

The drives are displayed for each RAID group in the aggregate.

You can see the RAID type of the drive (data, parity, dparity) in the `Position` column. If the `Position` column displays `shared`, then the drive is shared: if it is an HDD, it is a partitioned disk; if it is an SSD, it is part of a storage pool.

## Example: A Flash Pool aggregate using an SSD storage pool and data partitions

```
cluster1::> storage aggregate show-status nodeA_fp_1
```

```
Owner Node: cluster1-a
```

```
Aggregate: nodeA_fp_1 (online, mixed_raid_type, hybrid) (block checksums)
```

```
Plex: /nodeA_fp_1/plex0 (online, normal, active, pool0)
```

```
RAID Group /nodeA_fp_1/plex0/rg0 (normal, block checksums, raid_dp)
```

Position	Disk	Pool	Type	RPM	Usable Size	Physical Size	Status
shared	2.0.1	0	SAS	10000	472.9GB	547.1GB	(normal)
shared	2.0.3	0	SAS	10000	472.9GB	547.1GB	(normal)
shared	2.0.5	0	SAS	10000	472.9GB	547.1GB	(normal)
shared	2.0.7	0	SAS	10000	472.9GB	547.1GB	(normal)
shared	2.0.9	0	SAS	10000	472.9GB	547.1GB	(normal)
shared	2.0.11	0	SAS	10000	472.9GB	547.1GB	(normal)

```
RAID Group /nodeA_flashpool_1/plex0/rg1
```

```
(normal, block checksums, raid4) (Storage Pool: SmallSP)
```

Position	Disk	Pool	Type	RPM	Usable Size	Physical Size	Status
shared	2.0.13	0	SSD	-	186.2GB	745.2GB	(normal)
shared	2.0.12	0	SSD	-	186.2GB	745.2GB	(normal)

```
8 entries were displayed.
```

### Assign local tiers (aggregates) to storage VMs (SVMs)

If you assign one or more local tiers (aggregates) to a storage virtual machine (storage VM or SVM, formerly known as Vserver), then you can use only those local tiers to contain volumes for that storage VM (SVM).

#### What you'll need

The storage VM and the local tiers you want to assign to that storage VM must already exist.

#### About this task

Assigning local tiers to your storage VMs helps you keep your storage VMs isolated from each other; this is especially important in a multi-tenancy environment.

#### Steps

1. Check the list of local tiers (aggregates) already assigned to the SVM:

```
vserver show -fields aggr-list
```



The aggregates currently assigned to the SVM are displayed. If there are no aggregates assigned, "-" is displayed.

2. Add or remove assigned aggregates, depending on your requirements:

If you want to...	Use this command...
Assign additional aggregates	<code>vserver add-aggregates</code>
Unassign aggregates	<code>vserver remove-aggregates</code>

The listed aggregates are assigned to or removed from the SVM. If the SVM already has volumes that use an aggregate that is not assigned to the SVM, a warning message is displayed, but the command is completed successfully. Any aggregates that were already assigned to the SVM and that were not named in the command are unaffected.

### Example

In the following example, the aggregates `aggr1` and `aggr2` are assigned to SVM `svm1`:

```
vserver add-aggregates -vserver svm1 -aggregates aggr1,aggr2
```

### Determine which volumes reside on a local tier (aggregate)

You might need to determine which volumes reside on a local tier (aggregate) before performing operations on the local tier, such as relocating it or taking it offline.

### Steps

1. To display the volumes that reside on an aggregate, enter

```
volume show -aggregate aggregate_name
```

All volumes that reside on the specified aggregate are displayed.

### Determine and control a volume's space usage in a local tier (aggregate)

You can determine which FlexVol volumes are using the most space in a local tier (aggregate) and specifically which features within the volume.

The `volume show-footprint` command provides information about a volume's footprint, or its space usage within the containing aggregate.

The `volume show-footprint` command shows details about the space usage of each volume in an aggregate, including offline volumes. This command bridges the gap between the output of the `volume show-space` and `aggregate show-space` commands. All percentages are calculated as a percent of aggregate size.

The following example shows the `volume show-footprint` command output for a volume called `testvol`:

```
cluster1::> volume show-footprint testvol
```

```
Vserver : thevs
Volume  : testvol
```

Feature	Used	Used%
Volume Data Footprint	120.6MB	4%
Volume Guarantee	1.88GB	71%
Flexible Volume Metadata	11.38MB	0%
Delayed Frees	1.36MB	0%
Total Footprint	2.01GB	76%

The following table explains some of the key rows of the output of the `volume show-footprint` command and what you can do to try to decrease space usage by that feature:

Row/feature name	Description/contents of row	Some ways to decrease
Volume Data Footprint	The total amount of space used in the containing aggregate by a volume's data in the active file system and the space used by the volume's Snapshot copies. This row does not include reserved space.	<ul style="list-style-type: none"> <li>Deleting data from the volume.</li> <li>Deleting Snapshot copies from the volume.</li> </ul>
Volume Guarantee	The amount of space reserved by the volume in the aggregate for future writes. The amount of space reserved depends on the guarantee type of the volume.	Changing the type of guarantee for the volume to <code>none</code> .
Flexible Volume Metadata	The total amount of space used in the aggregate by the volume's metadata files.	No direct method to control.
Delayed Frees	Blocks that ONTAP used for performance and cannot be immediately freed. For SnapMirror destinations, this row has a value of 0 and is not displayed.	No direct method to control.
File Operation Metadata	The total amount of space reserved for file operation metadata.	No direct method to control.
Total Footprint	The total amount of space that the volume uses in the aggregate. It is the sum of all of the rows.	Any of the methods used to decrease space used by a volume.

## Related information

[NetApp Technical Report 3483: Thin Provisioning in a NetApp SAN or IP SAN Enterprise Environment](#)

### Determine space usage in a local tier (aggregate)

You can view how much space is used by all of the volumes in one or more local tiers (aggregates) so that you can take actions to free more space.

You can view space usage by all volumes in one or more aggregates with the `aggregate show-space` command. This helps you see which volumes are consuming the most space in their containing aggregates so that you can take actions to free more space.

The used space in an aggregate is directly affected by the space used in the FlexVol volumes it contains. Measures that you take to increase space in a volume also affect space in the aggregate.

The following rows are included in the `aggregate show-space` command output:

- **Volume Footprints**

The total of all volume footprints within the aggregate. It includes all of the space that is used or reserved by all data and metadata of all volumes in the containing aggregate.

- **Aggregate Metadata**

The total file system metadata required by the aggregate, such as allocation bitmaps and inode files.

- **Snapshot Reserve**

The amount of space reserved for aggregate Snapshot copies, based on volume size. It is considered used space and is not available to volume or aggregate data or metadata.

- **Snapshot Reserve Unusable**

The amount of space originally allocated for aggregate Snapshot reserve that is unavailable for aggregate Snapshot copies because it is being used by volumes associated with the aggregate. Can occur only for aggregates with a non-zero aggregate Snapshot reserve.

- **Total Used**

The sum of all space used or reserved in the aggregate by volumes, metadata, or Snapshot copies.

- **Total Physical Used**

The amount of space being used for data now (rather than being reserved for future use). Includes space used by aggregate Snapshot copies.

The following example shows the `aggregate show-space` command output for an aggregate whose Snapshot reserve is 5%. If the Snapshot reserve was 0, the row would not be displayed.

```
cluster1::> storage aggregate show-space
```

```
Aggregate : wqa_gx106_aggr1
```

Feature	Used	Used%
-----	-----	-----
Volume Footprints	101.0MB	0%
Aggregate Metadata	300KB	0%
Snapshot Reserve	5.98GB	5%
Total Used	6.07GB	5%
Total Physical Used	34.82KB	0%

### Relocate ownership of a local tier (aggregate) within an HA pair

You can change the ownership of local tiers (aggregates) among the nodes in an HA pair without interrupting service from the local tiers.

Both nodes in an HA pair are physically connected to each other's disks or array LUNs. Each disk or array LUN is owned by one of the nodes.

Ownership of all disks or array LUNs within a local tier (aggregate) changes temporarily from one node to the other when a takeover occurs. However, local tiers relocation operations can also permanently change the ownership (for example, if done for load balancing). The ownership changes without any data-copy processes or physical movement of the disks or array LUNs.

### About this task

- Because volume count limits are validated programmatically during local tier relocation operations, it is not necessary to check for this manually.

If the volume count exceeds the supported limit, the local tier relocation operation fails with a relevant error message.

- You should not initiate local tier relocation when system-level operations are in progress on either the source or the destination node; likewise, you should not start these operations during the local tier relocation.

These operations can include the following:

- Takeover
- Giveback
- Shutdown
- Another local tier relocation operation
- Disk ownership changes
- Local tier or volume configuration operations
- Storage controller replacement
- ONTAP upgrade

- ONTAP revert

- If you have a MetroCluster configuration, you should not initiate local tier relocation while disaster recovery operations (*switchover*, *healing*, or *switchback*) are in progress.
- If you have a MetroCluster configuration and initiate local tier relocation on a switched-over local tier, the operation might fail because it exceeds the DR partner's volume limit count.
- You should not initiate local tier relocation on aggregates that are corrupt or undergoing maintenance.
- Before initiating the local tier relocation, you should save any core dumps on the source and destination nodes.

### Steps

1. View the aggregates on the node to confirm which aggregates to move and ensure they are online and in good condition:

```
storage aggregate show -node source-node
```

The following command shows six aggregates on the four nodes in the cluster. All aggregates are online. Node1 and Node3 form an HA pair and Node2 and Node4 form an HA pair.

```
cluster::> storage aggregate show
Aggregate      Size Available Used% State  #Vols  Nodes  RAID Status
-----
aggr_0        239.0GB   11.13GB   95% online    1 node1  raid_dp,
normal
aggr_1        239.0GB   11.13GB   95% online    1 node1  raid_dp,
normal
aggr_2        239.0GB   11.13GB   95% online    1 node2  raid_dp,
normal
aggr_3        239.0GB   11.13GB   95% online    1 node2  raid_dp,
normal
aggr_4        239.0GB   238.9GB    0% online    5 node3  raid_dp,
normal
aggr_5        239.0GB   239.0GB    0% online    4 node4  raid_dp,
normal
6 entries were displayed.
```

2. Issue the command to start the aggregate relocation:

```
storage aggregate relocation start -aggregate-list aggregate-1, aggregate-2...
-node source-node -destination destination-node
```

The following command moves the aggregates `aggr_1` and `aggr_2` from Node1 to Node3. Node3 is Node1's HA partner. The aggregates can be moved only within the HA pair.

```
cluster::> storage aggregate relocation start -aggregate-list aggr_1,
aggr_2 -node node1 -destination node3
Run the storage aggregate relocation show command to check relocation
status.
node1::storage aggregate>
```

3. Monitor the progress of the aggregate relocation with the `storage aggregate relocation show` command:

```
storage aggregate relocation show -node source-node
```

The following command shows the progress of the aggregates that are being moved to Node3:

```
cluster::> storage aggregate relocation show -node node1
Source Aggregate   Destination   Relocation Status
-----
node1
    aggr_1         node3        In progress, module: waf1
    aggr_2         node3        Not attempted yet
2 entries were displayed.
node1::storage aggregate>
```

When the relocation is complete, the output of this command shows each aggregate with a relocation status of “Done”.

### Delete a local tier (aggregate)

You can delete a local tier (aggregate) if there are no volumes on the local tier.

The `storage aggregate delete` command deletes a storage aggregate. The command fails if there are volumes present on the aggregate. If the aggregate has an object store attached to it, then in addition to deleting the aggregate, the command deletes the objects in the object store as well. No changes are made to the object store configuration as part of this command.

The following example deletes an aggregate named “aggr1”:

```
> storage aggregate delete -aggregate aggr1
```

### Commands for aggregate relocation

There are specific ONTAP commands for relocating aggregate ownership within an HA pair.

If you want to...	Use this command...
-------------------	---------------------

Start the aggregate relocation process	<code>storage aggregate relocation start</code>
Monitor the aggregate relocation process	<code>storage aggregate relocation show</code>

### Related information

[ONTAP 9 Commands](#)

### Commands for managing aggregates

You use the `storage aggregate` command to manage your aggregates.

If you want to...	Use this command...
Display the size of the cache for all Flash Pool aggregates	<code>storage aggregate show -fields hybrid-cache-size-total -hybrid-cache-size -total &gt;0</code>
Display disk information and status for an aggregate	<code>storage aggregate show-status</code>
Display spare disks by node	<code>storage aggregate show-spare-disks</code>
Display the root aggregates in the cluster	<code>storage aggregate show -has-mroot true</code>
Display basic information and status for aggregates	<code>storage aggregate show</code>
Display the type of storage used in an aggregate	<code>storage aggregate show -fields storage-type</code>
Bring an aggregate online	<code>storage aggregate online</code>
Delete an aggregate	<code>storage aggregate delete</code>
Put an aggregate into the restricted state	<code>storage aggregate restrict</code>
Rename an aggregate	<code>storage aggregate rename</code>
Take an aggregate offline	<code>storage aggregate offline</code>
Change the RAID type for an aggregate	<code>storage aggregate modify -raidtype</code>

### Related information

[ONTAP 9 Commands](#)

## **Add capacity (disks) to a local tier (aggregate)**

### **Add capacity (disks) to a local tier (aggregate)**

Using different methods, you follow a specific workflow to add capacity.

- [Workflow to add capacity to a local tier \(aggregate\)](#)
- [Methods to create space in a local tier \(aggregate\)](#)

You can add disks to a local tier and add drives to a node or shelf.

If needed, you can correct misaligned spare partitions.

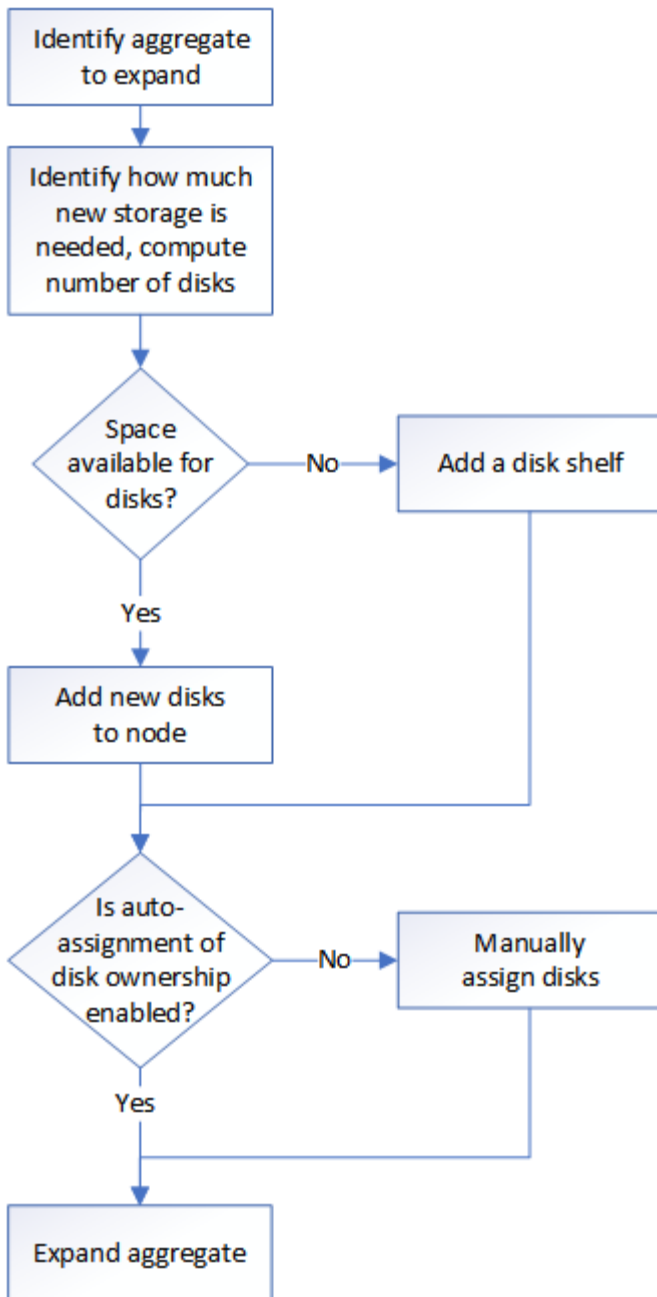
- [Add disks to a local tier \(aggregate\)](#)
- [Add drives to a node or shelf](#)
- [Correct misaligned spare partitions](#)

### **Workflow to add capacity to a local tier (expanding an aggregate)**

To add capacity to a local tier (expand an aggregate) you must first identify which local tier you want to add to, determine how much new storage is needed, install new disks, assign disk ownership, and create a new RAID group, if needed.

You can use either System Manager or the CLI to add capacity.





**Methods to create space in an local tier (aggregate)**

If a local tier (aggregate) runs out of free space, various problems can result that range from loss of data to disabling a volume’s guarantee. There are multiple ways to make more space in a local tier.

All of the methods have various consequences. Prior to taking any action, you should read the relevant section in the documentation.

The following are some common ways to make space in local tier, in order of least to most consequences:

- Add disks to the local tier.
- Move some volumes to another local tier with available space.
- Shrink the size of volume-guaranteed volumes in the local tier.

- Delete unneeded volume Snapshot copies if the volume's guarantee type is "none".
- Delete unneeded volumes.
- Enable space-saving features, such as deduplication or compression.
- (Temporarily) disable features that are using a large amount of metadata .

#### **Add capacity to a local tier (add disks to an aggregate)**

You can add disks to a local tier (aggregate) so that it can provide more storage to its associated volumes.

The process you follow depends on the interface that you use—System Manager or the CLI.

## System Manager (ONTAP 9.8 and later)

### Use System Manager to add capacity (ONTAP 9.8 and later)

You can add capacity to a local tier by adding capacity disks.

#### About this task

You perform this task only if you have installed ONTAP 9.8 or later. If you installed an earlier version of ONTAP, refer to [Use System Manager to add capacity \(ONTAP 9.7 or earlier\)](#).

#### Steps

1. Click **Storage > Tiers**.
2. Click  next to the name of the local tier to which you want to add capacity.
3. Click **Add Capacity**.



If there are no spare disks that you can add, then the **Add Capacity** option is not shown, and you cannot increase the capacity of the local tier.

4. Perform the following steps, based on the version of ONTAP that is installed:

If this version of ONTAP is installed...	Perform these steps...
ONTAP 9.8, 9.9, or 9.10.1	<ol style="list-style-type: none"><li>1. If the node contains multiple storage tiers, then select the number of disks you want to add to the local tier. Otherwise, if the node contains only a single storage tier, the added capacity is estimated automatically.</li><li>2. Click <b>Add</b>.</li></ol>
Beginning with ONTAP 9.11.1	<ol style="list-style-type: none"><li>1. Select the disk type and number of disks.</li><li>2. If you want to add disks to a new RAID group, check the check box. The RAID allocation is displayed.</li><li>3. Click <b>Save</b>.</li></ol>

5. (Optional) The process takes some time to complete. If you want to run the process in the background, select **Run in Background**.
6. After the process completes, you can view the increased capacity amount in the local tier information at **Storage > Tiers**.

## System Manager (ONTAP 9.7 and earlier)

### Use System Manager to add capacity (ONTAP 9.7 and earlier)

You can add capacity to a local tier (aggregate) by adding capacity disks.

#### About this task

You perform this task only if you have installed ONTAP 9.7 or earlier. If you installed ONTAP 9.8 or later, refer to [Use System Manager to add capacity \(ONTAP 9.8 or later\)](#).

#### Steps

1. (For ONTAP 9.7 only) Click **(Return to classic version)**.
2. Click **Hardware and Diagnostics > Aggregates**.
3. Select the aggregate to which you want to add capacity disks, and then click **Actions > Add Capacity**.



You should add disks that are of the same size as the other disks in the aggregate.

4. (For ONTAP 9.7 only) Click **Switch to the new experience**.
5. Click **Storage > Tiers** to verify the size of the new aggregate.

## CLI

### Use the CLI to add capacity

The procedure for adding partitioned disks to an aggregate is similar to the procedure for adding unpartitioned disks.

#### What you'll need

You must know what the RAID group size is for the aggregate you are adding the storage to.

#### About this task

When you expand an aggregate, you should be aware of whether you are adding partition or unpartitioned disks to the aggregate. When you add unpartitioned drives to an existing aggregate, the size of the existing RAID groups is inherited by the new RAID group, which can affect the number of parity disks required. If an unpartitioned disk is added to a RAID group composed of partitioned disks, the new disk is partitioned, leaving an unused spare partition.

When you provision partitions, you must ensure that you do not leave the node without a drive with both partitions as spare. If you do, and the node experiences a controller disruption, valuable information about the problem (the core file) might not be available to provide to the technical support.



Do not use the `disklist` command to expand your aggregates. This could cause partition misalignment.

#### Steps

1. Show the available spare storage on the system that owns the aggregate:

```
storage aggregate show-spare-disks -original-owner node_name
```

You can use the `-is-disk-shared` parameter to show only partitioned drives or only unpartitioned drives.

```
cl1-s2::> storage aggregate show-spare-disks -original-owner cl1-s2
-is-disk-shared true
```

```
Original Owner: cl1-s2
```

```
Pool0
```

```
Shared HDD Spares
```

```
Local Local
Data
```

```
Root Physical
```

```
Disk Usable Size Status Type RPM Checksum Usable
```

```
-----
```

```
1.0.1 BSAS 7200 block 753.8GB
73.89GB 828.0GB zeroed
```

```
1.0.2 BSAS 7200 block 753.8GB
0B 828.0GB zeroed
```

```
1.0.3 BSAS 7200 block 753.8GB
0B 828.0GB zeroed
```

```
1.0.4 BSAS 7200 block 753.8GB
0B 828.0GB zeroed
```

```
1.0.8 BSAS 7200 block 753.8GB
0B 828.0GB zeroed
```

```
1.0.9 BSAS 7200 block 753.8GB
0B 828.0GB zeroed
```

```
1.0.10 BSAS 7200 block 0B
73.89GB 828.0GB zeroed
```

```
2 entries were displayed.
```

## 2. Show the current RAID groups for the aggregate:

```
storage aggregate show-status aggr_name
```

```

c11-s2::> storage aggregate show-status -aggregate data_1

Owner Node: c11-s2
Aggregate: data_1 (online, raid_dp) (block checksums)
Plex: /data_1/plex0 (online, normal, active, pool0)
RAID Group /data_1/plex0/rg0 (normal, block checksums)

Physical
Position Disk Pool Type RPM Size Usable
Size Status
-----
shared 1.0.10 0 BSAS 7200 753.8GB
828.0GB (normal)
shared 1.0.5 0 BSAS 7200 753.8GB
828.0GB (normal)
shared 1.0.6 0 BSAS 7200 753.8GB
828.0GB (normal)
shared 1.0.11 0 BSAS 7200 753.8GB
828.0GB (normal)
shared 1.0.0 0 BSAS 7200 753.8GB
828.0GB (normal)
5 entries were displayed.

```

### 3. Simulate adding the storage to the aggregate:

```

storage aggregate add-disks -aggregate aggr_name -diskcount
number_of_disks_or_partitions -simulate true

```

You can see the result of the storage addition without actually provisioning any storage. If any warnings are displayed from the simulated command, you can adjust the command and repeat the simulation.

```

c11-s2::> storage aggregate add-disks data_1 -diskcount 5 -simulate
true

Addition of disks would succeed for aggregate "data_1" on node "c11-
s2". The
following disks would be used to add to the aggregate: 1.0.2, 1.0.3,
1.0.4, 1.0.8, 1.0.9.

```

### 4. Add the storage to the aggregate:

```

storage aggregate add-disks -aggregate aggr_name -raidgroup new -diskcount
number_of_disks_or_partitions

```

When creating a Flash Pool aggregate, if you are adding disks with a different checksum than the aggregate, or if you are adding disks to a mixed checksum aggregate, you must use the `-checksumstyle` parameter.

If you are adding disks to a Flash Pool aggregate, you must use the `-disktype` parameter to specify the disk type.

You can use the `-disksize` parameter to specify a size of the disks to add. Only disks with approximately the specified size are selected for addition to the aggregate.

```
c11-s2::> storage aggregate add-disks -aggregate data_1 -raidgroup
new -diskcount 5
```

5. Verify that the storage was added successfully:

```
storage aggregate show-status -aggregate aggr_name
```

```
cl1-s2::> storage aggregate show-status -aggregate data_1
```

```
Owner Node: cl1-s2
```

```
Aggregate: data_1 (online, raid_dp) (block checksums)
```

```
Plex: /data_1/plex0 (online, normal, active, pool0)
```

```
RAID Group /data_1/plex0/rg0 (normal, block checksums)
```

```
Physical                                                                 Usable
      Position Disk                                          Pool Type      RPM      Size
Size Status
-----
shared  1.0.10                                           0  BSAS      7200  753.8GB
828.0GB (normal)
shared  1.0.5                                           0  BSAS      7200  753.8GB
828.0GB (normal)
shared  1.0.6                                           0  BSAS      7200  753.8GB
828.0GB (normal)
shared  1.0.11                                          0  BSAS      7200  753.8GB
828.0GB (normal)
shared  1.0.0                                           0  BSAS      7200  753.8GB
828.0GB (normal)
shared  1.0.2                                           0  BSAS      7200  753.8GB
828.0GB (normal)
shared  1.0.3                                           0  BSAS      7200  753.8GB
828.0GB (normal)
shared  1.0.4                                           0  BSAS      7200  753.8GB
828.0GB (normal)
shared  1.0.8                                           0  BSAS      7200  753.8GB
828.0GB (normal)
shared  1.0.9                                           0  BSAS      7200  753.8GB
828.0GB (normal)
10 entries were displayed.
```

6. Verify that the node still has at least one drive with both the root partition and the data partition as spare:

```
storage aggregate show-spare-disks -original-owner node_name
```



```
cl1-s2::> storage aggregate show-spare-disks -original-owner cl1-s2
-is-disk-shared true
```

```
Original Owner: cl1-s2
```

```
Pool0
```

```
Shared HDD Spares
```

```
Local
Local
Root Physical
Disk Usable Size Status Type RPM Checksum Usable
-----
1.0.1 73.89GB 828.0GB zeroed BSAS 7200 block 753.8GB
1.0.10 73.89GB 828.0GB zeroed BSAS 7200 block 0B
2 entries were displayed.
```

### Add drives to a node or shelf

You add drives to a node or shelf to increase the number of hot spares or to add space to local tier (aggregate).

#### About this task

The drive you want to add must be supported by your platform.

[NetApp Hardware Universe](#)

The minimum number of drives you should add in a single procedure is six. Adding a single drive might reduce performance.

#### Steps

1. Check the NetApp Support Site for newer drive and shelf firmware and Disk Qualification Package files.

If your node or shelf does not have the latest versions, update them before installing the new drive.

Drive firmware is automatically updated (nondisruptively) on new drives that do not have current firmware versions.

2. Properly ground yourself.
3. Gently remove the bezel from the front of the platform.
4. Identify the correct slot for the new drive.



The correct slots for adding drives vary depending on the platform model and ONTAP version. In some cases you need to add drives to specific slots in sequence. For example, in an AFF A800 you add the drives at specific intervals leaving clusters of empty slots. Whereas, in an AFF A220 you add new drives to the next empty slots running from the outside towards the middle of the shelf.

See the [NetApp Hardware Universe](#) to identify the correct slots for your configuration.

5. Insert the new drive:
  - a. With the cam handle in the open position, use both hands to insert the new drive.
  - b. Push until the drive stops.
  - c. Close the cam handle so that the drive is fully seated into the mid plane and the handle clicks into place. Be sure to close the cam handle slowly so that it aligns correctly with the face of the drive.
6. Verify that the drive's activity LED (green) is illuminated.

When the drive's activity LED is solid, it means that the drive has power. When the drive's activity LED is blinking, it means that the drive has power and I/O is in progress. If the drive firmware is automatically updating, the LED blinks.

7. To add another drive, repeat Steps 4 through 6.

The new drives are not recognized until they are assigned to a node. You can assign the new drives manually, or you can wait for ONTAP to automatically assign the new drives if your node follows the rules for drive auto-assignment.

8. After the new drives have all been recognized, verify that they have been added and their ownership is specified correctly.

## Steps

1. Display the list of disks:

```
storage aggregate show-spare-disks
```

You should see the new drives, owned by the correct node.

2. Zero the newly added drives:

```
storage disk zerospares
```

Drives that have been used previously in an ONTAP local tier (aggregate) must be zeroed before they can be added to another aggregate. Zeroing the drives now can prevent delays in case you need to quickly increase the size of a local tier. The drive zeroing command runs in the background and can take hours to complete, depending on the size of the non-zeroed drives in the node.

## Results

The new drives are ready. You can add them to a local tier (aggregate), place them onto the list of hot spares, or add them when you create a new local tier.

### Correct misaligned spare partitions

When you add partitioned disks to a local tier (aggregate), you must leave a disk with

both the root and data partition available as a spare for every node. If you do not and your node experiences a disruption, ONTAP cannot dump the core to the spare data partition.

### What you'll need

You must have both a spare data partition and a spare root partition on the same type of disk owned by the same node.

### Steps

1. Using the CLI, display the spare partitions for the node:

```
storage aggregate show-spare-disks -original-owner node_name
```

Note which disk has a spare data partition (`spare_data`) and which disk has a spare root partition (`spare_root`). The spare partition will show a non-zero value under the `Local Data Usable` or `Local Root Usable` column.

2. Replace the disk with a spare data partition with the disk with the spare root partition:

```
storage disk replace -disk spare_data -replacement spare_root -action start
```

You can copy the data in either direction; however, copying the root partition takes less time to complete.

3. Monitor the progress of the disk replacement:

```
storage aggregate show-status -aggregate aggr_name
```

4. After the replacement operation is complete, display the spares again to confirm that you have a full spare disk:

```
storage aggregate show-spare-disks -original-owner node_name
```

You should see a spare disk with usable space under both "Local Data Usable" and `Local Root Usable`.

### Example

You display your spare partitions for node `c1-01` and see that your spare partitions are not aligned:

```
c1::> storage aggregate show-spare-disks -original-owner c1-01
```

```
Original Owner: c1-01
```

```
Pool0
```

```
Shared HDD Spares
```

Disk	Type	RPM	Checksum	Local Data Usable	Local Root Usable	Physical Size
1.0.1	BSAS	7200	block	753.8GB	0B	828.0GB
1.0.10	BSAS	7200	block	0B	73.89GB	828.0GB

You start the disk replacement job:

```
c1::> storage disk replace -disk 1.0.1 -replacement 1.0.10 -action start
```

While you are waiting for the replacement operation to finish, you display the progress of the operation:

```
c1::> storage aggregate show-status -aggregate aggr0_1

Owner Node: c1-01
Aggregate: aggr0_1 (online, raid_dp) (block checksums)
Plex: /aggr0_1/plex0 (online, normal, active, pool0)
RAID Group /aggr0_1/plex0/rg0 (normal, block checksums)

          Usable Physical
Position Disk   Pool Type   RPM      Size      Size Status
-----
shared  1.0.1     0   BSAS   7200   73.89GB   828.0GB (replacing, copy in
progress)
shared  1.0.10    0   BSAS   7200   73.89GB   828.0GB (copy 63% completed)
shared  1.0.0     0   BSAS   7200   73.89GB   828.0GB (normal)
shared  1.0.11    0   BSAS   7200   73.89GB   828.0GB (normal)
shared  1.0.6     0   BSAS   7200   73.89GB   828.0GB (normal)
shared  1.0.5     0   BSAS   7200   73.89GB   828.0GB (normal)
```

After the replacement operation is complete, confirm that you have a full spare disk:

```
ie2220::> storage aggregate show-spare-disks -original-owner c1-01

Original Owner: c1-01
Pool0
  Shared HDD Spares

          Local      Local
          Data      Root   Physical
Disk   Type   RPM Checksum Usable  Usable  Size
-----
1.0.1  BSAS   7200 block   753.8GB  73.89GB 828.0GB
```

## Manage disks

### Overview of managing disks

You can perform various procedures to manage disks in your system.

- **Aspects of managing disks**
  - [When you need to update the Disk Qualification Package](#)

- [How hot spare disks work](#)
- [How low spare warnings can help you manage your spare disks](#)
- [Additional root-data partitioning management options](#)
- **Disk and partition ownership**
  - [Disk and partition ownership](#)
- **Failed disk removal**
  - [Remove a failed disk](#)
- **Disk sanitization**
  - [Disk sanitization](#)

## How hot spare disks work

A hot spare disk is a disk that is assigned to a storage system and is ready for use, but is not in use by a RAID group and does not hold any data.

If a disk failure occurs within a RAID group, the hot spare disk is automatically assigned to the RAID group to replace the failed disks. The data of the failed disk is reconstructed on the hot spare replacement disk in the background from the RAID parity disk. The reconstruction activity is logged in the `/etc/message` file and an AutoSupport message is sent.

If the available hot spare disk is not the same size as the failed disk, a disk of the next larger size is chosen and then downsized to match the size of the disk that it is replacing.

## Spare requirements for multi-disk carrier disk

Maintaining the proper number of spares for disks in multi-disk carriers is critical for optimizing storage redundancy and minimizing the amount of time that ONTAP must spend copying disks to achieve an optimal disk layout.

You must maintain a minimum of two hot spares for multi-disk carrier disks at all times. To support the use of the Maintenance Center and to avoid issues caused by multiple concurrent disk failures, you should maintain at least four hot spares for steady state operation, and replace failed disks promptly.

If two disks fail at the same time with only two available hot spares, ONTAP might not be able to swap the contents of both the failed disk and its carrier mate to the spare disks. This scenario is called a stalemate. If this happens, you are notified through EMS messages and AutoSupport messages. When the replacement carriers become available, you must follow the instructions that are provided by the EMS messages. For more information, see Knowledge Base article [RAID Layout Cannot Be Autocorrected - AutoSupport message](#)

## How low spare warnings can help you manage your spare disks

By default, warnings are issued to the console and logs if you have fewer than one hot spare drive that matches the attributes of each drive in your storage system.

You can change the threshold value for these warning messages to ensure that your system adheres to best practices.

## About this task

You should set the `“min_spare_count”` RAID option to `“2”` to ensure that you always have the minimum

recommended number of spare disks.

### Step

1. Set the option to “2”:

```
storage raid-options modify -node nodename -name min_spare_count -value 2
```

### Additional root-data partitioning management options

Beginning with ONTAP 9.2, a new root-data partitioning option is available from the Boot Menu that provides additional management features for disks that are configured for root-data partitioning.

The following management features are available under the Boot Menu Option 9.

- **Unpartition all disks and remove their ownership information**

This option is useful if your system is configured for root-data partitioning and you need to reinitialize it with a different configuration.

- **Clean configuration and initialize node with partitioned disks**

This option is useful for the following:

- Your system is not configured for root-data partitioning and you would like to configure it for root-data partitioning
- Your system is incorrectly configured for root-data partitioning and you need to correct it
- You have an AFF platform or a FAS platform with only SSDs attached that is configured for the previous version of root-data partitioning and you want to upgrade it to the newer version of root-data partitioning to gain increased storage efficiency

- **Clean configuration and initialize node with whole disks**

This option is useful if you need to:

- Unpartition existing partitions
- Remove local disk ownership
- Reinitialize your system with whole disks using RAID-DP

### When you need to update the Disk Qualification Package

The Disk Qualification Package (DQP) adds full support for newly qualified drives. Before you update drive firmware or add new drive types or sizes to a cluster, you must update the DQP. A best practice is to also update the DQP regularly; for example, every quarter or semi-annually.

You need to download and install the DQP in the following situations:

- Whenever you add a new drive type or size to the node

For example, if you already have 1-TB drives and add 2-TB drives, you need to check for the latest DQP update.

- Whenever you update the disk firmware
- Whenever newer disk firmware or DQP files are available
- Whenever you upgrade to a new version of ONTAP.

The DQP is not updated as part of an ONTAP upgrade.

## Related information

[NetApp Downloads: Disk Qualification Package](#)

[NetApp Downloads: Disk Drive Firmware](#)

## Disk and partition ownership

### Disk and partition ownership

You can manage the ownership of disks and partitions.

You can perform the following tasks:

- [Display disk and partition ownership](#)

You can view disk ownership to determine which node controls the storage. You can also view the partition ownership on systems that use shared disks.

- [Manually assign ownership of partitioned disks](#)

You can set the ownership of the container disk or the partitions manually or by using auto-assignment—just as you do for unpartitioned disks.

- [Configure automatic assignment of disk ownership](#)

You can configure ONTAP to automatically assign disk ownership according to a disk's stack, shelf, or bay.

- [Remove a failed disk](#)

A disk that has failed completely is no longer considered by ONTAP to be a usable disk, and you can immediately disconnect the disk from the shelf.

- [Remove ownership from a disk](#)

ONTAP writes disk ownership information to the disk. Before you remove a spare disk or its shelf from a node, you should remove its ownership information so that it can be properly integrated into another node.

### Display disk and partition ownership

You can view disk ownership to determine which node controls the storage. You can also view the partition ownership on systems that use shared disks.

### Steps

1. Display the ownership of physical disks:

```
storage disk show -ownership
```

```
cluster::> storage disk show -ownership
Disk      Aggregate Home      Owner    DR Home  Home ID      Owner ID    DR
Home ID  Reserver  Pool
-----  -
-----  -
1.0.0    aggr0_2  node2    node2    -        2014941509  2014941509  -
2014941509 Pool0
1.0.1    aggr0_2  node2    node2    -        2014941509  2014941509  -
2014941509 Pool0
1.0.2    aggr0_1  node1    node1    -        2014941219  2014941219  -
2014941219 Pool0
1.0.3    -        node1    node1    -        2014941219  2014941219  -
2014941219 Pool0
```

2. If you have a system that uses shared disks, you can display the partition ownership:

```
storage disk show -partition-ownership
```

```
cluster::> storage disk show -partition-ownership
                                     Root      Data
Container Container
Disk      Aggregate Root Owner  Owner ID  Data Owner  Owner ID  Owner
Owner ID
-----  -
-----  -
1.0.0    -        node1    1886742616  node1    1886742616  node1
1886742616
1.0.1    -        node1    1886742616  node1    1886742616  node1
1886742616
1.0.2    -        node2    1886742657  node2    1886742657  node2
1886742657
1.0.3    -        node2    1886742657  node2    1886742657  node2
1886742657
```

### Manually assign disk ownership

Disks must be owned by a node before they can be used in a local tier (aggregate).

If your cluster is not configured to use automatic disk ownership assignment, you must assign ownership manually.

You cannot reassign ownership of a disk that is in use in a local tier.

### Steps

1. Using the CLI, display all unowned disks:



```
storage disk show -container-type unassigned
```

## 2. Assign each disk:

```
storage disk assign -disk disk_name -owner owner_name
```

You can use the wildcard character to assign more than one disk at once. If you are reassigning a spare disk that is already owned by a different node, you must use the “-force” option.

### Manually assign ownership of partitioned disks overview

Using the CLI, you can set the ownership of the container disk or the partitions manually or by using auto-assignment—just as you do for unpartitioned disks.



If a container disk fails in a half-populated shelf and is replaced, ONTAP will not auto-assign ownership. In this case, any assignment of new disks will need to be done manually. To make auto-assign work on half-populated shelves, place disks equally on lower half and 6 on far right bays to begin with. That is, 6 disks from bays 0-5 and 6 disks from bays 18-23. After the container disk is assigned in an ADP-configured system, ONTAP’s software will handle any partitioning and partition assignments that are required, without user intervention.

You can perform the following tasks in the CLI:

## Manually assign disks with root-data partitioning

For root-data partitioning, there are three owned entities (the container disk and the two partitions) collectively owned by the HA pair.

The container disk and the two partitions do not all need to be owned by the same node in the HA pair as long as they are all owned by one of the nodes in the HA pair. However, when you use a partition in a local tier (aggregate), it must be owned by the same node that owns the local tier.

### Steps

1. Use the CLI to display the current ownership for the partitioned disk:

```
storage disk show -disk disk_name -partition-ownership
```

2. Set the CLI privilege level to advanced:

```
set -privilege advanced
```

3. Enter the appropriate command, depending on which ownership entity you want to assign ownership for:

If you want to assign ownership for the...	Use this command...
Container disk	<code>storage disk assign -disk <i>disk_name</i> -owner <i>owner_name</i></code>
Data partition	<code>storage disk assign -disk <i>disk_name</i> -owner <i>owner_name</i> -data true</code>
Root partition	<code>storage disk assign -disk <i>disk_name</i> -owner <i>owner_name</i> -root true</code>

If any of the ownership entities are already owned, then you must include the “-force” option.

## Manually assign disks with root-data-data partitioning

For root-data-data partitioning, there are four owned entities (the container disk and the three partitions) collectively owned by the HA pair.

Root-data-data partitioning creates one small partition as the root partition and two larger, equally sized partitions for data.

### About this task

Parameters must be used with the `disk assign` command to assign the proper partition of a root-data-data partitioned disk. You cannot use these parameters with disks that are part of a storage pool. The default value is “false”.

- The `-data1 true` parameter assigns the “data1” partition of a root-data1-data2 partitioned disk.
- The `-data2 true` parameter assigns the “data2” partition of a root-data1-data2 partitioned disk.

### Steps

1. Use the CLI to display the current ownership for the partitioned disk:

```
storage disk show -disk disk_name -partition-ownership
```

2. Set the CLI privilege level to advanced:

```
set -privilege advanced
```

3. Enter the appropriate command, depending on which ownership entity you want to assign ownership for:

If you want to assign ownership for the...	Use this command...
Container disk	<code>storage disk assign -disk <i>disk_name</i> -owner <i>owner_name</i></code>
Data1 partition	<code>storage disk assign -disk <i>disk_name</i> -owner <i>owner_name</i> -data1 true</code>
Data2 partition	<code>storage disk assign -disk <i>disk_name</i> -owner <i>owner_name</i> -data2 true</code>
Root partition	<code>storage disk assign -disk <i>disk_name</i> -owner <i>owner_name</i> -root true</code>

If any of the ownership entities are already owned, then you must include the “-force” option.

### Configure automatic assignment of disk ownership

You can use the CLI to configure ONTAP to automatically assign disk ownership according to a disk’s stack, shelf, or bay. If configured, automatic disk ownership

assignments occur 10 minutes after system initialization and every five minutes during normal system operation.

### What you'll need

- Your system must adhere to the requirements for automatic disk ownership.
- If you have multiple stacks or shelves that must have different ownership, one disk must have been manually assigned on each stack or shelf so that automatic ownership assignment works on each stack or shelf.

### Which disk auto-assignment policy to use



Use the “bay autoassign-policy” only for entry level platforms. If you try to use the “bay autoassign-policy” for a non-entry level platform, it will fail.

You can typically use the default auto-assignment policy, which is equivalent to the “stack” policy for most systems, and to the “bay” policy for entry-level systems (AFF A2xx, FAS2xxx). However, for some configurations, you might need to change the auto-assignment policy.

You must select the appropriate auto-assignment based on your configuration:

If you are using...	Then use this auto-assignment policy...
Stand-alone entry-level system	stack
Entry-level systems in an HA configuration with a single, shared shelf	bay
Entry-level systems in an HA configuration with one stack of two or more shelves	shelf
MetroCluster configurations with one stack per node, two or more shelves	shelf
All other configurations	stack

### About this task

The behavior of the “default” automatic assignment policy depends on the system model. For entry level models, the “default” policy is equivalent to the “bay” policy. For all other systems, it is equivalent to the “stack” policy.

### Steps

1. Configure automatic disk assignment:

```
storage disk option modify -autoassign-policy autoassign_policy -node node_name
```

- Use *stack* as the *autoassign\_policy* to configure automatic ownership at the stack or loop level.
- Use *shelf* as the *autoassign\_policy* to configure automatic ownership at the shelf level.
- Use *bay* as the *autoassign\_policy* to configure automatic ownership at the bay level.

2. Verify the automatic assignment settings for the disks:

```
storage disk option show
```

```
cluster1::> storage disk option show
```

Node	BKg. FW. Upd.	Auto Copy	Auto Assign	Auto Assign Policy
cluster1-1	on	on	on	default
cluster1-2	on	on	on	default

### Set up an active-passive configuration on nodes using root-data partitioning

When an HA pair is configured to use root-data partitioning by the factory, ownership of the data partitions is split between both nodes in the pair for use in an active-active configuration. If you want to use the HA pair in an active-passive configuration, you must update partition ownership before creating your data local tier (aggregate).

#### What you'll need

- You should have decided which node will be the active node and which node will be the passive node.
- Storage failover must be configured on the HA pair.

#### About this task

This task is performed on two nodes: Node A and Node B.

This procedure is designed for nodes for which no data local tier (aggregate) has been created from the partitioned disks.

#### Steps

All commands are inputted at the cluster shell.

1. View the current ownership of the data partitions:

```
storage aggregate show-spare-disks
```

The output shows that half of the data partitions are owned by one node and half are owned by the other node. All of the data partitions should be spare.

```
cluster1::> storage aggregate show-spare-disks
```

```
Original Owner: cluster1-01
```

```
Pool0
```

```
Partitioned Spares
```

```
Local
```

```
Local
```

```
Root Physical
```

```
Data
```

```
Disk
```

```
Type
```

```
RPM Checksum
```

```
Usable
```

Usable	Size			
1.0.0	0B	828.0GB	BSAS	7200 block 753.8GB
1.0.1	73.89GB	828.0GB	BSAS	7200 block 753.8GB
1.0.5	0B	828.0GB	BSAS	7200 block 753.8GB
1.0.6	0B	828.0GB	BSAS	7200 block 753.8GB
1.0.10	0B	828.0GB	BSAS	7200 block 753.8GB
1.0.11	0B	828.0GB	BSAS	7200 block 753.8GB

Original Owner: cluster1-02  
Pool0  
Partitioned Spares

Local				Local
Local	Root	Physical		Data
Usable	Disk	Size	Type	RPM Checksum
Usable	Usable	Size		Usable
1.0.2	0B	828.0GB	BSAS	7200 block 753.8GB
1.0.3	0B	828.0GB	BSAS	7200 block 753.8GB
1.0.4	0B	828.0GB	BSAS	7200 block 753.8GB
1.0.7	0B	828.0GB	BSAS	7200 block 753.8GB
1.0.8	73.89GB	828.0GB	BSAS	7200 block 753.8GB
1.0.9	0B	828.0GB	BSAS	7200 block 753.8GB

12 entries were displayed.

2. Enter the advanced privilege level:

set advanced

3. For each data partition owned by the node that will be the passive node, assign it to the active node:

```
storage disk assign -force -data true -owner active_node_name -disk disk_name
```

You do not need to include the partition as part of the disk name.

You would enter a command similar to the following example for each data partition you need to reassign:

```
storage disk assign -force -data true -owner cluster1-01 -disk 1.0.3
```

#### 4. Confirm that all of the partitions are assigned to the active node.

```
cluster1::*> storage aggregate show-spare-disks

Original Owner: cluster1-01
Pool0
Partitioned Spares

Local
Local
Root Physical
Disk Usable Size Type RPM Checksum Usable
-----
-----
1.0.0 0B 828.0GB BSAS 7200 block 753.8GB
1.0.1 73.89GB 828.0GB BSAS 7200 block 753.8GB
1.0.2 0B 828.0GB BSAS 7200 block 753.8GB
1.0.3 0B 828.0GB BSAS 7200 block 753.8GB
1.0.4 0B 828.0GB BSAS 7200 block 753.8GB
1.0.5 0B 828.0GB BSAS 7200 block 753.8GB
1.0.6 0B 828.0GB BSAS 7200 block 753.8GB
1.0.7 0B 828.0GB BSAS 7200 block 753.8GB
1.0.8 0B 828.0GB BSAS 7200 block 753.8GB
1.0.9 0B 828.0GB BSAS 7200 block 753.8GB
1.0.10 0B 828.0GB BSAS 7200 block 753.8GB
1.0.11 0B 828.0GB BSAS 7200 block 753.8GB
```

```

Original Owner: cluster1-02
  Pool0
    Partitioned Spares
                                     Local
Local
                                     Data
Root Physical
  Disk                               Type      RPM Checksum      Usable
Usable      Size
-----
1.0.8                               BSAS      7200 block        0B
73.89GB   828.0GB
13 entries were displayed.

```

Note that cluster1-02 still owns a spare root partition.

- Return to administrative privilege:

```
set admin
```

- Create your data aggregate, leaving at least one data partition as spare:

```
storage aggregate create new_aggr_name -diskcount number_of_partitions -node
active_node_name
```

The data aggregate is created and is owned by the active node.

### Set up an active-passive configuration on nodes using root-data-data partitioning

When an HA pair is configured to use root-data-data partitioning by the factory, ownership of the data partitions is split between both nodes in the pair for use in an active-active configuration. If you want to use the HA pair in an active-passive configuration, you must update partition ownership before creating your data local tier (aggregate).

#### What you'll need

- You should have decided which node will be the active node and which node will be the passive node.
- Storage failover must be configured on the HA pair.

#### About this task

This task is performed on two nodes: Node A and Node B.

This procedure is designed for nodes for which no data local tier (aggregate) has been created from the partitioned disks.

#### Steps

All commands are input at the cluster shell.



1. View the current ownership of the data partitions:

```
storage aggregate show-spare-disks -original-owner passive_node_name -fields  
local-usable-data1-size, local-usable-data2-size
```

The output shows that half of the data partitions are owned by one node and half are owned by the other node. All of the data partitions should be spare.

2. Enter the advanced privilege level:

```
set advanced
```

3. For each data1 partition owned by the node that will be the passive node, assign it to the active node:

```
storage disk assign -force -data1 -owner active_node_name -disk disk_name
```

You do not need to include the partition as part of the disk name

4. For each data2 partition owned by the node that will be the passive node, assign it to the active node:

```
storage disk assign -force -data2 -owner active_node_name -disk disk_name
```

You do not need to include the partition as part of the disk name

5. Confirm that all of the partitions are assigned to the active node:

```
storage aggregate show-spare-disks
```

```
cluster1::*> storage aggregate show-spare-disks  
  
Original Owner: cluster1-01  
Pool0  
Partitioned Spares  
  
Local  
Local  
Data  
Root Physical  
Disk  
Usable      Size      Type      RPM Checksum      Usable  
-----  
1.0.0  
0B 828.0GB   BSAS      7200 block        753.8GB  
1.0.1  
73.89GB 828.0GB   BSAS      7200 block        753.8GB  
1.0.2  
0B 828.0GB   BSAS      7200 block        753.8GB  
1.0.3  
0B 828.0GB   BSAS      7200 block        753.8GB  
1.0.4  
BSAS      7200 block        753.8GB
```

```

0B 828.0GB
  1.0.5                BSAS    7200 block    753.8GB
0B 828.0GB
  1.0.6                BSAS    7200 block    753.8GB
0B 828.0GB
  1.0.7                BSAS    7200 block    753.8GB
0B 828.0GB
  1.0.8                BSAS    7200 block    753.8GB
0B 828.0GB
  1.0.9                BSAS    7200 block    753.8GB
0B 828.0GB
  1.0.10               BSAS    7200 block    753.8GB
0B 828.0GB
  1.0.11               BSAS    7200 block    753.8GB
0B 828.0GB

```

Original Owner: cluster1-02

Pool0

Partitioned Spares

```

Local
Local
Root Physical
Disk
Usable      Size
-----
1.0.8                BSAS    7200 block    0B
73.89GB  828.0GB
13 entries were displayed.

```

Note that cluster1-02 still owns a spare root partition.

6. Return to administrative privilege:

```
set admin
```

7. Create your data aggregate, leaving at least one data partition as spare:

```
storage aggregate create new_aggr_name -diskcount number_of_partitions -node
active_node_name
```

The data aggregate is created and is owned by the active node.

8. Alternatively, you can use ONTAP's recommend aggregate layout which includes best practices for RAID group layout and spare counts:

```
storage aggregate auto-provision
```

## Remove ownership from a disk

ONTAP writes disk ownership information to the disk. Before you remove a spare disk or its shelf from a node, you should remove its ownership information so that it can be properly integrated into another node.

### What you'll need

The disk you want to remove ownership from must meet the following requirements:

- It must be a spare disk.

You cannot remove ownership from a disk that is being used in an local tier (aggregate).

- It cannot be in the maintenance center.
- It cannot be undergoing sanitization.
- It cannot have failed.

It is not necessary to remove ownership from a failed disk.

### About this task

If you have automatic disk assignment enabled, ONTAP could automatically reassign ownership before you remove the disk from the node. For this reason, you disable the automatic ownership assignment until the disk is removed, and then you re-enable it.

### Steps

1. If disk ownership automatic assignment is on, use the CLI to turn it off:

```
storage disk option modify -node node_name -autoassign off
```

2. If needed, repeat the previous step for the node's HA partner.
3. Remove the software ownership information from the disk:

```
storage disk removeowner disk_name
```

To remove ownership information from multiple disks, use a comma-separated list.

Example:

```
storage disk removeowner sys1:0a.23,sys1:0a.24,sys1:0a.25
```

4. If the disk is partitioned for root-data partitioning, remove ownership from the partitions by entering both of the following commands:

```
storage disk removeowner -disk disk_name -root true
```

```
storage disk removeowner -disk disk_name -data true
```

Both partitions are no longer owned by any node.

5. If you previously turned off automatic assignment of disk ownership, turn it on after the disk has been

removed or reassigned:

```
storage disk option modify -node node_name -autoassign on
```

6. If needed, repeat the previous step for the node's HA partner.

## Remove a failed disk

A disk that has completely failed is no longer counted by ONTAP as a usable disk, and you can immediately disconnect the disk from the disk shelf. However, you should leave a partially failed disk connected long enough for the Rapid RAID Recovery process to complete.

### About this task

If you are removing a disk because it has failed or because it is producing excessive error messages, you should not use the disk again in this or any other storage system.

### Steps

1. Use the CLI to find the disk ID of the failed disk:

```
storage disk show -broken
```

If the disk does not appear in the list of failed disks, it might have partially failed, with a Rapid RAID Recovery in process. In this case, you should wait until the disk is present in the list of failed disks (which means that the Rapid RAID Recovery process is complete) before removing the disk.

2. Determine the physical location of the disk you want to remove:

```
storage disk set-led -action on -disk disk_name 2
```

The fault LED on the face of the disk is lit.

3. Remove the disk from the disk shelf, following the instructions in the hardware guide for your disk shelf model.

## Disk sanitization

### Disk sanitization overview

Disk sanitization is the process of physically obliterating data by overwriting disks or SSDs with specified byte patterns or random data so that recovery of the original data becomes impossible. Using the sanitization process ensures that no one can recover the data on the disks.

This functionality is available through the nodeshell in all ONTAP 9 releases, and starting with ONTAP 9.6 in maintenance mode.

The disk sanitization process uses three successive default or user-specified byte overwrite patterns for up to seven cycles per operation. The random overwrite pattern is repeated for each cycle.

Depending on the disk capacity, the patterns, and the number of cycles, the process can take several hours. Sanitization runs in the background. You can start, stop, and display the status of the sanitization process. The sanitization process contains two phases: the "Formatting phase" and the "Pattern overwrite phase".

## Formatting phase

The operation performed for the formatting phase depends on the class of disk being sanitized, as shown in the following table:

Disk class	Formatting phase operation
Capacity HDDs	Skipped
Performance HDDs	SCSI format operation
SSDs	SCSI sanitize operation

## Pattern overwrite phase

The specified overwrite patterns are repeated for the specified number of cycles.

When the sanitization process is complete, the specified disks are in a sanitized state. They are not returned to spare status automatically. You must return the sanitized disks to the spare pool before the newly sanitized disks are available to be added to another aggregate.

### When disk sanitization cannot be performed

Disk sanitization is not supported for all disk types. In addition, there are circumstances in which disk sanitization cannot be performed.

- It is not supported on all SSD part numbers.

For information about which SSD part numbers support disk sanitization, see the [Hardware Universe](#).

- It is not supported in takeover mode for systems in an HA pair.
- It cannot be performed on disks that were failed due to readability or writability problems.
- It does not perform its formatting phase on ATA drives.
- If you are using the random pattern, it cannot be performed on more than 100 disks at one time.
- It is not supported on array LUNs.
- If you sanitize both SES disks in the same ESH shelf at the same time, you see errors on the console about access to that shelf, and shelf warnings are not reported for the duration of the sanitization.

However, data access to that shelf is not interrupted.

### What happens if disk sanitization is interrupted

If disk sanitization is interrupted by user intervention or an unexpected event such as a power outage, ONTAP takes action to return the disks that were being sanitized to a known state, but you must also take action before the sanitization process can finish.

Disk sanitization is a long-running operation. If the sanitization process is interrupted by power failure, system panic, or manual intervention, the sanitization process must be repeated from the beginning. The disk is not designated as sanitized.

If the formatting phase of disk sanitization is interrupted, ONTAP must recover any disks that were corrupted by the interruption. After a system reboot and once every hour, ONTAP checks for any sanitization target disk that did not complete the formatting phase of its sanitization. If any such disks are found, ONTAP recovers them.

The recovery method depends on the type of the disk. After a disk is recovered, you can rerun the sanitization process on that disk; for HDDs, you can use the `-s` option to specify that the formatting phase is not repeated again.

#### **Tips for creating and backing up local tiers (aggregates) containing data to be sanitized**

If you are creating or backing up local tiers (aggregates) to contain data that might need to be sanitized, following some simple guidelines will reduce the time it takes to sanitize your data.

- Make sure your local tiers containing sensitive data are not larger than they need to be.

If they are larger than needed, sanitization requires more time, disk space, and bandwidth.

- When you back up local tiers containing sensitive data, avoid backing them up to local tier that also contain large amounts of nonsensitive data.

This reduces the resources required to move nonsensitive data before sanitizing sensitive data.

#### **Sanitize a disk**

Sanitizing a disk allows you to remove data from a disk or a set of disks on decommissioned or inoperable systems so that the data can never be recovered.

Two methods are available to sanitize disks using the CLI:

## Sanitize a disk with “maintenance mode” commands (ONTAP 9.6 and later releases)

Beginning with ONTAP 9.6, you can perform disk sanitization in maintenance mode.

### Before you begin

- The disks cannot be self-encrypting disks (SED).

You must use the `storage encryption disk sanitize` command to sanitize an SED.

### Encryption of data at rest

### Steps

1. Boot into maintenance mode.
2. If the disks you want to sanitize are partitioned, unpartition each disk:



The command to unpartition a disk is only available at the diag level and should be performed only under NetApp Support supervision. It is highly recommended that you contact NetApp Support before you proceed.

You can also refer to the Knowledge Base article [How to unpartition a spare drive in ONTAP](#)

```
disk unpartition disk_name
```

3. Sanitize the specified disks:

```
disk sanitize start [-p pattern1|-r [-p pattern2|-r [-p pattern3|-r]]] [-c cycle_count] disk_list
```



Do not turn off power to the node, disrupt the storage connectivity, or remove target disks while sanitizing. If sanitizing is interrupted during the formatting phase, the formatting phase must be restarted and allowed to finish before the disks are sanitized and ready to be returned to the spare pool. If you need to abort the sanitization process, you can do so by using the `disk sanitize abort` command. If the specified disks are undergoing the formatting phase of sanitization, the abort does not occur until the phase is complete.

`-p pattern1 -p pattern2 -p pattern3` specifies a cycle of one to three user-defined hex byte overwrite patterns that can be applied in succession to the disks being sanitized. The default pattern is three passes, using 0x55 for the first pass, 0xaa for the second pass, and 0x3c for the third pass.

`-r` replaces a patterned overwrite with a random overwrite for any or all of the passes.

`-c cycle_count` specifies the number of times that the specified overwrite patterns are applied. The default value is one cycle. The maximum value is seven cycles.

`disk_list` specifies a space-separated list of the IDs of the spare disks to be sanitized.

4. If desired, check the status of the disk sanitization process:

```
disk sanitize status [disk_list]
```

5. After the sanitization process is complete, return the disks to spare status for each disk:

```
disk sanitize release disk_name
```

6. Exit maintenance mode.



## Sanitize a disk with “nodeshell” commands (all ONTAP 9 releases)

For all versions of ONTAP 9, when disk sanitization is enabled using nodeshell commands, some low-level ONTAP commands are disabled. After disk sanitization is enabled on a node, it cannot be disabled.

### Before you begin

- The disks must be spare disks; they must be owned by a node, but not used in a local tier (aggregate).

If the disks are partitioned, neither partition can be in use in a local tier (aggregate).

- The disks cannot be self-encrypting disks (SED).

You must use the `storage encryption disk sanitize` command to sanitize an SED.

### Encryption of data at rest

- The disks cannot be part of a storage pool.

### Steps

1. If the disks you want to sanitize are partitioned, unpartition each disk:



The command to unpartition a disk is only available at the diag level and should be performed only under NetApp Support supervision. **It is highly recommended that you contact NetApp Support before you proceed.** You can also refer to the Knowledge Base article [How to unpartition a spare drive in ONTAP](#).

```
disk unpartition disk_name
```

2. Enter the nodeshell for the node that owns the disks you want to sanitize:

```
system node run -node node_name
```

3. Enable disk sanitization:

```
options licensed_feature.disk_sanitization.enable on
```

You are asked to confirm the command because it is irreversible.

4. Switch to the nodeshell advanced privilege level:

```
priv set advanced
```

5. Sanitize the specified disks:

```
disk sanitize start [-p pattern1|-r [-p pattern2|-r [-p pattern3|-r]]] [-c  
cycle_count] disk_list
```



Do not turn off power to the node, disrupt the storage connectivity, or remove target disks while sanitizing. If sanitizing is interrupted during the formatting phase, the formatting phase must be restarted and allowed to finish before the disks are sanitized and ready to be returned to the spare pool. If you need to abort the sanitization process, you can do so by using the `disk sanitize abort` command. If the specified disks are undergoing the formatting phase of sanitization, the abort does not occur until the phase is complete.

`-p pattern1 -p pattern2 -p pattern3` specifies a cycle of one to three user-defined hex byte overwrite patterns that can be applied in succession to the disks being sanitized. The default pattern is three passes, using 0x55 for the first pass, 0xaa for the second pass, and 0x3c for the third pass.

`-r` replaces a patterned overwrite with a random overwrite for any or all of the passes.

`-c cycle_count` specifies the number of times that the specified overwrite patterns are applied.

The default value is one cycle. The maximum value is seven cycles.

`disk_list` specifies a space-separated list of the IDs of the spare disks to be sanitized.

6. If you want to check the status of the disk sanitization process:

```
disk sanitize status [disk_list]
```

7. After the sanitization process is complete, return the disks to spare status:

```
disk sanitize release disk_name
```

8. Return to the nodeshell admin privilege level:

```
priv set admin
```

9. Return to the ONTAP CLI:

```
exit
```

10. Determine whether all of the disks were returned to spare status:

```
storage aggregate show-spare-disks
```

If...	Then...
All of the sanitized disks are listed as spares	You are done. The disks are sanitized and in spare status.

Some of the sanitized disks are not listed as spares

Complete the following steps:

a. Enter advanced privilege mode:

```
set -privilege advanced
```

b. Assign the unassigned sanitized disks to the appropriate node for each disk:

```
storage disk assign -disk disk_name -owner  
node_name
```

c. Return the disks to spare status for each disk:

```
storage disk unfailed -disk disk_name -s -q
```

d. Return to administrative mode:

```
set -privilege admin
```

## Result

The specified disks are sanitized and designated as hot spares. The serial numbers of the sanitized disks are written to `/etc/log/sanitized_disks`.

The specified disks' sanitization logs, which show what was completed on each disk, is written to `/mroot/etc/log/sanitization.log`.

## Commands for managing disks

You can use the `storage disk` and `storage aggregate` commands to manage your disks.

If you want to...	Use this command...
Display a list of spare disks, including partitioned disks, by owner	<code>storage aggregate show-spare-disks</code>
Display the disk RAID type, current usage, and RAID group by aggregate	<code>storage aggregate show-status</code>
Display the RAID type, current usage, aggregate, and RAID group, including spares, for physical disks	<code>storage disk show -raid</code>
Display a list of failed disks	<code>storage disk show -broken</code>
Display the pre-cluster (nodescope) drive name for a disk	<code>storage disk show -primary-paths (advanced)</code>

Illuminate the LED for a particular disk or shelf	<code>storage disk set-led</code>
Display the checksum type for a specific disk	<code>storage disk show -fields checksum-compatibility</code>
Display the checksum type for all spare disks	<code>storage disk show -fields checksum-compatibility -container-type spare</code>
Display disk connectivity and placement information	<code>storage disk show -fields disk,primary-port,secondary-name,secondary-port,shelf,bay</code>
Display the pre-cluster disk names for specific disks	<code>storage disk show -disk diskname -fields diskpathnames</code>
Display the list of disks in the maintenance center	<code>storage disk show -maintenance</code>
Display SSD wear life	<code>storage disk show -ssd-wear</code>
Unpartition a shared disk	<code>storage disk unpartition (available at diagnostic level)</code>
Zero all non-zeroed disks	<code>storage disk zerospares</code>
Stop an ongoing sanitization process on one or more specified disks	<code>system node run -node nodename -command disk sanitize</code>
Display storage encryption disk information	<code>storage encryption disk show</code>
Retrieve authentication keys from all linked key management servers	<code>security key-manager restore</code>

### Related information

[ONTAP 9 Commands](#)

### Commands for displaying space usage information

You use the `storage aggregate` and `volume` commands to see how space is being used in your aggregates and volumes and their Snapshot copies.

To display information about...	Use this command...
---------------------------------	---------------------

Aggregates, including details about used and available space percentages, Snapshot reserve size, and other space usage information	<code>storage aggregate show</code> <code>storage aggregate show-space -fields snap-size-total,used-including-snapshot-reserve</code>
How disks and RAID groups are used in an aggregate, and RAID status	<code>storage aggregate show-status</code>
The amount of disk space that would be reclaimed if you deleted a specific Snapshot copy	<code>volume snapshot compute-reclaimable</code>
The amount of space used by a volume	<code>volume show -fields size,used,available,percent-used</code> <code>volume show-space</code>
The amount of space used by a volume in the containing aggregate	<code>volume show-footprint</code>

### Related information

[ONTAP 9 Commands](#)

### Commands for displaying information about storage shelves

You use the `storage shelf show` command to display configuration and error information for your disk shelves.

If you want to display...	Use this command...
General information about shelf configuration and hardware status	<code>storage shelf show</code>
Detailed information for a specific shelf, including stack ID	<code>storage shelf show -shelf</code>
Unresolved, customer actionable, errors by shelf	<code>storage shelf show -errors</code>
Bay information	<code>storage shelf show -bay</code>
Connectivity information	<code>storage shelf show -connectivity</code>
Cooling information, including temperature sensors and cooling fans	<code>storage shelf show -cooling</code>
Information about I/O modules	<code>storage shelf show -module</code>
Port information	<code>storage shelf show -port</code>

If you want to display...	Use this command...
Power information, including PSUs (power supply units), current sensors, and voltage sensors	<code>storage shelf show -power</code>

### Related information

[ONTAP 9 Commands](#)

## Manage RAID configurations

### Overview of managing RAID configurations

You can perform various procedures to manage RAID configurations in your system.

- **Aspects of managing RAID configurations:**
  - [Default RAID policies for local tiers \(aggregates\)](#)
  - [RAID protection levels for disks](#)
- **Drive and RAID group information for a local tier (aggregate)**
  - [Determine drive and RAID group information for a local tier \(aggregate\)](#)
- **RAID configuration conversions**
  - [Convert from RAID-DP to RAID-TEC](#)
  - [Convert from RAID-TEC to RAID-DP](#)
- **RAID group sizing**
  - [Considerations for sizing RAID groups](#)
  - [Customize the size of your RAID group](#)

### Default RAID policies for local tiers (aggregates)

Either RAID-DP or RAID-TEC is the default RAID policy for all new local tiers (aggregates). The RAID policy determines the parity protection you have in the event of a disk failure.

RAID-DP provides double-parity protection in the event of a single or double disk failure. RAID-DP is the default RAID policy for the following local tier (aggregate) types:

- All flash local tiers
- Flash Pool local tiers
- Performance hard disk drive (HDD) local tiers

A new RAID policy called RAID-TEC is available. RAID-TEC is supported on all disk types and all platforms, including AFF. Local tiers that contain larger disks have a higher possibility of concurrent disk failures. RAID-TEC helps to mitigate this risk by providing triple-parity protection so that your data can survive up to three simultaneous disk failures. RAID-TEC is the default RAID policy for capacity HDD local tiers with disks that are 6 TB or larger.

## RAID protection levels for disks

ONTAP supports three levels of RAID protection for local tiers (aggregates). The level of RAID protection determines the number of parity disks available for data recovery in the event of disk failures.

With RAID protection, if there is a data disk failure in a RAID group, ONTAP can replace the failed disk with a spare disk and use parity data to reconstruct the data of the failed disk.

- **RAID4**

With RAID4 protection, ONTAP can use one spare disk to replace and reconstruct the data from one failed disk within the RAID group.

- **RAID-DP**

With RAID-DP protection, ONTAP can use up to two spare disks to replace and reconstruct the data from up to two simultaneously failed disks within the RAID group.

- **RAID-TEC**

With RAID-TEC protection, ONTAP can use up to three spare disks to replace and reconstruct the data from up to three simultaneously failed disks within the RAID group.

### Related information

[NetApp Technical Report 3437: Storage Subsystem Resiliency Guide](#)

### Drive and RAID group information for a local tier (aggregate)

Some local tier (aggregate) administration tasks require that you know what types of drives compose the local tier, their size, checksum, and status, whether they are shared with other local tiers, and the size and composition of the RAID groups.

#### Step

1. Show the drives for the aggregate, by RAID group:

```
storage aggregate show-status aggr_name
```

The drives are displayed for each RAID group in the aggregate.

You can see the RAID type of the drive (data, parity, dparity) in the `Position` column. If the `Position` column displays `shared`, then the drive is shared: if it is an HDD, it is a partitioned disk; if it is an SSD, it is part of a storage pool.

## Example: A Flash Pool aggregate using an SSD storage pool and data partitions

```
cluster1::> storage aggregate show-status nodeA_fp_1
```

```
Owner Node: cluster1-a
```

```
Aggregate: nodeA_fp_1 (online, mixed_raid_type, hybrid) (block checksums)
```

```
Plex: /nodeA_fp_1/plex0 (online, normal, active, pool0)
```

```
RAID Group /nodeA_fp_1/plex0/rg0 (normal, block checksums, raid_dp)
```

Position	Disk	Pool	Type	RPM	Usable Size	Physical Size	Status
shared	2.0.1	0	SAS	10000	472.9GB	547.1GB	(normal)
shared	2.0.3	0	SAS	10000	472.9GB	547.1GB	(normal)
shared	2.0.5	0	SAS	10000	472.9GB	547.1GB	(normal)
shared	2.0.7	0	SAS	10000	472.9GB	547.1GB	(normal)
shared	2.0.9	0	SAS	10000	472.9GB	547.1GB	(normal)
shared	2.0.11	0	SAS	10000	472.9GB	547.1GB	(normal)

```
RAID Group /nodeA_flashpool_1/plex0/rg1
```

```
(normal, block checksums, raid4) (Storage Pool: SmallSP)
```

Position	Disk	Pool	Type	RPM	Usable Size	Physical Size	Status
shared	2.0.13	0	SSD	-	186.2GB	745.2GB	(normal)
shared	2.0.12	0	SSD	-	186.2GB	745.2GB	(normal)

```
8 entries were displayed.
```

## Convert from RAID-DP to RAID-TEC

If you want the added protection of triple-parity, you can convert from RAID-DP to RAID-TEC. RAID-TEC is recommended if the size of the disks used in your local tier (aggregate) is greater than 4 TiB.

### What you'll need

The local tier (aggregate) that is to be converted must have a minimum of six disks.

### About this task

Hard disk drive (HDD) local tiers can be converted from RAID-DP to RAID-TEC. This includes HDD tiers in Flash Pool local tiers.

### Steps

1. Verify that the aggregate is online and has a minimum of six disks:

```
storage aggregate show-status -aggregate aggregate_name
```



2. Convert the aggregate from RAID-DP to RAID-TEC:

```
storage aggregate modify -aggregate aggregate_name -raidtype raid_tec
```

3. Verify that the aggregate RAID policy is RAID-TEC:

```
storage aggregate show aggregate_name
```

### Convert from RAID-TEC to RAID-DP

If you reduce the size of your local tier (aggregate) and no longer need triple parity, you can convert your RAID policy from RAID-TEC to RAID-DP and reduce the number of disks you need for RAID parity.

#### What you'll need

The maximum RAID group size for RAID-TEC is larger than the maximum RAID group size for RAID-DP. If the largest RAID-TEC group size is not within the RAID-DP limits, you cannot convert to RAID-DP.

#### Steps

1. Verify that the aggregate is online and has a minimum of six disks:

```
storage aggregate show-status -aggregate aggregate_name
```

2. Convert the aggregate from RAID-TEC to RAID-DP:

```
storage aggregate modify -aggregate aggregate_name -raidtype raid_dp
```

3. Verify that the aggregate RAID policy is RAID-DP:

```
storage aggregate show aggregate_name
```

### Considerations for sizing RAID groups

Configuring an optimum RAID group size requires a trade-off of factors. You must decide which factors—speed of RAID rebuild, assurance against risk of data loss due to drive failure, optimizing I/O performance, and maximizing data storage space—are most important for the (local tier) aggregate that you are configuring.

When you create larger RAID groups, you maximize the space available for data storage for the same amount of storage used for parity (also known as the “parity tax”). On the other hand, when a disk fails in a larger RAID group, reconstruction time is increased, impacting performance for a longer period of time. In addition, having more disks in a RAID group increases the probability of a multiple disk failure within the same RAID group.

#### HDD or array LUN RAID groups

You should follow these guidelines when sizing your RAID groups composed of HDDs or array LUNs:

- All RAID groups in an local tier (aggregate) should have the same number of disks.

While you can have up to 50% less or more than the number of disks in different raid groups on one local tier, this might lead to performance bottlenecks in some cases, so it is best avoided.

- The recommended range of RAID group disk numbers is between 12 and 20.

The reliability of performance disks can support a RAID group size of up to 28, if needed.

- If you can satisfy the first two guidelines with multiple RAID group disk numbers, you should choose the larger number of disks.

#### **SSD RAID groups in Flash Pool local tiers (aggregates)**

The SSD RAID group size can be different from the RAID group size for the HDD RAID groups in a Flash Pool local tier (aggregate). Usually, you should ensure that you have only one SSD RAID group for a Flash Pool local tier, to minimize the number of SSDs required for parity.

#### **SSD RAID groups in SSD local tiers (aggregates)**

You should follow these guidelines when sizing your RAID groups composed of SSDs:

- All RAID groups in a local tier (aggregate) should have a similar number of drives.

The RAID groups do not have to be exactly the same size, but you should avoid having any RAID group that is less than one half the size of other RAID groups in the same local tier when possible.

- For RAID-DP, the recommended range of RAID group size is between 20 and 28.

#### **Customize the size of your RAID groups**

You can customize the size of your RAID groups to ensure that your RAID group sizes are appropriate for the amount of storage you plan to include for a local tier (aggregate).

#### **About this task**

For standard local tiers (aggregates), you change the size of RAID groups for each local tier separately. For Flash Pool local tiers, you can change the RAID group size for the SSD RAID groups and the HDD RAID groups independently.

The following list outlines some facts about changing the RAID group size:

- By default, if the number of disks or array LUNs in the most recently created RAID group is less than the new RAID group size, disks or array LUNs will be added to the most recently created RAID group until it reaches the new size.
- All other existing RAID groups in that local tier remain the same size, unless you explicitly add disks to them.
- You can never cause a RAID group to become larger than the current maximum RAID group size for the local tier.
- You cannot decrease the size of already created RAID groups.
- The new size applies to all RAID groups in that local tier (or, in the case of a Flash Pool local tier, all RAID groups for the affected RAID group type—SSD or HDD).

#### **Steps**

1. Use the applicable command:

<b>If you want to...</b>	<b>Enter the following command...</b>
--------------------------	---------------------------------------

Change the maximum RAID group size for the SSD RAID groups of a Flash Pool aggregate	<code>storage aggregate modify -aggregate aggr_name -cache-raid-group-size size</code>
Change the maximum size of any other RAID groups	<code>storage aggregate modify -aggregate aggr_name -maxraidsize size</code>

## Examples

The following command changes the maximum RAID group size of the aggregate `n1_a4` to 20 disks or array LUNs:

```
storage aggregate modify -aggregate n1_a4 -maxraidsize 20
```

The following command changes the maximum RAID group size of the SSD cache RAID groups of the Flash Pool aggregate `n1_cache_a2` to 24:

```
storage aggregate modify -aggregate n1_cache_a2 -cache-raid-group-size 24
```

## Manage Flash Pool local tiers (aggregates)

### Manage Flash Pool tiers (aggregates)

You can perform various procedures to manage Flash Pool tiers (aggregates) in your system.

- **Caching policies**
  - [Flash Pool local tier \(aggregate\) caching policies](#)
  - [Manage Flash Pool caching policies](#)
- **SSD partitioning**
  - [Flash Pool SSD partitioning for Flash Pool local tiers \(aggregates\) using storage pools](#)
- **Candidacy and cache size**
  - [Determine Flash Pool candidacy and optimal cache size](#)
- **Flash Pool creation**
  - [Create a Flash Pool local tier \(aggregate\) using physical SSDs](#)
  - [Create a Flash Pool local tier \(aggregate\) using SSD storage pools](#)

### Flash Pool local tier (aggregate) caching policies

Caching policies for the volumes in a Flash Pool local tier (aggregate) let you deploy Flash as a high performance cache for your working data set while using lower-cost HDDs for less frequently accessed data. If you are providing cache to two or more Flash Pool local tiers, you should use Flash Pool SSD partitioning to share SSDs across the local tiers in the Flash Pool.

Caching policies are applied to volumes that reside in Flash Pool local tiers. You should understand how caching policies work before changing them.

In most cases, the default caching policy of “auto” is the best caching policy to use. The caching policy should

be changed only if a different policy provides better performance for your workload. Configuring the wrong caching policy can severely degrade volume performance; the performance degradation could increase gradually over time.

Caching policies combine a read caching policy and a write caching policy. The policy name concatenates the names of the read caching policy and the write caching policy, separated by a hyphen. If there is no hyphen in the policy name, the write caching policy is “none”, except for the “auto” policy.

Read caching policies optimize for future read performance by placing a copy of the data in the cache in addition to the stored data on HDDs. For read caching policies that insert data into the cache for write operations, the cache operates as a *write-through* cache.

Data inserted into the cache by using the write caching policy exists only in cache; there is no copy in HDDs. Flash Pool cache is RAID protected. Enabling write caching makes data from write operations available for reads from cache immediately, while deferring writing the data to HDDs until it ages out of the cache.

If you move a volume from a Flash Pool local tier to a single-tier local tier, it loses its caching policy; if you later move it back to a Flash Pool local tier, it is assigned the default caching policy of “auto”. If you move a volume between two Flash Pool local tier, the caching policy is preserved.

### **Change a caching policy**

You can use the CLI to change the caching policy for a volume that resides on a Flash Pool local tier by using the `-caching-policy` parameter with the `volume create` command.

When you create a volume on a Flash Pool local tier, by default, the “auto” caching policy is assigned to the volume.

## **Manage Flash Pool caching policies**

### **Overview of managing Flash Pool caching policies**

Using the CLI, you can perform various procedures to manage Flash Pool caching policies in your system.

- **Preparation**
  - [Determine whether to modify the caching policy of Flash Pool local tiers \(aggregates\)](#)
- **Caching policies modification**
  - [Modify caching policies of Flash Pool local tiers \(aggregates\)](#)
  - [Set the cache-retention policy for Flash Pool local tiers \(aggregates\)](#)

### **Determine whether to modify the caching policy of Flash Pool local tiers (aggregates)**

You can assign cache-retention policies to volumes in Flash Pool local tiers (aggregates) to determine how long the volume data remains in the Flash Pool cache. However, in some cases changing the cache-retention policy might not impact the amount of time the volume’s data remains in the cache.

### **About this task**

If your data meets any of the following conditions, changing your cache-retention policy might not have an impact:

- Your workload is sequential.

- Your workload does not reread the random blocks cached in the solid state drives (SSDs).
- The cache size of the volume is too small.

## Steps

The following steps check for the conditions that must be met by the data. The task must be done using the CLI in advanced privilege mode.

1. Use the CLI to view the workload volume:

```
statistics start -object workload_volume
```

2. Determine the workload pattern of the volume:

```
statistics show -object workload_volume -instance volume-workload -counter sequential_reads
```

3. Determine the hit rate of the volume:

```
statistics show -object waf1_hya_vvol -instance volume -counter read_ops_replaced_ppercent|wc_write_blks_overwritten_percent
```

4. Determine the Cacheable Read and Project Cache Alloc of the volume:

```
system node run -node node_name waf1 awa start aggr_name
```

5. Display the AWA summary:

```
system node run -node node_name waf1 awa print aggr_name
```

6. Compare the volume's hit rate to the Cacheable Read.

If the hit rate of the volume is greater than the Cacheable Read, then your workload does not reread random blocks cached in the SSDs.

7. Compare the volume's current cache size to the Project Cache Alloc.

If the current cache size of the volume is greater than the Project Cache Alloc, then the size of your volume cache is too small.

## Modify caching policies of Flash Pool local tiers (aggregates)

You should modify the caching policy of a volume only if a different caching policy is expected to provide better performance. You can modify the caching policy of a volume on a Flash Pool local tier (aggregate).

### What you'll need

You must determine whether you want to modify your caching policy.

### About this task

In most cases, the default caching policy of "auto" is the best caching policy that you can use. The caching policy should be changed only if a different policy provides better performance for your workload. Configuring the wrong caching policy can severely degrade volume performance; the performance degradation could

increase gradually over time. You should use caution when modifying caching policies. If you experience performance issues with a volume for which the caching policy has been changed, you should return the caching policy to “auto”.

### Step

1. Use the CLI to modify the volume’s caching policy:

```
volume modify -volume volume_name -caching-policy policy_name
```

### Example

The following example modifies the caching policy of a volume named “vol2” to the policy “none”:

```
volume modify -volume vol2 -caching-policy none
```

### Set the cache-retention policy for Flash Pool local tiers (aggregates)

You can assign cache-retention policies to volumes in Flash Pool local tiers (aggregates). Data in volumes with a high cache-retention policy remains in cache longer and data in volumes with a low cache-retention policy is removed sooner. This increases performance of your critical workloads by making high priority information accessible at a faster rate for a longer period of time.

### What you’ll need

You should know whether your system has any conditions that might prevent the cache-retention policy from having an impact on how long your data remains in cache.

### Steps

Use the CLI in advanced privilege mode to perform the following steps:

1. Change the privilege setting to advanced:

```
set -privilege advanced
```

2. Verify the volume’s cache-retention policy:

By default the cache retention policy is “normal”.

3. Set the cache-retention policy:

ONTAP Version	Command
ONTAP 9.0, 9.1	<pre>priority hybrid-cache set volume_name read-cache=read_cache_value write- cache=write_cache_value cache- retention- priority=cache_retention_policy</pre> <p>Set <code>cache_retention_policy</code> to high for data that you want to remain in cache longer. Set <code>cache_retention_policy</code> to low for data that you want to remove from cache sooner.</p>

ONTAP 9.2 or later

```
volume modify -volume volume_name  
-vserver vserver_name -caching-policy  
policy_name.
```

4. Verify that the volume's cache-retention policy is changed to the option you selected.
5. Return the privilege setting to admin:

```
set -privilege admin
```

### Flash Pool SSD partitioning for Flash Pool local tiers (aggregates) using storage pools

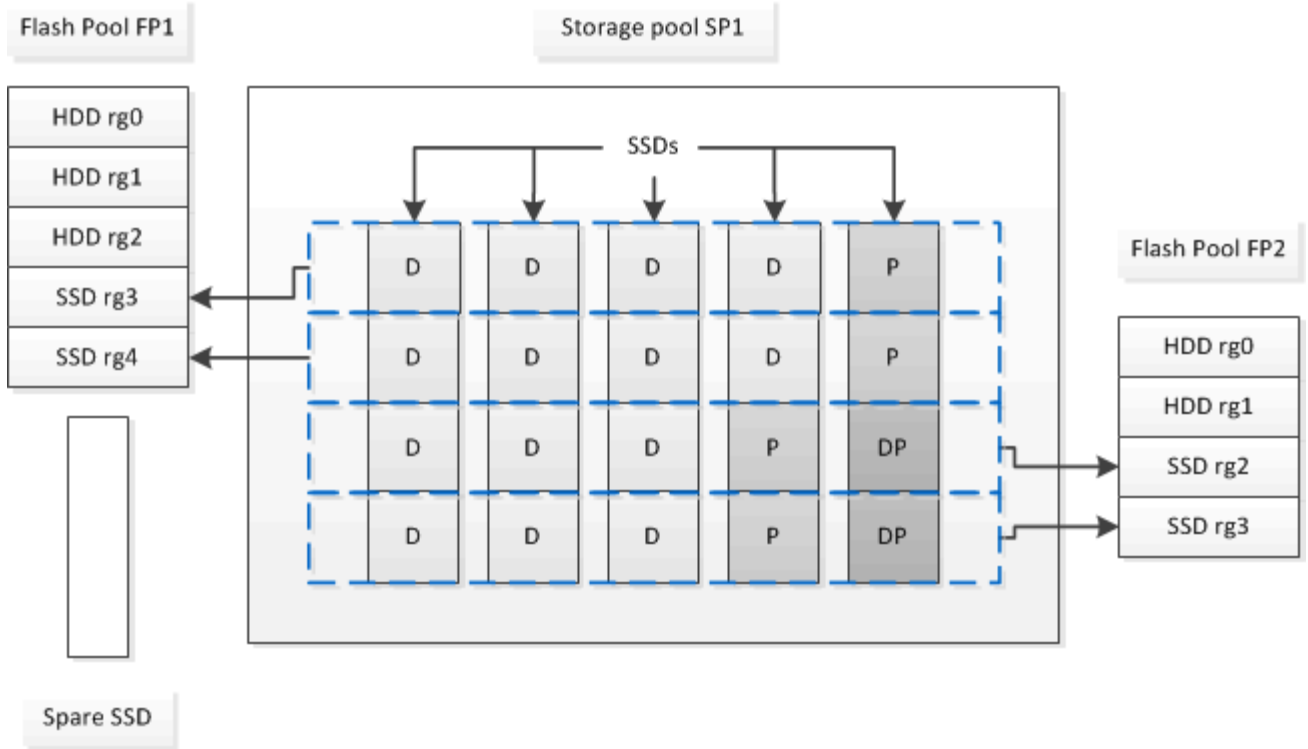
If you are providing cache to two or more Flash Pool local tiers (aggregates), you should use Flash Pool Solid-State Drive (SSD) partitioning. Flash Pool SSD partitioning allows SSDs to be shared by all the local tiers that use the Flash Pool. This spreads the cost of parity over multiple local tiers, increases SSD cache allocation flexibility, and maximizes SSD performance.

For an SSD to be used in a Flash Pool local tier, the SSD must be placed in a storage pool. You cannot use SSDs that have been partitioned for root-data partitioning in a storage pool. After the SSD is placed in the storage pool, the SSD can no longer be managed as a stand-alone disk and cannot be removed from the storage pool unless you destroy the local tiers associated with the Flash Pool and you destroy the storage pool.

SSD storage pools are divided into four equal allocation units. SSDs added to the storage pool are divided into four partitions and one partition is assigned to each of the four allocation units. The SSDs in the storage pool must be owned by the same HA pair. By default, two allocation units are assigned to each node in the HA pair. Allocation units must be owned by the node that owns the local tier it is serving. If more Flash cache is required for local tiers on one of the nodes, the default number of allocation units can be shifted to decrease the number on one node and increase the number on the partner node.

You can use only one spare SSD for a storage pool. If the storage pool provides allocation units to Flash Pool local tiers owned by both nodes in the HA pair, then the spare SSD can be owned by either node. However, if the storage pool provides allocation units only to Flash Pool local tiers owned by one of the nodes in the HA pair, then the SSD spare must be owned by that same node.

The following illustration is an example of Flash Pool SSD partitioning. The SSD storage pool provides cache to two Flash Pool local tiers:



Storage pool SP1 is composed of five SSDs and a hot spare SSD. Two of the storage pool's allocation units are allocated to Flash Pool FP1, and two are allocated to Flash Pool FP2. FP1 has a cache RAID type of RAID4. Therefore, the allocation units provided to FP1 contain only one partition designated for parity. FP2 has a cache RAID type of RAID-DP. Therefore, the allocation units provided to FP2 include a parity partition and a double-parity partition.

In this example, two allocation units are allocated to each Flash Pool local tier. However, if one Flash Pool local tier required a larger cache, you could allocate three of the allocation units to that Flash Pool local tier, and only one to the other.

### Determine Flash Pool candidacy and optimal cache size

Before converting an existing local tier (aggregate) to a Flash Pool local tier, you can determine whether the local tier is I/O bound and the best Flash Pool cache size for your workload and budget. You can also check whether the cache of an existing Flash Pool local tier is sized correctly.

#### What you'll need

You should know approximately when the local tier you are analyzing experiences its peak load.

#### Steps

1. Enter advanced mode:

```
set advanced
```

2. If you need to determine whether an existing local tier (aggregate) would be a good candidate for conversion to a Flash Pool aggregate, determine how busy the disks in the aggregate are during a period of peak load, and how that is affecting latency:

```
statistics show-periodic -object disk:raid_group -instance raid_group_name
```



```
-counter disk_busy|user_read_latency -interval 1 -iterations 60
```

You can decide whether reducing latency by adding Flash Pool cache makes sense for this aggregate.

The following command shows the statistics for the first RAID group of the aggregate “aggr1”:

```
statistics show-periodic -object disk:raid_group -instance /aggr1/plex0/rg0  
-counter disk_busy|user_read_latency -interval 1 -iterations 60
```

### 3. Start Automated Workload Analyzer (AWA):

```
storage automated-working-set-analyzer start -node node_name -aggregate  
aggr_name
```

AWA begins collecting workload data for the volumes associated with the specified aggregate.

### 4. Exit advanced mode:

```
set admin
```

Allow AWA to run until one or more intervals of peak load have occurred. AWA collects workload statistics for the volumes associated with the specified aggregate, and analyzes data for up to one rolling week in duration. Running AWA for more than one week will report only on data collected from the most recent week. Cache size estimates are based on the highest loads seen during the data collection period; the load does not need to be high for the entire data collection period.

### 5. Enter advanced mode:

```
set advanced
```

### 6. Display the workload analysis:

```
storage automated-working-set-analyzer show -node node_name -instance
```

### 7. Stop AWA:

```
storage automated-working-set-analyzer stop node_name
```

All workload data is flushed and is no longer available for analysis.

### 8. Exit advanced mode:

```
set admin
```

## Create a Flash Pool local tier (aggregate) using physical SSDs

You create a Flash Pool local tier (aggregate) by enabling the feature on an existing local tier composed of HDD RAID groups, and then adding one or more SSD RAID groups to that local tier. This results in two sets of RAID groups for that local tier: SSD RAID groups (the SSD cache) and HDD RAID groups.

### What you’ll need

- You must have identified a valid local tier composed of HDDs to convert to a Flash Pool local tier.

- You must have determined write-caching eligibility of the volumes associated with the local tier, and completed any required steps to resolve eligibility issues.
- You must have determined the SSDs you will be adding, and these SSDs must be owned by the node on which you are creating the Flash Pool local tier.
- You must have determined the checksum types of both the SSDs you are adding and the HDDs already in the local tier.
- You must have determined the number of SSDs you are adding and the optimal RAID group size for the SSD RAID groups.

Using fewer RAID groups in the SSD cache reduces the number of parity disks required, but larger RAID groups require RAID-DP.

- You must have determined the RAID level you want to use for the SSD cache.
- You must have determined the maximum cache size for your system and determined that adding SSD cache to your local tier will not cause you to exceed it.
- You must have familiarized yourself with the configuration requirements for Flash Pool local tiers.

### About this task

After you add an SSD cache to an local tier to create a Flash Pool local tier, you cannot remove the SSD cache to convert the local tier back to its original configuration.

By default, the RAID level of the SSD cache is the same as the RAID level of the HDD RAID groups. You can override this default selection by specifying the “raidtype” option when you add the first SSD RAID groups.

### Steps

1. Mark the local tier (aggregate) as eligible to become a Flash Pool aggregate:

```
storage aggregate modify -aggregate aggr_name -hybrid-enabled true
```

If this step does not succeed, determine write-caching eligibility for the target aggregate.

2. Add the SSDs to the aggregate by using the `storage aggregate add` command.
  - You can specify the SSDs by ID or by using the `diskcount` and `disktype` parameters.
  - If the HDDs and the SSDs do not have the same checksum type, or if the aggregate is a mixed-checksum aggregate, then you must use the `checksumstyle` parameter to specify the checksum type of the disks you are adding to the aggregate.
  - You can specify a different RAID type for the SSD cache by using the `raidtype` parameter.
  - If you want the cache RAID group size to be different from the default for the RAID type you are using, you should change it now, by using the `-cache-raid-group-size` parameter.

## Create a Flash Pool local tier (aggregate) using SSD storage pools

### Overview of creating a Flash Pool local tier (aggregate) using SSD storage pools

You can perform various procedures to create a Flash Pool local tier (aggregate) using SSD storage pools:

- **Preparation**
  - [Determine whether a Flash Pool local tier \(aggregate\) is using an SSD storage pool](#)

- **SSD storage pool creation**
  - [Create an SSD storage pool](#)
  - [Add SSDs to an SSD storage pool](#)
- **Flash Pool creation using SSD storage pools**
  - [Create a Flash Pool local tier \(aggregate\) using SSD storage pool allocation units](#)
  - [Determine the impact to cache size of adding SSDs to an SSD storage pool](#)

#### Determine whether a Flash Pool local tier (aggregate) is using an SSD storage pool

You can configure a Flash Pool (local tier) aggregate by adding one or more allocation units from an SSD storage pool to an existing HDD local tier.

You manage Flash Pool local tiers differently when they use SSD storage pools to provide their cache than when they use discrete SSDs.

#### Step

1. Display the aggregate's drives by RAID group:

```
storage aggregate show-status aggr_name
```

If the aggregate is using one or more SSD storage pools, the value for the `Position` column for the SSD RAID groups is displayed as `Shared`, and the name of the storage pool is displayed next to the RAID group name.

#### Add cache to a local tier (aggregate) by creating an SSD storage pool

You can provision cache by converting an existing local tier (aggregate) to a Flash Pool local tier (aggregate) by adding solid state drives (SSDs).

You can create solid state drive (SSD) storage pools to provide SSD cache for two to four Flash Pool local tiers (aggregates). Flash Pool aggregates enable you to deploy flash as high performance cache for your working data set while using lower-cost HDDs for less frequently accessed data.

#### About this task

- You must supply a disk list when creating or adding disks to a storage pool.

Storage pools do not support a `diskcount` parameter.

- The SSDs used in the storage pool should be the same size.

The procedure that you follow depends on the interface that you use—System Manager or the CLI.

## System Manager

### Use System Manager to add an SSD cache (ONTAP 9.7 only)



Use the CLI procedure if you are using an ONTAP version other than 9.7

#### Steps

1. Click **(Return to classic version)**.
2. Click **Storage > Aggregates & Disks > Aggregates**.
3. Select the local tier (aggregate), and then click **Actions > Add Cache**.
4. Select the cache source as "storage pools" or "dedicated SSDs".
5. Click **(Switch to the new experience)**.
6. Click **Storage > Tiers** to verify the size of the new aggregate.

#### CLI

### Use the CLI to create an SSD storage pool

#### Steps

1. Determine the names of the available spare SSDs:

```
storage aggregate show-spare-disks -disk-type SSD
```

The SSDs used in a storage pool can be owned by either node of an HA pair.

2. Create the storage pool:

```
storage pool create -storage-pool sp_name -disk-list disk1,disk2,...
```

3. **Optional:** Verify the newly created storage pool:

```
storage pool show -storage-pool sp_name
```

## Results

After the SSDs are placed into the storage pool, they no longer appear as spares on the cluster, even though the storage provided by the storage pool has not yet been allocated to any Flash Pool caches. You cannot add SSDs to a RAID group as discrete drives; their storage can be provisioned only by using the allocation units of the storage pool to which they belong.

### Create a Flash Pool local tier (aggregate) using SSD storage pool allocation units

You can configure a Flash Pool local tier (aggregate) by adding one or more allocation units from an SSD storage pool to an existing HDD local tier.

#### What you'll need

- You must have identified a valid local tier composed of HDDs to convert to a Flash Pool local tier.
- You must have determined write-caching eligibility of the volumes associated with the local tier, and completed any required steps to resolve eligibility issues.

- You must have created an SSD storage pool to provide the SSD cache to this Flash Pool local tier.

Any allocation unit from the storage pool that you want to use must be owned by the same node that owns the Flash Pool local tier.

- You must have determined how much cache you want to add to the local tier.

You add cache to the local tier by allocation units. You can increase the size of the allocation units later by adding SSDs to the storage pool if there is room.

- You must have determined the RAID type you want to use for the SSD cache.

After you add a cache to the local tier from SSD storage pools, you cannot change the RAID type of the cache RAID groups.

- You must have determined the maximum cache size for your system and determined that adding SSD cache to your local tier will not cause you to exceed it.

You can see the amount of cache that will be added to the total cache size by using the `storage pool show` command.

- You must have familiarized yourself with the configuration requirements for Flash Pool local tier.

### About this task

If you want the RAID type of the cache to be different from that of the HDD RAID groups, you must specify the cache RAID type when you add the SSD capacity. After you add the SSD capacity to the local tier, you can no longer change the RAID type of the cache.

After you add an SSD cache to a local tier to create a Flash Pool local tier, you cannot remove the SSD cache to convert the local tier back to its original configuration.

### Steps

1. Mark the aggregate as eligible to become a Flash Pool aggregate:

```
storage aggregate modify -aggregate aggr_name -hybrid-enabled true
```

If this step does not succeed, determine write-caching eligibility for the target aggregate.

2. Show the available SSD storage pool allocation units:

```
storage pool show-available-capacity
```

3. Add the SSD capacity to the aggregate:

```
storage aggregate add aggr_name -storage-pool sp_name -allocation-units  
number_of_units
```

If you want the RAID type of the cache to be different from that of the HDD RAID groups, you must change it when you enter this command by using the `raidtype` parameter.

You do not need to specify a new RAID group; ONTAP automatically puts the SSD cache into separate RAID groups from the HDD RAID groups.

You cannot set the RAID group size of the cache; it is determined by the number of SSDs in the storage

pool.

The cache is added to the aggregate and the aggregate is now a Flash Pool aggregate. Each allocation unit added to the aggregate becomes its own RAID group.

4. Confirm the presence and size of the SSD cache:

```
storage aggregate show aggregate_name
```

The size of the cache is listed under `Total Hybrid Cache Size`.

## Related information

[NetApp Technical Report 4070: Flash Pool Design and Implementation Guide](#)

### Determine the impact to cache size of adding SSDs to an SSD storage pool

If adding SSDs to a storage pool causes your platform model's cache limit to be exceeded, ONTAP does not allocate the newly added capacity to any Flash Pool local tiers (aggregates). This can result in some or all of the newly added capacity being unavailable for use.

#### About this task

When you add SSDs to an SSD storage pool that has allocation units already allocated to Flash Pool local tiers (aggregates), you increase the cache size of each of those local tiers and the total cache on the system. If none of the storage pool's allocation units have been allocated, adding SSDs to that storage pool does not affect the SSD cache size until one or more allocation units are allocated to a cache.

#### Steps

1. Determine the usable size of the SSDs you are adding to the storage pool:

```
storage disk show disk_name -fields usable-size
```

2. Determine how many allocation units remain unallocated for the storage pool:

```
storage pool show-available-capacity sp_name
```

All unallocated allocation units in the storage pool are displayed.

3. Calculate the amount of cache that will be added by applying the following formula:

$(4 - \text{number of unallocated allocation units}) \times 25\% \times \text{usable size} \times \text{number of SSDs}$

### Add SSDs to an SSD storage pool

When you add solid state drives (SSDs) to an SSD storage pool, you increase the storage pool's physical and usable sizes and allocation unit size. The larger allocation unit size also affects allocation units that have already been allocated to local tiers (aggregates).

#### What you'll need

You must have determined that this operation will not cause you to exceed the cache limit for your HA pair.

ONTAP does not prevent you from exceeding the cache limit when you add SSDs to an SSD storage pool, and doing so can render the newly added storage capacity unavailable for use.

### About this task

When you add SSDs to an existing SSD storage pool, the SSDs must be owned by one node or the other of the same HA pair that already owned the existing SSDs in the storage pool. You can add SSDs that are owned by either node of the HA pair.

The SSD you add to the storage pool must be the same size as disk currently used in the storage pool.

### Steps

1. **Optional:** View the current allocation unit size and available storage for the storage pool:

```
storage pool show -instance sp_name
```

2. Find available SSDs:

```
storage disk show -container-type spare -type SSD
```

3. Add the SSDs to the storage pool:

```
storage pool add -storage-pool sp_name -disk-list disk1,disk2...
```

The system displays which Flash Pool aggregates will have their size increased by this operation and by how much, and prompts you to confirm the operation.

### Commands for managing SSD storage pools

ONTAP provides the `storage pool` command for managing SSD storage pools.

If you want to...	Use this command...
Display how much storage a storage pool is providing to which aggregates	<code>storage pool show-aggregate</code>
Display how much cache would be added to the overall cache capacity for both RAID types (allocation unit data size)	<code>storage pool show -instance</code>
Display the disks in a storage pool	<code>storage pool show-disks</code>
Display the unallocated allocation units for a storage pool	<code>storage pool show-available-capacity</code>
Change the ownership of one or more allocation units of a storage pool from one HA partner to the other	<code>storage pool reassign</code>

### Related information

[ONTAP 9 Commands](#)

# FabricPool tier management

## FabricPool tier management overview

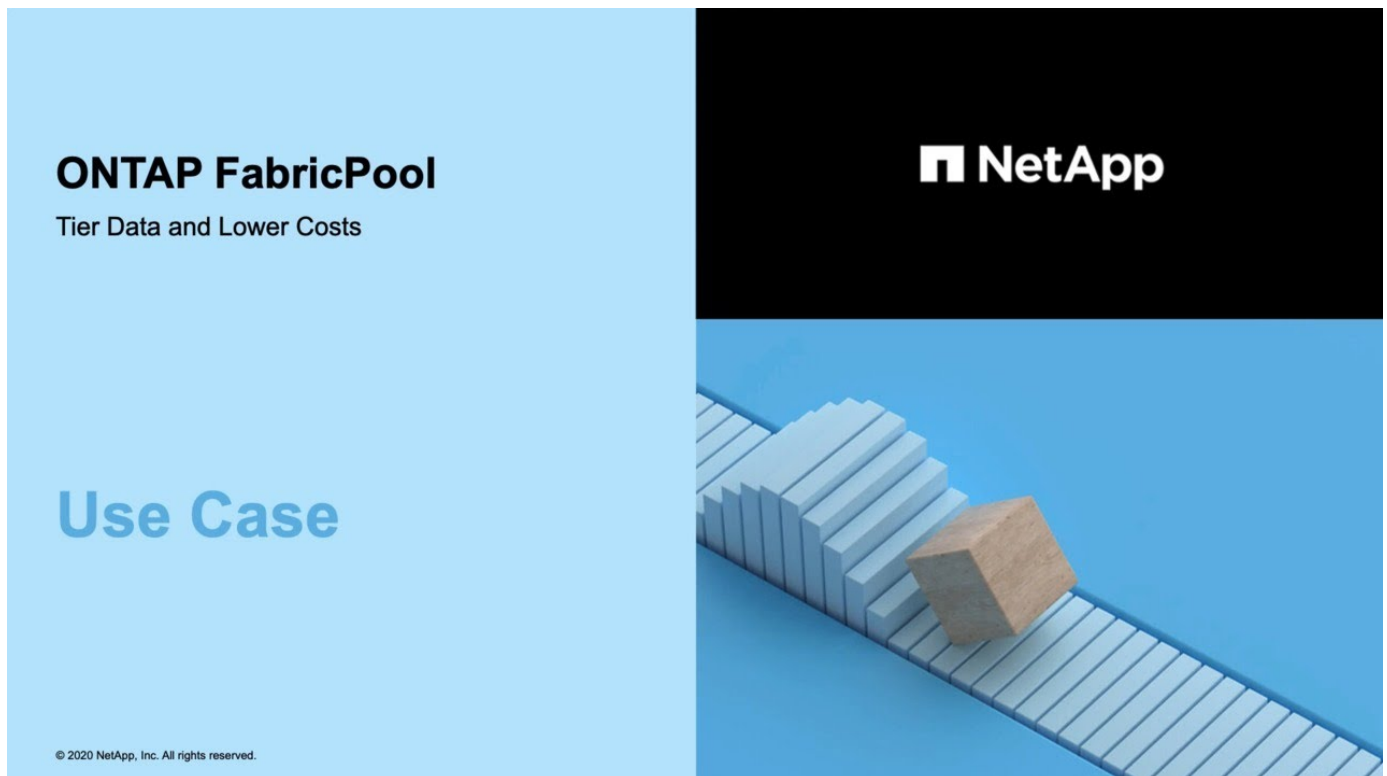
You can use FabricPool to automatically tier data depending on how frequently the data is accessed.

FabricPool is a hybrid storage solution that uses an all flash (all SSD) aggregate as the performance tier and an object store as the cloud tier. Using a FabricPool helps you reduce storage cost without compromising performance, efficiency, or protection.

The cloud tier can be located on NetApp StorageGRID or ONTAP S3 (beginning with ONTAP 9.8), or one of the following service providers:

- Alibaba cloud
- Amazon S3
- Google Cloud
- IBM cloud
- Microsoft Azure Blob Storage

## Tier Data and Lower Costs Use Case video



## Related information

See also the [NetApp Cloud Tiering](#) documentation.



## Benefits of storage tiers by using FabricPool

Configuring an aggregate to use FabricPool enables you to use storage tiers. You can efficiently balance the performance and cost of your storage system, monitor and optimize the space utilization, and perform policy-based data movement between storage tiers.

- You can optimize storage performance and reduce storage cost by storing data in a tier based on whether the data is frequently accessed.

- Frequently accessed (“hot”) data is stored in the *performance tier*.

The performance tier uses high-performance primary storage, such as an all flash (all SSD) aggregate of the storage system.

- Infrequently accessed (“cold”) data is stored in the *cloud tier*, also known as the *capacity tier*.

The cloud tier uses an object store that is less costly and does not require high performance.

- You have the flexibility in specifying the tier in which data should be stored.

You can specify one of the supported tiering policy options at the volume level. The options enable you to efficiently move data across tiers as data becomes hot or cold.

### Types of FabricPool tiering policies

- You can choose one of the supported object stores to use as the cloud tier for FabricPool.
- You can monitor the space utilization in a FabricPool-enabled aggregate.
- You can see how much data in a volume is inactive by using inactive data reporting.
- You can reduce the on-premise footprint of the storage system.

You save physical space when you use a cloud-based object store for the cloud tier.

## Considerations and requirements for using FabricPool

You should familiarize yourself with a few considerations and requirements about using FabricPool.

### General considerations and requirements

- You must be running ONTAP 9.2 at the minimum to use FabricPool.
- You must be running ONTAP 9.4 or later releases for the following FabricPool functionality:
  - The `auto` tiering policy

### Types of FabricPool tiering policies

- Specifying the tiering minimum cooling period
- Inactive data reporting (IDR)
- Using Microsoft Azure Blob Storage for the cloud as the cloud tier for FabricPool

- Using FabricPool with ONTAP Select
- You must be running ONTAP 9.5 or later releases for the following FabricPool functionality:
  - Specifying the tiering fullness threshold
  - Using IBM Cloud Object Storage as the cloud tier for FabricPool
  - NetApp Volume Encryption (NVE) of the cloud tier, enabled by default.
- You must be running ONTAP 9.6 or later releases for the following FabricPool functionality:
  - The `all` tiering policy
  - Inactive data reporting enabled manually on HDD aggregates
  - Inactive data reporting enabled automatically for SSD aggregates when you upgrade to ONTAP 9.6 and at time aggregate is created, except on low end systems with less than 4 CPU, less than 6 GB of RAM, or when WAFL-buffer-cache size is less than 3 GB.

ONTAP monitors system load, and if the load remains high for 4 continuous minutes, IDR is disabled, and is not automatically enabled. You can reenable IDR manually, however, manually enabled IDR is not automatically disabled.

- Using Alibaba Cloud Object Storage as the cloud tier for FabricPool
- Using Google Cloud Platform as the cloud tier for FabricPool
- Volume move without cloud tier data copy
- You must be running ONTAP 9.7 or later releases for the following FabricPool functionality:
  - Non transparent HTTP and HTTPS proxy to provide access to only whitelisted access points, and to provide auditing and reporting capabilities.
  - FabricPool mirroring to tier cold data to two object stores simultaneously
  - FabricPool mirrors on MetroCluster configurations
  - NDMP dump and restore enabled by default on FabricPool attached aggregates.



If the backup application uses a protocol other than NDMP, such as NFS or SMB, all data being backed up in the performance tier becomes hot and can affect tiering of that data to the cloud tier. Non-NDMP reads can cause data migration from the cloud tier back to the performance tier.

### NDMP Backup and Restore Support for FabricPool

- You must be running ONTAP 9.8 or later for the following FabricPool functionality:
  - Cloud migration control to enable you to override the default tiering policy
  - Promoting data to the performance tier
  - FabricPool with SnapLock Enterprise
  - Minimum cooling period maximum of 183 days
  - Object tagging using user-created custom tags
  - FabricPools on HDD platforms and aggregates

HDD FabricPools are supported with SAS, FSAS, BSAS and MSATA disks only on systems with 6 or more CPU cores, including the following models:

- FAS9000
- FAS8700
- FAS8300
- FAS8200
- FAS8080
- FAS8060
- FAS8040
- FAS2750
- FAS2720
- FAS2650
- FAS2620

Check [Hardware Universe](#) for the latest supported models.

- FabricPool is supported on all platforms capable of running ONTAP 9.2 except for the following:
  - FAS8020
  - FAS2554
  - FAS2552
  - FAS2520

- FabricPool supports the following aggregate types:

- On AFF systems, you can use only all flash (all SSD) aggregates for FabricPool.

You cannot use Flash Pool aggregates, which contain both SSDs and HDDs.

- On FAS systems, you can use either all flash (all SSD) or HDD aggregates for FabricPool.
- On Cloud Volumes ONTAP and ONTAP Select, you can use either SSD or HDD aggregates for FabricPool.

However, using SSD aggregates is recommended.

- FabricPool supports using the following object stores as the cloud tier:

- NetApp StorageGRID 10.3 or later
- NetApp ONTAP S3 (ONTAP 9.8 and later)
- Alibaba Cloud Object Storage
- Amazon Web Services Simple Storage Service (AWS S3)
- Google Cloud Storage
- IBM Cloud Object Storage
- Microsoft Azure Blob Storage for the cloud

- The object store “bucket” (container) you plan to use must have already been set up, must have at least 10 GB of storage space, and must not be renamed.
- HA pairs that use FabricPool require intercluster LIFs to communicate with the object store.
- You cannot detach an object store bucket from the FabricPool configuration after it is attached.

- If you use throughput floors (QoS Min), the tiering policy on the volumes must be set to `none` before the aggregate can be attached to FabricPool.

Other tiering policies prevent the aggregate from being attached to FabricPool.

- You should follow the best practice guidelines for using FabricPool in specific scenarios.

[NetApp Technical Report 4598: FabricPool Best Practices in ONTAP 9](#)

### **Additional considerations when using Cloud Volumes ONTAP**

Cloud Volumes ONTAP does not require a FabricPool license, regardless of the object store provider you are using.

### **Additional considerations for tiering data accessed by SAN protocols**

When tiering data that is accessed by SAN protocols, NetApp recommends using private clouds, like StorageGRID, due to connectivity considerations.

### **Functionality or features not supported by FabricPool**

- Object stores with WORM enabled and object versioning enabled.
- Information lifecycle management (ILM) policies that are applied to object store buckets

ILM typically includes various movement and deletion policies. These policies can be disruptive to the data in the cloud tier of FabricPool. Using FabricPool with ILM policies that are configured on object stores can result in data loss.

- 7-Mode data transition using the ONTAP CLI commands or the 7-Mode Transition Tool
- FlexArray Virtualization
- RAID SyncMirror, except in a MetroCluster configuration
- SnapLock volumes when using ONTAP 9.7 and earlier releases
- Tape backup using SMTape for FabricPool-enabled aggregates
- The Auto Balance functionality
- Volumes using a space guarantee other than `none`

FabricPool does not support attaching a cloud tier to an aggregate that contains volumes using a space guarantee other than `none`. For example, a volume using a space guarantee of `volume (-space -guarantee volume)` is not supported.

- Clusters with DP\_Optimized license
- Flash Pool aggregates

### **About FabricPool tiering policies**

FabricPool tiering policies enable you to move data efficiently across tiers as data becomes hot or cold. Understanding the tiering policies helps you select the right policy that suits your storage management needs.

## Types of FabricPool tiering policies

FabricPool tiering policies determine when or whether the user data blocks of a volume in FabricPool are moved to the cloud tier, based on the volume “temperature” of hot (active) or cold (inactive). The volume “temperature” increases when it is accessed frequently and decreases when it is not. Some tiering policies have an associated tiering minimum cooling period, which sets the time that user data in a volume of FabricPool must remain inactive for the data to be considered “cold” and moved to the cloud tier.

The FabricPool tiering policy is specified at the volume level. Four options are available:

- The `snapshot-only` tiering policy (the default) moves user data blocks of the volume Snapshot copies that are not associated with the active file system to the cloud tier.

The tiering minimum cooling period is 2 days. You can modify the default setting for the tiering minimum cooling period with the `-tiering-minimum-cooling-days` parameter in the advanced privilege level of the `volume create` and `volume modify` commands. Valid values are 2 to 183 days using ONTAP 9.8 and later. If you are using a version of ONTAP earlier than 9.8, valid values are 2 to 63 days.

- The `auto` tiering policy, supported only on ONTAP 9.4 and later releases, moves cold user data blocks in both the Snapshot copies and the active file system to the cloud tier.

The default tiering minimum cooling period is 31 days and applies to the entire volume, for both the active file system and the Snapshot copies.

You can modify the default setting for the tiering minimum cooling period with the `-tiering-minimum-cooling-days` parameter in the advanced privilege level of the `volume create` and `volume modify` commands. Valid values are 2 to 183 days.

- The `all` tiering policy, supported only on ONTAP 9.6 and later, moves all user data blocks in both the active file system and Snapshot copies to the cloud tier. It replaces the `backup` tiering policy.

The tiering minimum cooling period does not apply because the data moves the cloud tier as soon as the tiering scan runs, and you cannot modify the setting.

- The `none` tiering policy keeps data of a volume in the performance tier, preventing it from being moved to the cloud tier.

The tiering minimum cooling period does not apply because the data never moves to the cloud tier, and you cannot modify the setting.

The `volume show` command output shows the tiering policy of a volume. A volume that has never been used with FabricPool shows the `none` tiering policy in the output.

## What happens when you modify the tiering policy of a volume in FabricPool

You can modify the tiering policy of a volume by performing a `volume modify` operation. You must understand how changing the tiering policy might affect how long it takes for data to become cold and be moved to the cloud tier.

- Changing the tiering policy from `snapshot-only` or `none` to `auto` causes ONTAP to send user data blocks in the active file system that are already cold to the cloud tier, even if those user data blocks were not previously eligible for the cloud tier.
- Changing the tiering policy to `all` from another policy causes ONTAP to move all user blocks in the active

file system and in the Snapshot copies to the cloud tier the next time the tiering scan runs.

Moving blocks back to the performance tier is not allowed.

- Changing the tiering policy from `auto` to `snapshot-only` or `none` does not cause active file system blocks that are already moved to the cloud tier to be moved back to the performance tier.

Volume reads are needed for the data to be moved back to the performance tier.

- Any time you change the tiering policy on a volume, the tiering minimum cooling period is reset to the default value for the policy.

### What happens to the tiering policy when you move a volume

- Unless you explicitly specify a different tiering policy, a volume retains its original tiering policy when it is moved in and out of a FabricPool-enabled aggregate.

However, the tiering policy takes effect only when the volume is in a FabricPool-enabled aggregate.

- The existing value of the `-tiering-minimum-cooling-days` parameter for a volume moves with the volume unless you specify a different tiering policy for the destination.

If you specify a different tiering policy, then the volume uses the default tiering minimum cooling period for that policy. This is the case whether the destination is FabricPool or not.

- You can move a volume across aggregates and at the same time modify the tiering policy.
- You should pay special attention when a `volume move` operation involves the `auto` tiering policy.

Assuming that both the source and the destination are FabricPool-enabled aggregates, the following table summarizes the outcome of a `volume move` operation that involves policy changes related to `auto`:

When you move a volume that has a tiering policy of...	And you change the tiering policy with the move to...	Then after the volume move...
<code>all</code>	<code>auto</code>	All data is moved to the performance tier.
<code>snapshot-only, none, or auto</code>	<code>auto</code>	Data blocks are moved to the same tier of the destination as they previously were on the source.
<code>auto or all</code>	<code>snapshot-only</code>	All data is moved to the performance tier.
<code>auto</code>	<code>all</code>	All user data is moved to the cloud tier.
<code>snapshot-only, auto or all</code>	<code>none</code>	All data is kept at the performance tier.

## What happens to the tiering policy when you clone a volume

- Beginning with ONTAP 9.8, a clone volume always inherits both the tiering policy and the cloud retrieval policy from the parent volume.

In releases earlier than ONTAP 9.8, a clone inherits the tiering policy from the parent except when the parent has the `all` tiering policy.

- If the parent volume has the `never` cloud retrieval policy, its clone volume must have either the `never` cloud retrieval policy or the `all` tiering policy, and a corresponding cloud retrieval policy `default`.
- The parent volume cloud retrieval policy cannot be changed to `never` unless all its clone volumes have a cloud retrieval policy `never`.

When you clone volumes, keep the following best practices in mind:

- The `-tiering-policy` option and `tiering-minimum-cooling-days` option of the clone only controls the tiering behavior of blocks unique to the clone. Therefore, we recommend using tiering settings on the parent FlexVol that are either move the same amount of data or move less data than any of the clones
- The cloud retrieval policy on the parent FlexVol should either move the same amount of data or should move more data than the retrieval policy of any of the clones

## How tiering policies work with cloud migration

FabricPool cloud data retrieval is controlled by tiering policies that determine data retrieval from the cloud tier to performance tier based on the read pattern. Read patterns can be either sequential or random.

The following table lists the tiering policies and the cloud data retrieval rules for each policy.

Tiering policy	Retrieval behavior
none	Sequential and random reads
snapshot-only	Sequential and random reads
auto	Random reads
all	No data retrieval

Beginning with ONTAP 9.8, the cloud migration control `cloud-retrieval-policy` option overrides the default cloud migration or retrieval behavior controlled by the tiering policy.

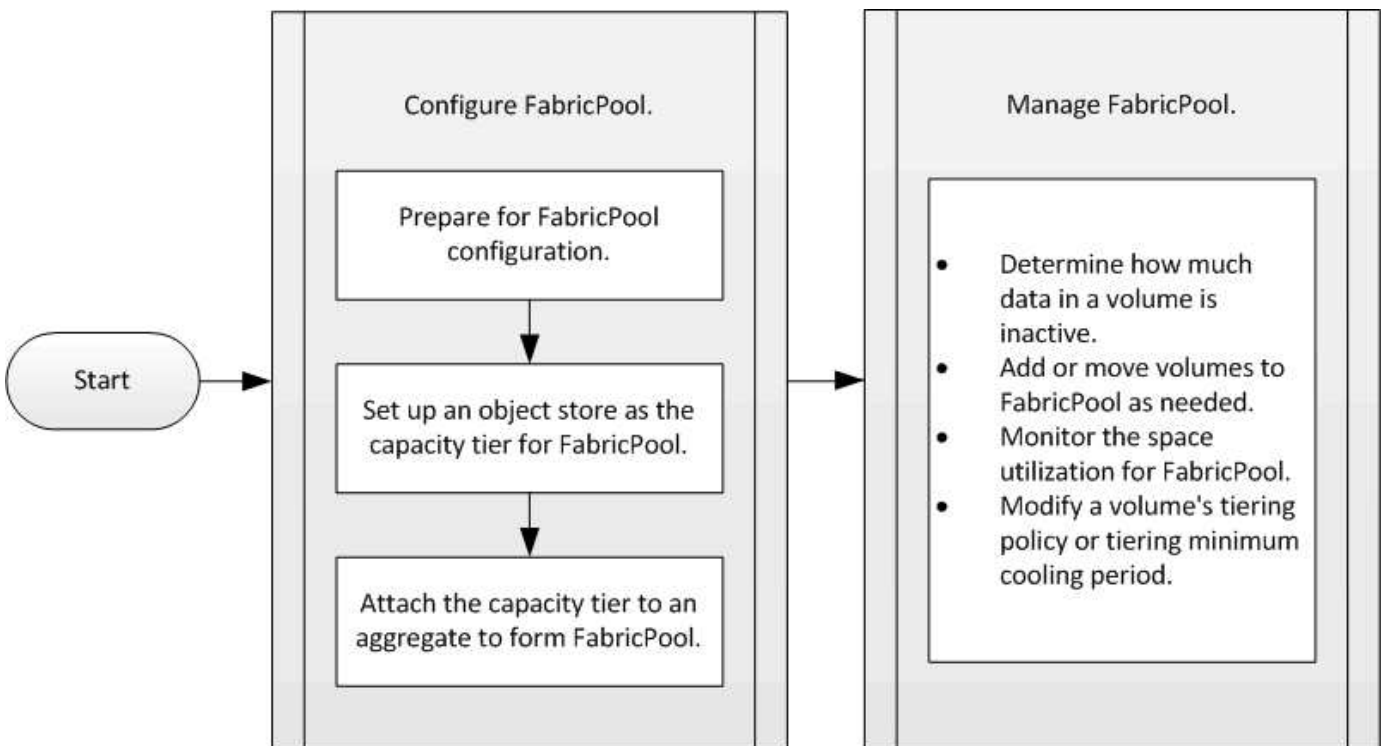
The following table lists the supported cloud retrieval policies and their retrieval behavior.

Cloud retrieval policy	Retrieval behavior
default	Tiering policy decides what data should be pulled back, so there is no change to cloud data retrieval with "default," <code>cloud-retrieval-policy</code> . This policy is the default value for any volume regardless of the hosted aggregate type.

on-read	All client-driven data read is pulled from cloud tier to performance tier.
never	No client-driven data is pulled from cloud tier to performance tier
promote	<ul style="list-style-type: none"> <li>• For tiering policy “none,” all cloud data is pulled from the cloud tier to the performance tier</li> <li>• For tiering policy “snapshot-only,” AFS data is pulled.</li> </ul>

## FabricPool management workflow

You can use the FabricPool workflow diagram to help you plan the configuration and management tasks.



## Configure FabricPool

### Prepare for FabricPool configuration

#### Prepare for FabricPool configuration overview

Configuring FabricPool helps you manage which storage tier (the local performance tier or the cloud tier) data should be stored based on whether the data is frequently accessed.

The preparation required for FabricPool configuration depends on the object store you use as the cloud tier.



## Add a connection to the cloud

Beginning with ONTAP 9.9.0, you can use System Manager to add a connection to the cloud.

You start by using NetApp Cloud Insights to configure a collector. During the configuration process, you copy a pairing code that is generated by Cloud Insights, and then you log on to a cluster using System Manager. There, you add a cloud connection using that pairing code. The rest of the process is completed in Cloud Insights.

### Steps

1. In Cloud Insights, during the process to configure a collector, copy the generated pairing code.
2. Using System Manager with ONTAP 9.9.0 or later, log on to the cluster.
3. Go to **Cluster > Settings**.
4. In the Cloud Connections section, select **Add** to add a connection.
5. Enter a name for the connection, and paste the pairing code in the space provided.
6. Select **Add**.
7. Return to Cloud Insights to complete the configuration of the collector.

For additional information about Cloud Insights, refer to [Cloud Insights documentation](#).

## Install a FabricPool license

The FabricPool license you might have used in the past is changing and is being retained only for configurations that aren't supported within Cloud Manager. Starting August 21, 2021, new Cloud Tiering BYOL licensing was introduced for tiering configurations that are supported within Cloud Manager using the Cloud Tiering service.

[Learn more about the new Cloud Tiering BYOL licensing.](#)

Configurations that are supported by Cloud Manager must use the Digital Wallet page in Cloud Manager to license tiering for ONTAP clusters. This requires you to set up a Cloud Manager account and set up tiering for the particular object storage provider you plan to use. Cloud Manager currently supports tiering to the following object storage: Amazon S3, Azure Blob storage, Google Cloud Storage, S3-compatible object storage, and StorageGRID.

[Learn more about the Cloud tiering service.](#)

You can download and activate a FabricPool license using System Manager if you have one of the configurations that is not supported within Cloud Manager:

- ONTAP installations in Dark Sites
- ONTAP clusters that are tiering data to IBM Cloud Object Storage or Alibaba Cloud Object Storage

The FabricPool license is a cluster-wide license. It includes an entitled usage limit that you purchase for object storage that is associated with FabricPool in the cluster. The usage across the cluster must not exceed the capacity of the entitled usage limit. If you need to increase the usage limit of the license, you should contact your sales representative.


FabricPool licenses are available in perpetual or term-based, 1- or 3- year, formats.

A term-based FabricPool license with 10 TB of free capacity is available for first time FabricPool orders for existing clusters configurations not supported within Cloud Manager. Free capacity is not available with perpetual licenses.

A license is not required if you use NetApp StorageGRID or ONTAP S3 for the cloud tier. Cloud Volumes ONTAP does not require a FabricPool license, regardless of the provider you are using.

This task is supported only by uploading the license file to the cluster using System Manager.

### Steps

1. Download the NetApp License File (NLF) for the FabricPool license from the [NetApp Support Site](#).
2. Perform the following actions using System Manager to upload the FabricPool license to the cluster:
  - a. In the **Cluster > Settings** pane, on the **Licenses** card, click .
  - b. On the **License** page, click **+ Add**.
  - c. In the **Add License** dialog box, click **Browse** to select the NLF you downloaded, and then click **Add** to upload the file to the cluster.

### Related information

[ONTAP FabricPool \(FP\) Licensing Overview](#)

[NetApp Software License Search](#)

[NetApp TechComm TV: FabricPool playlist](#)

### Install a CA certificate if you use StorageGRID

Unless you plan to disable certificate checking for StorageGRID, you must install a StorageGRID CA certificate on the cluster so that ONTAP can authenticate with StorageGRID as the object store for FabricPool.

### About this task

ONTAP 9.4 and later releases enable you to disable certificate checking for StorageGRID.

### Steps

1. Contact your StorageGRID administrator to obtain the StorageGRID system's CA certificate.
2. Use the `security certificate install` command with the `-type server-ca` parameter to install the StorageGRID CA certificate on the cluster.

The fully qualified domain name (FQDN) you enter must match the custom common name on the StorageGRID CA certificate.

### Update an expired certificate

To update an expired certificate, the best practice is to use a trusted CA to generate the new server certificate. In addition, you should ensure that the certificate is updated on the StorageGRID server and on the ONTAP cluster at the same time to keep any downtime to a minimum.

### Related information

[StorageGRID Resources](#)

## Install a CA certificate if you use ONTAP S3

Unless you plan to disable certificate checking for ONTAP S3, you must install a ONTAP S3 CA certificate on the cluster so that ONTAP can authenticate with ONTAP S3 as the object store for FabricPool.

### Steps

1. Obtain the ONTAP S3 system's CA certificate.
2. Use the `security certificate install` command with the `-type server-ca` parameter to install the ONTAP S3 CA certificate on the cluster.

The fully qualified domain name (FQDN) you enter must match the custom common name on the ONTAP S3 CA certificate.

## Update an expired certificate

To update an expired certificate, the best practice is to use a trusted CA to generate the new server certificate. In addition, you should ensure that the certificate is updated on the ONTAP S3 server and on the ONTAP cluster at the same time to keep any downtime to a minimum.

### Related information

[S3 configuration](#)

## Set up an object store as the cloud tier for FabricPool

### Set up an object store as the cloud tier for FabricPool overview

Setting up FabricPool involves specifying the configuration information of the object store (StorageGRID, ONTAP S3, Alibaba Cloud Object Storage, AWS S3, Google Cloud Storage Platform, IBM Cloud Object Storage, or Microsoft Azure Blob Storage for the cloud) that you plan to use as the cloud tier for FabricPool.

### Set up StorageGRID as the cloud tier

If you are running ONTAP 9.2 or later, you can set up StorageGRID as the cloud tier for FabricPool. When tiering data that is accessed by SAN protocols, NetApp recommends using private clouds, like StorageGRID, due to connectivity considerations.

### Considerations for using StorageGRID with FabricPool

- You need to install a CA certificate for StorageGRID, unless you explicitly disable certificate checking.
- You must not enable StorageGRID object versioning on the object store bucket.
- A FabricPool license is not required.
- If a StorageGRID node is deployed in a virtual machine with storage assigned from a NetApp AFF system, confirm that the volume does not have a FabricPool tiering policy enabled.

Disabling FabricPool tiering for volumes used with StorageGRID nodes simplifies troubleshooting and storage operations.



Never use FabricPool to tier any data related to StorageGRID back to StorageGRID itself. Tiering StorageGRID data back to StorageGRID increases troubleshooting and operational complexity.

### **About this task**

Load balancing is enabled for StorageGRID in ONTAP 9.8 and later. When the server's hostname resolves to more than one IP address, ONTAP establishes client connections with all the IP addresses returned (up to a maximum of 16 IP addresses). The IP addresses are picked up in a round-robin method when connections are established.

### **Procedures**

You can set up StorageGRID as the cloud tier for FabricPool with ONTAP System Manager or the ONTAP CLI.

## System Manager

1. Click **Storage > Tiers > Add Cloud Tier** and select StorageGRID as the object store provider.
2. Complete the requested information.
3. If you want to create a cloud mirror, click **Add as FabricPool Mirror**.

A FabricPool mirror provides a method for you to seamlessly replace a data store, and it helps to ensure that your data is available in the event of disaster.

## CLI

1. Specify the StorageGRID configuration information by using the `storage aggregate object-store config create` command with the `-provider-type SGWS` parameter.

- The `storage aggregate object-store config create` command fails if ONTAP cannot access StorageGRID with the provided information.
- You use the `-access-key` parameter to specify the access key for authorizing requests to the StorageGRID object store.
- You use the `-secret-password` parameter to specify the password (secret access key) for authenticating requests to the StorageGRID object store.
- If the StorageGRID password is changed, you should update the corresponding password stored in ONTAP immediately.

Doing so enables ONTAP to access the data in StorageGRID without interruption.

- Setting the `-is-certificate-validation-enabled` parameter to `false` disables certificate checking for StorageGRID.

```
cluster1::> storage aggregate object-store config create
-object-store-name mySGWS -provider-type SGWS -server mySGWSserver
-container-name mySGWScontainer -access-key mySGWSkey
-secret-password mySGWSpass
```

2. Display and verify the StorageGRID configuration information by using the `storage aggregate object-store config show` command.

The `storage aggregate object-store config modify` command enables you to modify the StorageGRID configuration information for FabricPool.

## Set up ONTAP S3 as the cloud tier

If you are running ONTAP 9.8 or later, you can set up ONTAP S3 as the cloud tier for FabricPool.

### What you'll need

You must have the ONTAP S3 server name and the IP address of its associated LIFs on the remote cluster.

There must be intercluster LIFs on both local and remote clusters.

## Creating intercluster LIFs for remote FabricPool tiering

### About this task

Load balancing is enabled for ONTAP S3 servers in ONTAP 9.8 and later. When the server's hostname resolves to more than one IP address, ONTAP establishes client connections with all the IP addresses returned (up to a maximum of 16 IP addresses). The IP addresses are picked up in a round-robin method when connections are established.

### Procedures

You can set up ONTAP S3 as the cloud tier for FabricPool with ONTAP System Manager or the ONTAP CLI.

## System Manager

1. Click **Storage > Tiers > Add Cloud Tier** and select ONTAP S3 as the object store provider.
2. Complete the requested information.
3. If you want to create a cloud mirror, click **Add as FabricPool Mirror**.

A FabricPool mirror provides a method for you to seamlessly replace a data store, and it helps to ensure that your data is available in the event of disaster.

## CLI

1. Add entries for the S3 server and LIFs to your DNS server.

Option	Description
<b>If you use an external DNS server</b>	Give the S3 server name and IP addresses to the DNS server administrator.
<b>If you use your local system's DNS hosts table</b>	Enter the following command:  <pre>dns host create -vserver svm_name -address ip_address -hostname s3_server_name</pre>

2. Specify the ONTAP S3 configuration information by using the `storage aggregate object-store config create` command with the `-provider-type ONTAP_S3` parameter.

- The `storage aggregate object-store config create` command fails if the local ONTAP system cannot access the ONTAP S3 server with the information provided.
- You use the `-access-key` parameter to specify the access key for authorizing requests to the ONTAP S3 server.
- You use the `-secret-password` parameter to specify the password (secret access key) for authenticating requests to the ONTAP S3 server.
- If the ONTAP S3 server password is changed, you should immediately update the corresponding password stored in the local ONTAP system.

Doing so enables access to the data in the ONTAP S3 object store without interruption.

- Setting the `-is-certificate-validation-enabled` parameter to `false` disables certificate checking for ONTAP S3.

```
cluster1::> storage aggregate object-store config create  
-object-store-name myS3 -provider-type ONTAP_S3 -server myS3server  
-container-name myS3container -access-key myS3key  
-secret-password myS3pass
```

3. Display and verify the ONTAP\_S3 configuration information by using the `storage aggregate object-store config show` command.

The `storage aggregate object-store config modify` command enables you to modify the `ONTAP_S3` configuration information for FabricPool.

## Set up Alibaba Cloud Object Storage as the cloud tier

If you are running ONTAP 9.6 or later, you can set up Alibaba Cloud Object Storage as the cloud tier for FabricPool.

### Considerations for using Alibaba Cloud Object Storage with FabricPool

- You might need a FabricPool license.

Newly ordered AFF systems come with 10 TB of free capacity for using FabricPool. If you need additional capacity on an AFF system, if you use Alibaba Cloud Object Storage on a non-AFF system, or if you upgrade from an existing cluster, you need a FabricPool license.

- On AFF and FAS systems and ONTAP Select, FabricPool supports the following Alibaba Object Storage Service classes:
  - Alibaba Object Storage Service Standard
  - Alibaba Object Storage Service Infrequent Access

[Alibaba Cloud: Introduction to storage classes](#)

Contact your NetApp sales representative for information about storage classes not listed.

### Steps

1. Specify the Alibaba Cloud Object Storage configuration information by using the `storage aggregate object-store config create` command with the `-provider-type AliCloud` parameter.
  - The `storage aggregate object-store config create` command fails if ONTAP cannot access Alibaba Cloud Object Storage with the provided information.
  - You use the `-access-key` parameter to specify the access key for authorizing requests to the Alibaba Cloud Object Storage object store.
  - If the Alibaba Cloud Object Storage password is changed, you should update the corresponding password stored in ONTAP immediately.

Doing so enables ONTAP to access the data in Alibaba Cloud Object Storage without interruption.

```
storage aggregate object-store config create my_ali_oss_store_1
-provider-type AliCloud -server oss-us-east-1.aliyuncs.com
-container-name my-ali-oss-bucket -access-key DXJRXHPXHYXA9X31X3JX
```

2. Display and verify the Alibaba Cloud Object Storage configuration information by using the `storage aggregate object-store config show` command.

The `storage aggregate object-store config modify` command enables you to modify the Alibaba Cloud Object Storage configuration information for FabricPool.



## Set up AWS S3 as the cloud tier

If you are running ONTAP 9.2 or later, you can set up AWS S3 as the cloud tier for FabricPool. If you are running ONTAP 9.5 or later, you can set up AWS Commercial Cloud Services (C2S) for FabricPool.

### Considerations for using AWS S3 with FabricPool

- You might need a FabricPool license.
  - Newly ordered AFF systems come with 10 TB of free capacity for using FabricPool.

If you need additional capacity on an AFF system, if you use AWS S3 on a non-AFF system, or if you upgrade from an existing cluster, you need a FabricPool license.

If you order FabricPool for the first time for an existing cluster, a FabricPool license with 10 TB of free capacity is available.

- The LIF that ONTAP uses to connect with the AWS S3 object server must be on a 10 Gbps port.
- On AFF and FAS systems and ONTAP Select, FabricPool supports the following Amazon S3 storage classes:
  - Amazon S3 Standard
  - Amazon S3 Standard - Infrequent Access (Standard - IA)
  - Amazon S3 One Zone - Infrequent Access (One Zone - IA)
  - Amazon S3 Intelligent-Tiering
  - Amazon Commercial Cloud Services

[Amazon Web Services \(AWS\) Documentation: Amazon S3 Storage Classes](#)

Contact your sales representative for information about storage classes not listed.

- On Cloud Volumes ONTAP, FabricPool supports tiering from General Purpose SSD (gp2) and Throughput Optimized HDD (st1) volumes of Amazon Elastic Block Store (EBS).

### Steps

1. Specify the AWS S3 configuration information by using the `storage aggregate object-store config create` command with the `-provider-type AWS_S3` parameter.

- You use the `-auth-type CAP` parameter to obtain credentials for C2S access.

When you use the `-auth-type CAP` parameter, you must use the `-cap-url` parameter to specify the full URL to request temporary credentials for C2S access.

- The `storage aggregate object-store config create` command fails if ONTAP cannot access AWS S3 with the provided information.
- You use the `-access-key` parameter to specify the access key for authorizing requests to the AWS S3 object store.
- You use the `-secret-password` parameter to specify the password (secret access key) for authenticating requests to the AWS S3 object store.
- If the AWS S3 password is changed, you should update the corresponding password stored in ONTAP immediately.

Doing so enables ONTAP to access the data in AWS S3 without interruption.

```
cluster1::> storage aggregate object-store config create
-object-store-name my_aws_store -provider-type AWS_S3
-server s3.amazonaws.com -container-name my-aws-bucket
-access-key DXJRXHPXHYXA9X31X3JX
```

```
cluster1::> storage aggregate object-store config create -object
-store-name my_c2s_store -provider-type AWS_S3 -auth-type CAP -cap
-url
https://123.45.67.89/api/v1/credentials?agency=XYZ&mission=TESTACCT&r
ole=S3FULLACCESS -server my-c2s-s3server-fqdn -container my-c2s-s3-
bucket
```

2. Display and verify the AWS S3 configuration information by using the `storage aggregate object-store config show` command.

The `storage aggregate object-store config modify` command enables you to modify the AWS S3 configuration information for FabricPool.

### Set up AWS S3 as the cloud tier

If you are running ONTAP 9.2 or later, you can set up AWS S3 as the cloud tier for FabricPool. If you are running ONTAP 9.5 or later, you can set up AWS Commercial Cloud Services (C2S) for FabricPool.

#### Considerations for using AWS S3 with FabricPool

- You might need a FabricPool license.
  - Newly ordered AFF systems come with 10 TB of free capacity for using FabricPool.

If you need additional capacity on an AFF system, if you use AWS S3 on a non-AFF system, or if you upgrade from an existing cluster, you need a FabricPool license.

If you order FabricPool for the first time for an existing cluster, a FabricPool license with 10 TB of free capacity is available.

- The LIF that ONTAP uses to connect with the AWS S3 object server must be on a 10 Gbps port.
- On AFF and FAS systems and ONTAP Select, FabricPool supports the following Amazon S3 storage classes:
  - Amazon S3 Standard
  - Amazon S3 Standard - Infrequent Access (Standard - IA)
  - Amazon S3 One Zone - Infrequent Access (One Zone - IA)
  - Amazon S3 Intelligent-Tiering
  - Amazon Commercial Cloud Services

Contact your sales representative for information about storage classes not listed.

- On Cloud Volumes ONTAP, FabricPool supports tiering from General Purpose SSD (gp2) and Throughput Optimized HDD (st1) volumes of Amazon Elastic Block Store (EBS).

## Steps

1. Specify the AWS S3 configuration information by using the `storage aggregate object-store config create` command with the `-provider-type AWS_S3` parameter.

- You use the `-auth-type CAP` parameter to obtain credentials for C2S access.

When you use the `-auth-type CAP` parameter, you must use the `-cap-url` parameter to specify the full URL to request temporary credentials for C2S access.

- The `storage aggregate object-store config create` command fails if ONTAP cannot access AWS S3 with the provided information.
- You use the `-access-key` parameter to specify the access key for authorizing requests to the AWS S3 object store.
- You use the `-secret-password` parameter to specify the password (secret access key) for authenticating requests to the AWS S3 object store.
- If the AWS S3 password is changed, you should update the corresponding password stored in ONTAP immediately.

Doing so enables ONTAP to access the data in AWS S3 without interruption.

```
cluster1::> storage aggregate object-store config create
-object-store-name my_aws_store -provider-type AWS_S3
-server s3.amazonaws.com -container-name my-aws-bucket
-access-key DXJRXHPXHYXA9X31X3JX
```

```
cluster1::> storage aggregate object-store config create -object
-store-name my_c2s_store -provider-type AWS_S3 -auth-type CAP -cap
-url
https://123.45.67.89/api/v1/credentials?agency=XYZ&mission=TESTACCT&r
ole=S3FULLACCESS -server my-c2s-s3server-fqdn -container my-c2s-s3-
bucket
```

2. Display and verify the AWS S3 configuration information by using the `storage aggregate object-store config show` command.

The `storage aggregate object-store config modify` command enables you to modify the AWS S3 configuration information for FabricPool.

## Set up Google Cloud Storage as the cloud tier

If you are running ONTAP 9.6 or later, you can set up Google Cloud Storage as the cloud tier for FabricPool.

### Additional considerations for using Google Cloud Storage with FabricPool

- You might need a FabricPool license.

Newly ordered AFF systems come with 10 TB of free capacity for using FabricPool. If you need additional capacity on an AFF system, if you use Google Cloud Storage on a non-AFF system, or if you upgrade from an existing cluster, you need a FabricPool license.

- The LIF that ONTAP uses to connect with the Google Cloud Storage object server must be on a 10 Gbps port.
- On AFF and FAS systems and ONTAP Select, FabricPool supports the following Google Cloud Object storage classes:
  - Google Cloud Multi-Regional
  - Google Cloud Regional
  - Google Cloud Nearline
  - Google Cloud Coldline

[Google Cloud: Storage Classes](#)

### Steps

1. Specify the Google Cloud Storage configuration information by using the `storage aggregate object-store config create` command with the `-provider-type GoogleCloud` parameter.
  - The `storage aggregate object-store config create` command fails if ONTAP cannot access Google Cloud Storage with the provided information.
  - You use the `-access-key` parameter to specify the access key for authorizing requests to the Google Cloud Storage object store.
  - If the Google Cloud Storage password is changed, you should update the corresponding password stored in ONTAP immediately.

Doing so enables ONTAP to access the data in Google Cloud Storage without interruption.

```
storage aggregate object-store config create my_gcp_store_1 -provider
-type GoogleCloud -container-name my-gcp-bucket1 -access-key
GOOGAUZZUV2USCFGHGQ511I8
```

2. Display and verify the Google Cloud Storage configuration information by using the `storage aggregate object-store config show` command.

The `storage aggregate object-store config modify` command enables you to modify the Google Cloud Storage configuration information for FabricPool.

## Set up IBM Cloud Object Storage as the cloud tier

If you are running ONTAP 9.5 or later, you can set up IBM Cloud Object Storage as the cloud tier for FabricPool.

### Considerations for using IBM Cloud Object Storage with FabricPool

- You might need a FabricPool license.

Newly ordered AFF systems come with 10 TB of free capacity for using FabricPool. If you need additional capacity on an AFF system, if you use IBM Cloud Object Storage on a non-AFF system, or if you upgrade from an existing cluster, you need a FabricPool license.

If you order FabricPool for the first time for an existing cluster, a FabricPool license with 10 TB of free capacity is available.

- The LIF that ONTAP uses to connect with the IBM Cloud object server must be on a 10 Gbps port.

### Steps

1. Specify the IBM Cloud Object Storage configuration information by using the `storage aggregate object-store config create` command with the `-provider-type IBM_COS` parameter.
  - The `storage aggregate object-store config create` command fails if ONTAP cannot access IBM Cloud Object Storage with the provided information.
  - You use the `-access-key` parameter to specify the access key for authorizing requests to the IBM Cloud Object Storage object store.
  - You use the `-secret-password` parameter to specify the password (secret access key) for authenticating requests to the IBM Cloud Object Storage object store.
  - If the IBM Cloud Object Storage password is changed, you should update the corresponding password stored in ONTAP immediately.

Doing so enables ONTAP to access the data in IBM Cloud Object Storage without interruption.

```
storage aggregate object-store config create
-object-store-name MyIBM -provider-type IBM_COS
-server s3.us-east.objectstorage.softlayer.net
-container-name my-ibm-cos-bucket -access-key DXJRXHPXHYXA9X31X3JX
```

2. Display and verify the IBM Cloud Object Storage configuration information by using the `storage aggregate object-store config show` command.

The `storage aggregate object-store config modify` command enables you to modify the IBM Cloud Object Storage configuration information for FabricPool.

## Set up Azure Blob Storage for the cloud as the cloud tier

If you are running ONTAP 9.4 or later, you can set up Azure Blob Storage for the cloud as the cloud tier for FabricPool.

### Considerations for using Microsoft Azure Blob Storage with FabricPool

- You might need a FabricPool license.

Newly ordered AFF systems come with 10 TB of free capacity for using FabricPool. If you need additional capacity on an AFF system, if you use Azure Blob Storage on a non-AFF system, or if you upgrade from an existing cluster, you need a FabricPool license.

If you order FabricPool for the first time for an existing cluster, a FabricPool license with 10 TB of free capacity is available.

- A FabricPool license is not required if you are using Azure Blob Storage with Cloud Volumes ONTAP.
- The LIF that ONTAP uses to connect with the Azure Blob Storage object server must be on a 10 Gbps port.
- FabricPool currently does not support Azure Stack, which is on-premises Azure services.
- At the account level in Microsoft Azure Blob Storage, FabricPool supports only hot and cool storage tiers.

FabricPool does not support blob-level tiering. It also does not support tiering to Azure's archive storage tier.

### About this task

FabricPool currently does not support Azure Stack, which is on-premises Azure services.

### Steps

1. Specify the Azure Blob Storage configuration information by using the `storage aggregate object-store config create` command with the `-provider-type Azure_Cloud` parameter.
  - The `storage aggregate object-store config create` command fails if ONTAP cannot access Azure Blob Storage with the provided information.
  - You use the `-azure-account` parameter to specify the Azure Blob Storage account.
  - You use the `-azure-private-key` parameter to specify the access key for authenticating requests to Azure Blob Storage.
  - If the Azure Blob Storage password is changed, you should update the corresponding password stored in ONTAP immediately.

Doing so enables ONTAP to access the data in Azure Blob Storage without interruption.

```
cluster1::> storage aggregate object-store config create
-object-store-name MyAzure -provider-type Azure_Cloud
-server blob.core.windows.net -container-name myAzureContainer
-azure-account myAzureAcct -azure-private-key myAzureKey
```

2. Display and verify the Azure Blob Storage configuration information by using the `storage aggregate object-store config show` command.

The `storage aggregate object-store config modify` command enables you to modify the Azure Blob Storage configuration information for FabricPool.

## Set up object stores for FabricPool in a MetroCluster configuration

If you are running ONTAP 9.7 or later, you can set up a mirrored FabricPool on a MetroCluster configuration to tier cold data to object stores in two different fault zones.

### What you'll need

- The MetroCluster configuration is set up and properly configured.
- Two object stores are set up on the appropriate MetroCluster sites.
- Containers are configured on each of the object stores.
- IP spaces are created or identified on the two MetroCluster configurations and their names match.

### About this task

- FabricPool in MetroCluster requires that the underlying mirrored aggregate and the associated object store configuration must be owned by the same MetroCluster configuration.
- You cannot attach an aggregate to an object store that is created in the remote MetroCluster site.
- You must create object store configurations on the MetroCluster configuration that owns the aggregate.

### Step

1. Specify the object store configuration information on each MetroCluster site by using the `storage object-store config create` command.

In this example, FabricPool is required on only one cluster in the MetroCluster configuration. Two object store configurations are created for that cluster, one for each object store bucket.

```
storage aggregate
  object-store config create -object-store-name mccl-ostore-config-s1
-provider-type SGWS -server
  <SGWS-server-1> -container-name <SGWS-bucket-1> -access-key <key>
-secret-password <password> -encrypt
  <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
ipspace
  <IPSpace>
```

```
storage aggregate object-store config create -object-store-name mccl-
ostore-config-s2
  -provider-type SGWS -server <SGWS-server-2> -container-name <SGWS-
bucket-2> -access-key <key> -secret-password <password> -encrypt
<true|false> -provider <provider-type>
  -is-ssl-enabled <true|false> ipspace <IPSpace>
```

This example sets up FabricPool on the second cluster in the MetroCluster configuration.

```
storage aggregate
  object-store config create -object-store-name mcc2-ostore-config-s1
  -provider-type SGWS -server
    <SGWS-server-1> -container-name <SGWS-bucket-3> -access-key <key>
  -secret-password <password> -encrypt
    <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
  ipspace
    <IPSpace>
```

```
storage aggregate
  object-store config create -object-store-name mcc2-ostore-config-s2
  -provider-type SGWS -server
    <SGWS-server-2> -container-name <SGWS-bucket-4> -access-key <key>
  -secret-password <password> -encrypt
    <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
  ipspace
    <IPSpace>
```

#### **Attach the cloud tier to a local tier (aggregate)**

After setting up an object store as the cloud tier, you specify the local tier (aggregate) to use by attaching it to FabricPool. In ONTAP 9.5 and later, you can also attach local tiers (aggregates) that contain qualified FlexGroup volume constituents.

#### **What you'll need**

When you use the ONTAP CLI to set up an aggregate for FabricPool, the aggregate must already exist.




When you use System Manager to set up a local tier for FabricPool, you can create the local tier and set it up to use for FabricPool at the same time.

#### **Procedures**

You can attach a local tier (aggregate) to a FabricPool object store with ONTAP System Manager or the ONTAP CLI.



## System Manager

1. Navigate to **Storage > Tiers**, select a cloud tier, then click .
2. Select **Attach local tiers**.
3. Under **Add as Primary** verify that the volumes are eligible to attach.
4. If necessary, select **Convert volumes to thin provisioned**.
5. Click **Save**.

## CLI

### To attach an object store to an aggregate with the CLI:

1. **Optional:** To see how much data in a volume is inactive, follow the steps in [Determining how much data in a volume is inactive by using inactive data reporting](#).

Seeing how much data in a volume is inactive can help you decide which aggregate to use for FabricPool.

2. Attach the object store to an aggregate by using the `storage aggregate object-store attach` command.

If the aggregate has never been used with FabricPool and it contains existing volumes, then the volumes are assigned the default `snapshot-only` tiering policy.

```
cluster1::> storage aggregate object-store attach -aggregate myaggr
-object-store-name Amazon01B1
```

You can use the `allow-flexgroup true` option to attach aggregates that contain FlexGroup volume constituents.

3. Display the object store information and verify that the attached object store is available by using the `storage aggregate object-store show` command.

```
cluster1::> storage aggregate object-store show

Aggregate      Object Store Name      Availability State
-----      -
myaggr        Amazon01B1             available
```

## Tier data to local bucket


Beginning with ONTAP 9.8, you can tier data to local object storage using ONTAP S3.

Tiering data to a local bucket provides a simple alternative to moving data to a different local tier. This procedure uses an existing bucket on the local cluster, or you can let ONTAP automatically create a new storage VM and a new bucket.

Keep in mind that once you attach to a local tier (aggregate) the cloud tier cannot be unattached.

An S3 license is required for this workflow, which creates a new S3 server and new bucket, or uses existing ones. A FabricPool license is not required for this workflow.

### Step

1. Tier data to a local bucket: click **Tiers**, select a tier, then click .
2. If necessary, enable thin provisioning.
3. Choose an existing tier or create a new one.
4. If necessary, edit the existing tiering policy.

## Manage FabricPool

### Manage FabricPool overview

To help you with your storage tiering needs, ONTAP enables you to display how much data in a volume is inactive, add or move volumes to FabricPool, monitor the space utilization for FabricPool, or modify a volume's tiering policy or tiering minimum cooling period.

### Determine how much data in a volume is inactive by using inactive data reporting

Seeing how much data in a volume is inactive enables you to make good use of storage tiers. Information in inactive data reporting helps you decide which aggregate to use for FabricPool, whether to move a volume in to or out of FabricPool, or whether to modify the tiering policy of a volume.

### What you'll need

You must be running ONTAP 9.4 or later to use the inactive data reporting functionality.

### About this task

- Inactive data reporting is not supported on some aggregates.

You cannot enable inactive data reporting when FabricPool cannot be enabled, including the following instances:


- Root aggregates
- MetroCluster aggregates running ONTAP versions earlier than 9.7
- Flash Pool (hybrid aggregates, or SnapLock aggregates)
- Inactive data reporting is enabled by default on aggregates where any volumes have adaptive compression enabled.
- Inactive data reporting is enabled by default on all SSD aggregates in ONTAP 9.6.
- Inactive data reporting is enabled by default on FabricPool aggregate in ONTAP 9.4 and ONTAP 9.5.
- You can enable inactive data reporting on non-FabricPool aggregates using the ONTAP CLI, including HDD aggregates, beginning with ONTAP 9.6.

### Procedure

You can determine how much data is inactive with ONTAP System Manager or the ONTAP CLI.

## System Manager

1. Choose one of the following options:

- When you have existing HDD aggregates, navigate to **Storage > Tiers** and click  for the aggregate on which you want to enable inactive data reporting.
- When no cloud tiers are configured, navigate to **Dashboard** and click the **Enable inactive data reporting** link under **Capacity**.

## CLI

**To enable inactive data reporting with the CLI:**

1. If the aggregate for which you want to see inactive data reporting is not used in FabricPool, enable inactive data reporting for the aggregate by using the `storage aggregate modify` command with the `-is-inactive-data-reporting-enabled true` parameter.

```
cluster1::> storage aggregate modify -aggregate aggr1 -is-inactive
-data-reporting-enabled true
```

You need to explicitly enable the inactive data reporting functionality on an aggregate that is not used for FabricPool.

You cannot and do not need to enable inactive data reporting on a FabricPool-enabled aggregate because the aggregate already comes with inactive data reporting. The `-is-inactive-data-reporting-enabled` parameter does not work on FabricPool-enabled aggregates.

The `-fields is-inactive-data-reporting-enabled` parameter of the `storage aggregate show` command shows whether inactive data reporting is enabled on an aggregate.

2. To display how much data is inactive on a volume, use the `volume show` command with the `-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent` parameter.

```
cluster1::> volume show -fields performance-tier-inactive-user-
data,performance-tier-inactive-user-data-percent

vserver volume performance-tier-inactive-user-data performance-tier-
inactive-user-data-percent
-----
-----
vsim1   vol0   0B           0%
vs1     vs1rv1 0B           0%
vs1     vv1     10.34MB      0%
vs1     vv2     10.38MB      0%
4 entries were displayed.
```

- The `performance-tier-inactive-user-data` field displays how much user data stored in the aggregate is inactive.

- The `performance-tier-inactive-user-data-percent` field displays what percent of the data is inactive across the active file system and Snapshot copies.
- For an aggregate that is not used for FabricPool, inactive data reporting uses the tiering policy to decide how much data to report as cold.
  - For the `none` tiering policy, 31 days is used.
  - For the `snapshot-only` and `auto`, inactive data reporting uses `tiering-minimum-cooling-days`.
  - For the `ALL` policy, inactive data reporting assumes the data will tier within a day.

Until the period is reached, the output shows “-” for the amount of inactive data instead of a value.
- On a volume that is part of FabricPool, what ONTAP reports as inactive depends on the tiering policy that is set on a volume.
  - For the `none` tiering policy, ONTAP reports the amount of the entire volume that is inactive for at least 31 days. You cannot use the `-tiering-minimum-cooling-days` parameter with the `none` tiering policy.
  - For the `ALL`, `snapshot-only`, and `auto` tiering policies, inactive data reporting is not supported.

## Add or move volumes to FabricPool as needed

### Create a volume for FabricPool

You can add volumes to FabricPool by creating new volumes directly in the FabricPool-enabled aggregate or by moving existing volumes from another aggregate to the FabricPool-enabled aggregate.

When you create a volume for FabricPool, you have the option to specify a tiering policy. If no tiering policy is specified, the created volume uses the default `snapshot-only` tiering policy. For a volume with the `snapshot-only` or `auto` tiering policy, you can also specify the tiering minimum cooling period.

### What you'll need

- Setting a volume to use the `auto` tiering policy or specifying the tiering minimum cooling period requires ONTAP 9.4 or later.
- Using FlexGroup volumes requires ONTAP 9.5 or later.
- Setting a volume to use the `all` tiering policy requires ONTAP 9.6 or later.
- Setting a volume to use the `-cloud-retrieval-policy` parameter requires ONTAP 9.8 or later.

### Steps

1. Create a new volume for FabricPool by using the `volume create` command.
  - The `-tiering-policy` optional parameter enables you to specify the tiering policy for the volume.

You can specify one of the following tiering policies:

- `snapshot-only` (default)

- `auto`
- `all`
- `backup` (deprecated)
- `none`

### Types of FabricPool tiering policies

- The `-cloud-retrieval-policy` optional parameter enables cluster administrators with the advanced privilege level to override the default cloud migration or retrieval behavior controlled by the tiering policy.

You can specify one of the following cloud retrieval policies:

- `default`

The tiering policy determines what data is pulled back, so there is no change to cloud data retrieval with `default` `cloud-retrieval-policy`. This means the behavior is the same as in pre-ONTAP 9.8 releases:

- If the tiering policy is `none` or `snapshot-only`, then “default” means that any client-driven data read is pulled from the cloud tier to performance tier.
- If the tiering policy is `auto`, then any client-driven random read is pulled but not sequential reads.
- If the tiering policy is `all` then no client-driven data is pulled from the cloud tier.

- `on-read`

All client-driven data reads are pulled from the cloud tier to performance tier.

- `never`

No client-driven data is pulled from the cloud tier to performance tier

- `promote`

- For tiering policy `none`, all cloud data is pulled from the cloud tier to the performance tier
- For tiering policy `snapshot-only`, all active filesystem data is pulled from the cloud tier to the performance tier.

- The `-tiering-minimum-cooling-days` optional parameter in the advanced privilege level enables you to specify the tiering minimum cooling period for a volume that uses the `snapshot-only` or `auto` tiering policy.

Beginning with ONTAP 9.8, you can specify a value between 2 and 183 for the tiering minimum cooling days. If you are using a version of ONTAP earlier than 9.8, you can specify a value between 2 and 63 for the tiering minimum cooling days.

### Example of creating a volume for FabricPool

The following example creates a volume called “myvol1” in the “myFabricPool” FabricPool-enabled aggregate. The tiering policy is set to `auto` and the tiering minimum cooling period is set to 45 days:

```
cluster1::*> volume create -vserver myVS -aggregate myFabricPool
-volume myvol1 -tiering-policy auto -tiering-minimum-cooling-days 45
```

## Related information

[FlexGroup volumes management](#)

### Move a volume to FabricPool

When you move a volume to FabricPool, you have the option to specify or change the tiering policy for the volume with the move. Beginning with ONTAP 9.8, when you move a non-FabricPool volume with inactive data reporting enabled, FabricPool uses a heat map to read tierable blocks, and moves cold data to the capacity tier on the FabricPool destination.

### What you'll need

You must understand how changing the tiering policy might affect how long it takes for data to become cold and be moved to the cloud tier.

[What happens to the tiering policy when you move a volume](#)

### About this task

If a non-FabricPool volume has inactive data reporting enabled, when you move a volume with tiering-policy `auto` or `snapshot-only` to a FabricPool, FabricPool reads the temperature tierable blocks from a heat map file and uses that temperature to move the cold data directly to the capacity tier on the FabricPool destination.

You should not use the `-tiering-policy` option on volume move if you are using ONTAP 9.8 and you want FabricPools to use inactive data reporting information to move data directly to the capacity tier. Using this option causes FabricPools to ignore the temperature data and instead follow the move behavior of releases prior to ONTAP 9.8.

### Step

1. Use the `volume move start` command to move a volume to FabricPool.

The `-tiering-policy` optional parameter enables you to specify the tiering policy for the volume.

You can specify one of the following tiering policies:

- `snapshot-only` (default)
- `auto`
- `all`
- `none`

[Types of FabricPool tiering policies](#)

### Example of moving a volume to FabricPool

The following example moves a volume named "myvol2" of the "vs1" SVM to the "dest\_FabricPool" FabricPool-enabled aggregate. The volume is explicitly set to use the `none` tiering policy:

```
cluster1::> volume move start -vserver vs1 -volume myvol2
-destination-aggregate dest_FabricPool -tiering-policy none
```

## Object tagging using user-created custom tags

### Object tagging using user-created custom tags overview

Beginning with ONTAP 9.8, FabricPool supports object tagging using user-created custom tags to enable you to classify and sort objects for easier management. If you are a user with the admin privilege level, you can create new object tags, and modify, delete, and view existing tags.

### Assign a new tag during volume creation

You can create a new object tag when you want to assign one or more tags to new objects that are tiered from a new volume you create. You can use tags to help you classify and sort tiering objects for easier data management. Beginning with ONTAP 9.8, you can use System Manager to create object tags.

### About this task

You can set tags only on FabricPool volumes attached to StorageGRID. These tags are retained during a volume move.

- A maximum of 4 tags per volume is allowed
- In the CLI, each object tag must be a key-value pair separated by an equal sign ("=")
- In the CLI, multiple tags must be separated by a comma (",")
- Each tag value can contain a maximum of 127 characters
- Each tag key must start with either an alphabetic character or an underscore.

Keys must contain only alphanumeric characters and underscores, and the maximum number of characters allowed is 127.

## Procedure

You can assign object tags with ONTAP System Manager or the ONTAP CLI.

## System Manager

1. Navigate to **Storage > Tiers**.
2. Locate a storage tier with volumes you want to tag.
3. Click the **Volumes** tab.
4. Locate the volume you want to tag and in the **Object Tags** column select **Click to enter tags**.
5. Enter a key and value.
6. Click **Apply**.

## CLI

1. Use the `volume create` command with the `-tiering-object-tags` option to create a new volume with the specified tags. You can specify multiple tags in comma-separated pairs:

```
volume create [ -vserver <vserver name> ] -volume <volume_name>
-tiering-object-tags <key1=value1> [
    ,<key2=value2>,<key3=value3>,<key4=value4> ]
```

The following example creates a volume named `fp_volume1` with three object tags.

```
vol create -volume fp_volume1 -vserver vs0 -tiering-object-tags
project=fabricpool,type=abc,content=data
```

## Modify an existing tag

You can change the name of a tag, replace tags on existing objects in the object store, or add a different tag to new objects that you plan to add later.

### About this task

Using the `volume modify` command with the `-tiering-object-tags` option replaces existing tags with the new value you provide.

## Procedure



## System Manager

1. Navigate to **Storage > Tiers**.
2. Locate a storage tier with volumes containing tags you want to modify.
3. Click the **Volumes** tab.
4. Locate the volume with tags you want to modify, and in the **Object Tags** column click the tag name.
5. Modify the tag.
6. Click **Apply**.

## CLI

1. Use the `volume modify` command with the `-tiering-object-tags` option to modify an existing tag.

```
volume modify [ -vserver <vserver name> ] -volume <volume_name>  
-tiering-object-tags <key1=value1> [ ,<key2=value2>,  
<key3=value3>,<key4=value4> ]
```

The following example changes the name of the existing tag `type=abc` to `type=xyz`.

```
vol create -volume fp_volume1 -vserver vs0 -tiering-object-tags  
project=fabricpool,type=xyz,content=data
```

## Delete a tag

You can delete object tags when you no longer want them set on a volume or on objects in the object store.

## Procedure

You can delete object tags with ONTAP System Manager or the ONTAP CLI.

## System Manager

1. Navigate to **Storage > Tiers**.
2. Locate a storage tier with volumes containing tags you want to delete.
3. Click the **Volumes** tab.
4. Locate the volume with tags you want to delete, and in the **Object Tags** column click the tag name.
5. To delete the tag, click the trash can icon.
6. Click **Apply**.

## CLI

1. Use the `volume modify` command with the `-tiering-object-tags` option followed by an empty value (`""`) to delete an existing tag.

The following example deletes the existing tags on `fp_volume1`.

```
vol modify -volume fp_volume1 -vserver vs0 -tiering-object-tags ""
```

## View existing tags on a volume

You can view the existing tags on a volume to see what tags are available before appending new tags to the list.

### Step

1. Use the `volume show` command with the `-tiering-object-tags` option to view existing tags on a volume.

```
volume show [ -vserver <vserver name> ] -volume <volume_name> -fields  
-tiering-object-tags
```

## Check object tagging status on FabricPool volumes

You can check if tagging is complete on one or more FabricPool volumes.

### Step

1. Use the `vol show` command with the `-fieldsneeds-object-retagging` option to see if tagging is in progress, if it has completed, or if tagging is not set.

```
vol show -fields needs-object-retagging [ -instance | -volume <volume  
name>]
```

One of the following values is displayed:

- `true` — the object tagging scanner has not yet to run or needs to run again for this volume

- `false` — the object tagging scanner has completed tagging for this volume
- `<->` — the object tagging scanner is not applicable for this volume. This happens for volumes that are not residing on FabricPools.

### Monitor the space utilization for FabricPool

You need to know how much data is stored in the performance and cloud tiers for FabricPool. That information helps you determine whether you need to change the tiering policy of a volume, increase the FabricPool licensed usage limit, or increase the storage space of the cloud tier.

#### Steps

1. Monitor the space utilization for FabricPool-enabled aggregates by using one of the following commands to display the information:

If you want to display...	Then use this command:
The used size of the cloud tier in an aggregate	<code>storage aggregate show with the -instance parameter</code>
Details of space utilization within an aggregate, including the object store's referenced capacity	<code>storage aggregate show-space with the -instance parameter</code>
Space utilization of the object stores that are attached to the aggregates, including how much license space is being used	<code>storage aggregate object-store show-space</code>
A list of volumes in an aggregate and the footprints of their data and metadata	<code>volume show-footprint</code>

In addition to using CLI commands, you can use Active IQ Unified Manager (formerly OnCommand Unified Manager), along with FabricPool Advisor, which is supported on ONTAP 9.4 and later clusters, or System Manager to monitor the space utilization.

The following example shows ways of displaying space utilization and related information for FabricPool:

```
cluster1::> storage aggregate show-space -instance
```

```
Aggregate: MyFabricPool
...
Aggregate Display Name:
MyFabricPool
...
Total Object Store Logical Referenced
Capacity: -
Object Store Logical Referenced Capacity
Percentage: -
...
Object Store
Size: -
Object Store Space Saved by Storage
Efficiency: -
Object Store Space Saved by Storage Efficiency
Percentage: -
Total Logical Used
Size: -
Logical Used
Percentage: -
Logical Unreferenced
Capacity: -
Logical Unreferenced
Percentage: -
```

```
cluster1::> storage aggregate show -instance
```

```
Aggregate: MyFabricPool
...
Composite: true
Capacity Tier Used Size:
...
```

```

cluster1::> volume show-footprint

Vserver : vs1
Volume  : rootvol

Feature                               Used      Used%
-----
Volume Footprint                       KB        %
Volume Guarantee                       MB        %
Flexible Volume Metadata                KB        %
Delayed Frees                           KB        %
Total Footprint                         MB        %

Vserver : vs1
Volume  : vol

Feature                               Used      Used%
-----
Volume Footprint                       KB        %
Footprint in Performance Tier           KB        %
Footprint in Amazon01                  KB        %
Flexible Volume Metadata                MB        %
Delayed Frees                           KB        %
Total Footprint                         MB        %
...

```

2. Take one of the following actions as needed:

If you want to...	Then...
Change the tiering policy of a volume	Follow the procedure in <a href="#">Managing storage tiering by modifying a volume's tiering policy or tiering minimum cooling period</a> .
Increase the FabricPool licensed usage limit	Contact your NetApp or partner sales representative.  <a href="#">NetApp Support</a>
Increase the storage space of the cloud tier	Contact the provider of the object store that you use for the cloud tier.

### Manage storage tiering by modifying a volume's tiering policy or tiering minimum cooling period

You can change the tiering policy of a volume to control whether data is moved to the cloud tier when it becomes inactive (*cold*). For a volume with the `snapshot-only` or

`auto` tiering policy, you can also specify the tiering minimum cooling period that user data must remain inactive before it is moved to the cloud tier.

### What you'll need

Changing a volume to the `auto` tiering policy or modifying the tiering minimum cooling period requires ONTAP 9.4 or later.

### About this task

Changing the tiering policy of a volume changes only the subsequent tiering behavior for the volume. It does not retroactively move data to the cloud tier.

Changing the tiering policy might affect how long it takes for data to become cold and be moved to the cloud tier.

### [What happens when you modify the tiering policy of a volume in FabricPool](#)

### Steps

1. Modify the tiering policy for an existing volume by using the `volume modify` command with the `-tiering-policy` parameter:

You can specify one of the following tiering policies:

- `snapshot-only` (default)
- `auto`
- `all`
- `none`

### [Types of FabricPool tiering policies](#)

2. If the volume uses the `snapshot-only` or `auto` tiering policy and you want to modify the tiering minimum cooling period, use the `volume modify` command with the `-tiering-minimum-cooling-days` optional parameter in the advanced privilege level.

You can specify a value between 2 and 183 for the tiering minimum cooling days. If you are using a version of ONTAP earlier than 9.8, you can specify a value between 2 and 63 for the tiering minimum cooling days.

### Example of modifying the tiering policy and the tiering minimum cooling period of a volume

The following example changes the tiering policy of the volume "myvol" in the SVM "vs1" to `auto` and the tiering minimum cooling period to 45 days:

```
cluster1::> volume modify -vserver vs1 -volume myvol
-tiering-policy auto -tiering-minimum-cooling-days 45
```

### Archive volumes with FabricPool (video)

This video shows a quick overview of using System Manager to archive a volume to a cloud tier with FabricPool.

[NetApp video: Archiving volumes with FabricPool \(backup + volume move\)](#)

## Related information

[NetApp TechComm TV: FabricPool playlist](#)

## Use cloud migration controls to override a volume's default tiering policy

You can change a volume's default tiering policy for controlling user data retrieval from the cloud tier to performance tier by using the `-cloud-retrieval-policy` option introduced in ONTAP 9.8.

### What you'll need

- Modifying a volume using the `-cloud-retrieval-policy` option requires ONTAP 9.8 or later.
- You must have the advanced privilege level to perform this operation.
- You should understand the behavior of tiering policies with `-cloud-retrieval-policy`.

[How tiering policies work with cloud migration](#)

### Step

1. Modify the tiering policy behavior for an existing volume by using the `volume modify` command with the `-cloud-retrieval-policy` option:

```
volume create -volume <volume_name> -vserver <vserver_name> - tiering-  
policy <policy_name> -cloud-retrieval-policy
```

```
vol modify -volume fp_volume4 -vserver vs0 -cloud-retrieval-policy  
promote
```

## Promote data to the performance tier

### Promote data to the performance tier overview

Beginning with ONTAP 9.8, if you are a cluster administrator at the advanced privilege level, you can proactively promote data to the performance tier from the cloud tier using a combination of the `tiering-policy` and the `cloud-retrieval-policy` setting.

### About this task

You might do this if you want to stop using FabricPool on a volume, or if you have a `snapshot-only` tiering policy and you want to bring restored Snapshot copy data back to the performance tier.

### Promote all data from a FabricPool volume to the performance tier

You can proactively retrieve all data on a FabricPool volume in the Cloud and promote it to the performance tier.

## Step

1. Use the `volume modify` command to set `tiering-policy` to `none` and `cloud-retrieval-policy` to `promote`.

```
volume modify -vserver <vserver-name> -volume <volume-name> -tiering
-policy none -cloud-retrieval-policy promote
```

## Promote file system data to the performance tier

You can proactively retrieve active file system data from a restored Snapshot copy in the cloud tier and promote it to the performance tier.

## Step

1. Use the `volume modify` command to set `tiering-policy` to `snapshot-only` and `cloud-retrieval-policy` to `promote`.

```
volume modify -vserver <vserver-name> -volume <volume-name> -tiering
-policy snapshot-only cloud-retrieval-policy promote
```

## Check the status of a performance tier promotion

You can check the status of performance tier promotion to determine when the operation is complete.

## Step

1. Use the `volume object-store` command with the `tiering` option to check the status of the performance tier promotion.

```
volume object-store tiering show [ -instance | -fields <fieldname>, ...
] [ -vserver <vserver name> ] *Vserver
[[-volume] <volume name>] *Volume [ -node <nodename> ] *Node Name [ -vol
-dsid <integer> ] *Volume DSID
[ -aggregate <aggregate name> ] *Aggregate Name
```



```

volume object-store tiering show v1 -instance

                Vserver: vs1
                Volume: v1
                Node Name: node1
                Volume DSID: 1023
                Aggregate Name: a1
                State: ready
                Previous Run Status: completed
                Aborted Exception Status: -
                Time Scanner Last Finished: Mon Jan 13 20:27:30 2020
                Scanner Percent Complete: -
                Scanner Current VBN: -
                Scanner Max VBNs: -
                Time Waiting Scan will be scheduled: -
                Tiering Policy: snapshot-only
                Estimated Space Needed for Promotion: -
                Time Scan Started: -
                Estimated Time Remaining for scan to complete: -
                Cloud Retrieve Policy: promote

```

### Trigger scheduled migration and tiering

Beginning with ONTAP 9.8, you can trigger a tiering scan request at any time when you prefer not to wait for the default tiering scan.

#### Step

1. Use the `volume object-store` command with the `trigger` option to request migration and tiering.

```

volume object-store tiering trigger [ -vserver <vserver name> ] *VServer
Name [-volume] <volume name> *Volume Name

```

## Manage FabricPool mirrors

### Manage FabricPool mirrors overview

To ensure data is accessible in data stores in the event of a disaster, and to enable you to replace a data store, you can configure a FabricPool mirror by adding a second data store to synchronously tier data to two data stores . You can add a second data store to new or existing FabricPool configurations, monitor the mirror status, display FabricPool mirror details, promote a mirror, and remove a mirror. You must be running ONTAP 9.7 or later.

## Create a FabricPool mirror

To create a FabricPool mirror, you attach two object stores to a single FabricPool. You can create a FabricPool mirror either by attaching a second object store to an existing, single object store FabricPool configuration, or you can create a new, single object store FabricPool configuration and then attach a second object store to it. You can also create FabricPool mirrors on MetroCluster configurations.

### What you'll need

- You must have already created the two object stores using the `storage aggregate object-store config` command.
- If you are creating FabricPool mirrors on MetroCluster configurations:
  - You must have already set up and configured the MetroCluster
  - You must have created the object store configurations on the selected cluster.

If you are creating FabricPool mirrors on both clusters in a MetroCluster configuration, you must have created object store configurations on both of the clusters.

- If you are not using on premises object stores for MetroCluster configurations, you should ensure that one of the following scenarios exists:
  - Object stores are in different availability zones
  - Object stores are configured to keep copies of objects in multiple availability zones

[Setting up object stores for FabricPool in a MetroCluster configuration](#)

### About this task

The object store you use for the FabricPool mirror must be different from the primary object store.

The procedure for creating a FabricPool mirror is the same for both MetroCluster and non-MetroCluster configurations.

### Steps

1. If you are not using an existing FabricPool configuration, create a new one by attaching an object store to an aggregate using the `storage aggregate object-store attach` command.

This example creates a new FabricPool by attaching an object store to an aggregate.

```
cluster1::> storage aggregate object-store attach -aggregate aggr1 -name my-store-1
```

2. Attach a second object store to the aggregate using the `storage aggregate object-store mirror` command.

This example attaches a second object store to an aggregate to create a FabricPool mirror.

```
cluster1::> storage aggregate object-store mirror -aggregate aggr1 -name
my-store-2
```

### Monitor FabricPool mirror resync status

When you replace a primary object store with a mirror, you might have to wait for the mirror to resync with the primary data store.

#### About this task

If the FabricPool mirror is in sync, no entries are displayed.

#### Step

1. Monitor mirror resync status using the `storage aggregate object-store show-resync-status` command.

```
aggregate1::> storage aggregate object-store show-resync-status
-aggregate aggr1
```

Aggregate	Primary	Mirror	Complete Percentage
aggr1	my-store-1	my-store-2	40%

### Display FabricPool mirror details

You can display details about a FabricPool mirror to see what object stores are in the configuration and whether the object store mirror is in sync with the primary object store.

#### Step

1. Display information about a FabricPool mirror using the `storage aggregate object-store show` command.

This example displays the details about the primary and mirror object stores in a FabricPool mirror.

```
cluster1::> storage aggregate object-store show
```

Aggregate	Object Store Name	Availability	Mirror Type
aggr1	my-store-1	available	primary
	my-store-2	available	mirror

This example displays details about the FabricPool mirror, including whether the mirror is degraded due to a resync operation.

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-mirror-degraded
```

aggregate	object-store-name	mirror-type	is-mirror-degraded
aggr1	my-store-1	primary	-
	my-store-2	mirror	false

### Promote a FabricPool mirror

You can reassign the object store mirror as the primary object store by promoting it. When the object store mirror becomes the primary, the original primary automatically becomes the mirror.

#### What you'll need

- The FabricPool mirror must be in sync
- The object store must be operational

#### About this task

You can replace the original object store with an object store from a different cloud provider. For instance, your original mirror might be an AWS object store, but you can replace it with an Azure object store.

#### Step

1. Promote an object store mirror by using the `storage aggregate object-store modify -aggregate` command.

```
cluster1::> storage aggregate object-store modify -aggregate aggr1 -name my-store-2 -mirror-type primary
```

### Remove a FabricPool mirror

You can remove a FabricPool mirror if you no longer need to replicate an object store.

#### What you'll need

The primary object store must be operational, otherwise, the command fails.

#### Step

1. Remove an object store mirror in a FabricPool by using the `storage aggregate object-store unmirror -aggregate` command.

```
cluster1::> storage aggregate object-store unmirror -aggregate aggr1
```

## Replace an existing object store using a FabricPool mirror

You can use FabricPool mirror technology to replace one object store with another one. The new object store does not have to use the same cloud provider as the original object store.

### About this task

You can replace the original object store with an object store that uses a different cloud provider. For instance, your original object store might use AWS as the cloud provider, but you can replace it with an object store that uses Azure as the cloud provider, and vice versa. However, the new object store must retain the same object size as the original.

### Steps

1. Create a FabricPool mirror by adding a new object store to an existing FabricPool using the `storage aggregate object-store mirror` command.

```
cluster1::> storage aggregate object-store mirror -aggregate aggr1 -name my-AZURE-store
```

2. Monitor the mirror resync status using the `storage aggregate object-store show-resync-status` command.

```
cluster1::> storage aggregate object-store show-resync-status -aggregate aggr1
```

Aggregate	Primary	Mirror	Complete Percentage
-----	-----	-----	-----
aggr1	my-AWS-store	my-AZURE-store	40%

3. Verify the mirror is in sync using the `storage aggregate object-store> show -fields mirror-type, is-mirror-degraded` command.

```
cluster1::> storage aggregate object-store show -fields mirror-type, is-mirror-degraded
```

aggregate	object-store-name	mirror-type	is-mirror-degraded
aggr1	my-AWS-store	primary	-
	my-AZURE-store	mirror	false

- Swap the primary object store with the mirror object store using the `storage aggregate object-store modify` command.

```
cluster1::> storage aggregate object-store modify -aggregate aggr1 -name my-AZURE-store -mirror-type primary
```

- Display details about the FabricPool mirror using the `storage aggregate object-store show -fields mirror-type, is-mirror-degraded` command.

This example displays the information about the FabricPool mirror, including whether the mirror is degraded (not in sync).

```
cluster1::> storage aggregate object-store show -fields mirror-type, is-mirror-degraded
```

aggregate	object-store-name	mirror-type	is-mirror-degraded
aggr1	my-AZURE-store	primary	-
	my-AWS-store	mirror	false

- Remove the FabricPool mirror using the `storage aggregate object-store unmirror` command.

```
cluster1::> storage aggregate object-store unmirror -aggregate aggr1
```

- Verify that the FabricPool is back in a single object store configuration using the `storage aggregate object-store show -fields mirror-type, is-mirror-degraded` command.

```
cluster1::> storage aggregate object-store show -fields mirror-type, is-mirror-degraded
```

aggregate	object-store-name	mirror-type	is-mirror-degraded
aggr1	my-AZURE-store	primary	-

## Replace a FabricPool mirror on a MetroCluster configuration

If one of the object stores in a FabricPool mirror is destroyed or becomes permanently unavailable on a MetroCluster configuration, you can make the object store the mirror if it is not the mirror already, remove the damaged object store from FabricPool mirror, and then add a new object store mirror to the FabricPool.

### Steps

1. If the damaged object store is not already the mirror, make the object store the mirror with the `storage aggregate object-store modify` command.

```
storage aggregate object-store modify -aggregate -aggregate fp_aggr1_A01
-name mccl_ostore1 -mirror-type mirror
```

2. Remove the object store mirror from the FabricPool by using the `storage aggregate object-store unmirror` command.

```
storage aggregate object-store unmirror -aggregate <aggregate name>
-name mccl_ostore1
```

3. You can force tiering to resume on the primary data store after you remove the mirror data store by using the `storage aggregate object-store modify` with the `-force-tiering-on-metrocluster true` option.

The absence of a mirror interferes with the replication requirements of a MetroCluster configuration.

```
storage aggregate object-store modify -aggregate <aggregate name> -name
mccl_ostore1 -force-tiering-on-metrocluster true
```

4. Create a replacement object store by using the `storage aggregate object-store config create` command.

```
storage aggregate object-store config create -object-store-name
mccl_ostore3 -cluster clusterA -provider-type SGWS -server <SGWS-server-
1> -container-name <SGWS-bucket-1> -access-key <key> -secret-password
<password> -encrypt <true|false> -provider <provider-type> -is-ssl
-enabled <true|false> ipspace <IPSpace>
```

5. Add the object store mirror to the FabricPool mirror using the `storage aggregate object-store mirror` command.

```
storage aggregate object-store mirror -aggregate aggr1 -name
mcc1_ostore3-mc
```

6. Display the object store information using the `storage aggregate object-store show` command.

```
storage aggregate object-store show -fields mirror-type,is-mirror-
degraded
```

```
aggregate      object-store-name mirror-type      is-mirror-degraded
-----
aggr1          mcc1_ostore1-mc    primary        -
               mcc1_ostore3-mc    mirror         true
```

7. Monitor the mirror resync status using the `storage aggregate object-store show-resync-status` command.

```
storage aggregate object-store show-resync-status -aggregate aggr1
```

```
Aggregate      Primary      Mirror      Complete
-----
aggr1          mcc1_ostore1-mc mcc1_ostore3-mc 40%
```

## Commands for managing aggregates with FabricPool

You use the `storage aggregate object-store` commands to manage object stores for FabricPool. You use the `storage aggregate` commands to manage aggregates for FabricPool. You use the `volume` commands to manage volumes for FabricPool.

If you want to...	Use this command:
Define the configuration for an object store so that ONTAP can access it	<code>storage aggregate object-store config create</code>
Modify object store configuration attributes	<code>storage aggregate object-store config modify</code>
Rename an existing object store configuration	<code>storage aggregate object-store config rename</code>



Delete the configuration of an object store	<code>storage aggregate object-store config delete</code>
Display a list of object store configurations	<code>storage aggregate object-store config show</code>
Attach a second object store to a new or existing FabricPool as a mirror	<code>storage aggregate object-store mirror</code> with the <code>-aggregate</code> and <code>-name</code> parameter in the admin privilege level
Remove an object store mirror from an existing FabricPool mirror	<code>storage aggregate object-store unmirror</code> with the <code>-aggregate</code> and <code>-name</code> parameter in the admin privilege level
Monitor FabricPool mirror resync status	<code>storage aggregate object-store show-resync-status</code>
Display FabricPool mirror details	<code>storage aggregate object-store show</code>
Promote an object store mirror to replace a primary object store in a FabricPool mirror configuration	<code>storage aggregate object-store modify</code> with the <code>-aggregate</code> parameter in the admin privilege level
Test the latency and performance of an object store without attaching the object store to an aggregate	<code>storage aggregate object-store profiler start</code> with the <code>-object-store-name</code> and <code>-node</code> parameter in the advanced privilege level
Monitor the object store profiler status	<code>storage aggregate object-store profiler show</code> with the <code>-object-store-name</code> and <code>-node</code> parameter in the advanced privilege level
Abort the object store profiler when it is running	<code>storage aggregate object-store profiler abort</code> with the <code>-object-store-name</code> and <code>-node</code> parameter in the advanced privilege level
Attach an object store to an aggregate for using FabricPool	<code>storage aggregate object-store attach</code>
Attach an object store to an aggregate that contains a FlexGroup volume for using FabricPool	<code>storage aggregate object-store attach</code> with the <code>allow-flexgroup true</code>
Display details of the object stores that are attached to FabricPool-enabled aggregates	<code>storage aggregate object-store show</code>

Display the aggregate fullness threshold used by the tiering scan	<code>storage aggregate object-store show with the -fields tiering-fullness-threshold</code> parameter in the advanced privilege level
Display space utilization of the object stores that are attached to FabricPool-enabled aggregates	<code>storage aggregate object-store show-space</code>
Enable inactive data reporting on an aggregate that is not used for FabricPool	<code>storage aggregate modify</code> with the <code>-is -inactive-data-reporting-enabled true</code> parameter
Display whether inactive data reporting is enabled on an aggregate	<code>storage aggregate show</code> with the <code>-fields is-inactive-data-reporting-enabled</code> parameter
Display information about how much user data is cold within an aggregate	<code>storage aggregate show-space</code> with the <code>-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent</code> parameter
<p>Create a volume for FabricPool, including specifying the following:</p> <ul style="list-style-type: none"> <li>• The tiering policy</li> <li>• The tiering minimum cooling period (for the <code>snapshot-only</code> or <code>auto</code> tiering policy)</li> </ul>	<p><code>volume create</code></p> <ul style="list-style-type: none"> <li>• You use the <code>-tiering-policy</code> parameter to specify the tiering policy.</li> <li>• You use the <code>-tiering-minimum-cooling -days</code> parameter in the advanced privilege level to specify the tiering minimum cooling period.</li> </ul>
<p>Modify a volume for FabricPool, including modifying the following:</p> <ul style="list-style-type: none"> <li>• The tiering policy</li> <li>• The tiering minimum cooling period (for the <code>snapshot-only</code> or <code>auto</code> tiering policy)</li> </ul>	<p><code>volume modify</code></p> <ul style="list-style-type: none"> <li>• You use the <code>-tiering-policy</code> parameter to specify the tiering policy.</li> <li>• You use the <code>-tiering-minimum-cooling -days</code> parameter in the advanced privilege level to specify the tiering minimum cooling period.</li> </ul>
<p>Display FabricPool information related to a volume, including the following:</p> <ul style="list-style-type: none"> <li>• The tiering minimum cooling period</li> <li>• How much user data is cold</li> </ul>	<p><code>volume show</code></p> <ul style="list-style-type: none"> <li>• You use the <code>-fields tiering-minimum-cooling-days</code> parameter in the advanced privilege level to display the tiering minimum cooling period.</li> <li>• You use the <code>-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent</code> parameter to display how much user data is cold.</li> </ul>

Move a volume in to or out of FabricPool	<code>volume move start</code> You use the <code>-tiering -policy</code> optional parameter to specify the tiering policy for the volume.
Modify the threshold for reclaiming unreferenced space (the defragmentation threshold) for FabricPool	<code>storage aggregate object-store modify</code> with the <code>-unreclaimed-space-threshold</code> parameter in the advanced privilege level
Modify the threshold for the percent full the aggregate becomes before the tiering scan begins tiering data for FabricPool  FabricPool continues to tier cold data to a cloud tier until the local tier reaches 98% capacity.	<code>storage aggregate object-store modify</code> with the <code>-tiering-fullness-threshold</code> parameter in the advanced privilege level
Display the threshold for reclaiming unreferenced space for FabricPool	<code>storage aggregate object-store show</code> or <code>storage aggregate object-store show-space</code> command with the <code>-unreclaimed-space -threshold</code> parameter in the advanced privilege level

## SVM data mobility

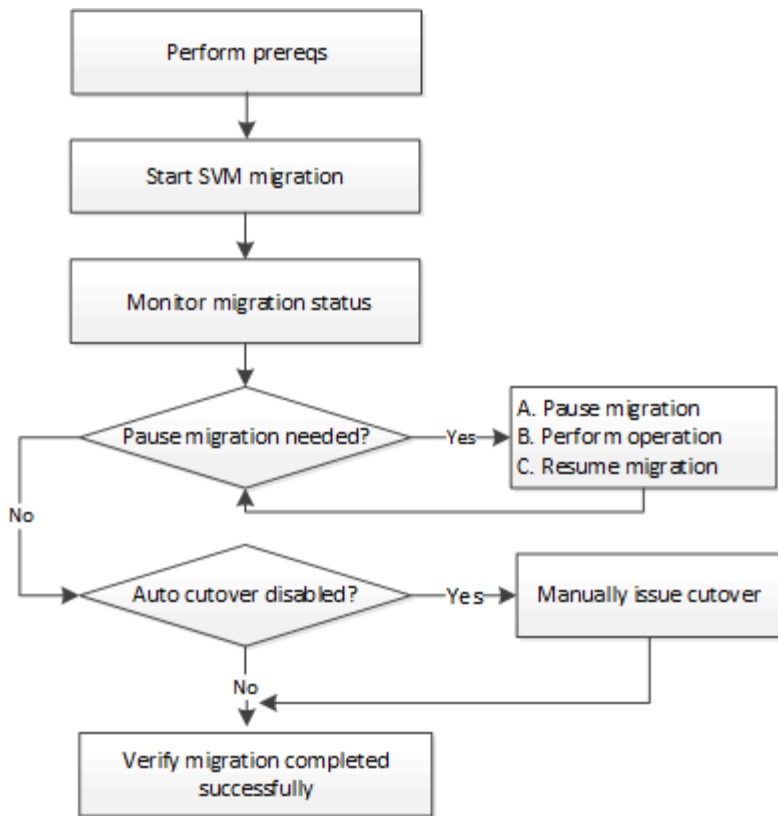
### SVM data mobility overview

Beginning with ONTAP 9.10.1, cluster administrators can non-disruptively relocate an SVM from a source cluster to a destination cluster to manage capacity and load balancing, or to enable equipment upgrades or data center consolidations. The feature is supported only on AFF arrays.

The SVM's name and UUID remain unchanged after migration, as well as the data LIF name, IP address, and object names, such as the volume name. The UUID of the objects in the SVM will be different.

### SVM migration workflow

The diagram depicts the typical workflow for an SVM migration. You start an SVM migration from the destination cluster. You can monitor the migration from either the source or the destination. You can perform a manual cutover or an automatic cutover. An automatic cutover is performed by default.



## Supported configurations

The table indicates the configurations supported and the ONTAP releases in which support is available.

Configuration supported in...	ONTAP 9.10.1	ONTAP 9.11.1
AFF arrays only	Yes	Yes
Total arrays/Node pairs	1	3
Migrate with a data center and a max network latency of 2ms	Yes	Yes

## Prerequisites

- You are a cluster administrator
- The source and destination clusters are peered to each other
- The source and destination clusters have the Data Protection Bundle license installed
- All nodes in the source cluster must be running ONTAP 9.10.1 or later
- All nodes in the source cluster must be running the same ONTAP version
- The destination cluster is at the same or newer effective cluster version (ECV) as the source cluster
- The source and destination clusters are in the same data network
- The source SVM contains fewer than the maximum number of supported data volumes for the release.

The maximum number of data volumes supported is 100.

- Sufficient space for volume placement is available on the destination
- Onboard Key Manager must be configured on the destination if the source SVM has encrypted volumes

## Conflicting operations

You should check for operations that can conflict with an SVM migration:

- No failover operations are in progress
- WAFLIRON cannot be running
- Fingerprint is not in progress
- Vol move, rehost, clone, create, convert or analytics are not running

## Supported features

The table indicates the features supported and the ONTAP releases in which support is available.

Feature supported in...	ONTAP 9.10.1	ONTAP 9.11.1	Additional information
NFS v3, NFS v4.1, and NFS v4.2 protocols	Yes	Yes	
NetApp Volume Encryption	Yes	Yes	
Asynchronous SnapMirror source	No	Yes	<ul style="list-style-type: none"><li>• Transfers can continue as normal on FlexVol SnapMirror relationships during most of the migration.</li><li>• Any ongoing transfers are canceled during cutover and new transfers fail during cutover and they cannot be restarted until the migration completes.</li><li>• Scheduled transfers that were canceled or missed during the migration are not automatically started after the migrate completes.</li></ul> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> When a SnapMirror source is migrated, ONTAP does not prevent deletion of the volume after migration until the SnapMirror update takes place after. This happens because SnapMirror-related information for migrated SnapMirror source volumes is known only after first update after migrate is complete.</div>
SVM peering for SnapMirror applications	No	Yes	
External key manager	No	Yes	

Fanout relationships (the migrating source has a SnapMirror source volume with more than one destination)	No	Yes	
Job schedule replication	No	Yes	In ONTAP 9.10.1, job schedules are not replicated during migration and must be manually created on the destination. Beginning with ONTAP 9.11.1, job schedules used by the source are replicated automatically during migration.

## Unsupported features

The following features are not supported with SVM migration:

- Anti-ransomware
- Asynchronous SnapMirror destination
- Auditing
- Cloud Volumes ONTAP
- Data protection volume
- FabricPools
- FAS arrays
- Flash Pool aggregates
- FlexCache volumes
- FlexGroup volumes
- IPsec policy
- IPv6 LIFs
- iSCSI workloads
- Load-sharing mirrors
- MetroCluster
- NDMP
- SAN, NVMe over fiber, CIFS, VSCAN, NFS v4.0, vStorage, S3 replication
- SMTape
- SnapLock
- SVM-DR
- SVM migration when the source cluster's Onboard Key Manager (OKM) has Common Criteria (CC) mode enabled
- Synchronous SnapMirror, SnapMirror Business Continuity
- System Manager
- Qtree, Quota
- VIP/BGP LIF

- Virtual Storage Console for VMware vSphere (VSC is part of the [ONTAP Tools for VMware vSphere virtual appliance](#) beginning with VSC 7.0.)
- Volume clones

## Migrate an SVM

After an SVM migration has completed, clients are cut over to the destination cluster automatically and the unnecessary SVM is removed from the source cluster. Automatic cutover and automatic source cleanup are enabled by default. If necessary, you can disable client auto-cutover to suspend the migration before cutover occurs and you can also disable automatic source SVM cleanup.

- You can use the `-auto-cutover false` option to suspend the migration when automatic client cutover normally occurs and then manually perform the cutover later.

[Manually cutover clients after SVM migration](#)

- You can use the advance privilege `-auto-source-cleanup false` option to disable the removal of the source SVM after cutover and then trigger source cleanup manually later, after cutover.

[Manually remove source SVM after cutover](#)

## Migrate an SVM with automatic cutover enabled

By default, clients are cut over to the destination cluster automatically when the migration is complete, and the unnecessary SVM is removed from the source cluster.

### Steps

1. From the destination cluster, run the migration prechecks:

```
dest_cluster> vserver migrate start -vserver SVM_name -source-cluster
cluster_name -check-only true
```

2. From the destination cluster, start the SVM migration:

```
dest_cluster> vserver migrate start -vserver SVM_name -source-cluster
cluster_name
```

3. Check the migration status:

```
dest_cluster> vserver migrate show
```

The status displays `migrate-complete` when the SVM migration is finished.

## Migrate an SVM with automatic client cutover disabled

You can use the `-auto-cutover false` option to suspend the migration when automatic client cutover normally occurs and then manually perform the cutover later. See “Manually cut over clients after SVM migration.”

### Steps

1. From the destination cluster, run the migration prechecks:

```
dest_cluster> vserver migrate start -vserver SVM_name -source-cluster
cluster_name -check-only true
```

2. From the destination cluster, start the SVM migration:

```
dest_cluster> vserver migrate start -vserver SVM_name -source-cluster
cluster_name -auto-cutover false
```

3. Check the migration status:

```
dest_cluster> vserver migrate show
```

The status displays ready-for-cutover when SVM migration completes the asynchronous data transfers, and it is ready for cutover operation.

## Migrate an SVM with source cleanup disabled

You can use the advance privilege `-auto-source-cleanup false` option to disable the removal of the source SVM after cutover and then trigger source cleanup manually later, after cutover. See “Manually clean up source after cutover.”

### Steps

1. From the destination cluster, run the migration prechecks:

```
dest_cluster*> vserver migrate start -vserver SVM_name -source-cluster
cluster_name -check-only true
```

2. From the destination cluster, start the SVM migration:

```
dest_cluster*> vserver migrate start -vserver SVM_name -source-cluster
cluster_name -auto-source-cleanup false
```

3. Check the migration status:

```
dest_cluster*> vserver migrate show
```

The status displays ready-for-source-cleanup when SVM migration cutover is complete, and it is ready to remove the SVM on the source cluster.

## Monitor volume migration

In addition to monitoring the overall SVM migration with the `vserver migrate show` command, you can monitor the migration status of the volumes the SVM contains.

### Steps

1. Check volume migration status:

```
dest_clust> vserver migrate show-volume
```

## Pause and resume SVM migration

You might want to pause an SVM migration before the migration cutover begins. You can



pause an SVM migration using the `vserver migrate pause` command.

### Pause migration

You can pause an SVM migration before client cutover starts by using the `vserver migrate pause` command.

#### Steps

1. From the destination cluster, pause the migration:

```
dest_cluster> vserver migrate pause -vserver <vserver name>
```

### Resume migrations

When you're ready to resume a paused SVM migration or when an SVM migration fails, you can use the `vserver migrate resume` command.

#### Step

1. Resume SVM migration:

```
dest_cluster> vserver migrate resume
```

2. Verify that the SVM migration has resumed, and monitor the progress:

```
dest_cluster> vserver migrate show
```

### Cancel an SVM migration

If you need to cancel an SVM migration before it completes, you can use the `vserver migrate abort` command. You can cancel an SVM migration only when the operation is in the paused or failed state. You cannot cancel an SVM migration when the status is "cutover-started" or after cutover is complete. You cannot use the `abort` option when an SVM migration is in progress.

#### Steps

1. Check the migration status:

```
dest_cluster> vserver migrate show -vserver <vserver name>
```

2. Cancel the migration:

```
dest_cluster> vserver migrate abort -vserver <vserver name>
```

Check the progress of the cancel operation:

```
dest_cluster> vserver migrate show
```

The migration status shows `migrate-aborting` while the cancel operation is in progress. When the cancel operation completes, the migration status shows nothing.

## Manually cut over clients

By default, client cutover to the destination cluster is performed automatically after the SVM migration reaches "ready-for-cutover" state. If you choose to disable automatic client cutover, you need to perform the client cutover manually.

### Steps

1. Manually execute client cutover:

```
dest_cluster> vserver migrate cutover -vserver <vserver name>
```

2. Check the status of the cutover operation:

```
dest_cluster> vserver migrate show
```

## Manually remove source SVM after client cutover

If you performed the SVM migration with source cleanup disabled, you can remove the source SVM manually after client cutover is complete.

### Steps

1. Verify they status is ready for source cleanup:

```
dest_cluster> vserver migrate show
```

2. Clean up the source:

```
dest_cluster> vserver migrate source-cleanup -vserver <vserver_name>
```

## HA pair management

### HA pair management overview

Cluster nodes are configured in high-availability (HA) pairs for fault tolerance and nondisruptive operations. If a node fails or if you need to bring a node down for routine maintenance, its partner can take over its storage and continue to serve data from it. The partner gives back storage when the node is brought back on line.

The HA pair controller configuration consists of a pair of matching FAS/AFF storage controllers (local node and partner node). Each of these nodes is connected to the other's disk shelves. When one node in an HA pair encounters an error and stops processing data, its partner detects the failed status of the partner and takes over all data processing from that controller.

*Takeover* is the process in which a node assumes control of its partner's storage.

*Giveback* is the process in which the storage is returned to the partner.

By default, takeovers occur automatically in any of the following situations:

- A software or system failure occurs on a node that leads to a panic. The HA pair controllers automatically

fail over to their partner node. After the partner has recovered from the panic and booted up, the node automatically performs a giveback, returning the partner to normal operation.

- A system failure occurs on a node, and the node cannot reboot. For example, when a node fails because of a power loss, HA pair controllers automatically fail over to their partner node and serve data from the surviving storage controller.



If the storage for a node also loses power at the same time, a standard takeover is not possible.

- Heartbeat messages are not received from the node's partner. This could happen if the partner experienced a hardware or software failure (for example, an interconnect failure) that did not result in a panic but still prevented it from functioning correctly.
- You halt one of the nodes without using the `-f` or `-inhibit-takeover true` parameter.



In a two-node cluster with cluster HA enabled, halting or rebooting a node using the `-inhibit-takeover true` parameter causes both nodes to stop serving data unless you first disable cluster HA and then assign epsilon to the node that you want to remain online.

- You reboot one of the nodes without using the `-inhibit-takeover true` parameter. (The `-onboot` parameter of the `storage failover` command is enabled by default.)
- The remote management device (Service Processor) detects failure of the partner node. This is not applicable if you disable hardware-assisted takeover.

You can also manually initiate takeovers with the `storage failover takeover` command.

## How hardware-assisted takeover works

Enabled by default, the hardware-assisted takeover feature can speed up the takeover process by using a node's remote management device (Service Processor).

When the remote management device detects a failure, it quickly initiates the takeover rather than waiting for ONTAP to recognize that the partner's heartbeat has stopped. If a failure occurs without this feature enabled, the partner waits until it notices that the node is no longer giving a heartbeat, confirms the loss of heartbeat, and then initiates the takeover.

The hardware-assisted takeover feature uses the following process to avoid that wait:

1. The remote management device monitors the local system for certain types of failures.
2. If a failure is detected, the remote management device immediately sends an alert to the partner node.
3. Upon receiving the alert, the partner initiates takeover.

### System events that trigger hardware-assisted takeover

The partner node might generate a takeover depending on the type of alert it receives from the remote management device (Service Processor).

Alert	Takeover initiated upon receipt?	Description
abnormal_reboot	No	An abnormal reboot of the node occurred.

l2_watchdog_reset	Yes	The system watchdog hardware detected an L2 reset. The remote management device detected a lack of response from the system CPU and reset the system.
loss_of_heartbeat	No	The remote management device is no longer receiving the heartbeat message from the node. This alert does not refer to the heartbeat messages between the nodes in the HA pair; it refers to the heartbeat between the node and its local remote management device.
periodic_message	No	A periodic message is sent during a normal hardware-assisted takeover operation.
power_cycle_via_sp	Yes	The remote management device cycled the system power off and on.
power_loss	Yes	A power loss occurred on the node. The remote management device has a power supply that maintains power for a short period after a power loss, allowing it to report the power loss to the partner.
power_off_via_sp	Yes	The remote management device powered off the system.
reset_via_sp	Yes	The remote management device reset the system.
test	No	A test message is sent to verify a hardware-assisted takeover operation.

## How automatic takeover and giveback works

The automatic takeover and giveback operations can work together to reduce and avoid client outages.

By default, if one node in the HA pair panics, reboots, or halts, the partner node automatically takes over and then returns storage when the affected node reboots. The HA pair then resumes a normal operating state.

Automatic takeovers may also occur if one of the nodes become unresponsive.

Automatic giveback occurs by default. If you would rather control giveback impact on clients, you can disable automatic giveback and use the `storage failover modify -auto-giveback false -node <node>` command. Before performing the automatic giveback (regardless of what triggered it), the partner node waits for a fixed amount of time as controlled by the `-delay- seconds` parameter of the `storage failover modify` command. The default delay is 600 seconds. By delaying the giveback, the process results in two brief outages: one during takeover and one during giveback.

This process avoids a single, prolonged outage that includes time required for:

- The takeover operation
- The taken-over node to boot up to the point at which it is ready for the giveback
- The giveback operation

If the automatic giveback fails for any of the non-root aggregates, the system automatically makes two additional attempts to complete the giveback.



During the takeover process, the automatic giveback process starts before the partner node is ready for the giveback. When the time limit of the automatic giveback process expires and the partner node is still not ready, the timer restarts. As a result, the time between the partner node being ready and the actual giveback being performed might be shorter than the automatic giveback time.

## What happens during takeover

When a node takes over its partner, it continues to serve and update data in the partner's aggregates and volumes.

The following steps occur during the takeover process:

1. If the negotiated takeover is user-initiated, aggregated data is moved from the partner node to the node that is performing the takeover. A brief outage occurs as the current owner of each aggregate (except for the root aggregate) changes over to the takeover node. This outage is briefer than an outage that occurs during a takeover without aggregate relocation.
  - You can monitor the progress using the `storage failover show-takeover` command.
  - You can avoid the aggregate relocation during this takeover instance by using the `-bypass -optimization` parameter with the `storage failover takeover` command.



Aggregates are relocated serially during planned takeover operations to reduce client outage. If aggregate relocation is bypassed, longer client outage occurs during planned takeover events.

2. If the user-initiated takeover is a negotiated takeover, the target node gracefully shuts down, followed by takeover of the target node's root aggregate and any aggregates that were not relocated in Step 1.
3. Before the storage takeover begins, data LIFs (logical interfaces) migrate from the target node to the takeover node, or to any other node in the cluster based on LIF failover rules. You can avoid the LIF migration by using the `-skip-lif-migration` parameter with the `storage failover takeover` command.
4. Existing SMB sessions are disconnected when takeover occurs.



Due to the nature of the SMB protocol, all SMB sessions are disrupted (except for SMB 3.0 sessions connected to shares with the Continuous Availability property set). SMB 1.0 and SMB 2.x sessions cannot reconnect after a takeover event; therefore, takeover is disruptive and some data loss could occur.

5. SMB 3.0 sessions that are established to shares with the Continuous Availability property enabled can reconnect to the disconnected shares after a takeover event. If your site uses SMB 3.0 connections to Microsoft Hyper-V and the Continuous Availability property is enabled on the associated shares, takeovers are non-disruptive for those sessions.

## What happens if a node performing a takeover panics

If the node that is performing the takeover panics within 60 seconds of initiating takeover, the following events occur:

- The node that panicked reboots.
- After it reboots, the node performs self-recovery operations and is no longer in takeover mode.

- Failover is disabled.
- If the node still owns some of the partner's aggregates, after enabling storage failover, return these aggregates to the partner using the `storage failover giveback` command.

## What happens during giveback

The local node returns ownership to the partner node when issues are resolved, when the partner node boots up, or when giveback is initiated.

The following process takes place in a normal giveback operation. In this discussion, Node A has taken over Node B. Any issues on Node B have been resolved and it is ready to resume serving data.

1. Any issues on Node B are resolved and it displays the following message: `Waiting for giveback`
2. The giveback is initiated by the `storage failover giveback` command or by automatic giveback if the system is configured for it. This initiates the process of returning ownership of Node B's aggregates and volumes from Node A back to Node B.
3. Node A returns control of the root aggregate first.
4. Node B completes the process of booting up to its normal operating state.
5. As soon as Node B reaches the point in the boot process where it can accept the non-root aggregates, Node A returns ownership of the other aggregates, one at a time, until giveback is complete. You can monitor the progress of the giveback by using the `storage failover show-giveback` command.



The `storage failover show-giveback` command does not (nor is it intended to) display information about all operations occurring during the storage failover giveback operation. You can use the `storage failover show` command to display additional details about the current failover status of the node, such as if the node is fully functional, takeover is possible, and giveback is complete.

I/O resumes for each aggregate after giveback is complete for that aggregate, which reduces its overall outage window.

## HA policy and its effect on takeover and giveback

ONTAP automatically assigns an HA policy of CFO (controller failover) and SFO (storage failover) to an aggregate. This policy determines how storage failover operations occur for the aggregate and its volumes.

The two options, CFO and SFO, determine the aggregate control sequence ONTAP uses during storage failover and giveback operations.

Although the terms CFO and SFO are sometimes used informally to refer to storage failover (takeover and giveback) operations, they actually represent the HA policy assigned to the aggregates. For example, the terms SFO aggregate or CFO aggregate simply refer to the aggregate's HA policy assignment.

HA policies affect takeover and giveback operations as follows:

- Aggregates created on ONTAP systems (except for the root aggregate containing the root volume) have an HA policy of SFO. Manually initiated takeover is optimized for performance by relocating SFO (non-root) aggregates serially to the partner before takeover. During the giveback process, aggregates are given back serially after the taken-over system boots and the management applications come online, enabling the node to receive its aggregates.

- Because aggregate relocation operations entail reassigning aggregate disk ownership and shifting control from a node to its partner, only aggregates with an HA policy of SFO are eligible for aggregate relocation.
- The root aggregate always has an HA policy of CFO and is given back at the start of the giveback operation. This is necessary to allow the taken-over system to boot. All other aggregates are given back serially after the taken-over system completes the boot process and the management applications come online, enabling the node to receive its aggregates.



Changing the HA policy of an aggregate from SFO to CFO is a Maintenance mode operation. Do not modify this setting unless directed to do so by a customer support representative.

## How background updates affect takeover and giveback

Background updates of the disk firmware will affect HA pair takeover, giveback, and aggregate relocation operations differently, depending on how those operations are initiated.

The following list describes how background disk firmware updates affect takeover, giveback, and aggregate relocation:

- If a background disk firmware update occurs on a disk on either node, manually initiated takeover operations are delayed until the disk firmware update finishes on that disk. If the background disk firmware update takes longer than 120 seconds, takeover operations are aborted and must be restarted manually after the disk firmware update finishes. If the takeover was initiated with the `-bypass-optimization` parameter of the `storage failover takeover` command set to `true`, the background disk firmware update occurring on the destination node does not affect the takeover.
- If a background disk firmware update is occurring on a disk on the source (or takeover) node and the takeover was initiated manually with the `-options` parameter of the `storage failover takeover` command set to `immediate`, takeover operations start immediately.
- If a background disk firmware update is occurring on a disk on a node and it panics, takeover of the panicked node begins immediately.
- If a background disk firmware update is occurring on a disk on either node, giveback of data aggregates is delayed until the disk firmware update finishes on that disk.
- If the background disk firmware update takes longer than 120 seconds, giveback operations are aborted and must be restarted manually after the disk firmware update completes.
- If a background disk firmware update is occurring on a disk on either node, aggregate relocation operations are delayed until the disk firmware update finishes on that disk. If the background disk firmware update takes longer than 120 seconds, aggregate relocation operations are aborted and must be restarted manually after the disk firmware update finishes. If aggregate relocation was initiated with the `-override-destination-checks` of the `storage aggregate relocation` command set to `true`, the background disk firmware update occurring on the destination node does not affect aggregate relocation.

## Automatic takeover commands

Automatic takeover is enabled by default on all supported NetApp FAS, AFF, and ASA platforms. You might need to change the default behavior and control when automatic takeovers occur when the partner node reboots, panics, or halts.

If you want takeover to occur automatically when the partner node...	Use this command...
--	---------------------

Reboots or halts	<code>storage failover modify -node nodename -onreboot true</code>
Panics	<code>storage failover modify -node nodename -onpanic true</code>

### Enable email notification if the takeover capability is disabled

To receive prompt notification if the takeover capability becomes disabled, you should configure your system to enable automatic email notification for the “takeover impossible” EMS messages:

- `ha.takeoverImpVersion`
- `ha.takeoverImpLowMem`
- `ha.takeoverImpDegraded`
- `ha.takeoverImpUnsync`
- `ha.takeoverImpIC`
- `ha.takeoverImpHotShelf`
- `ha.takeoverImpNotDef`

### Automatic giveback commands

By default, the take-over partner node automatically gives back storage when the off-line node is brought back on line, thus restoring the high-availability pair relationship. In most cases, this is the desired behavior. If you need to disable automatic giveback - for example, if you want to investigate the cause of the takeover before giving back – you need to be aware of the interaction of non-default settings.

If you want to...	Use this command...
<p>Enable automatic giveback so that giveback occurs as soon as the taken-over node boots, reaches the Waiting for Giveback state, and the Delay before Auto Giveback period has expired.</p> <p>The default setting is true.</p>	<code>storage failover modify -node nodename -auto-giveback true</code>
<p>Disable automatic giveback. The default setting is true.</p> <p><b>Note:</b> Setting this parameter to false does not disable automatic giveback after takeover on panic; automatic giveback after takeover on panic must be disabled by setting the <code>-auto-giveback-after-panic</code> parameter to false.</p>	<code>storage failover modify -node nodename -auto-giveback false</code>
<p>Disable automatic giveback after takeover on panic (this setting is enabled by default).</p>	<code>storage failover modify -node nodename -auto-giveback-after-panic false</code>



Delay automatic giveback for a specified number of seconds (the default is 600). This option determines the minimum time that a node remains in takeover before performing an automatic giveback.	<code>storage failover modify -node nodename -delay-seconds seconds</code>
---	--

### How variations of the storage failover modify command affect automatic giveback

The operation of automatic giveback depends on how you configure the parameters of the storage failover modify command.

The following table lists the default settings for the `storage failover modify` command parameters that apply to takeover events not caused by a panic.

Parameter	Default setting
<code>-auto-giveback true   false</code>	<code>true</code>
<code>-delay-seconds integer (seconds)</code>	600
<code>-onreboot true   false</code>	<code>true</code>

The following table describes how combinations of the `-onreboot` and `-auto-giveback` parameters affect automatic giveback for takeover events not caused by a panic.

<code>storage failover modify</code> parameters used	Cause of takeover	Does automatic giveback occur?
<code>-onreboot true</code>	reboot command	Yes
<code>-auto-giveback true</code>	halt command, or power cycle operation issued from the Service Processor	Yes
<code>-onreboot true</code>	reboot command	Yes
<code>-auto-giveback false</code>	halt command, or power cycle operation issued from the Service Processor	No
<code>-onreboot false</code>	reboot command	N/A In this case, takeover does not occur
<code>-auto-giveback true</code>	halt command, or power cycle operation issued from the Service Processor	Yes

<code>-onreboot false</code>	reboot command	No
<code>-auto-giveback false</code>	halt command, or power cycle operation issued from the Service Processor	No

The `-auto-giveback` parameter controls giveback after panic and all other automatic takeovers. If the `-onreboot` parameter is set to `true` and a takeover occurs due to a reboot, then automatic giveback is always performed, regardless of whether the `-auto-giveback` parameter is set to `true`.

The `-onreboot` parameter applies to reboots and halt commands issued from ONTAP. When the `-onreboot` parameter is set to `false`, a takeover does not occur in the case of a node reboot. Therefore, automatic giveback cannot occur, regardless of whether the `-auto-giveback` parameter is set to `true`. A client disruption occurs.

**The effects of automatic giveback parameter combinations that apply to panic situations.**

The following table lists the `storage failover modify` command parameters that apply to panic situations:

Parameter	Default setting
<code>-onpanic true   false</code>	<code>true</code>
<code>-auto-giveback-after-panic true   false</code> (Privilege: Advanced)	<code>true</code>
<code>-auto-giveback true   false</code>	<code>true</code>

The following table describes how parameter combinations of the `storage failover modify` command affect automatic giveback in panic situations.



Be aware that takeover can occur for other reasons in the event of a node panic. For example, if a node panics but the panic packet is not received by its partner, the partner might perform a heartbeat loss takeover. In this case, giveback would not be controlled by the `-auto-giveback-after-panic` parameter but would instead be controlled by the `-onfailure` parameter.

storage failover parameters used	Does automatic giveback occur after panic?
<code>-onpanic true</code> <code>-auto-giveback true</code> <code>-auto-giveback-after-panic true</code>	Yes
<code>-onpanic true</code> <code>-auto-giveback true</code> <code>-auto-giveback-after-panic false</code>	Yes

-onpanic true -auto-giveback false -auto-giveback-after-panic true	Yes
-onpanic true -auto-giveback false -auto-giveback-after-panic false	No
-onpanic false If -onpanic is set to false, takeover/giveback does not occur, regardless of the value set for -auto-giveback or -auto-giveback-after-panic	No

If you modify the default settings, the `-onpanic` parameter can override automatic giveback, as shown in the table above.



- If the `-onpanic` parameter is set to `true`, automatic giveback is always performed if a panic occurs unless you have changed the default settings for the `-auto-giveback` and `-auto-giveback-after-panic` parameters. If both of these parameters are changed from their default (`true`) to `false`, then an automatic giveback will not occur after a panic, even if the `-onpanic` parameter is set to `true`.
- If the `-onpanic` parameter is set to `false`, a takeover does not occur and clients experience a disruption in ONTAP data services. Therefore, automatic giveback cannot occur, even if the `-auto-giveback-after-panic` parameter is set to `true`.



- Takeover might occur for other reasons during node panic. In such cases, giveback is not controlled by the `auto-giveback-after-panic` setting.
- If the `-onpanic` parameter is set to `true`, automatic giveback is always performed if a panic occurs unless you have changed the default settings for the `-auto-giveback` and `-auto-giveback-after-panic` parameters. If both of these parameters are changed from their default (`true`) to `false`, then an automatic giveback will not occur after a panic, even if the `-onpanic` parameter is set to `true`.
- If the `-onpanic` parameter is set to `false`, takeover does not occur. Therefore, automatic giveback cannot occur, even if the `-auto-giveback-after-panic` parameter is set to `true`. A client disruption occurs.

## Manual takeover commands

You can perform a takeover manually when maintenance is required on the partner, and in other similar situations. Depending on the state of the partner, the command you use to perform the takeover varies.

If you want to...	Use this command...
Take over the partner node	<code>storage failover takeover</code>
Monitor the progress of the takeover as the partner's aggregates are moved to the node doing the takeover	<code>storage failover show-takeover</code>

Display the storage failover status for all nodes in the cluster	<code>storage failover show</code>
Take over the partner node without migrating LIFs	<code>storage failover takeover -skip-lif -migration-before-takeover true</code>
Take over the partner node even if there is a disk mismatch	<code>storage failover takeover -skip-lif -migration-before-takeover true</code>
Take over the partner node even if there is an ONTAP version mismatch  <b>Note:</b> This option is only used during the nondisruptive ONTAP upgrade process.	<code>storage failover takeover -option allow -version-mismatch</code>
Take over the partner node without performing aggregate relocation	<code>storage failover takeover -bypass -optimization true</code>
Take over the partner node before the partner has time to close its storage resources gracefully	<code>storage failover takeover -option immediate</code>

Before you issue the storage failover command with the `immediate` option, you must migrate the data LIFs to another node by using the following command: `network interface migrate-all -node node`



If you specify the `storage failover takeover -option immediate` command without first migrating the data LIFs, data LIF migration from the node is significantly delayed even if the `skip-lif-migration-before-takeover` option is not specified.

Similarly, if you specify the `immediate` option, negotiated takeover optimization is bypassed even if the `bypass-optimization` option is set to `false`.

### Moving epsilon for certain manually initiated takeovers

You should move epsilon if you expect that any manually initiated takeovers could result in your storage system being one unexpected node failure away from a cluster-wide loss of quorum.

#### About this task

To perform planned maintenance, you must take over one of the nodes in an HA pair. Cluster-wide quorum must be maintained to prevent unplanned client data disruptions for the remaining nodes. In some instances, performing the takeover can result in a cluster that is one unexpected node failure away from cluster-wide loss of quorum.

This can occur if the node being taken over holds epsilon or if the node with epsilon is not healthy. To maintain a more resilient cluster, you can transfer epsilon to a healthy node that is not being taken over.

Typically, this would be the HA partner.

Only healthy and eligible nodes participate in quorum voting. To maintain cluster-wide quorum, more than  $N/2$  votes are required (where  $N$  represents the sum of healthy, eligible, online nodes). In clusters with an even number of online nodes, epsilon adds additional voting weight toward maintaining quorum for the node to which it is assigned.



Although cluster formation voting can be modified by using the `cluster modify -eligibility false` command, you should avoid this except for situations such as restoring the node configuration or prolonged node maintenance. If you set a node as ineligible, it stops serving SAN data until the node is reset to eligible and rebooted. NAS data access to the node might also be affected when the node is ineligible.

## Steps

1. Verify the cluster state and confirm that epsilon is held by a healthy node that is not being taken over:
  - a. Change to the advanced privilege level, confirming that you want to continue when the advanced mode prompt appears (\*>):

```
set -privilege advanced
```

- b. Determine which node holds epsilon:

```
cluster show
```

In the following example, Node1 holds epsilon:

Node	Health	Eligibility	Epsilon
Node1	true	true	true
Node2	true	true	false

If the node you want to take over does not hold epsilon, proceed to Step 4.

2. Remove epsilon from the node that you want to take over:

```
cluster modify -node Node1 -epsilon false
```

3. Assign epsilon to the partner node (in this example, Node2):

```
cluster modify -node Node2 -epsilon true
```

4. Perform the takeover operation:

```
storage failover takeover -ofnode node_name
```

5. Return to the admin privilege level:

```
set -privilege admin
```

## Manual giveback commands

You can perform a normal giveback, a giveback in which you terminate processes on the partner node, or a forced giveback.



Prior to performing a giveback, you must remove the failed drives in the taken-over system as described in [Disks and aggregates management](#).

## If giveback is interrupted

If the takeover node experiences a failure or a power outage during the giveback process, that process stops and the takeover node returns to takeover mode until the failure is repaired or the power is restored.

However, this depends upon the stage of giveback in which the failure occurred. If the node encountered failure or a power outage during partial giveback state (after it has given back the root aggregate), it will not return to takeover mode. Instead, the node returns to partial-giveback mode. If this occurs, complete the process by repeating the giveback operation.

## If giveback is vetoed

If giveback is vetoed, you must check the EMS messages to determine the cause. Depending on the reason or reasons, you can decide whether you can safely override the vetoes.

The `storage failover show-giveback` command displays the giveback progress and shows which subsystem vetoed the giveback, if any. Soft vetoes can be overridden, while hard vetoes cannot be, even if forced. The following tables summarize the soft vetoes that should not be overridden, along with recommended workarounds.

You can review the EMS details for any giveback vetoes by using the following command:

```
event log show -node * -event gb*
```

## Giveback of the root aggregate

These vetoes do not apply to aggregate relocation operations:

Vetoing subsystem module	Workaround
vfiler_low_level	<p>Terminate the SMB sessions causing the veto, or shutdown the SMB application that established the open sessions.</p> <p>Overriding this veto might cause the application using SMB to disconnect abruptly and lose data.</p>
Disk Check	<p>All failed or bypassed disks should be removed before attempting giveback. If disks are sanitizing, you should wait until the operation completes.</p> <p>Overriding this veto might cause an outage caused by aggregates or volumes going offline due to reservation conflicts or inaccessible disks.</p>

## Giveback of the SFO aggregates

These vetoes do not apply to aggregate relocation operations:

Vetoing subsystem module	Workaround
--------------------------	------------

Lock Manager	<p>Gracefully shutdown the SMB applications that have open files, or move those volumes to a different aggregate.</p> <p>Overriding this veto results in loss of SMB lock state, causing disruption and data loss.</p>
Lock Manager NDO	<p>Wait until the locks are mirrored.</p> <p>Overriding this veto causes disruption to Microsoft Hyper-V virtual machines.</p>
RAID	<p>Check the EMS messages to determine the cause of the veto:</p> <p>If the veto is due to nvfile, bring the offline volumes and aggregates online.</p> <p>If disk add or disk ownership reassignment operations are in progress, wait until they complete.</p> <p>If the veto is due to an aggregate name or UUID conflict, troubleshoot and resolve the issue.</p> <p>If the veto is due to mirror resync, mirror verify, or offline disks, the veto can be overridden and the operation restarts after giveback.</p>
Disk Inventory	<p>Troubleshoot to identify and resolve the cause of the problem.</p> <p>The destination node might be unable to see disks belonging to an aggregate being migrated.</p> <p>Inaccessible disks can result in inaccessible aggregates or volumes.</p>
Volume Move Operation	<p>Troubleshoot to identify and resolve the cause of the problem.</p> <p>This veto prevents the volume move operation from aborting during the important cutover phase. If the job is aborted during cutover, the volume might become inaccessible.</p>

### Commands for performing a manual giveback

You can manually initiate a giveback on a node in an HA pair to return storage to the original owner after completing maintenance or resolving any issues that caused the takeover.

If you want to...	Use this command...
Give back storage to a partner node	<code>storage failover giveback -ofnode nodename</code>

Give back storage even if the partner is not in the waiting for giveback mode	<pre>storage failover giveback -ofnode nodename -require-partner-waiting false</pre> <p>Do not use this option unless a longer client outage is acceptable.</p>
Give back storage even if processes are vetoing the giveback operation (force the giveback)	<pre>storage failover giveback -ofnode nodename -override-vetoes true</pre> <p>Use of this option can potentially lead to longer client outage, or aggregates and volumes not coming online after the giveback.</p>
Give back only the CFO aggregates (the root aggregate)	<pre>storage failover giveback -ofnode nodename -only-cfo-aggregates true</pre>
Monitor the progress of giveback after you issue the giveback command	<pre>storage failover show-giveback</pre>

## Testing takeover and giveback

After you configure all aspects of your HA pair, you need to verify that it is operating as expected in maintaining uninterrupted access to both nodes' storage during takeover and giveback operations. Throughout the takeover process, the local (or takeover) node should continue serving the data normally provided by the partner node. During giveback, control and delivery of the partner's storage should return to the partner node.

### Steps

1. Check the cabling on the HA interconnect cables to make sure that they are secure.
2. Verify that you can create and retrieve files on both nodes for each licensed protocol.
3. Enter the following command:

```
storage failover takeover -ofnode partnernode
```

See the man page for command details.

4. Enter either of the following commands to confirm that takeover occurred:

```
storage failover show-takeover
```

```
storage failover show
```

If you have the `storage failover` command's `-auto-giveback` option enabled:

Node	Partner	Takeover Possible	State Description
------	---------	-------------------	-------------------



node 1	node 2	-	Waiting for giveback
node 2	node 1	false	In takeover, Auto giveback will be initiated in number of seconds

If you have the `storage failover` command's `-auto-giveback` option disabled:

Node	Partner	Takeover Possible	State Description
node 1	node 2	-	Waiting for giveback
node 2	node 1	false	In takeover

5. Display all the disks that belong to the partner node (Node2) that the takeover node (Node1) can detect:

```
storage disk show -home node2 -ownership
```

The following command displays all disks belonging to Node2 that Node1 can detect:

```
cluster::> storage disk show -home node2 -ownership
```

Disk	Aggregate	Home	Owner	DR Home	Home ID	Owner ID	DR Home ID	Reserve r	Pool
1.0.2	-	node2	node2	-	4078312453	4078312453	-	4078312452	Pool0
1.0.3	-	node2	node2	-	4078312453	4078312453	-	4078312452	Pool0

6. Confirm that the takeover node (Node1) controls the partner node's (Node2) aggregates:

```
aggr show -fields home-id,home-name, is-home
```

aggregate	home-id	home-name	is-home
aggr0_1	2014942045	node1	true
aggr0_2	4078312453	node2	false
aggr1_1	2014942045	node1	true
aggr1_2	4078312453	node2	false

During takeover, the "is-home" value of the partner node's aggregates is false.

7. Give back the partner node's data service after it displays the "Waiting for giveback" message:

```
storage failover giveback -ofnode partnernode
```

8. Enter either of the following commands to observe the progress of the giveback operation:

```
storage failover show-giveback
```

```
storage failover show
```

9. Proceed, depending on whether you saw the message that giveback was completed successfully:

If takeover and giveback...	Then...
Are completed successfully	Repeat Step 2 through Step 8 on the partner node.
Fail	Correct the takeover or giveback failure and then repeat this procedure.

## Commands for monitoring an HA pair

You can use ONTAP commands to monitor the status of the HA pair. If a takeover occurs, you can also determine what caused the takeover.

If you want to check	Use this command
Whether failover is enabled or has occurred, or reasons why failover is not currently possible	<code>storage failover show</code>
View the nodes on which the storage failover HA-mode setting is enabled You must set the value to <code>ha</code> for the node to participate in a storage failover (HA pair) configuration. The <code>non-ha</code> value is used only in a stand-alone, or single node cluster configuration.	<code>storage failover show -fields mode</code>
Whether hardware-assisted takeover is enabled	<code>storage failover hwassist show</code>
The history of hardware-assisted takeover events that have occurred	<code>storage failover hwassist stats show</code>
The progress of a takeover operation as the partner's aggregates are moved to the node doing the takeover	<code>storage failover show-takeover</code>
The progress of a giveback operation in returning aggregates to the partner node	<code>storage failover show-giveback</code>
Whether an aggregate is home during takeover or giveback operations	<code>aggregate show -fields home-id,owner-id,home-name,owner-name,is-home</code>
Whether cluster HA is enabled (applies only to two node clusters)	<code>cluster ha show</code>
The HA state of the components of an HA pair (on systems that use the HA state)	<code>ha-config show</code> This is a Maintenance mode command.

## Node states displayed by storage failover show-type commands

The following list describes the node states that the `storage failover show` command displays.

Node State	Description
------------	-------------

Connected to partner_name, Automatic takeover disabled.	The HA interconnect is active and can transmit data to the partner node. Automatic takeover of the partner is disabled.
Waiting for partner_name, Giveback of partner spare disks pending.	The local node cannot exchange information with the partner node over the HA interconnect. Giveback of SFO aggregates to the partner is done, but partner spare disks are still owned by the local node. <ul style="list-style-type: none"> <li>• Run the <code>storage failover show-giveback</code> command for more information.</li> </ul>
Waiting for partner_name. Waiting for partner lock synchronization.	The local node cannot exchange information with the partner node over the HA interconnect, and is waiting for partner lock synchronization to occur.
Waiting for partner_name. Waiting for cluster applications to come online on the local node.	The local node cannot exchange information with the partner node over the HA interconnect, and is waiting for cluster applications to come online.
Takeover scheduled. target node relocating its SFO aggregates in preparation of takeover.	Takeover processing has started. The target node is relocating ownership of its SFO aggregates in preparation for takeover.
Takeover scheduled. target node has relocated its SFO aggregates in preparation of takeover.	Takeover processing has started. The target node has relocated ownership of its SFO aggregates in preparation for takeover.
Takeover scheduled. Waiting to disable background disk firmware updates on local node. A firmware update is in progress on the node.	Takeover processing has started. The system is waiting for background disk firmware update operations on the local node to complete.
Relocating SFO aggregates to taking over node in preparation of takeover.	The local node is relocating ownership of its SFO aggregates to the taking-over node in preparation for takeover.
Relocated SFO aggregates to taking over node. Waiting for taking over node to takeover.	Relocation of ownership of SFO aggregates from the local node to the taking-over node has completed. The system is waiting for takeover by the taking-over node.
Relocating SFO aggregates to partner_name. Waiting to disable background disk firmware updates on the local node. A firmware update is in progress on the node.	Relocation of ownership of SFO aggregates from the local node to the taking-over node is in progress. The system is waiting for background disk firmware update operations on the local node to complete.

<p>Relocating SFO aggregates to partner_name. Waiting to disable background disk firmware updates on partner_name. A firmware update is in progress on the node.</p>	<p>Relocation of ownership of SFO aggregates from the local node to the taking-over node is in progress. The system is waiting for background disk firmware update operations on the partner node to complete.</p>
<p>Connected to partner_name. Previous takeover attempt was aborted because reason. Local node owns some of partner's SFO aggregates. Reissue a takeover of the partner with the <code>-bypass-optimization</code> parameter set to true to takeover remaining aggregates, or issue a giveback of the partner to return the relocated aggregates.</p>	<p>The HA interconnect is active and can transmit data to the partner node. The previous takeover attempt was aborted because of the reason displayed under reason. The local node owns some of its partner's SFO aggregates.</p> <ul style="list-style-type: none"> <li>• Either reissue a takeover of the partner node, setting the <code>-bypass-optimization</code> parameter to true to takeover the remaining SFO aggregates, or perform a giveback of the partner to return relocated aggregates.</li> </ul>
<p>Connected to partner_name. Previous takeover attempt was aborted. Local node owns some of partner's SFO aggregates. Reissue a takeover of the partner with the <code>-bypass-optimization</code> parameter set to true to takeover remaining aggregates, or issue a giveback of the partner to return the relocated aggregates.</p>	<p>The HA interconnect is active and can transmit data to the partner node. The previous takeover attempt was aborted. The local node owns some of its partner's SFO aggregates.</p> <ul style="list-style-type: none"> <li>• Either reissue a takeover of the partner node, setting the <code>-bypass-optimization</code> parameter to true to takeover the remaining SFO aggregates, or perform a giveback of the partner to return relocated aggregates.</li> </ul>
<p>Waiting for partner_name. Previous takeover attempt was aborted because reason. Local node owns some of partner's SFO aggregates. Reissue a takeover of the partner with the <code>"-bypass-optimization"</code> parameter set to true to takeover remaining aggregates, or issue a giveback of the partner to return the relocated aggregates.</p>	<p>The local node cannot exchange information with the partner node over the HA interconnect. The previous takeover attempt was aborted because of the reason displayed under reason. The local node owns some of its partner's SFO aggregates.</p> <ul style="list-style-type: none"> <li>• Either reissue a takeover of the partner node, setting the <code>-bypass-optimization</code> parameter to true to takeover the remaining SFO aggregates, or perform a giveback of the partner to return relocated aggregates.</li> </ul>
<p>Waiting for partner_name. Previous takeover attempt was aborted. Local node owns some of partner's SFO aggregates. Reissue a takeover of the partner with the <code>"-bypass-optimization"</code> parameter set to true to takeover remaining aggregates, or issue a giveback of the partner to return the relocated aggregates.</p>	<p>The local node cannot exchange information with the partner node over the HA interconnect. The previous takeover attempt was aborted. The local node owns some of its partner's SFO aggregates.</p> <ul style="list-style-type: none"> <li>• Either reissue a takeover of the partner node, setting the <code>-bypass-optimization</code> parameter to true to takeover the remaining SFO aggregates, or perform a giveback of the partner to return relocated aggregates.</li> </ul>

Connected to partner_name. Previous takeover attempt was aborted because failed to disable background disk firmware update (BDFU) on local node.	The HA interconnect is active and can transmit data to the partner node. The previous takeover attempt was aborted because the background disk firmware update on the local node was not disabled.
Connected to partner_name. Previous takeover attempt was aborted because reason.	The HA interconnect is active and can transmit data to the partner node. The previous takeover attempt was aborted because of the reason displayed under reason.
Waiting for partner_name. Previous takeover attempt was aborted because reason.	The local node cannot exchange information with the partner node over the HA interconnect. The previous takeover attempt was aborted because of the reason displayed under reason.
Connected to partner_name. Previous takeover attempt by partner_name was aborted because reason.	The HA interconnect is active and can transmit data to the partner node. The previous takeover attempt by the partner node was aborted because of the reason displayed under reason.
Connected to partner_name. Previous takeover attempt by partner_name was aborted.	The HA interconnect is active and can transmit data to the partner node. The previous takeover attempt by the partner node was aborted.
Waiting for partner_name. Previous takeover attempt by partner_name was aborted because reason.	The local node cannot exchange information with the partner node over the HA interconnect. The previous takeover attempt by the partner node was aborted because of the reason displayed under reason.
Previous giveback failed in module: module name. Auto giveback will be initiated in number of seconds seconds.	<p>The previous giveback attempt failed in module module_name. Auto giveback will be initiated in number of seconds seconds.</p> <ul style="list-style-type: none"> <li>• Run the <code>storage failover show-giveback</code> command for more information.</li> </ul>
Node owns partner's aggregates as part of the non-disruptive controller upgrade procedure.	The node owns its partner's aggregates due to the non- disruptive controller upgrade procedure currently in progress.
Connected to partner_name. Node owns aggregates belonging to another node in the cluster.	The HA interconnect is active and can transmit data to the partner node. The node owns aggregates belonging to another node in the cluster.
Connected to partner_name. Waiting for partner lock synchronization.	The HA interconnect is active and can transmit data to the partner node. The system is waiting for partner lock synchronization to complete.

Connected to partner_name. Waiting for cluster applications to come online on the local node.	The HA interconnect is active and can transmit data to the partner node. The system is waiting for cluster applications to come online on the local node.
Non-HA mode, reboot to use full NVRAM.	Storage failover is not possible. The HA mode option is configured as non_ha. <ul style="list-style-type: none"> <li>You must reboot the node to use all of its NVRAM.</li> </ul>
Non-HA mode. Reboot node to activate HA.	Storage failover is not possible. <ul style="list-style-type: none"> <li>The node must be rebooted to enable HA capability.</li> </ul>
Non-HA mode.	Storage failover is not possible. The HA mode option is configured as non_ha. <ul style="list-style-type: none"> <li>You must run the <code>storage failover modify -mode ha -node nodename</code> command on both nodes in the HA pair and then reboot the nodes to enable HA capability.</li> </ul>

## Commands for enabling and disabling storage failover

Use the following commands to enable and disable storage failover functionality.

If you want to...	Use this command...
Enable takeover	<code>storage failover modify -enabled true -node nodename</code>
Disable takeover	<code>storage failover modify -enabled false -node nodename</code>



You should only disable storage failover if required as part of a maintenance procedure.

## Halt or reboot a node without initiating takeover in a two-node cluster

You halt or reboot a node in a two-node cluster without initiating takeover when you perform certain hardware maintenance on a node or a shelf and you want to limit down time by keeping the partner node up, or when there are issues preventing a manual takeover and you want to keep the partner node's aggregates up and serving data. Additionally, if technical support is assisting you with troubleshooting problems, they might have you perform this procedure as part of those efforts.

### About this task

- Before you inhibit takeover (using the `-inhibit-takeover true` parameter), you disable cluster HA.



- In a two-node cluster, cluster HA ensures that the failure of one node does not disable the cluster. However, if you do not disable cluster HA before using the `-inhibit-takeover true` parameter, both nodes stop serving data.
- If you attempt to halt or reboot a node before disabling cluster HA, ONTAP issues a warning and instructs you to disable cluster HA.

- You migrate LIFs (logical interfaces) to the partner node that you want to remain online.
- If on the node you are halting or rebooting there are aggregates you want to keep, you move them to the node that you want to remain online.

## Steps

1. Verify both nodes are healthy:

```
cluster show
```

For both nodes, `true` appears in the `Health` column.

```
cluster::> cluster show
Node          Health  Eligibility
-----
node1         true   true
node2         true   true
```

2. Migrate all LIFs from the node that you will halt or reboot to the partner node:  
`network interface migrate-all -node node_name`
3. If on the node you will halt or reboot there are aggregates you want to keep online when the node is down, relocate them to the partner node; otherwise, go to the next step.
  - a. Show the aggregates on the node you will halt or reboot:  
`storage aggregates show -node node_name`

For example, `node1` is the node that will be halted or rebooted:

```

cluster::> storage aggregates show -node node1
Aggregate  Size  Available  Used%  State  #Vols  Nodes  RAID
Status
-----  -
aggr0_node_1_0
          744.9GB  32.68GB  96%  online        2  node1  raid_dp,
normal
aggr1      2.91TB  2.62TB  10%  online        8  node1  raid_dp,
normal
aggr2      4.36TB  3.74TB  14%  online       12  node1  raid_dp,
normal
test2_aggr 2.18TB  2.18TB  0%   online        7  node1  raid_dp,
normal
4 entries were displayed.

```

b. Move the aggregates to the partner node:

```

storage aggregate relocation start -node node_name -destination node_name
-aggregate-list aggregate_name

```

For example, aggregates `aggr1`, `aggr2` and `test2_aggr` are being moved from `node1` to `node2`:

```

storage aggregate relocation start -node node1 -destination node2 -aggregate
-list aggr1,aggr2,test2_aggr

```

4. Disable cluster HA:

```

cluster ha modify -configured false

```

The return output confirms HA is disabled: Notice: HA is disabled



This operation does not disable storage failover.

5. Halt or reboot and inhibit takeover of the target node, by using the appropriate command:

- `system node halt -node node_name -inhibit-takeover true`
- `system node reboot -node node_name -inhibit-takeover true`



In the command output, you will see a warning asking you if you want to proceed, enter `y`.

6. Verify that the node that is still online is in a healthy state (while the partner is down):

```

cluster show

```



For the online node, `true` appears in the `Health` column.



In the command output, you will see a warning that cluster HA is not configured. You can ignore the warning at this time.

7. Perform the actions that required you to halt or reboot the node.

8. Boot the offlined node from the `LOADER` prompt:

```
boot_ontap
```

9. Verify both nodes are healthy:

```
cluster show
```

For both nodes, `true` appears in the `Health` column.



In the command output, you will see a warning that cluster HA is not configured. You can ignore the warning at this time.

10. Reenable cluster HA:

```
cluster ha modify -configured true
```

11. If earlier in this procedure you relocated aggregates to the partner node, move them back to their home node; otherwise, go to the next step:

```
storage aggregate relocation start -node node_name -destination node_name  
-aggregate-list aggregate_name
```

For example, aggregates `aggr1`, `aggr2` and `test2_aggr` are being moved from node `node2` to node `node1`:

```
storage aggregate relocation start -node node2 -destination node1 -aggregate  
-list aggr1,aggr2,test2_aggr
```

12. Revert LIFs to their home ports:

a. View LIFs that are not at home:

```
network interface show -is-home false
```

b. If there are non-home LIFs that were not migrated from the down node, verify it is safe to move them before reverting.

c. If it is safe to do so, revert all LIFs home.

```
network interface revert *
```

## Rest API management with System Manager

### Rest API management with System Manager

The REST API log captures the API calls that System Manager issues to ONTAP. You can use the log to understand the nature and sequence of the calls needed to perform the various ONTAP administrative tasks.

#### How System Manager uses the REST API and API log

There are several ways that REST API calls are issued by System Manager to ONTAP.

## When does System Manager issue API calls

Here are the most important examples of when System Manager issues ONTAP REST API calls.

### Automatic page refresh

System Manager automatically issues API calls in the background to refresh the displayed information, such as on the dashboard page.

### Display action by user

One or more API calls are issued when you display a specific storage resource or a collection of resources from the System Manager UI.

### Update action by user

An API call is issued when you add, modify, or delete an ONTAP resource from the System Manager UI.

### Reissuing an API call

You can also manually reissue an API call by clicking a log entry. This displays the raw JSON output from the call.

## Where to find more information

- [ONTAP 9 Automation docs](#)

## Accessing the REST API log

You can access the log containing a record of the ONTAP REST API calls made by System Manager. When displaying the log, you can also reissue API calls and review the output.

### Steps

1. At the top of the page, click  to display the REST API log.

The most recent entries are displayed at the bottom of the page.

2. On the left, click **DASHBOARD** and observe the new entries being created for the API calls issued to refresh the page.
3. Click **STORAGE** and then click **Qtrees**.

This causes System Manager to issue a specific API call to retrieve a list of the Qtrees.

4. Locate the log entry describing the API call which has the form:

```
GET /api/storage/qtrees
```

You will see additional HTTP query parameters included with the entry, such as `max_records`.

5. Click the log entry to reissue the GET API call and display the raw JSON output.

Example

```

1 {
2   "records": [
3     {
4       "svm": {
5         "uuid": "19507946-e801-11e9-b984-00a0986ab770",
6         "name": "SMQA",
7         "_links": {
8           "self": {
9             "href": "/api/svm/svms/19507946-e801-11e9-b984-
10            00a0986ab770"
11           }
12         },
13         "volume": {
14           "uuid": "1e173258-f98b-11e9-8f05-00a0986abd71",
15           "name": "vol_vol_test2_dest_dest",
16           "_links": {
17             "self": {
18               "href": "/api/storage/volumes/1e173258-f98b-11e9-8f05-
19              00a0986abd71"
20             }
21           },
22           "id": 1,
23           "name": "test2",
24           "security_style": "mixed",
25           "unix_permissions": 777,
26           "export_policy": {
27             "name": "default",
28             "id": 12884901889,
29             "_links": {
30               "self": {
31                 "href": "/api/protocols/nfs/export-policies/12884901889"
32               }
33             }
34           },
35           "path": "/vol_vol_test2_dest_dest/test2",
36           "_links": {
37             "self": {
38               "href": "/api/storage/qtrees/1e173258-f98b-11e9-8f05-
39              00a0986abd71/1"
40             }
41           },
42         ],

```

```
43     "num_records": 1,  
44     "_links": {  
45         "self": {  
46             "href":  
         "/api/storage/qtrees?max_records=20&fields=*&name=!%22%22"  
47         }  
48     }  
49 }
```

# Volume administration

## Volume and LUN management with System Manager

### Volume administration overview with System Manager

Beginning with ONTAP 9.7, you can use System Manager to manage logical storage, such as FlexVol volumes and LUNs, qtrees, storage efficiency, and quotas.

If you are using the classic System Manager (available only in ONTAP 9.7 and earlier), refer to [Managing logical storage](#)

### Manage volumes

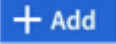



After you display a list of volumes in System Manager, you can perform various actions to manage the volumes.

#### Steps


1. In System Manager, click **Storage > Volumes**.

The list of volumes is displayed.

2. You can perform the following:

To perform this task...	Take these actions...
Add a volume	Click  <b>Add</b> . See <a href="#">Add a volume</a> .
Manage multiple volumes	Check the boxes next to the volumes. <ul style="list-style-type: none"><li>• Click  <b>Delete</b> to delete the selected volumes.</li><li>• Click  <b>Protect</b> to assign a protection policy to the selected volumes.</li><li>• Click  <b>More</b> to select one of the following actions to perform for all selected volumes:<ul style="list-style-type: none"><li>◦ Enable quota</li><li>◦ Take offline</li><li>◦ Move</li><li>◦ Show Deleted Volumes</li></ul></li></ul>

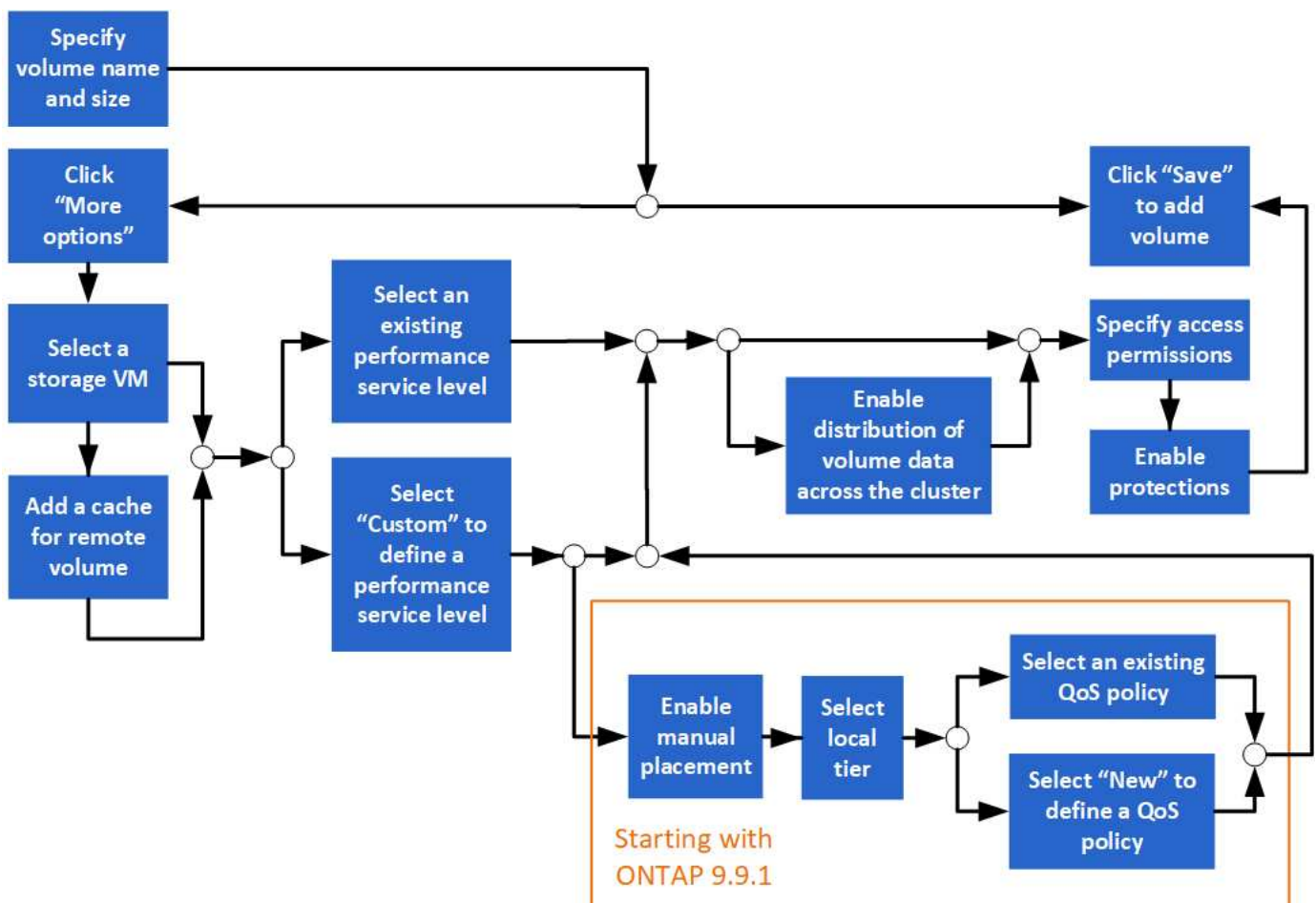
## Manage a single volume

Next to the volume, click , then select one of the following actions to perform:

- Edit
- Resize (Beginning with ONTAP 9.10.1, and only for online volumes and DP FlexVol volumes)
- Delete
- Clone
- Take Offline (or Bring Online)
- Enable Quota (or Disable Quota)
- Edit Export Policy
- Edit Mount Path
- Move
- Edit Cloud Tier Settings
- Protect

## Add a volume

You can create a volume and add it to an existing storage VM that is configured for NFS or SMB service.



## Before you Start

A storage VM that is configured for NFS or SMB service should exist in the cluster.

### Steps

1. Go to **Storage > Volumes**.
2. Click **+ Add**.
3. Specify a name and size for the volume.
4. Perform one of the following steps:

Click this button...	To perform this action...
<b>Save</b>	The volume is created and added using the system defaults. No additional steps are required.
<b>More Options</b>	Proceed to <a href="#">Step 5</a> to define the specifications for the volume.

5. The volume name and size are shown if you previously specified them. Otherwise, enter the name and size.
6. Select a storage VM from the pull-down list.

Only storage VMs configured with the NFS protocol are listed. If only one storage VM configured with the NFS protocol is available, the **Storage VM** field is not shown.

7. To add a cache for the remote volume, select **Add a cache for remote volume** and specify the following values:
  - Select a cluster.
  - Select a storage VM.
  - Select the volume that you want to be a cache volume.
8. In the **Storage and Optimization** section, specify the following values:
  - a. The capacity of the volume is already shown, but you can modify it.
  - b. In the **Performance Service Level** field, select a service level:

When you select this service level...	This occurs...
An existing service level, such as "Extreme", "Performance", or "Value".  Only the service levels that are valid for the system platform (AFF, FAS, or others) are displayed.	A local tier or tiers are automatically chosen. Proceed to <a href="#">Step 9</a> .
Custom	Proceed to <a href="#">Step 8c</a> to define a new service level.

- c. Beginning with ONTAP 9.9.1, you can use System Manager to manually select the local tier on which you want to place the volume you are creating (if you have selected the "Custom" service level).



This option is not available if you select **Add as a cache for a remote volume** or **Distribute volume data across the cluster** (see below).

When you make this choice...	You perform these steps...
<b>Manual placement</b>	Manual placement is enabled. The <b>Distribute volume data across the cluster</b> selection is disabled (see below). Proceed to <a href="#">Step 8d</a> to complete the process.
No selection	Manual placement is not enabled. The local tier is automatically selected. Proceed to <a href="#">Step 9</a> .

- d. Select a local tier from the pull-down menu.
- e. Select a QoS policy.

Select "Existing" to choose from a list of existing policies, or select "New" to enter the specifications of a new policy.

9. In the **Optimization options** section, determine if you want to distribute the volume data across the cluster:

When you make this choice...	This occurs...
<b>Distribute volume data across the cluster</b>	The volume you are adding becomes a FlexGroup volume. This option is not available if you previously selected <b>Manual placement</b> .
No selection	The volume you are adding becomes a FlexVol volume by default.

10. In the **Access Permissions** section, specify the access permissions for the protocols for which the volume is configured.

Beginning with ONTAP 9.11.1, the new volume will not be shareable by default. You can specify the default access permissions by ensuring the following check boxes are checked:

- **Export via NGS:** Creates the volume with the "default" export policy that grants users full access to the data.
- **Share via SMB/CIFS:** Creates a share with an auto-generated name, which you can edit. Access is granted to "Everyone". Also, you can specify the permission level.

11. In the **Protection** section, specify the protections for the volume. If you select **Enable SnapMirror (Local or Remote)**, then specify the protection policy and settings for the destination cluster from the pull-down lists.

12. Click **Save**.

The volume is created and added to the cluster and storage VM.

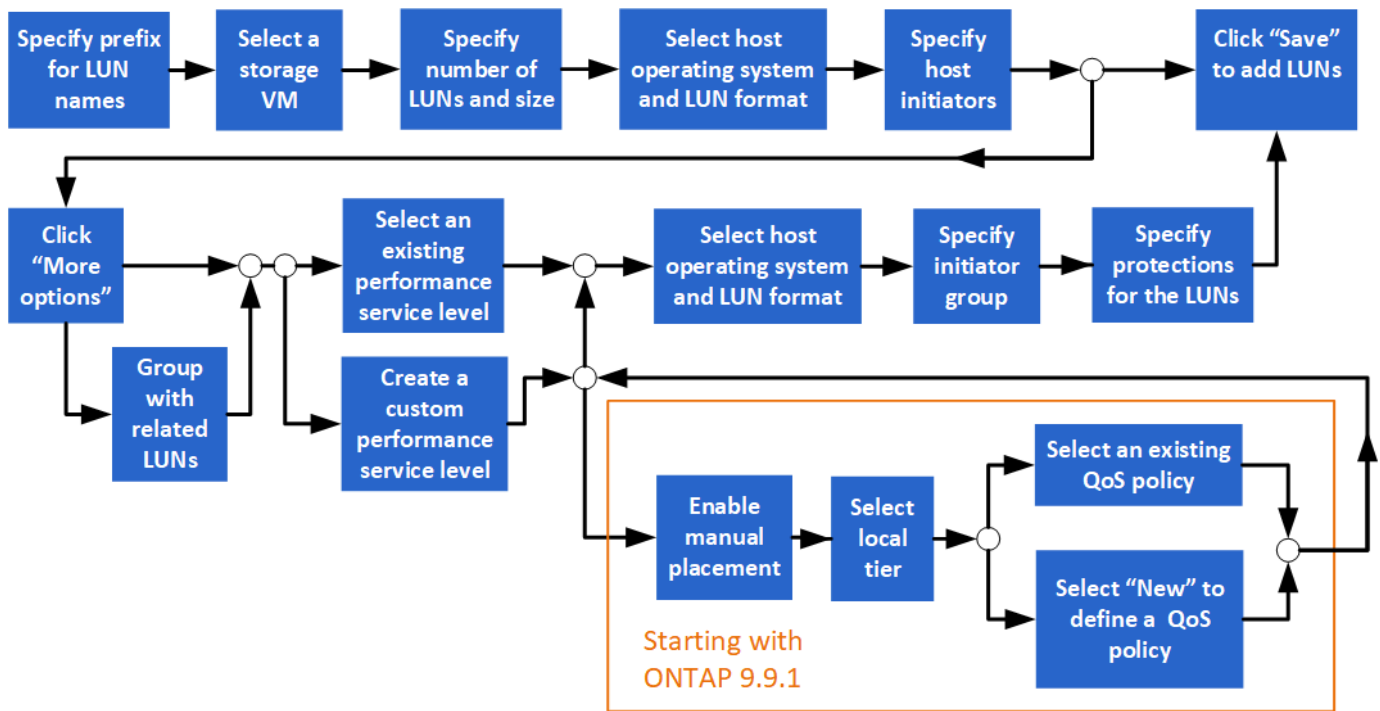


You can also save the specifications of this volume to an Ansible Playbook. For more details, go to [Use Ansible Playbooks to add or edit volumes or LUNs](#).

## Add LUNs

You can create LUNs and add them to an existing storage VM that is configured with the SAN protocol.





### Before you Start

A storage VM that is configured for SAN service should exist in the cluster.

### Steps

1. Go to **Storage > LUNs**.
2. Click **+ Add**.
3. Specify a prefix that will be used at the start of each LUN name. (If you are creating only one LUN, enter the LUN name.)
4. Select a storage VM from the pull-down list.

Only storage VMs that are configured for the SAN protocol are listed. If only one storage VM that is configured for the SAN protocol is available, then the **Storage VM** field is not displayed.

5. Indicate how many LUNs you want to create and the size of each LUN.
6. Select the host operating system and LUN format from the pull-down lists.
7. Enter the host initiators, and separate them with commas.
8. Perform one of the following actions:

Click this button...	To perform this action...
<b>Save</b>	The LUNs are created with the specifications you entered. System defaults are used for other specifications. No additional steps are required.
<b>More Options</b>	Proceed to <a href="#">Step 9</a> to define additional specifications for the LUNs.

9. The LUN prefix is already shown if you previously entered it, but you can modify it. Otherwise, enter the prefix.
10. Select a storage VM from the pull-down list.

Only storage VMs that are configured for the SAN protocol are listed. If only one storage VM that is configured for the SAN protocol is available, then the **Storage VM** field is not displayed.

11. Determine how you want the LUNs to be grouped:

When you make this choice...	This occurs...
<b>Group with related LUNs</b>	The LUNs will be grouped together with related LUNs on an existing volume on the storage VM.
No selection	The LUNs will be grouped together on a volume called "container".

12. In the **Storage and Optimization** section, specify the following values:

- a. The number and capacity of the LUNs are already shown if you previously entered them, but you can modify them. Otherwise, enter the values.
- b. In the **Performance Service Level** field, select a service level:

When you select this service level...	This occurs...
An existing service level, such as "Extreme", "Performance", or "Value".  Only the service levels that are valid for the system platform (AFF, FAS, or others) are displayed.	A local tier is automatically chosen. Proceed to <a href="#">Step 13</a> .
Custom	Proceed to <a href="#">Step 12c</a> to define a new service level.

- c. Beginning with ONTAP 9.9.1, you can use System Manager to manually select the local tier on which you want to place the LUNs you are creating (if you have selected the "Custom" service level).

When you make this choice...	You perform these steps...
<b>Manual placement</b>	Manual placement is enabled. Proceed to <a href="#">Step 12d</a> to complete the process.
No selection	Manual selection is not enabled. The local tier is automatically selected. Proceed to <a href="#">Step 13</a> .

- d. Select a local tier from the pull-down menu.
- e. Select a QoS policy.

Select "Existing" to choose from a list of existing policies, or select "New" to enter the specifications of a new policy.

13. In the **Host Information** section, the host operating system and LUN format are already shown, but you can modify them.

14. Under **Host Mapping**, select the type of initiators for the LUNs:

- **Existing initiator group:** Select an initiator group for the list that displays.
- **New initiator group using existing initiator groups:** Specify the name of the new group, and select

the group or groups that you want to use to create the new group.

- **Host initiators:** Specify a name from the new initiator group, and click **+Add Initiator** to add initiators to the group.

15. In the **Protection** section, specify the protections for the LUNs.

If you select **Enable SnapMirror (Local or Remote)**, then specify the protection policy and settings for the destination cluster from the pull-down lists.

16. Click **Save**.

The LUNs are created and added to the cluster and storage VM.



You can also save the specifications of these LUNs to an Ansible Playbook. For more details, go to [Use Ansible Playbooks to add or edit volumes or LUNs](#).

## Expand storage

Using System Manager, you can increase the size of your volume or LUN so that more space is available to your host. The size of a LUN cannot exceed the size of the containing volume.

- [Increase the size of a volume](#)
- [Increase the size of a LUN](#)


Also, you can add a LUN to an existing volume. The processes are different when using System Manager with ONTAP 9.7 or 9.8

- [Add a LUN to an existing volume \(ONTAP 9.7\)](#)
- [Add a LUN to an existing volume \(ONTAP 9.8\)](#)

Also, beginning with ONTAP 9.8, you can use System Manager to add a LUN to an existing volume.


### Increase the size of a volume

#### Steps

1. Click **Storage > Volumes**.
2. Hover over the name of the volume you want to increase in size.
3. Click .
4. Select **Edit**.
5. Increase the capacity value.

### Increase the size of a LUN

#### Steps

1. Click **Storage > LUNs**.
2. Hover over the name of the LUN you want to increase in size.
3. Click .

4. Select **Edit**.
5. Increase the capacity value.

### Add a LUN to an existing volume (ONTAP 9.7)

To use System Manager with ONTAP 9.7 to add a LUN to an existing volume, you should switch to the Classical View first.

#### Steps

1. Log in to System Manager in ONTAP 9.7.
2. Click **Classical View**.
3. Select **Storage > LUNs > Create**
4. Specify the details to create the LUN.
5. Specify to which existing volume or qtree the LUN should be added.

### Add a LUN to an existing volume (ONTAP 9.8)

Beginning with ONTAP 9.8, you can use System Manager to add a LUN to an existing volume that already has a least one LUN.

#### Steps

1. Click **Storage > LUNs**.
2. Click **Add+**.
3. Complete the fields in the **Add LUNs** window.
4. Select **More Options**.
5. Select the checkbox labeled **Group with related LUNs**.
6. In the drop-down field, select a LUN that exists on the volume to which you want to add another LUN.
7. Complete the rest of the fields. For **Host Mapping**, click one of the radio buttons:
  - **Existing initiator group** lets you select an existing group from a list.
  - **New initiator group** lets you enter a new group in the field.

## Recover deleted volumes

If you have accidentally deleted one or more FlexVol volumes, you can use System Manager to recover these volumes. Beginning with ONTAP 9.8, you can also use System Manager to recover FlexGroup volumes. You can also delete the volumes permanently by purging the volumes.

The volume retention time can be set on a storage VM level. By default, the volume retention time is set to 12 hours.

### Selecting deleted volumes

#### Steps

1. Click **Storage > Volumes**.
2. Click **More > Show Deleted Volumes**.

3. Select the volumes and click the desired action to recover or permanently delete the volumes.

## Resetting the volume configurations

Deleting a volume deletes the associated configurations of the volume. Recovering a volume does not reset all the configurations. Perform the following tasks manually after recovering a volume to bring the volume back to its original state:

### Steps

1. Rename the volume.
2. Set up a junction path (NAS).
3. Create mappings for LUNs in the volume (SAN).
4. Associate a Snapshot policy and export policy with the volume.
5. Add new quota policy rules for the volume.
6. Add a QOS policy for the volume.

## Save storage space using compression, compaction, and deduplication

For volumes on non-AFF clusters, you can run deduplication, data compression, and data compaction together or independently to achieve optimal space savings.

- Deduplication eliminates duplicate data blocks.
- Data compression compresses the data blocks to reduce the amount of physical storage that is required.
- Data compaction stores more data in less space to increase storage efficiency.



These tasks are supported for volumes on non-AFF clusters. Beginning with ONTAP 9.2, all inline storage efficiency features, such as inline deduplication and inline compression, are enabled by default on AFF volumes.

### Steps

1. Click **Storage > Volumes**.
2. Next to the name of the volume for which you want to save storage, click .
3. Click **Edit** and scroll to **Storage Efficiency**.
4. *Optional:* If you want to enable background deduplication, ensure the checkbox is checked.
5. *Optional:* If you want to enable background compression, specify the storage efficiency policy and ensure the checkbox is checked.
6. *Optional:* If you want to enable inline compression, ensure the checkbox is checked.

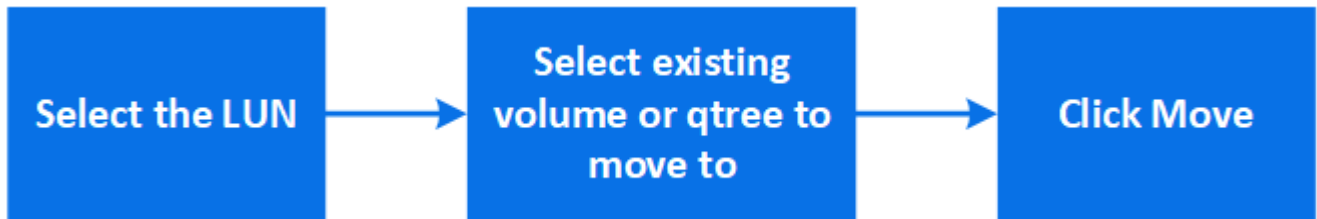
## Balance loads by moving LUNs

You can move a LUN to another volume within the storage VM to balance the load, or you can move it to a volume with a higher performance service level to improve performance.

### Move restrictions

- A LUN cannot be moved to a qtree within the same volume.

- A LUN created from a file using the CLI cannot be moved with System Manager.
- LUNs that are online and serving data cannot be moved.
- LUNs cannot be moved if the allocated space in the destination volume cannot contain the LUN (even if autogrow is enabled on the volume).
- LUNs on SnapLock volumes cannot be moved with System Manager.



### Steps

1. Click **Storage > LUNs**.
2. Select the LUN that you want to move and click **Move**.
3. Select an existing volume to which you want to move the LUN. If the volume contains qtrees, select the qtree.



While the Move operation is in progress, the LUN is displayed on both the origin and destination volume.

## Balance loads by moving volumes to another tier

Beginning with ONTAP 9.8, you can use System Manager to move a volume to another tier to balance the load.

Beginning with ONTAP 9.9.1, you can also move volumes based on analysis of active and inactive data storage. For more information, see [File System Analytics overview](#).

### Steps

1. Click **Storage > Volumes**.
2. Select the volume or volumes that you want to move, and then click **Move**.
3. Select an existing tier (aggregate) to which you want to move the volume or volumes.

## Use Ansible Playbooks to add or edit volumes or LUNs

Beginning with ONTAP 9.9.1, you can use Ansible Playbooks with System Manager when you want to add or edit volumes or LUNs.

This feature lets you use the same configuration multiple times or use the same configuration with slight changes when you add or edit volumes or LUNs.

### Enable or disable Ansible Playbooks

You can enable or disable the use of Ansible Playbooks with System Manager.

### Steps

1. In System Manager, go to the UI settings in the cluster settings page:

### **Cluster > Settings**

2. Under **UI Settings**, change the slider switch to "Enabled" or "Disabled".

## **Save a volume configuration to an Ansible Playbook**

When you create or modify the configuration of a volume, you can save the configuration as Ansible Playbook files.

### **Steps**

1. Add or Edit the volume:

#### **Volume > Add (or Volume > Edit)**

2. Specify or edit the configuration values of the volume.
3. Select **Save to Ansible Playbook** to save the configuration to Ansible Playbook files.

A zip file is downloaded that contains the following files:

- **variable.yaml**: The values you entered or modified to add or edit the volume.
- **volumeAdd.yaml** (or **volumeEdit.yaml**): The test cases that are required to create or modify the values when reading the inputs from the `variable.yaml` file.

## **Save a LUN configuration to an Ansible Playbook**

When you create or modify the configuration of a LUN, you can save the configuration as Ansible Playbook files.

### **Steps**

1. Add or Edit the LUN:

#### **LUN > Add (or LUN > Edit)**

2. Specify or edit the configuration values of the LUN.
3. Select **Save to Ansible Playbook** to save the configuration to Ansible Playbook files:

A zip file is downloaded that contains the following files:

- **variable.yaml**: The values you entered or modified to add or edit the LUN.
- **lunAdd.yaml** (or **lunEdit.yaml**): The test cases that are required to create or modify the values when reading the inputs from the `variable.yaml` file.


## **Download Ansible Playbook files from global search results**

You can download Ansible Playbook files when you do a global search.

### **Steps**

1. In the search field, enter "volume" or "LUN" or "Playbook".
2. Find the search result, either "Volume Management (Ansible Playbook)" or "LUN Management (Ansible

Playbook)”).

3. Click on  to download the Ansible Playbook files.

## Work with Ansible Playbook files

Ansible Playbook files can be modified and run to specify configurations for volumes and LUNs.

### About this task

You use two files to perform an operation (either an “add” or an “edit”):

If you want to...	Use this variable file...	And use this run file...
Add a volume	volumeAdd-variable.yaml	valueAdd.yaml
Edit a volume	volumeEdit-variable.yaml	volumeEdit.yaml
Add a LUN	lunAdd-variable.yaml	lunAdd.yaml
Edit a LUN	lunEdit-variable.yaml	lunEdit.yaml

### Steps

1. Modify the variables file.

The file contains the various values that you use to configure the volume or LUN.

- If you do not change the values, leave them commented.
- If you modify the values, remove the commenting.

2. Run the associated run file.

The run file contains the test cases that are required to create or modify the values when reading the inputs from the variable file.

3. Enter your user login credentials.


## Manage storage efficiency policies

Beginning with ONTAP 9.8, you can use System Manager to enable, disable, add, edit, or delete efficiency policies for storage VMs on FAS systems.



This function is not available on AFF systems.



### Steps

1. Select **Storage > Storage VMs**
2. Select the storage VM for which you want to manage efficiency policies.
3. On the **Settings** tab, select  in the **Efficiency Policy** section. The efficiency policies for that storage VM are displayed.

You can perform the following tasks:

- **Enable or disable** an efficiency policy by clicking the toggle button in the Status column.



- **Add** an efficiency policy by clicking on **Add+**.
- **Edit** an efficiency policy by clicking on  to the right of the policy name and selecting **Edit**.
- **Delete** an efficiency policy by clicking on  to the right of the policy name and selecting **Delete**.

## Manage resources using quotas

Beginning with ONTAP 9.7, you can configure and manage usage quotas with System Manager.

If you are using the ONTAP CLI to configure and manage usage quotas, refer to the [Logical Storage Management Guide](#).

If you are using legacy OnCommand System Manager for ONTAP 9.7 and earlier releases to configure and manage usage quotas, see the following for your release:

- [ONTAP 9.6 and 9.7 Documentation](#)
- [ONTAP 9.5 Documentation](#)
- [ONTAP 9.4 Documentation](#)
- [ONTAP 9.3 Documentation](#)
- [ONTAP 9.2 Archived Documentation](#)
- [ONTAP 9.0 Archived Documentation](#)

### Quota overview

Quotas provide a way to restrict or track the disk space and number of files used by a user, group, or qtree. Quotas are applied to a specific volume or qtree.

You can use quotas to track and limit resource usage in volumes and provide notification when resource usage reaches specific levels.

Quotas can be soft or hard. Soft quotas cause ONTAP to send a notification when specified limits are exceeded, and hard quotas prevent a write operation from succeeding when specified limits are exceeded.

## Set quotas to limit resource use

Add quotas to limit the amount of disk space the quota target can use.

You can set a hard limit and a soft limit for a quota.

Hard quotas impose a hard limit on system resources; any operation that would result in exceeding the limit fails. Soft quotas send a warning message when resource usage reaches a certain level, but they do not affect data access operations, so you can take appropriate action before the quota is exceeded.

### Steps

1. Click **Storage > Quotas**.
2. Click **Add**.

## Clone volumes and LUNs for testing

You can clone volumes and LUNs to create temporary, writable copies for testing. The clones reflect the current, point-in-time state of the data. You can also use clones to give additional users access to data without giving them access to production data.




The FlexClone license should be installed on the storage system.

### Cloning a volume

Create a clone of a volume, as follows:

#### Steps


1. Click **Storage > Volumes**.
2. Click  next to the name of the volume you want to clone.
3. Select **Clone** from the list.
4. Specify a name for the clone and complete the other selections.
5. Click **Clone** and verify that the volume clone appears in the list of volumes.

Alternatively, you can clone a volume from the **Overview** that displays when you view volume details.

### Cloning a LUN

Create a clone of a LUN, as follows:

#### Steps

1. Click **Storage > LUNs**.
2. Click  next to the name of the LUN you want to clone.
3. Select **Clone** from the list.
4. Specify a name for the clone and complete the other selections.
5. Click **Clone** and verify that the LUN clone appears in the list of LUNs.

Alternatively, you can clone a LUN from the **Overview** that displays when you view LUN details.

When you create a LUN clone, System Manager automatically enables the deletion of the clone when space is needed.

## Search, filter, and sort information in System Manager

You can search for various actions and objects in System Manager. You can also search table data for specific entries.

System Manager provides two types of searching:

- [Global searching](#)

When you enter a search argument in the field at the top of each page, System Manager searches throughout the interface to find matches. You can then sort and filter the results.

- [Table-grid searching](#)

Beginning with ONTAP 9.8, when you enter a search argument in the field at the top of a table grid, System Manager searches only the columns and rows of that table to find matches.

## Global searching

At the top of each page in System Manager, you can use a global search field to search various objects and actions in the interface. For example, you can search for different objects by name, pages available in the navigator column (on the left side), various action items, like "Add Volume" or "Add License", and links to external help topics. You can also filter and sort the results.



For better results, perform searching, filtering, and sorting one minute after logging in and five minutes after creating, modifying, or deleting an object.

## Getting search results

The search is not case-sensitive. You can enter a variety of text strings to find the page, actions, or topics you need. Up to 20 results are listed. If more results are found, you can click **Show more** to view all results. The following examples describe typical searches:

Type of search	Sample search string	Sample search results
By object name	vol_	vol_lun_dest on storage VM: svm0 (Volume) /vol/vol...est1/lun on storage VM: svm0 (LUN) svm0:vol_lun_dest1 role: Destination (Relationship)
By location in interface	volume	Add Volume (Action) Protection – Overview (Page) Recover deleted volume (Help)
By actions	add	Add Volume (Action) Network – Overview (Page) Expand volumes and LUNs (Help)
By help content	san	Storage – Overview (Page) SAN overview (Help) Provision SAN storage for databases (Help)

## Filtering search results


You can narrow the results with filters, as shown in the following examples:

Filter	Syntax	Sample search string
By object type	<type>:<objectName>	volume:vol_2
By object size	<type><size-symbol><number><units>	luns<500mb
By broken disks	“broken disk” or “unhealthy disk”	unhealthy disk

By network interface	<IP address>	172.22.108.21
----------------------	--------------	---------------

### Sorting search results

When you view all the search results, they are sorted alphabetically. You can sort the results by clicking

 **Filter** and selecting how you want to sort the results.

### Table-grid searching

Beginning with ONTAP 9.8, whenever System Manager displays information in a table-grid format, a search button appears at the top of the table.

When you click **Search**, a text field appears in which you can enter a search argument. System Manager searches the entire table and displays only the rows that contain text that matches your search argument.

You can use an asterisk ( \* ) as a "wildcard" character as a substitute for characters. For example, searching for `vol*` might provide rows that contain the following:

- vol\_122\_D9
- vol\_lun\_dest1
- vol2866
- volspec1
- volum\_dest\_765
- volume
- volume\_new4
- volume9987

## Monitor capacity in System Manager

Using System Manager, you can view how much storage capacity has been used and how much is still available for a cluster. Also, beginning with ONTAP 9.10.1, you can use System Manager to view historical data about the cluster's capacity and projections about how much capacity will be used or available in the future.

- [Capacity measurements in System Manager](#)
- [Measurements of used capacity](#)
- [Measurement terms](#)
- [Capacity measurement units](#)
- [View capacity measurements for the cluster](#)

### Capacity measurements in System Manager

System capacity can be measured as physical space or logical space. Recent versions of System Manager use measurements of both physical and logical capacity.

The differences between the two measurements are explained in the following descriptions:

- **Physical capacity:** Physical space refers to the physical blocks of storage used in the volume. The value for physical used capacity is typically smaller than the value for logical used capacity due to the reduction of data from storage efficiency features (such as deduplication and compression).
- **Logical capacity:** Logical space refers to the usable space (the logical blocks) in a volume. Logical space refers to how theoretical space can be used, without accounting for results of deduplication or compression. The value for logical space used is derived from the amount of physical space used plus the savings from storage efficiency features (such as deduplication and compression) that have been configured. This measurement often appears larger than the physical used capacity because it includes Snapshot copies, clones, and other components, and it does not reflect the data compression and other reductions in the physical space. Thus, the total logical capacity could be higher than the provisioned space.



In System Manager, capacity representations do not account for root storage tier (aggregate) capacities.

### Measurements of used capacity

Measurements of used capacity are displayed differently depending on the version of System Manager you are using, as explained in the following table:

Version of System Manager	Term used for capacity	Type of capacity referred to
9.5 and 9.6 (Classic view)	Used	Physical space used
9.7 and 9.8	Used	Logical space used (if storage efficiency settings have been enabled)
9.9.1 and later	Logical Used	Logical space used (if storage efficiency settings have been enabled)

### Measurement terms

The following terms are used when describing capacity:

- **Physical used:** Displays the amount of capacity used in the physical blocks of a volume.
- **Physical used %:** Displays the percentage of capacity used in the physical blocks of a volume compared to the provisioned size.
- **Logical used:** Displays the amount of used space without considering the space saved by storage efficiency features.
- **Logical used %:** Displays the percentage of the current logical used capacity compared to the provisioned size, excluding the Snapshot reserve of the volume. This value can be greater than 100%, because it includes efficiency savings in the volume.

### Capacity measurement units

System Manager calculates storage capacity based on binary units of 1024 (2<sup>10</sup>) bytes. In ONTAP 9.10.0 and earlier, these units were displayed in System Manager as KB, MB, GB, TB, and PB. Beginning with ONTAP

9.10.1, they are displayed in System Manager as KiB, MiB, GiB, TiB, and PiB.



The units used in System Manager for throughput continue to be KB/s, MB/s, GB/s, TB/s, and PB/s for all releases of ONTAP.

Capacity unit displayed in System Manager for ONTAP 9.10.0 and earlier	Capacity unit displayed in System Manager for ONTAP 9.10.1	Calculation	Value in bytes
KB	KiB	1024	1024 bytes
MB	MiB	1024 * 1024	1,048,576 bytes
GB	GiB	1024 * 1024 * 1024	1,073,741,824 bytes
TB	TiB	1024 * 1024 * 1024 * 1024	1,099,511,627,776 bytes
PB	PiB	1024 * 1024 * 1024 * 1024 * 1024	1,125,898,010,834,824 bytes

#### Additional information:

[Logical space reporting and enforcement for volumes](#)


#### View capacity measurements for the cluster

You can view capacity measurements for the cluster on the Dashboard in System Manager.

#### Before you begin

To view data related to the capacity in the cloud, you must have an account with Active IQ Digital Advisor and be connected.

#### Steps

1. In System Manager, click **Dashboard**.
2. In the **Capacity** section, you can view the following:
  - Total used capacity of the cluster
  - Total available capacity of the cluster
  - Percentages of used and available capacity.
  - Ratio of data reduction.
  - Amount of capacity used in the cloud.
  - History of capacity usage.
  - Projection of capacity usage
3. Click  to view more details about the capacity of the cluster.

# Logical storage management with the CLI

## Logical storage management overview with the CLI

Using the ONTAP CLI, you can create and manage FlexVol volumes, use FlexClone technology to create efficient copies of volumes, files, and LUNs, create qtrees and quotas, and manage efficiency features like deduplication and compression.

You should use these procedures under the following circumstances:

- You want to understand the range of ONTAP FlexVol volume capabilities and storage efficiency features.
- You want to use the command-line interface (CLI), not System Manager or an automated scripting tool.

## Create and manage volumes

### Create a volume

You can create a volume and specify its junction point and other properties by using the `volume create` command.

### What you'll need

The SVM for the new volume and the aggregate that will supply the storage to the volume must already exist.

If the SVM has a list of associated aggregates, the aggregate must be included in the list.

### About this task

A volume must include a *junction path* for its data to be made available to clients. You can specify the junction path when you create a new volume. If you create a volume without specifying a junction path, you must *mount* the volume in the SVM namespace using the `volume mount` command.

### Steps

1. Create a volume:

```
volume create -vserver vserver_name -volume volume_name -aggregate
aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
{ntfs|unix|mixed} -user user_name_or_number -group group_name_or_number
-junction-path junction_path [-policy export_policy_name]
```

The `-security style`, `-user`, `-group`, `-junction-path`, and `-policy` options are for NAS namespaces only.

The choices for `-junction-path` are the following:

- Directly under root, for example, `/new_vol`

You can create a new volume and specify that it be mounted directly to the SVM root volume.

- Under an existing directory, for example, `/existing_dir/new_vol`

You can create a new volume and specify that it be mounted to an existing volume (in an existing hierarchy), expressed as a directory.

If you want to create a volume in a new directory (in a new hierarchy under a new volume), for example, `/new_dir/new_vol`, then you must first create a new parent volume that is junctioned to the SVM root volume. You would then create the new child volume in the junction path of the new parent volume (new directory).

2. Verify that the volume was created with the desired junction point:

```
volume show -vserver vserver_name -volume volume_name -junction
```

### Examples

The following command creates a new volume named `users1` on the SVM `vs1.example.com` and the aggregate `aggr1`. The new volume is made available at `/users`. The volume is 750 GB in size, and its volume guarantee is of type `volume` (by default).

```
cluster1::> volume create -vserver vs1.example.com -volume users1
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users1 -junction
```

Vserver	Volume	Junction		Junction Path	Junction Path Source
		Active	Path		
vs1.example.com	users1	true	/users		RW_volume

The following command creates a new volume named “home4” on the SVM “vs1.example.com” and the aggregate “aggr1”. The directory `/eng/` already exists in the namespace for the `vs1` SVM, and the new volume is made available at `/eng/home`, which becomes the home directory for the `/eng/` namespace. The volume is 750 GB in size, and its volume guarantee is of type `volume` (by default).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
```

Vserver	Volume	Junction		Junction Path	Junction Path Source
		Active	Path		
vs1.example.com	home4	true	/eng/home		RW_volume

## SAN volumes

### About SAN volumes

ONTAP provides three basic volume provisioning options: thick provisioning, thin provisioning, and semi-thick provisioning. Each option uses different ways to manage the volume space and the space requirements for ONTAP block sharing technologies.



Understanding how the options work enables you to choose the best option for your environment.



Putting SAN LUNs and NAS shares in the same FlexVol volume is not recommended. You should provision separate FlexVol volumes specifically for your SAN LUNs and you should provision separate FlexVol volumes specifically to your NAS shares. This simplifies management and replication deployments and parallels the way FlexVol volumes are supported in Active IQ Unified Manager (formerly OnCommand Unified Manager).

### Thin provisioning for volumes

When a thinly provisioned volume is created, ONTAP does not reserve any extra space when the volume is created. As data is written to the volume, the volume requests the storage it needs from the aggregate to accommodate the write operation. Using thin-provisioned volumes enables you to overcommit your aggregate, which introduces the possibility of the volume not being able to secure the space it needs when the aggregate runs out of free space.

You create a thin-provisioned FlexVol volume by setting its `-space-guarantee` option to `none`.

### Thick provisioning for volumes

When a thick-provisioned volume is created, ONTAP sets aside enough storage from the aggregate to ensure that any block in the volume can be written to at any time. When you configure a volume to use thick provisioning, you can employ any of the ONTAP storage efficiency capabilities, such as compression and deduplication, to offset the larger upfront storage requirements.

You create a thick-provisioned FlexVol volume by setting its `-space-slo` (service level objective) option to `thick`.

### Semi-thick provisioning for volumes

When a volume using semi-thick provisioning is created, ONTAP sets aside storage space from the aggregate to account for the volume size. If the volume is running out of free space because blocks are in use by block-sharing technologies, ONTAP makes an effort to delete protection data objects (Snapshot copies and FlexClone files and LUNs) to free up the space they are holding. As long as ONTAP can delete the protection data objects fast enough to keep pace with the space required for overwrites, the write operations continue to succeed. This is called a “best effort” write guarantee.



You cannot employ storage efficiency technologies such as deduplication, compression, and compaction on a volume that is using semi-thick provisioning.

You create a semi-thick-provisioned FlexVol volume by setting its `-space-slo` (service level objective) option to `semi-thick`.

### Use with space-reserved files and LUNs

A space-reserved file or LUN is one for which storage is allocated when it is created. Historically, NetApp has used the term “thin-provisioned LUN” to mean a LUN for which space reservation is disabled (a non-space-reserved LUN).



Non-space-reserved files are not generally referred to as “thin-provisioned files.”

The following table summarizes the major differences in how the three volume provisioning options can be used with space-reserved files and LUNs:

Volume provisioning	LUN/file space reservation	Overwrites	Protection data <sup>2</sup>	Storage efficiency <sup>3</sup>
Thick	Supported	Guaranteed <sup>1</sup>	Guaranteed	Supported
Thin	No effect	None	Guaranteed	Supported
Semi-thick	Supported	Best effort <sup>1</sup>	Best effort	Not supported

## Notes

1. The ability to guarantee overwrites or provide a best-effort overwrite assurance requires that space reservation is enabled on the LUN or file.
2. Protection data includes Snapshot copies, and FlexClone files and LUNs marked for automatic deletion (backup clones).
3. Storage efficiency includes deduplication, compression, any FlexClone files and LUNs not marked for automatic deletion (active clones), and FlexClone subfiles (used for Copy Offload).

## Support for SCSI thin-provisioned LUNs

ONTAP supports T10 SCSI thin-provisioned LUNs as well as NetApp thin-provisioned LUNs. T10 SCSI thin provisioning enables host applications to support SCSI features including LUN space reclamation and LUN space monitoring capabilities for blocks environments. T10 SCSI thin provisioning must be supported by your SCSI host software.

You use the ONTAP `space-allocation` setting to enable/disable support for the T10 thin provisioning on a LUN. You use the ONTAP `space-allocation enable` setting to enable T10 SCSI thin provisioning on a LUN.

The `[-space-allocation {enabled|disabled}]` command in the ONTAP Command Reference Manual has more information to enable/disable support for the T10 thin provisioning and to enable T10 SCSI thin provisioning on a LUN.

## ONTAP 9 Commands

### Configure volume provisioning options

You can configure a volume for thin provisioning, thick provisioning, or semi-thick provisioning.

### About this task

Setting the `-space-slo` option to `thick` ensures the following:

- The entire volume is preallocated in the aggregate. You cannot use the `volume create` or `volume modify` command to configure the volume's `-space-guarantee` option.
- 100% of the space required for overwrites is reserved. You cannot use the `volume modify` command to configure the volume's `-fractional-reserve` option

Setting the `-space-slo` option to `semi-thick` ensures the following:

- The entire volume is preallocated in the aggregate. You cannot use the `volume create` or `volume modify` command to configure the volume's `-space-guarantee` option.
- No space is reserved for overwrites. You can use the `volume modify` command to configure the volume's `-fractional-reserve` option.
- Automatic deletion of Snapshot copies is enabled.

## Step

1. Configure volume provisioning options:

```
volume create -vserver vserver_name -volume volume_name -aggregate  
aggregate_name -space-slo none|thick|semi-thick -space-guarantee none|volume
```

The `-space-guarantee` option defaults to `none` for AFF systems and for non-AFF DP volumes. Otherwise, it defaults to `volume`. For existing FlexVol volumes, use the `volume modify` command to configure provisioning options.

The following command configures `vol1` on SVM `vs1` for thin provisioning:

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-guarantee  
none
```

The following command configures `vol1` on SVM `vs1` for thick provisioning:

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-slo thick
```

The following command configures `vol1` on SVM `vs1` for semi-thick provisioning:

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-slo semi-  
thick
```

## Determine space usage in a volume or aggregate

Enabling a feature in ONTAP might consume space that you are not aware of or more space than you expected. ONTAP helps you determine how space is being consumed by providing three perspectives from which to view space: the volume, a volume's footprint within the aggregate, and the aggregate.

A volume can run out of space due to space consumption or insufficient space within the volume, aggregate, or a combination of both. By seeing a feature-oriented breakdown of space usage from different perspectives, you can assess which features you might want to adjust or turn off, or take other action (such as increase the size of the aggregate or volume).

You can view space usage details from any of these perspectives:

- The volume's space usage

This perspective provides details about space usage within the volume, including usage by Snapshot copies.

You see a volume's space usage by using the `volume show-space` command.

- The volume's footprint within the aggregate

This perspective provides details about the amount of space each volume is using in the containing aggregate, including the volume's metadata.

You see a volume's footprint with the aggregate by using the `volume show-footprint` command.

- The aggregate's space usage

This perspective includes totals of the volume footprints of all of the volumes contained in the aggregate, space reserved for aggregate Snapshot copies, and other aggregate metadata.

You can see the aggregate's space usage by using the `storage aggregate show-space` command.

Certain features, such as tape backup and deduplication, use space for metadata both from the volume and directly from the aggregate. These features show different space usage between the volume and volume footprint perspectives.

### Delete Snapshot copies automatically

You can define and enable a policy for automatically deleting Snapshot copies and FlexClone LUNs. Automatically deleting Snapshot copies and FlexClone LUNs can help you manage space utilization.

#### About this task

You can automatically delete Snapshot copies from read-write volumes and FlexClone LUNs from read-write parent volumes. You cannot set up automatic deletion of Snapshot copies from read-only volumes, for example, SnapMirror destination volumes.

#### Step

1. Define and enable a policy for automatically deleting Snapshot copies by using the `volume snapshot autodelete modify` command.

See the `volume snapshot autodelete modify man` page for information about the parameters that you can use with this command to define a policy that meets your needs.

The following command enables the automatic deletion of Snapshot copies and sets the trigger to `snap_reserve` for the `vol3` volume, which is part of the `vs0.example.com` storage virtual machine (SVM):

```
cluster1::> volume snapshot autodelete modify -vserver vs0.example.com
-volume vol3 -enabled true -trigger snap_reserve
```

The following command enables the automatic deletion of Snapshot copies and of FlexClone LUNs marked for autodeletion for the `vol3` volume, which is part of the `vs0.example.com` storage virtual machine

(SVM):

```
cluster1::> volume snapshot autodelete modify -vserver vs0.example.com
-volume vol3 -enabled true -trigger volume -commitment try -delete-order
oldest_first -destroy-list lun_clone,file_clone
```

Aggregate-level Snapshot copies work differently than volume-level Snapshot copies and are managed automatically by ONTAP. The option to delete aggregate Snapshot copies is always enabled and helps in managing space utilization.



If the trigger parameter is set to `snap_reserve` for an aggregate, the Snapshot copies are maintained until the space reserved crosses the threshold capacity. Therefore, even if the trigger parameter is not set to `snap_reserve`, the space used by the Snapshot copy in the command will be listed as 0 because these Snapshot copies are automatically deleted. Also, the space used by Snapshot copies in an aggregate is considered as free and is included in the available space parameter of the command.

### Configure volumes to automatically provide more space when they are full

When FlexVol volumes get full, ONTAP can use various methods to attempt to automatically provide more free space for the volume. You choose which methods ONTAP can use, and in which order, depending on the requirements imposed by your application and storage architecture.

#### About this task

ONTAP can automatically provide more free space for a full volume by using one or both of the following methods:

- Increase the size of the volume (known as *autogrow*).

This method is useful if the volume's containing aggregate has enough space to support a larger volume. You can configure ONTAP to set a maximum size for the volume. The increase is automatically triggered based on the amount of data being written to the volume in relation to the current amount of used space and any thresholds set.

Autogrow is not triggered to support Snapshot copy creation. If you attempt to create a Snapshot copy and there is insufficient space, the Snapshot copy creation fails, even with autogrow enabled.

- Delete Snapshot copies, FlexClone files, or FlexClone LUNs.

For example, you can configure ONTAP to automatically delete Snapshot copies that are not linked to Snapshot copies in cloned volumes or LUNs, or you can define which Snapshot copies you want ONTAP to delete first—your oldest or newest Snapshot copies. You can also determine when ONTAP should begin deleting Snapshot copies—for example, when the volume is nearly full or when the volume's Snapshot reserve is nearly full.

If you enable both of these methods, you can specify which method ONTAP tries first when a volume is nearly full. If the first method does not provide sufficient additional space to the volume, ONTAP tries the other method next.

By default, ONTAP tries to increase the size of the volume first. In most cases, the default configuration is preferable, because when a Snapshot copy is deleted, it cannot be restored. However, if you need to avoid growing the size of a volume whenever possible, you can configure ONTAP to delete Snapshot copies before increasing the size of the volume.

### Steps

1. If you want ONTAP to attempt to increase the size of the volume when it gets full, enable the autogrow capability for the volume by using the `volume autosize` command with `grow` mode.

Remember that when the volume grows, it consumes more free space from its associated aggregate. If you are depending on the volume's ability to grow whenever it needs to, you must monitor the free space in the associated aggregate and add more when needed.

2. If you want ONTAP to delete Snapshot copies, FlexClone files, or FlexClone LUNs when the volume gets full, enable autodelete for those object types.
3. If you enabled both the volume autogrow capability and one or more autodelete capabilities, select the first method that ONTAP should use to provide free space to a volume by using the `volume modify` command with the `-space-mgmt-try-first` option.

To specify increasing the size of the volume first (the default), use `volume_grow`. To specify deleting Snapshot copies first, use `snap_delete`.

### Configure volumes to automatically grow and shrink their size

You can configure FlexVol volumes to automatically grow and shrink according to how much space they currently require. Automatic growing helps prevent a volume from running out of space, if the aggregate can supply more space. Automatic shrinking prevents a volume from being larger than needed, freeing space in the aggregate for use by other volumes.

#### What you'll need

The FlexVol volume must be online.

#### About this task

Autoshrink can only be used in combination with autogrow to meet changing space demands and is not available alone. When autoshrink is enabled, ONTAP automatically manages the shrinking behavior of a volume to prevent an endless loop of autogrow and autoshrink actions.

As a volume grows, the maximum number of files it can contain might be automatically increased. When a volume is shrunk, the maximum number of files it can contain is left unchanged, and a volume cannot be automatically shrunk below the size that corresponds to its current maximum number of files. For this reason, it might not be possible to automatically shrink a volume all the way to its original size.

By default, the maximum size a volume can grow to is 120% of the size at which autogrow is enabled. If you need to ensure that the volume can grow to be larger than that, you must set the maximum size for the volume accordingly.

#### Step

1. Configure the volume to grow and shrink its size automatically:

```
volume autosize -vserver vservers_namevol_name -mode grow_shrink
```

The following command enables automatic size changes for a volume called test2. The volume is configured to begin shrinking when it is 60% full. The default values are used for when it will begin to grow and its maximum size.

```
cluster1::> volume autosize -vserver vs2 test2 -shrink-threshold-percent
60
vol autosize: Flexible volume "vs2:test2" autosize settings UPDATED.

Volume modify successful on volume: test2
```

### Requirements for enabling both autoshrink and automatic Snapshot copy deletion

The autoshrink functionality can be used with automatic Snapshot copy deletion if certain configuration requirements are met.

If you want to enable both the autoshrink functionality and automatic Snapshot copy deletion, your configuration must meet the following requirements:

- ONTAP must be configured to attempt to increase volume size before trying to delete Snapshot copies(the `-space-mgmt-try-first` option must be set to `volume_grow`).
- The trigger for automatic Snapshot copy deletion must be volume fullness(the `trigger` parameter must be set to `volume`).

### How the autoshrink functionality interacts with Snapshot copy deletion

Because the autoshrink functionality shrinks the size of a FlexVol volume, it can also affect when volume Snapshot copies are automatically deleted.

The autoshrink functionality interacts with automatic volume Snapshot copy deletion in the following ways:

- If both the `grow_shrink` autosize mode and automatic Snapshot copy deletion are enabled, when a volume size shrinks it can trigger an automatic Snapshot copy deletion.

This is because the Snapshot reserve is based on a percentage of the volume size (5 percent by default), and that percentage is now based on a smaller volume size. This can cause Snapshot copies to spill out of the reserve and be deleted automatically.

- If the `grow_shrink` autosize mode is enabled and you manually delete a Snapshot copy, it might trigger an automatic volume shrinkage.

### Address FlexVol volume fullness and overallocation alerts

ONTAP issues EMS messages when FlexVol volumes are running out of space so that you can take corrective action by providing more space for the full volume. Knowing the types of alerts and how to address them helps you ensure your data availability.

When a volume is described as *full*, it means that the percentage of the space in the volume available for use by the active file system (user data) has fallen below a (configurable) threshold. When a volume becomes *overallocated*, the space used by ONTAP for metadata and to support basic data access has been exhausted. Sometimes space normally reserved for other purposes can be used to keep the volume functioning, but space

reservation or data availability can be at risk.

Overallocation can be either logical or physical. *Logical overallocation* means that space reserved to honor future space commitments, such as space reservation, has been used for another purpose. *Physical overallocation* means that the volume is running out of physical blocks to use. Volumes in this state are at risk for refusing writes, going offline, or potentially causing a controller disruption.

A volume can be more than 100% full due to space used or reserved by metadata. However, a volume that is more than 100% full might or might not be overallocated. If qtrees-level and volume-level shares exist on the same FlexVol or SCVMM pool, the qtrees appear as directories on the FlexVol share. Therefore, you need to be careful not to delete them accidentally.

The following table describes the volume fullness and overallocation alerts, the actions you can take to address the issue, and the risks of not taking action:

Alert type	EMS level	Configurable?	Definition	Ways to address	Risk if no action taken
Nearly full	Debug	Y	The file system has exceeded the threshold set for this alert (the default is 95%). The percentage is the <code>Used total</code> minus the size of the Snapshot reserve.	<ul style="list-style-type: none"> <li>Increasing volume size</li> <li>Reducing user data</li> </ul>	No risk to write operations or data availability yet.
Full	Debug	Y	The file system has exceeded the threshold set for this alert (the default is 98%). The percentage is the <code>Used total</code> minus the size of the Snapshot reserve.	<ul style="list-style-type: none"> <li>Increasing volume size</li> <li>Reducing user data</li> </ul>	No risk to write operations or data availability yet, but the volume is approaching the stage where write operations could be at risk.
Logically overallocated	SVC Error	N	In addition to the file system being full, the space in the volume used for metadata has been exhausted.	<ul style="list-style-type: none"> <li>Increasing volume size</li> <li>Deleting Snapshot copies</li> <li>Reducing user data</li> <li>Disabling space reservation for files or LUNs</li> </ul>	Write operations to unreserved files could fail.



Alert type	EMS level	Configurable?	Definition	Ways to address	Risk if no action taken
Physically overallocated	Node Error	N	The volume is running out of physical blocks it can write to.	<ul style="list-style-type: none"> <li>Increasing volume size</li> <li>Deleting Snapshot copies</li> <li>Reducing user data</li> </ul>	Write operations are at risk, as well as data availability; the volume could go offline.

Every time a threshold is crossed for a volume, whether the fullness percentage is rising or falling, an EMS message is generated. When the fullness level of the volume falls below a threshold, a `volume ok` EMS message is generated.

#### Address aggregate fullness and overallocation alerts

ONTAP issues EMS messages when aggregates are running out of space so that you can take corrective action by providing more space for the full aggregate. Knowing the types of alerts and how you can address them helps you ensure your data availability.

When an aggregate is described as *full*, it means that the percentage of the space in the aggregate available for use by volumes has fallen below a predefined threshold. When an aggregate becomes *overallocated*, the space used by ONTAP for metadata and to support basic data access has been exhausted. Sometimes space normally reserved for other purposes can be used to keep the aggregate functioning, but volume guarantees for volumes associated with the aggregate or data availability can be at risk.

Overallocation can be either logical or physical. *Logical overallocation* means that space reserved to honor future space commitments, such as volume guarantees, has been used for another purpose. *Physical overallocation* means that the aggregate is running out of physical blocks to use. Aggregates in this state are at risk for refusing writes, going offline, or potentially causing a controller disruption.

The following table describes the aggregate fullness and overallocation alerts, the actions you can take to address the issue, and the risks of not taking action.

Alert type	EMS Level	Configurable?	Definition	Ways to address	Risk if no action taken
Nearly full	Debug	N	The amount of space allocated for volumes, including their guarantees, has exceeded the threshold set for this alert (95%). The percentage is the <code>Used</code> total minus the size of the Snapshot reserve.	<ul style="list-style-type: none"> <li>Adding storage to the aggregate</li> <li>Shrinking or deleting volumes</li> <li>Moving volumes to another aggregate with more space</li> <li>Removing volume guarantees (setting them to <code>none</code>)</li> </ul>	No risk to write operations or data availability yet.

Alert type	EM S Level	Configurable?	Definition	Ways to address	Risk if no action taken
Full	Debug	N	The file system has exceeded the threshold set for this alert (98%). The percentage is the <code>Used</code> total minus the size of the Snapshot reserve.	<ul style="list-style-type: none"> <li>• Adding storage to the aggregate</li> <li>• Shrinking or deleting volumes</li> <li>• Moving volumes to another aggregate with more space</li> <li>• Removing volume guarantees (setting them to <code>none</code>)</li> </ul>	Volume guarantees for volumes in the aggregate might be at risk, as well as write operations to those volumes.
Logically overloaded	SV C Error	N	In addition to the space reserved for volumes being full, the space in the aggregate used for metadata has been exhausted.	<ul style="list-style-type: none"> <li>• Adding storage to the aggregate</li> <li>• Shrinking or deleting volumes</li> <li>• Moving volumes to another aggregate with more space</li> <li>• Removing volume guarantees (setting them to <code>none</code>)</li> </ul>	Volume guarantees for volumes in the aggregate are at risk, as well as write operations to those volumes.
Physically overloaded	Node Error	N	The aggregate is running out of physical blocks it can write to.	<ul style="list-style-type: none"> <li>• Adding storage to the aggregate</li> <li>• Shrinking or deleting volumes</li> <li>• Moving volumes to another aggregate with more space</li> </ul>	Write operations to volumes in the aggregate are at risk, as well as data availability; the aggregate could go offline. In extreme cases, the node could experience a disruption.

Every time a threshold is crossed for an aggregate, whether the fullness percentage is rising or falling, an EMS message is generated. When the fullness level of the aggregate falls below a threshold, an `aggregate ok` EMS message is generated.

#### Considerations for setting fractional reserve

Fractional reserve, also called *LUN overwrite reserve*, enables you to turn off overwrite reserve for space-reserved LUNs and files in a FlexVol volume. This can help you maximize your storage utilization, but if your environment is negatively affected by write operations failing due to lack of space, you must understand the requirements that this configuration imposes.

The fractional reserve setting is expressed as a percentage; the only valid values are 0 and 100 percent. The fractional reserve setting is an attribute of the volume.

Setting fractional reserve to 0 increases your storage utilization. However, an application accessing data residing in the volume could experience a data outage if the volume is out of free space, even with the volume guarantee set to `volume`. With proper volume configuration and use, however, you can minimize the chance of writes failing. ONTAP provides a “best effort” write guarantee for volumes with fractional reserve set to 0 when *all* of the following requirements are met:

- Deduplication is not in use
- Compression is not in use
- FlexClone sub-files are not in use
- All FlexClone files and FlexClone LUNs are enabled for automatic deletion

This is not the default setting. You must explicitly enable automatic deletion, either at creation time or by modifying the FlexClone file or FlexClone LUN after it is created.

- ODX and FlexClone copy offload are not in use
- Volume guarantee is set to `volume`
- File or LUN space reservation is `enabled`
- Volume Snapshot reserve is set to 0
- Volume Snapshot copy automatic deletion is `enabled` with a commitment level of `destroy`, a `destroy list` of `lun_clone, vol_clone, cifs_share, file_clone, sfsr`, and a `trigger` of `volume`

This setting also ensures that FlexClone files and FlexClone LUNs are deleted when necessary.

Note that if your rate of change is high, in rare cases the Snapshot copy automatic deletion could fall behind, resulting in the volume running out of space, even with all of the above required configuration settings in use.

In addition, you can optionally use the volume autogrow capability to decrease the likelihood of volume Snapshot copies needing to be deleted automatically. If you enable the autogrow capability, you must monitor the free space in the associated aggregate. If the aggregate becomes full enough that the volume is prevented from growing, more Snapshot copies will probably be deleted as the free space in the volume is depleted.

If you cannot meet all of the above configuration requirements and you need to ensure that the volume does not run out of space, you must set the volume’s fractional reserve setting to 100. This requires more free space up front, but guarantees that data modification operations will succeed even when the technologies listed above are in use.

The default value and allowed values for the fractional reserve setting depend on the guarantee of the volume:

Volume guarantee	Default fractional reserve	Allowed values
Volume	100	0, 100
None	0	0, 100

## Display file or inode usage

FlexVol volumes have a maximum number of files that they can contain. Knowing how many files are contained by your volumes helps you determine whether you need to increase the number of (public) inodes for your volumes to prevent them from hitting their maximum file limit.

### About this task

Public inodes can be either free (they are not associated with a file) or used (they point to a file). The number of free inodes for a volume is the total number of inodes for the volume minus the number of used inodes (the number of files).

If qtree-level and volume-level shares exist on the same FlexVol or SCVMM pool, the qtrees appear as directories on the FlexVol share. Therefore, you need to be careful not to delete them accidentally.

### Step

1. To display inode usage for a volume, enter the following command:

```
df -i volume_name
```

You can omit the volume name; in this case, ONTAP displays the inode usage for all volumes in the cluster. You can also specify a storage virtual machine (SVM) to see only volumes on that SVM.

### Example

```
cm320c-rst::> df -i -vserver vs1
Filesystem          iused      ifree   %iused  Mounted on
/vol/cifs_test/    105        2928    3%      /home
/vol/root/         98         468    17%     ---
/vol/vola/         103       12047    0%     /nfsv4
3 entries were displayed.
```

## Control and monitor I/O performance to FlexVol volumes by using Storage QoS

You can control input/output (I/O) performance to FlexVol volumes by assigning volumes to Storage QoS policy groups. You might control I/O performance to ensure that workloads achieve specific performance objectives or to throttle a workload that negatively impacts other workloads.

### About this task

Policy groups enforce a maximum throughput limit (for example, 100 MB/s). You can create a policy group without specifying a maximum throughput, which enables you to monitor performance before you control the workload.

You can also assign SVMs, LUNs, and files to policy groups.

Note the following requirements about assigning a volume to a policy group:

- The volume must be contained by the SVM to which the policy group belongs.

You specify the SVM when you create the policy group.

- If you assign a volume to a policy group, then you cannot assign the volume's containing SVM or any child LUNs or files to a policy group.

For more information about how to use Storage QoS, see the [System Administration Reference](#).

### Steps

1. Use the `qos policy-group create` command to create a policy group.
2. Use the `volume create` command or the `volume modify` command with the `-qos-policy-group` parameter to assign a volume to a policy group.
3. Use the `qos statistics` commands to view performance data.
4. If necessary, use the `qos policy-group modify` command to adjust the policy group's maximum throughput limit.

### Delete a FlexVol volume

You can delete a FlexVol volume that is no longer required or if it contains corrupted data.

#### What you'll need

No applications must be accessing the data in the volume you want to delete.



If you accidentally delete a volume, see the Knowledge Base article [How to use the Volume Recovery Queue](#).

### Steps

1. If the volume has been mounted, unmount it:

```
volume unmount -vserver vserver_name -volume volume_name
```

2. If the volume is part of a SnapMirror relationship, delete the relationship by using the `snapmirror delete` command.
3. If the volume is online, take the volume offline:

```
volume offline -vserver vserver_name volume_name
```

4. Delete the volume:

```
volume delete -vserver vserver_name volume_name
```

### Result

The volume is deleted, along with any associated quota policies and qtrees.

### Protection against accidental volume deletion

Default volume delete behavior aids the recovery of accidentally deleted FlexVol volumes.

A `volume delete` request against a volume that has type `RW` or `DP` (as seen in `volume show` command

output) causes that volume to be moved to a partially deleted state. By default, it is retained in a recovery queue for at least 12 hours before being fully deleted.

For more information, see the KnowledgeBase article [How to use the Volume Recovery Queue](#).

## Delete directories

### Delete directories overview

Beginning with ONTAP 9.8, you can delete large directories with lower latencies. This improved method of directory delete can be implemented through a new REST API or using the ONTAP command line interface (CLI). For more information, see [Delete files and directories rapidly on the cluster](#)

Beginning with ONTAP 9.9.1, you can also use System Manager to perform a fast directory delete. For more information, see [Take corrective action based on analytics](#).

## Commands for managing FlexVol volumes

There are specific commands for managing FlexVol volumes using the ONTAP CLI.

If you want to...	Use this command...
Bring a volume online	<code>volume online</code>
Change the size of a volume	<code>volume size</code>
Determine the associated aggregate of a volume	<code>volume show</code>
Determine the associated aggregate for all volumes on a storage virtual machine (SVM)	<code>volume show -vserver -fields aggregate</code>
Determine the format of a volume	<code>volume show -fields block-type</code>
Mount a volume onto another volume using a junction	<code>volume mount</code>
Put a volume into the restricted state	<code>volume restrict</code>
Rename a volume	<code>volume rename</code>
Take a volume offline	<code>volume offline</code>

See the man page for each command for more information.

## Commands for displaying space usage information

You use the `storage aggregate` and `volume` commands to see how space is being used in your aggregates and volumes and their Snapshot copies.

To display information about...	Use this command...
Aggregates, including details about used and available space percentages, Snapshot reserve size, and other space usage information	<code>storage aggregate show storage aggregate show-space -fields snap-size-total,used-including-snapshot-reserve</code>
How disks and RAID groups are used in an aggregate, and RAID status	<code>storage aggregate show-status</code>
The amount of disk space that would be reclaimed if you deleted a specific Snapshot copy	<code>volume snapshot compute-reclaimable (advanced)</code>
The amount of space used by a volume	<code>volume show -fields size,used,available,percent-used volume show-space</code>
The amount of space used by a volume in the containing aggregate	<code>volume show-footprint</code>

## Move and copy volumes

### Move a FlexVol volume overview

You can move or copy volumes for capacity utilization, improved performance, and to satisfy service-level agreements.

Knowing how moving a FlexVol volume works helps you to determine whether the volume move satisfies service-level agreements and to understand where a volume move is in the volume move process.

FlexVol volumes are moved from one aggregate or node to another within the same storage virtual machine (SVM). A volume move does not disrupt client access during the move.

Moving a volume occurs in multiple phases:

- A new volume is made on the destination aggregate.
- The data from the original volume is copied to the new volume.

During this time, the original volume is intact and available for clients to access.

- At the end of the move process, client access is temporarily blocked.

During this time the system performs a final replication from the source volume to the destination volume, swaps the identities of the source and destination volumes, and changes the destination volume to the source volume.

- After completing the move, the system routes client traffic to the new source volume and resumes client access.

The move is not disruptive to client access because the time in which client access is blocked ends before clients notice a disruption and time out. Client access is blocked for 35 seconds by default. If the volume move operation cannot finish in the time that access is denied, the system aborts this final phase of the volume move

operation and allows client access. The system attempts the final phase three times by default. After the third attempt, the system waits an hour before attempting the final phase sequence again. The system runs the final phase of the volume move operation until the volume move is complete.

## Considerations and recommendations when moving volumes

Moving a volume has many considerations and recommendations that are influenced by the volume you are moving or by the system configuration, such as a MetroCluster configuration. You should understand the considerations and recommendations associated with moving volumes.

### General considerations and recommendations

- If you are upgrading the release family for a cluster, do not move a volume until after you upgrade all of the nodes in the cluster.

This recommendation prevents you from inadvertently attempting to move a volume from a newer release family to an older release family.

- The source volume must be consistent.
- If you have assigned one or more aggregates to the associated storage virtual machine (SVM), the destination aggregate must be one of the assigned aggregates.
- You cannot move a volume to or from a taken-over CFO aggregate.
- If a volume that contains LUNs is not NVFAIL enabled before you move it, the volume will be NVFAIL enabled after you move it.
- You can move a volume from a Flash Pool aggregate to another Flash Pool aggregate.
  - The caching policies of that volume are also moved.
  - The move might affect volume performance.
- You can move volumes between a Flash Pool aggregate and a non-Flash Pool aggregate.
  - If you move a volume from a Flash Pool aggregate to a non-Flash Pool aggregate, ONTAP displays a message warning you that the move might affect volume performance and asks whether you want to continue.
  - If you move a volume from a non-Flash Pool aggregate to a Flash Pool aggregate, ONTAP assigns the `auto` caching policy.
- Volumes have the data-at-rest protections of the aggregate they reside on. If you move a volume from an aggregate that consists of NSE drives to one that does not, the volume no longer has NSE data-at-rest protection.

### FlexClone volume considerations and recommendations

- FlexClone volumes cannot be offline when they are being moved.
- You can move FlexClone volumes from one aggregate to another aggregate on the same node or another node in the same SVM without initiating the `vol clone split start` command.

By initiating a volume move operation on a FlexClone volume, the clone volume is split during the move process to a different aggregate. After the volume move on the clone volume is complete, the volume that moved no longer appears as a clone, but appears instead as an independent volume without any clone relationship with the previous parent volume.



- FlexClone volume Snapshot copies are not lost after moving a clone.
- You can move FlexClone parent volumes from one aggregate to another aggregate.

When you move a FlexClone parent volume, a temporary volume is left behind that acts as a parent volume for all FlexClone volumes. No operations are allowed on the temporary volume except to take it offline or to delete it. After all FlexClone volumes are either split or destroyed, the temporary volume is cleaned up automatically.

- After you move a FlexClone child volume, the volume is no longer a FlexClone volume.
- FlexClone move operations are mutually exclusive from FlexClone copy or split operations.
- If a clone-splitting operation is in progress, moving a volume might fail.

You should not move a volume until clone-splitting operations are completed.

### **MetroCluster configuration considerations**

- During a volume move in a MetroCluster configuration, when a temporary volume is created on the destination aggregate on the source cluster a record of the temporary volume corresponding to the volume in the mirrored, but unassimilated, aggregate is also created on the surviving cluster.
- If a MetroCluster switchover occurs before the cutover, the destination volume has a record and is a temporary volume (a volume of type TMP).

Move job restarts on the surviving (disaster recovery) cluster, reports a failure, and cleans up all move-related items including the temporary volume. In any event where cleanup cannot be done correctly, an EMS is generated alerting the system administrator to do the necessary cleanup.

- If a MetroCluster switchover occurs after the cutover phase has started but before the move job has completed (that is, the move reached a stage where it can update the cluster to point to the destination aggregate), the move job restarts on the surviving (disaster recovery) cluster and runs to completion.

All move-related items are cleaned up including the temporary volume (original source). In any event where cleanup cannot be done correctly, an EMS is generated alerting the system administrator to do the necessary cleanup.

- Neither forced nor unforced MetroCluster switchbacks are allowed if there are any volume move operations in progress for volumes belonging to the switched over site.

Switchbacks are not blocked when volume move operations are in progress for volumes local to the surviving site.

- Unforced MetroCluster switchovers are blocked, but forced MetroCluster switchovers are not blocked if there are any volume move operations in progress.

### **Requirement for moving volumes in SAN environments**

Before you move a volume that contains LUNs or namespaces, you must meet certain requirements.

- For volumes containing one or more LUNs, you should have a minimum of two paths per LUN (LIFs) connecting to each node in the cluster.

This eliminates single points of failure and enables the system to survive component failures.

- For volumes containing namespaces, the cluster must be running ONTAP 9.6 or later.

Volume move is not supported for NVMe configurations running ONTAP 9.5.

## Move a volume

You can move a FlexVol volume to a different aggregate, node, or both within the same storage virtual machine (SVM) to balance storage capacity after determining that there is a storage capacity imbalance.

### About this task

By default, if the cutover operation fails to complete within 30 seconds, it will retry. You can adjust the default behavior by using the `-cutover-window` and `-cutover-action` parameters, both of which require advanced privilege level access. For details, see the `volume move start` man page.

### Steps

1. If you are moving a data protection mirror and you have not initialized the mirror relationship, initialize the mirror relationship by using the `snapmirror initialize` command.

Data protection mirror relationships must be initialized before you can move one of the volumes.

2. Determine an aggregate to which you can move the volume by using the `volume move target-aggr show` command.

The aggregate that you select must have enough space for the volume; that is, the available size is bigger than the volume that you are moving.

The following example shows that the `vs2` volume can be moved to any of the listed aggregates:

```
cluster1::> volume move target-aggr show -vserver vs2 -volume user_max
Aggregate Name    Available Size    Storage Type
-----
aggr2             467.9GB          hdd
node12a_aggr3    10.34GB          hdd
node12a_aggr2    10.36GB          hdd
node12a_aggr1    10.36GB          hdd
node12a_aggr4    10.36GB          hdd
5 entries were displayed.
```

3. Verify that the volume can be moved to the intended aggregate by using the `volume move start -perform-validation-only` command to run a validation check.
4. Move the volume by using the `volume move start` command.

The following command moves the `user_max` volume on the `vs2` SVM to the `node12a_aggr3` aggregate. The move runs as a background process.

```
cluster1::> volume move start -vserver vs2 -volume user_max
-destination-aggregate node12a_aggr3
```

- Determine the status of the volume move operation by using the `volume move show` command.

The following example shows the state of a volume move that completed the replication phase and is in the cutover phase:

```
cluster1::> volume move show
Vserver    Volume      State      Move Phase  Percent-Complete  Time-To-
Complete
-----
-----
vs2        user_max    healthy    cutover     -                  -
```

The volume move is complete when it no longer appears in the `volume move show` command output.

### Commands for moving volumes

There are specific ONTAP commands for managing volume movement.

If you want to...	Use this command...
Abort an active volume move operation.	<code>volume move abort</code>
Show status of a volume moving from one aggregate to another aggregate.	<code>volume move show</code>
Start moving a volume from one aggregate to another aggregate.	<code>volume move start</code>
Manage target aggregates for volume move.	<code>volume move target-aggr</code>
Trigger cutover of a move job.	<code>volume move trigger-cutover</code>
Change the amount of time client access is blocked if the default is not adequate.	<code>volume move start</code> or <code>volume move modify</code> with the <code>-cutover-window</code> parameter. The <code>volume move modify</code> command is an advanced command and the <code>-cutover-window</code> is an advanced parameter.

If you want to...	Use this command...
Determine what the system does if the volume move operation cannot be completed during the time client access is blocked.	<code>volume move start</code> or <code>volume move modify</code> with the <code>-cutover-action</code> parameter. The <code>volume move modify</code> command is an advanced command and the <code>-cutover-action</code> is an advanced parameter.

See the man page for each command for more information.

### Methods for copying a volume

Copying a volume creates a stand-alone copy of a volume that you can use for testing and other purposes. The method you use to copy a volume depends on the use case.

The method you use for copying a volume depends on whether you are copying it to the same aggregate or a different aggregate, and whether you want to retain Snapshot copies from the original volume. The following table lists characteristics of the copy and the methods used to create that copy.

If you want to copy a volume...	Then the method you use is...
Within the same aggregate and you do not want to copy Snapshot copies from the original volume.	Creating a FlexClone volume of the original volume.
To another aggregate and you do not want to copy Snapshot copies from the original volume.	Creating a FlexClone volume of the original volume, and then moving the volume to another aggregate by using the <code>volume move</code> command.
To another aggregate and preserve all of the Snapshot copies from the original volume.	Replicating the original volume using SnapMirror, and then breaking the SnapMirror relationship to make a read-write volume copy.

## Use FlexClone volumes to create efficient copies of your FlexVol volumes

### Use FlexClone volumes to create efficient copies of your FlexVol volumes overview

FlexClone volumes are writable, point-in-time copies of a parent FlexVol volume. FlexClone volumes are space-efficient because they share the same data blocks with their parent FlexVol volumes for common data. The Snapshot copy used to create a FlexClone volume is also shared with the parent volume.

You can clone an existing FlexClone volume to create another FlexClone volume. You can also create a clone of a FlexVol volume containing LUNs and LUN clones.

You can also split a FlexClone volume from its parent volume. Beginning with ONTAP 9.4, for non-guaranteed volumes on AFF systems, the split operation for FlexClone volumes shares the physical blocks and does not copy the data. Therefore, splitting of FlexClone volumes on AFF systems is faster than the FlexClone splitting operation in other FAS systems in ONTAP 9.4 and later releases.

You can create two types of FlexClone volumes: read-write FlexClone volumes and data protection FlexClone

volumes. While you can create a read-write FlexClone volume of a regular FlexVol volume, you must use only a SnapVault secondary volume to create a data protection FlexClone volume.

## Create a FlexClone volume

You can create a data protection FlexClone volume from a SnapMirror destination volume or from a parent FlexVol volume that is a SnapVault secondary volume. After you create a FlexClone volume, you cannot delete the parent volume while the FlexClone volume exists.

### What you'll need

- The FlexClone license must be installed on the cluster.
- The volume that you want to clone must be online.

### Step

1. Create a FlexClone volume:

```
volume clone create
```



While creating a read-write FlexClone volume from the read-write parent volume, you do not need to specify the base Snapshot copy. ONTAP creates a Snapshot copy if you do not name any specific Snapshot copy that is to be used as the base Snapshot copy for the clone. You must specify the base Snapshot copy for creating a FlexClone volume when the parent volume is a data protection volume.

### Example

- The following command creates a read-write FlexClone volume `vol1_clone` from the parent volume `vol1`:

```
volume clone create -vserver vs0 -flexclone vol1_clone -type RW -parent-volume vol1
```

- The following command creates a data protection FlexClone volume `vol_dp_clone` from the parent volume `dp_vol` by using the base Snapshot copy `snap1`:

```
volume clone create -vserver vs1 -flexclone vol_dp_clone -type DP -parent-volume dp_vol -parent-snapshot snap1
```

## Split a FlexClone volume from its parent volume

If you want a read-write FlexClone volume to have its own disk space rather than using that of its parent volume, you can split the FlexClone volume from its parent volume. Because this operation creates a copy of the data that is currently shared between the parent volume and the FlexClone volume, the operation can take some time to complete.

### About this task

Splitting a FlexClone volume from its parent volume consumes free space from the containing aggregate. If you do not have sufficient privileges to view the space available in your aggregate, you must contact your storage administrator to verify that there is sufficient space in the aggregate for the split operation to finish.

Beginning with ONTAP 9.4, for non-guaranteed volumes on AFF systems, the split operation for FlexClone

volumes shares the physical blocks and does not copy the data. Therefore, splitting of FlexClone volumes on AFF systems is faster than the FlexClone splitting operation in other FAS systems in ONTAP 9.4. The improved FlexClone splitting operation on AFF systems has the following benefits:

- Storage efficiency is preserved after splitting the clone from the parent.
- Existing Snapshot copies are not deleted.
- The operation is faster.
- The FlexClone volume can be split from any point in the clone hierarchy.

### Steps

1. Determine the amount of free space required to complete the split operation:

```
volume clone show -estimate -vserver vs1 -flexclone clone1 -parent-volume vol1
```

The following example provides information about the free space required to split a FlexClone volume clone1 from its parent volume vol1:

```
cluster1::> volume clone show -estimate -vserver vs1 -flexclone clone1 -parent-volume vol1
```

Vserver	FlexClone	Split Estimate
vs1	clone1	40.73MB

2. Verify that the aggregate containing the FlexClone volume and its parent has sufficient space:
  - a. Determine the amount of free space in the aggregate that contains the FlexClone volume and its parent:

```
storage aggregate show
```

- b. If the containing aggregate does not have enough free space available, add storage to the aggregate:

```
storage aggregate add-disks
```

3. Start the split operation:

```
volume clone split start -vserver vs1 -flexclone clone1 -parent-volume vol1
```

The following example shows how you can initiate the process to split the FlexClone volume clone1 from its parent volume vol1:

```

cluster1::> volume clone split start -vserver vs1 -flexclone clone1

Warning: Are you sure you want to split clone volume clone1 in Vserver
vs1 ?
{y|n}: y
[Job 1617] Job is queued: Split clone1.

```

4. Monitor the status of the FlexClone split operation:

```
volume clone split show -vserver vserver_name -flexclone clone_volume_name
```

The following example shows the status of the FlexClone split operation on an AFF system:

```

cluster1::> volume clone split show -vserver vs1 -flexclone clone1
                                Inodes
Blocks
-----
Vserver   FlexClone   Processed Total   Scanned   Updated   % Inode
% Block

Complete Complete
vs1       clone1      0          0          411247    153600    0
37

```

5. Verify that the split volume is no longer a FlexClone volume:

```
volume show -volume volume_name -fields clone-volume
```

The value of the `clone-volume` option is `false` for a volume that is not a FlexClone volume.

The following example shows how you can verify whether the volume `clone1` that is split from its parent is not a FlexClone volume.

```

cluster1::> volume show -volume clone1 -fields clone-volume
vserver volume **clone-volume**
----- **-----**
vs1       clone1 **false**

```

### Determine the space used by a FlexClone volume

You can determine the space used by a FlexClone volume based on its nominal size and the amount of space it shares with the parent FlexVol volume. When a FlexClone volume is created, it shares all of its data with its parent volume. Therefore, although the nominal

size of the FlexVol volume is the same as its parent's size, it uses very little free space from the aggregate.

### About this task

The free space used by a newly-created FlexClone volume is approximately 0.5 percent of its nominal size. This space is used to store the FlexClone volume's metadata.

New data written to either the parent or the FlexClone volume is not shared between the volumes. The increase in the amount of new data that gets written to the FlexClone volume leads to an increase in the space the FlexClone volume requires from its containing aggregate.

### Step

1. Determine the actual physical space used by the FlexClone volume using the `volume show` command.

The following example shows the total physical space used by the FlexClone volume:

```
cluster1::> volume show -vserver vs01 -volume clone_vol1 -fields
size,used,available,
percent-used,physical-used,physical-used-percent
vserver      volume      size  available  used   percent-used  physical-
used         physical-used-percent
-----
-----
vs01         clone_vol1  20MB  18.45MB   564KB    7%           196KB
1%
```

### Considerations for creating a FlexClone volume from a SnapMirror source or destination volume

You can create a FlexClone volume from the source or destination volume in an existing volume SnapMirror relationship. However, doing so could prevent future SnapMirror replication operations from completing successfully.

Replication might not work because when you create the FlexClone volume, you might lock a Snapshot copy that is used by SnapMirror. If this happens, SnapMirror stops replicating to the destination volume until the FlexClone volume is destroyed or is split from its parent. You have two options for addressing this issue:

- If you require the FlexClone volume on a temporary basis and can accommodate a temporary stoppage of the SnapMirror replication, you can create the FlexClone volume and either delete it or split it from its parent when possible.

The SnapMirror replication continues normally when the FlexClone volume is deleted or is split from its parent.

- If a temporary stoppage of the SnapMirror replication is not acceptable, you can create a Snapshot copy in the SnapMirror source volume, and then use that Snapshot copy to create the FlexClone volume. (If you are creating the FlexClone volume from the destination volume, you must wait until that Snapshot copy replicates to the SnapMirror destination volume.)

This method of creating a Snapshot copy in the SnapMirror source volume allows you to create the clone without locking a Snapshot copy that is in use by SnapMirror.



# Use FlexClone files and FlexClone LUNs to create efficient copies of files and LUNs

## Use FlexClone files and FlexClone LUNs to create efficient copies of files and LUNs overview

FlexClone files and FlexClone LUNs are writable, space-efficient clones of parent files and parent LUNs, and help in efficient utilization of the physical aggregate space. FlexClone files and FlexClone LUNs are supported only for FlexVol volumes.

FlexClone files and FlexClone LUNs utilize 0.4 percent of their size to store the metadata. Clones share the data blocks of their parent files and parent LUNs and occupy negligible storage space until clients write new data either to the parent file or LUN, or to the clone.

Clients can perform all file and LUN operations on both the parent and the clone entities.

You can use multiple methods to delete FlexClone files and FlexClone LUNs.

## Create a FlexClone file or FlexClone LUN

You can create space-efficient and time-efficient clones of files and LUNs present in FlexVol volumes or FlexClone volumes by using the `volume file clone create` command.

### What you'll need

- The FlexClone license must be installed on the cluster.
- If multiple block ranges are used for sub-LUN cloning or sub-file cloning, the block numbers must not overlap.
- If you are creating a sub-LUN or sub-file on volumes with adaptive compression enabled, the block ranges must not be misaligned.

This means that the source start block number and destination start block number must either be even aligned or odd aligned.

### About this task

Depending on the privileges assigned by the cluster administrator, an SVM administrator can create FlexClone files and FlexClone LUNs.

You can specify the autodelete setting for FlexClone files and FlexClone LUNs when you create and modify clones. By default, the autodelete setting is disabled.

You can overwrite an existing FlexClone file or FlexClone LUN when you create a clone by using the `volume file clone create` command with the `-overwrite-destination` parameter.

When the node reaches its maximum split load, the node temporarily stops accepting requests to create FlexClone files and FlexClone LUNs and issues an `EBUSY` error message. When the split load for the node falls below the maximum, the node accepts requests to create FlexClone files and FlexClone LUNs again. You should wait until the node has capacity to create the clones before trying the create request again.

### Steps

1. Create a FlexClone file or FlexClone LUN by using the `volume file clone create` command.

The following example shows how you can create a FlexClone file `file1_clone` of the parent file `file1_source`

in the volume vol1:

```
cluster1::> volume file clone create -vserver vs0 -volume vol1 -source
-path /file1_source -destination-path /file1_clone
```

For more information about using this command, see the man pages.

## Related information

[ONTAP 9 Commands](#)

## View node capacity for creating and deleting FlexClone files and FlexClone LUNs

You can view whether a node has capacity to receive new requests to create and delete FlexClone files and FlexClone LUNs by viewing the split load for the node. If the maximum split load is reached, no new requests are accepted until the split load falls below the maximum.

### About this task

When the node reaches its maximum split load, an `EBUSY` error message is issued in response to create and delete requests. When the split load for the node falls below the maximum, the node accepts requests to create and delete FlexClone files and FlexClone LUNs again.

A node can accept new requests when the Allowable Split Load field displays capacity, and the create request fits in the available capacity.

### Step

1. View how much capacity a node has to create and delete FlexClone files and FlexClone LUNs by using the `volume file clone split load show` command.

In the following example, the split load is displayed for all of the nodes in cluster1. All nodes in the cluster have capacity to create and delete FlexClone files and FlexClone LUNs as indicated by the Allowable Split Load field:

```
cluster1::> volume file clone split load show
Node           Max           Current       Token           Allowable
      Split Load Split Load  Reserved Load Split Load
-----
node1           15.97TB           0B           100MB           15.97TB
node2           15.97TB           0B           100MB           15.97TB
2 entries were displayed.
```

## View the space savings due to FlexClone files and FlexClone LUNs

You can view the percentage of disk space saved by block sharing within a volume containing FlexClone files and LUNs.

### Step

1. To view the space saving achieved due to FlexClone files and FlexClone LUNs, enter the following command:

```
df -s volname
```

volname is the name of the FlexVol volume.



If you run the `df -s` command on a deduplication-enabled FlexVol volume, you can view the space saved by both deduplication and FlexClone files and LUNs.

### Example

The following example shows the space saving on a FlexClone volume test1:

```
systemA> df -s test1
```

Filesystem	used	saved	%saved	Vserver
/vol/test1/	4828	5744	54%	vs1

### Methods to delete FlexClone files and FlexClone LUNs

You can use multiple methods to delete FlexClone files and FlexClone LUNs. Understanding what methods are available helps you plan how to manage clones.

You can use the following methods to delete FlexClone files and FlexClone LUNs:

- You can configure a FlexVol volume to automatically delete clones with autodelete enabled when the free space in a FlexVol volume decreases below a particular threshold.
- You can configure clients to delete clones by using the NetApp Manageability SDK.
- You can use clients to delete clones by using the NAS and SAN protocols.

The slower deletion method is enabled by default because this method does not use the NetApp Manageability SDK. However, you can configure the system to use the faster deletion method when you delete FlexClone files by using the `volume file clone deletion` commands.

### How a FlexVol volume can reclaim free space with autodelete setting

#### How a FlexVol volume can reclaim free space with autodelete setting overview

You can enable the autodelete setting of a FlexVol volume to automatically delete FlexClone files and FlexClone LUNs. By enabling autodelete, you can reclaim a target amount of free space in the volume when a volume is nearly full.

You can configure a volume to automatically start deleting FlexClone files and FlexClone LUNs when the free space in the volume decreases below a particular threshold value, and automatically stop deleting clones when a target amount of free space in the volume is reclaimed. Although, you cannot specify the threshold value that starts the automatic deletion of clones, you can specify whether a clone is eligible for deletion, and you can specify the target amount of free space for a volume.

A volume automatically deletes FlexClone files and FlexClone LUNs when the free space in the volume decreases below a particular threshold and when *both* of the following requirements are met:

- The autodelete capability is enabled for the volume that contains the FlexClone files and FlexClone LUNs.

You can enable the autodelete capability for a FlexVol volume by using the `volume snapshot autodelete modify` command. You must set the `-trigger` parameter to `volume` or `snap_reserve` for a volume to automatically delete FlexClone files and FlexClone LUNs.

- The autodelete capability is enabled for the FlexClone files and FlexClone LUNs.

You can enable autodelete for a FlexClone file or FlexClone LUN by using the `file clone create` command with the `-autodelete` parameter. As a result, you can preserve certain FlexClone files and FlexClone LUNs by disabling autodelete for the clones and ensuring that other volume settings do not override the clone setting.

### Configure a FlexVol volume to automatically delete FlexClone files and FlexClone LUNs

You can enable a FlexVol volume to automatically delete FlexClone files and FlexClone LUNs with autodelete enabled when the free space in the volume decreases below a particular threshold.

#### What you'll need

- The FlexVol volume must contain FlexClone files and FlexClone LUNs, and be online.
- The FlexVol volume must not be a read-only volume.

#### Steps

1. Enable automatic deletion of FlexClone files and FlexClone LUNs in the FlexVol volume by using the `volume snapshot autodelete modify` command.
  - For the `-trigger` parameter, you can specify `volume` or `snap_reserve`.
  - For the `-destroy-list` parameter, you must always specify `lun_clone`, `file_clone` regardless of whether you want to delete only one type of clone.

The following example shows how you can enable volume `vol1` to trigger the automatic deletion of FlexClone files and FlexClone LUNs for space reclamation until 25% of the volume consists of free space:

```
cluster1::> volume snapshot autodelete modify -vserver vs1 -volume
vol1 -enabled true -commitment disrupt -trigger volume -target-free
-space 25 -destroy-list lun_clone,file_clone
```

```
Volume modify successful on volume:vol1
```



While enabling FlexVol volumes for automatic deletion, if you set the value of the `-commitment` parameter to `destroy`, all the FlexClone files and FlexClone LUNs with the `-autodelete` parameter set to `true` might be deleted when the free space in the volume decreases below the specified threshold value. However, FlexClone files and FlexClone LUNs with the `-autodelete` parameter set to `false` will not be deleted.

2. Verify that automatic deletion of FlexClone files and FlexClone LUNs is enabled in the FlexVol volume by using the `volume snapshot autodelete show` command.

The following example shows that volume `vol1` is enabled for automatic deletion of FlexClone files and FlexClone LUNs:

```
cluster1::> volume snapshot autodelete show -vserver vs1 -volume vol1

Vserver Name: vs1
Volume Name: vol1
Enabled: true
Commitment: disrupt
Defer Delete: user_created
Delete Order: oldest_first
Defer Delete Prefix: (not specified)
Target Free Space: 25%
Trigger: volume
*Destroy List: lun_clone,file_clone*
Is Constituent Volume: false
```

3. Ensure that autodelete is enabled for the FlexClone files and FlexClone LUNs in the volume that you want to delete by performing the following steps:

- a. Enable automatic deletion of a particular FlexClone file or FlexClone LUN by using the `volume file clone autodelete` command.

You can force a specific FlexClone file or FlexClone LUN to be automatically deleted by using the `volume file clone autodelete` command with the `-force` parameter.

The following example shows that automatic deletion of the FlexClone LUN `lun1_clone` contained in volume `vol1` is enabled:

```
cluster1::> volume file clone autodelete -vserver vs1 -clone-path
/vol/vol1/lun1_clone -enabled true
```

You can enable autodelete when you create FlexClone files and FlexClone LUNs.

- b. Verify that the FlexClone file or FlexClone LUN is enabled for automatic deletion by using the `volume file clone show-autodelete` command.

The following example shows that the FlexClone LUN `lun1_clone` is enabled for automatic deletion:

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone
-path vol/vol1/lun1_clone
Vserver Name: vs1
Clone Path: vol/vol1/lun1_clone
**Autodelete Enabled: true**
```

For more information about using the commands, see the respective man pages.

### Prevent a specific FlexClone file or FlexClone LUN from being automatically deleted

If you configure a FlexVol volume to automatically delete FlexClone files and FlexClone LUNs, any clone that fits the criteria you specify might be deleted. If you have specific FlexClone files or FlexClone LUNs that you want to preserve, you can exclude them from the automatic FlexClone deletion process.

#### What you'll need

A FlexClone license must be installed.

#### About this task

When you create a FlexClone file or FlexClone LUN, by default the autodelete setting for the clone is disabled. FlexClone files and FlexClone LUNs with autodelete disabled are preserved when you configure a FlexVol volume to automatically delete clones to reclaim space on the volume.



If you set the `commitment` level on the volume to `try` or `disrupt`, you can individually preserve specific FlexClone files or FlexClone LUNs by disabling autodelete for those clones. However, if you set the `commitment` level on the volume to `destroy` and the destroy lists include `lun_clone`, `file_clone`, the volume setting overrides the clone setting, and all FlexClone files and FlexClone LUNs can be deleted regardless of the autodelete setting for the clones.

#### Steps

1. Prevent a specific FlexClone file or FlexClone LUN from being automatically deleted by using the `volume file clone autodelete` command.

The following example shows how you can disable autodelete for FlexClone LUN `lun1_clone` contained in `vol1`:

```
cluster1::> volume file clone autodelete -vserver vs1 -volume vol1
-clone-path lun1_clone -enable false
```

A FlexClone file or FlexClone LUN with autodelete disabled cannot be deleted automatically to reclaim space on the volume.

2. Verify that autodelete is disabled for the FlexClone file or FlexClone LUN by using the `volume file clone show-autodelete` command.

The following example shows that autodelete is false for the FlexClone LUN `lun1_clone`:

```

cluster1::> volume file clone show-autodelete -vserver vs1 -clone-path
vol/vol1/lun1_clone
Name: vs1
vol/vol1/lun1_clone
Enabled: false
Vserver
Clone Path:
Autodelete

```

### Commands for configuring deletion of FlexClone files

When clients delete FlexClone files without using the NetApp Manageability SDK, you can use the `volume file clone deletion` commands to enable faster deletion of FlexClone files from a FlexVol volume. Extensions for and minimum size of FlexClone files are used to enable faster deletion.

You can use the `volume file clone deletion` commands to specify a list of supported extensions and a minimum size requirement for FlexClone files in a volume. The faster deletion method is used only for FlexClone files that meet the requirements. For FlexClone files that do not meet the requirements, the slower deletion method is used.

When clients delete FlexClone files and FlexClone LUNs from a volume by using the NetApp Manageability SDK, the extension and size requirements do not apply because the faster deletion method is always used.

To...	Use this command...
Add an extension to the supported list of extensions for the volume	<code>volume file clone deletion add-extension</code>
Change the minimum size of FlexClone files that can be deleted from the volume by using the faster deletion method	<code>volume file clone deletion modify</code>
Remove an extension from the supported list of extensions for the volume	<code>volume file clone deletion remove-extension</code>
View the supported list of extensions and the minimum size of FlexClone files that clients can delete from the volume by using the faster deletion method	<code>volume file clone deletion show</code>

For detailed information about these commands, see the appropriate man page.

## Use qtrees to partition your FlexVol volumes

## Use qtrees to partition your FlexVol volumes overview

Qtrees enable you to partition your FlexVol volumes into smaller segments that you can manage individually. You can use qtrees to manage quotas, security style, and CIFS oplocks.

ONTAP creates a default qtree, called *qtree0*, for each volume. If you do not put data into a qtree, it resides in *qtree0*.

Qtree names must have no more than 64 characters.

Directories cannot be moved between qtrees. Only files can be moved between qtrees.

If you create qtree-level and volume-level shares on the same FlexVol or SCVMM pool, the qtrees appear as directories on the FlexVol share. Therefore, you need to be careful not to delete them accidentally.

### Obtain a qtree junction path

You can mount an individual qtree by obtaining the junction path or namespace path of the qtree. The qtree path displayed by the CLI command `qtree show -instance` is of the format `/vol/<volume_name>/<qtree_name>`. However, this path does not refer to the junction path or namespace path of the qtree.

#### About this task

You need to know the junction path of the volume to obtain the junction path or namespace path of the qtree.

#### Step

1. Use the `vserver volume junction-path` command to obtain the junction path of a volume.

The following example displays the junction path of the volume named `vol1` located on the storage virtual machine (SVM) named `vs0`:

```
cluster1::> volume show -volume vol1 -vserver vs0 -fields junction-path
-----
vs0 vol1 /vol1
```

From the above output, the volume's junction path is `/vol1`. Since qtrees are always rooted at the volume, the junction path or namespace path of the qtree will be `/vol1/qtree1`.

### Qtree name restrictions

Qtree names can be no more than 64 characters in length. In addition, using some special characters in qtree names, such as commas and spaces, can cause problems with other capabilities, and should be avoided.



## Convert a directory to a qtree

### Convert a directory to a qtree overview

If you have a directory at the root of a FlexVol volume that you want to convert to a qtree, you must migrate the data contained in the directory to a new qtree with the same name, using your client application.

#### About this task

The steps you take to convert a directory to a qtree depend on what client you use. The following process outlines the general tasks you need to complete:

#### Steps

1. Rename the directory to be made into a qtree.
2. Create a new qtree with the original directory name.
3. Use the client application to move the contents of the directory into the new qtree.
4. Delete the now-empty directory.



You cannot delete a directory if it is associated with an existing CIFS share.

### Convert a directory to a qtree using a Windows client

To convert a directory to a qtree using a Windows client, you rename the directory, create a qtree on the storage system, and move the directory's contents to the qtree.

#### About this task

You must use Windows Explorer for this procedure. You cannot use the Windows command-line interface or the DOS prompt environment.

#### Steps

1. Open Windows Explorer.
2. Click the folder representation of the directory you want to change.



The directory must reside at the root of its containing volume.

3. From the **File** menu, select **Rename** to give this directory a different name.
4. On the storage system, use the `volume qtree create` command to create a new qtree with the original name of the directory.
5. In Windows Explorer, open the renamed directory folder and select the files inside it.
6. Drag these files into the folder representation of the new qtree.



The more subfolders contained in the folder that you are moving, the longer the move operation takes.

7. From the **File** menu, select **Delete** to delete the renamed, now-empty directory folder.

## Convert a directory to a qtree using a UNIX client

To convert a directory to a qtree in UNIX, you rename the directory, create a qtree on the storage system, and move the directory's contents to the qtree.

### Steps

1. Open a UNIX client window.
2. Use the `mv` command to rename the directory.

```
client: mv /n/user1/vol1/dir1 /n/user1/vol1/olddir
```

3. From the storage system, use the `volume qtree create` command to create a qtree with the original name.

```
system1: volume qtree create /n/user1/vol1/dir1
```

4. From the client, use the `mv` command to move the contents of the old directory into the qtree.



The more subdirectories contained in a directory that you are moving, the longer the move operation will take.

```
client: mv /n/user1/vol1/olddir/* /n/user1/vol1/dir1
```

5. Use the `rmdir` command to delete the old, now-empty directory.

```
client: rmdir /n/user1/vol1/olddir
```


### After you finish

Depending on how your UNIX client implements the `mv` command, file ownership and permissions might not be preserved. If this occurs, update file owners and permissions to their previous values.

### Commands for managing and configuring qtrees

You can manage and configure qtrees by using specific ONTAP commands.

If you want to...	Use this command...
Create a qtree	<code>volume qtree create</code>
Display a filtered list of qtrees	<code>volume qtree show</code>

Delete a qtree	<pre>volume qtree delete</pre> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>The <code>qtree</code> command <code>volume qtree delete</code> will fail unless the qtree is empty or the <code>-force true</code> flag is added.</p> </div>
Modify a qtree's UNIX permissions	<pre>volume qtree modify -unix-permissions</pre>
Modify a qtree's CIFS oplocks setting	<pre>volume qtree oplocks</pre>
Modify a qtree's security setting	<pre>volume qtree security</pre>
Rename a qtree	<pre>volume qtree rename</pre>
Display a qtree's statistics	<pre>volume qtree statistics</pre>
Reset a qtree's statistics	<pre>volume qtree statistics -reset</pre>



The `volume rehost` command can cause other concurrent administrative operations targeted at that volume to fail.

## Logical space reporting and enforcement for volumes

### Logical space reporting and enforcement for volumes overview

Beginning with ONTAP 9.4, you can allow the logical space used in a volume and the amount of remaining storage space to be displayed to users. Beginning with 9.5, you can limit the amount of logical space consumed by users.

Logical space reporting and enforcement are disabled by default.

The following volume types support logical space reporting and enforcement.

Volume type	Is space reporting supported?	Is space enforcement supported?
FlexVol volumes	Yes, beginning with ONTAP 9.4	Yes, beginning with ONTAP 9.5
SnapMirror destination volumes	Yes, beginning with ONTAP 9.8	No
FlexGroup volumes	Yes, beginning with ONTAP 9.9.1	Yes, beginning with ONTAP 9.9.1

## What logical space reporting shows

When you enable logical space reporting on a volume, your system can display the amount of logical used and available space in addition to the total space in a volume. In addition, users on Linux and Windows client systems can see logical used and available space instead of physical used and physical available space.

Definitions:

- Physical space refers to the physical blocks of storage available or used in the volume.
- Logical space refers to the usable space in a volume.
- Logical space used is physical space used plus savings from storage efficiency features (such as deduplication and compression) that have been configured.

Beginning with ONTAP 9.5, you can enable logical space enforcement together with space reporting.

When enabled, logical space reporting displays the following parameters with the `volume show` command:

Parameter	Meaning
<code>-logical-used</code>	Displays information only about the volume or volumes that have the specified logical used size. This value includes all the space saved by the storage efficiency features along with the physically used space. This does not include Snapshot reserve but does consider Snapshot spill.
<code>-logical-used-by-afs</code>	Displays information only about the volume or volumes that have the specified logical size used by the active file system. This value differs from the <code>-logical-used</code> value by the amount of Snapshot spill that exceeds the Snapshot reserve.
<code>-logical-available</code>	When only logical space reporting is enabled, only physical-available space is displayed. When both space reporting and enforcement are enabled, it displays the amount of free space currently available considering space saved by the storage efficiency features as being used. This does not include the Snapshot reserve.
<code>-logical-used-percent</code>	Displays the percentage of the current <code>-logical-used</code> value with the provisioned size excluding Snapshot reserve of the volume.  This value can be greater than 100%, because the <code>-logical-used-by-afs</code> value includes efficiency savings in the volume. The <code>-logical-used-by-afs</code> value of a volume does not include Snapshot spill as used space. The <code>-physical-used</code> value of a volume includes Snapshot spill as used space.
<code>-used</code>	Displays the amount of used space without considering the space saved by storage efficiency features.

Enabling logical space reporting in the CLI also allows the Logical Used Space (%) and Logical Space values to display in System Manager

Client systems see logical space displayed as “used” space on the following system displays:

- **df** output on Linux systems
- Space details under Properties using Windows Explorer on Windows systems.



If logical space reporting is enabled without logical space enforcement, the total displayed on client systems can be higher than the provisioned space.

### What logical space enforcement does

When you enable logical space enforcement in ONTAP 9.5 and later, ONTAP counts the logical-used blocks in a volume to determine the amount of space that is still available in that volume. If there is no space available in a volume, the system returns an ENOSPC (out-of-space) error message.

Logical space enforcement ensures that users are notified when a volume is full or nearly full. Logical space enforcement returns three types of alerts to inform you about the available space in a volume:

- `Monitor.vol.full.inc.sav`: This alert is triggered when 98% of the logical space in the volume has been used.
- `Monitor.vol.nearFull.inc.sav`: This alert is triggered when 95% of the logical space in the volume has been used.
- `Vol.log.overalloc.inc.sav`: This alert is triggered when the logical space used in the volume is greater than the total size of the volume.

This alert tells you that adding to the size of the volume might not create available space since that space will already be consumed by overallocated logical blocks.



Total (logical space) should be equal to provisioned space excluding Snapshot reserve of the volume with logical space enforcement.

For more information, see [Configuring volumes to automatically provide more space when they are full](#)

### Enable logical space reporting and enforcement

Beginning with ONTAP 9.4, you can enable logical space reporting. Beginning with 9.5, you can enable logical space enforcement, or both reporting and enforcement together.

#### About this task

In addition to enabling logical space reporting and enforcement at the individual volume level, you can enable them at the SVM level for every volume that supports the functionality. If you enable logical space features for the entire SVM, you can also disable them for individual volumes.

Beginning with 9.8, if you enable logical space reporting on a SnapMirror source volume, it is automatically enabled on the destination volume after the transfer.



If the enforcement option is enabled on a SnapMirror source volume, the enforcement setting is transferred to the destination volume. However, because the destination volume does not support enforcement, the destination will report logical space consumption but not honor its enforcement.

## Choices

- Enable logical space reporting for a volume:

```
volume modify -vserver SVM-name -volume volume-name -size volume-size -is
-space-reporting-logical true
```

- Enable logical space enforcement for a volume:

```
volume modify -vserver SVM-name -volume volume-name -size volume-size -is
-space-enforcement-logical true
```

- Enable logical space reporting and enforcement together for a volume:

```
volume modify -vserver SVM-name -volume volume-name -size volume-size -is
-space-reporting-logical true -is-space-enforcement-logical true
```

- Enable logical space reporting or enforcement for a new SVM:

```
vserver create -vserver SVM-name -rootvolume root-volume-name -rootvolume
-security-style unix -data-services {desired-data-services} [-is-space-
reporting-logical true] [-is-space-enforcement-logical true]
```

- Enable logical space reporting or enforcement for an existing SVM:

```
vserver modify -vserver SVM-name {desired-data-services} [-is-space-reporting-
logical true] [-is-space-enforcement-logical true]
```

## Use quotas to restrict or track resource usage

### Overview of the quota process

#### Quota process

Quotas provide a way to restrict or track the disk space and number of files used by a user, group, or qtree. Quotas are applied to a specific FlexVol volume or qtree.

Quotas can be soft or hard. Soft quotas cause ONTAP to send a notification when specified limits are exceeded, and hard quotas prevent a write operation from succeeding when specified limits are exceeded.

When ONTAP receives a request from a user or user group to write to a FlexVol volume, it checks to see whether quotas are activated on that volume for the user or user group and determines the following:

- Whether the hard limit will be reached

If yes, the write operation fails when the hard limit is reached and the hard quota notification is sent.

- Whether the soft limit will be breached

If yes, the write operation succeeds when the soft limit is breached and the soft quota notification is sent.

- Whether a write operation will not exceed the soft limit

If yes, the write operation succeeds and no notification is sent.

## Differences among hard, soft, and threshold quotas

Hard quotas prevent operations while soft quotas trigger notifications.

Hard quotas impose a hard limit on system resources; any operation that would result in exceeding the limit fails. The following settings create hard quotas:

- Disk Limit parameter
- Files Limit parameter

Soft quotas send a warning message when resource usage reaches a certain level, but do not affect data access operations, so you can take appropriate action before the quota is exceeded. The following settings create soft quotas:

- Threshold for Disk Limit parameter
- Soft Disk Limit parameter
- Soft Files Limit parameter

Threshold and Soft Disk quotas enable administrators to receive more than one notification about a quota. Typically, administrators set the Threshold for Disk Limit to a value that is only slightly smaller than the Disk Limit, so that the threshold provides a "final warning" before writes start to fail.

### About quota notifications

Quota notifications are messages that are sent to the event management system (EMS) and also configured as SNMP traps.

Notifications are sent in response to the following events:

- A hard quota is reached; in other words, an attempt is made to exceed it
- A soft quota is exceeded
- A soft quota is no longer exceeded

Thresholds are slightly different from other soft quotas. Thresholds trigger notifications only when they are exceeded, not when they are no longer exceeded.

Hard-quota notifications are configurable by using the volume quota modify command. You can turn them off completely, and you can change their frequency, for example, to prevent sending of redundant messages.

Soft-quota notifications are not configurable because they are unlikely to generate redundant messages and their sole purpose is notification.

The following table lists the events that quotas send to the EMS system:

When this occurs...	This event is sent to the EMS...
A hard limit is reached in a tree quota	<code>waf1.quota.qtree.exceeded</code>
A hard limit is reached in a user quota on the volume	<code>waf1.quota.user.exceeded</code> (for a UNIX user) <code>waf1.quota.user.exceeded.win</code> (for a Windows user)

When this occurs...	This event is sent to the EMS...
A hard limit is reached in a user quota on a qtree	<code>waf1.quota.userQtree.exceeded</code> (for a UNIX user) <code>waf1.quota.userQtree.exceeded.win</code> (for a Windows user)
A hard limit is reached in a group quota on the volume	<code>waf1.quota.group.exceeded</code>
A hard limit is reached in a group quota on a qtree	<code>waf1.quota.groupQtree.exceeded</code>
A soft limit, including a threshold, is exceeded	<code>quota.softlimit.exceeded</code>
A soft limit is no longer exceeded	<code>quota.softlimit.normal</code>

The following table lists the SNMP traps that quotas generate:

When this occurs...	This SNMP trap is sent...
A hard limit is reached	<code>quotaExceeded</code>
A soft limit, including a threshold, is exceeded	<code>quotaExceeded</code> and <code>softQuotaExceeded</code>
A soft limit is no longer exceeded	<code>quotaNormal</code> and <code>softQuotaNormal</code>



Notifications contain qtree ID numbers rather than qtree names. You can correlate qtree names to ID numbers by using the `volume qtree show -id` command.

### Why you use quotas

You can use quotas to limit resource usage in FlexVol volumes, to provide notification when resource usage reaches specific levels, or to track resource usage.

You specify a quota for the following reasons:

- To limit the amount of disk space or the number of files that can be used by a user or group, or that can be contained by a qtree
- To track the amount of disk space or the number of files used by a user, group, or qtree, without imposing a limit
- To warn users when their disk usage or file usage is high

Use default, explicit, derived and tracking quotas to manage disk usage in the most efficient manner.

### What quota rules, quota policies, and quotas are

Quotas are defined in quota rules specific to FlexVol volumes. These quota rules are collected together in a quota policy of a storage virtual machine (SVM), and then



activated on each volume on the SVM.

A quota rule is always specific to a volume. Quota rules have no effect until quotas are activated on the volume defined in the quota rule.

A quota policy is a collection of quota rules for all the volumes of an SVM. Quota policies are not shared among SVMs. An SVM can have up to five quota policies, which enable you to have backup copies of quota policies. One quota policy is assigned to an SVM at any given time.

A quota is the actual restriction that ONTAP enforces or the actual tracking that ONTAP performs. A quota rule always results in at least one quota, and might result in many additional derived quotas. The complete list of enforced quotas is visible only in quota reports.

Activation is the process of triggering ONTAP to create enforced quotas from the current set of quota rules in the assigned quota policy. Activation occurs on a volume-by-volume basis. The first activation of quotas on a volume is called initialization. Subsequent activations are called either reinitialization or resizing, depending on the scope of the changes.




When you initialize or resize quotas on a volume, you are activating the quota rules in the quota policy that is currently assigned to the SVM.

### Quota targets and types

Quotas have a type: they can be either user, group, or tree. Quota targets specify the user, group, or qtree for which the quota limits are applied.

The following table lists the kinds of quota targets, what types of quotas each quota target is associated with, and how each quota target is represented:

Quota target	Quota type	How target is represented	Notes
user	user quota	UNIX user name UNIX UID  A file or directory whose UID matches the user  Windows user name in pre-Windows 2000 format  Windows SID  A file or directory with an ACL owned by the user's SID	User quotas can be applied for a specific volume or qtree.
group	group quota	UNIX group name UNIX GID  A file or directory whose GID matches the group	Group quotas can be applied for a specific volume or qtree.   ONTAP does not apply group quotas based on Windows IDs.

qtree	tree quota	qtree name	Tree quotas are applied to a particular volume and do not affect qtrees in other volumes.
""	user quotagroup quota  tree quota	Double quotation marks ("" )	A quota target of "" denotes a <i>default quota</i> . For default quotas, the quota type is determined by the value of the type field.

### Special kinds of quotas

#### How default quotas work

You can use default quotas to apply a quota to all instances of a given quota type. For example, a default user quota affects all users on the system for the specified FlexVol volume or qtree. In addition, default quotas enable you to modify your quotas easily.

You can use default quotas to automatically apply a limit to a large set of quota targets without having to create separate quotas for each target. For example, if you want to limit most users to 10 GB of disk space, you can specify a default user quota of 10 GB of disk space instead of creating a quota for each user. If you have specific users for whom you want to apply a different limit, you can create explicit quotas for those users. (Explicit quotas—quotas with a specific target or list of targets—override default quotas.)

In addition, default quotas enable you to use resizing rather than reinitialization when you want quota changes to take effect. For example, if you add an explicit user quota to a volume that already has a default user quota, you can activate the new quota by resizing.

Default quotas can be applied to all three types of quota target (users, groups, and qtrees).

Default quotas do not necessarily have specified limits; a default quota can be a tracking quota.

A quota is indicated by a target that is either an empty string ("" ) or an asterisk (\*), depending on the context:

- When you create a quota using the `volume quota policy rule create` command, setting the `-target` parameter to an empty string ("" ) creates a default quota.
- In the `volume quota policy rule create` command, the `-qtree` parameter specifies the name of the qtree to which the quota rule applies. This parameter is not applicable for tree type rules. For user or group type rules at the volume level, this parameter should contain "".
- In the output of the `volume quota policy rule show` command, a default quota appears with an empty string ("" ) as the target.
- In the output of the `volume quota report` command, a default quota appears with an asterisk (\*) as the ID and Quota Specifier.

#### Default user quota example

The following quotas file uses a default user quota to apply a 50-MB limit on each user for vol1:

```
#Quota target type          disk  files  thold  sdisk  sfile
#-----
*          user@/vol/vol1  50M
```

If any user on the system enters a command that would cause that user's data to take up more than 50 MB in vol1 (for example, writing to a file from an editor), the command fails.

### How you use explicit quotas

You can use explicit quotas to specify a quota for a specific quota target, or to override a default quota for a specific target.

An explicit quota specifies a limit for a particular user, group, or qtree. An explicit quota replaces any default quota that is in place for the same target.

When you add an explicit user quota for a user that has a derived user quota, you must use the same user mapping setting as the default user quota. Otherwise, when you resize quotas, the explicit user quota is rejected because it is considered a new quota.

Explicit quotas only affect default quotas at the same level (volume or qtree). For example, an explicit user quota for a qtree does not affect the default user quota for the volume that contains that qtree. However, the explicit user quota for the qtree overrides (replaces the limits defined by) the default user quota for that qtree.

### Examples of explicit quotas

The following quotas file contains a default user quota that limits all users in vol1 to 50 MB of space. However, one user, jsmith, is allowed 80 MB of space, because of the explicit quota (shown in bold):

```
#Quota target type          disk  files  thold  sdisk  sfile
#-----
*          user@/vol/vol1  50M
**jsmith   user@/vol/vol1  80M**
```

The following quotas entry restricts the specified user, represented by four IDs, to 500MB of disk space and 10,240 files in the vol1 volume:

```
jsmith,corp\jsmith,engineering\“john smith”,
S-1-5-32-544  user@/vol/vol1          500M      10K
```

The following quotas entry restricts the eng1 group to 150 MB of disk space and an unlimited number of files in the /vol/vol2/proj1 qtree:

```
eng1          group@/vol/vol2/proj1  150M
```

The following quotas entry restricts the proj1 qtree in the vol2 volume to 750 MB of disk space and 76,800 files:

```
/vol/vol2/proj1    tree                750M    75K
```

## How derived quotas work

A quota enforced as a result of a default quota, rather than an explicit quota (a quota with a specific target), is referred to as a *derived quota*.

The number and location of the derived quotas depends on the quota type:

- A default tree quota on a volume creates derived tree quotas for every qtree on the volume.
- A default user or group quota creates a derived user or group quota for every user or group that owns a file at the same level (volume or qtree).
- A default user or group quota on a volume creates a default user or group quota on every qtree that also has a tree quota.

The settings—including limits and user mapping—of derived quotas are the same as the settings of the corresponding default quotas. For example, a default tree quota with a 20-GB disk limit on a volume creates derived tree quotas with 20-GB disk limits on the qtrees in the volume. If a default quota is a tracking quota (with no limits), the derived quotas are also tracking quotas.

To see derived quotas, you can generate a quota report. In the report, a derived user or group quota is indicated by a Quota Specifier that is either blank or an asterisk (\*). A derived tree quota, however, has a Quota Specifier; to identify a derived tree quota, you must look for a default tree quota on the volume with the same limits.

Explicit quotas interact with derived quotas in the following ways:

- Derived quotas are not created if an explicit quota already exists for the same target.
- If a derived quota exists when you create an explicit quota for a target, you can activate the explicit quota by resizing rather than having to perform a full quota initialization.

## How you use tracking quotas

Tracking quotas generate reports of disk and file usage and do not limit resource usage. When tracking quotas are used, modifying quota values is less disruptive, because you can resize quotas rather than turning them off and back on.

To create a tracking quota, you omit the Disk Limit and Files Limit parameters. This tells ONTAP to monitor disk and files usage for that target at that level (volume or qtree), without imposing any limits. Tracking quotas are indicated in the output of `show` commands and the quota report with a dash ("-") for all limits.

You can also specify a *default tracking quota*, which applies to all instances of the target. Default tracking quotas enable you to track usage for all instances of a quota type (for example, all qtrees or all users). In addition, they enable you use resizing rather than reinitialization when you want quota changes to take effect.

## Examples

The following quotas file shows tracking quotas in place for a specific user, group, and qtree:

```
#Quota target      type          disk files thold sdisk sfile
#-----
kjones             user@/vol/vol1  -  -
eng1               group@/vol/vol1 -  -
proj1              tree@/vol/vol1  -  -
```

The following quotas file contains the three possible default tracking quotas (users, groups, and qtrees):

```
#Quota target      type          disk  files thold sdisk sfile
#-----
*               user@/vol/vol1  -  -
*               group@/vol/vol1 -  -
*               tree@/vol/vol1  -  -
```

### How quotas are applied

Understanding how quotas are applied enables you to configure quotas and set the expected limits.

Whenever an attempt is made to create a file or write data to a file in a FlexVol volume that has quotas enabled, the quota limits are checked before the operation proceeds. If the operation exceeds either the disk limit or the files limit, the operation is prevented.

Quota limits are checked in the following order:

1. The tree quota for that qtree (This check is not relevant if the file is being created or written to qtree0.)
2. The user quota for the user that owns the file on the volume
3. The group quota for the group that owns the file on the volume
4. The user quota for the user that owns the file on the qtree (This check is not relevant if the file is being created or written to qtree0.)
5. The group quota for the group that owns the file on the qtree (This check is not relevant if the file is being created or written to qtree0.)

The quota with the smallest limit might not be the one that is exceeded first. For example, if a user quota for volume vol1 is 100 GB, and the user quota for qtree q2 contained in volume vol1 is 20 GB, the volume limit could be reached first if that user has already written more than 80 GB of data in volume vol1 (but outside of qtree q2).

### Considerations for assigning quota policies

A quota policy is a grouping of the quota rules for all the FlexVol volumes of an SVM. You must be aware of certain considerations when assigning the quota policies.

- An SVM has one assigned quota policy at any given time. When an SVM is created, a blank quota policy is created and assigned to the SVM. This default quota policy has the name "default" unless a different name is specified when the SVM is created.

- An SVM can have up to five quota policies. If an SVM has five quota policies, you cannot create a new quota policy for the SVM until you delete an existing quota policy.
- When you need to create a quota rule or change quota rules for a quota policy, you can choose either of the following approaches:
  - If you are working in a quota policy that is assigned to an SVM, you need not assign the quota policy to the SVM.
  - If you are working in an unassigned quota policy and then assigning the quota policy to the SVM, you must have a backup of the quota policy that you can revert to if required.

For example, you can make a copy of the assigned quota policy, change the copy, assign the copy to the SVM, and rename the original quota policy.

- You can rename a quota policy even when it is assigned to the SVM.

## How quotas work with users and groups

### How quotas work with users and groups overview

When you specify a user or group as the target of a quota, the limits imposed by that quota are applied to that user or group. However, some special groups and users are handled differently. There are different ways to specify IDs for users, depending on your environment.

### How you specify UNIX users for quotas

You can specify a UNIX user for a quota using one of three formats: the user name, the UID, or a file or directory owned by the user.

To specify a UNIX user for a quota, you can use one of the following formats:

- The user name, such as jsmith.



You cannot use a UNIX user name to specify a quota if that name includes a backslash (\) or an @ sign. This is because ONTAP treats names containing these characters as Windows names.

- The UID, such as 20.
- The path of a file or directory owned by that user, so that the file's UID matches the user.



If you specify a file or directory name, you must select a file or directory that will last as long as the user account remains on the system.

Specifying a file or directory name for the UID does not cause ONTAP to apply a quota to that file or directory.

### How you specify Windows users for quotas

You can specify a Windows user for a quota using one of three formats: the Windows name in pre-Windows 2000 format, the SID, or a file or directory owned by the SID of the

user.

To specify a Windows user for a quota, you can use one of the following formats:

- The Windows name in pre-Windows 2000 format.
- The security ID (SID), as displayed by Windows in text form, such as S-1-5-32-544.
- The name of a file or directory that has an ACL owned by that user's SID.

If you specify a file or directory name, you must select a file or directory that will last as long as the user account remains on the system.

For ONTAP to obtain the SID from the ACL, the ACL must be valid.



If the file or directory exists in a UNIX-style qtree, or if the storage system uses UNIX mode for user authentication, ONTAP applies the user quota to the user whose **UID**, not SID, matches that of the file or directory.

Specifying a file or directory name to identify a user for a quota does not cause ONTAP to apply a quota to that file or directory.

### How default user and group quotas create derived quotas

When you create default user or group quotas, corresponding derived user or group quotas are automatically created for every user or group that owns files at the same level.

Derived user and group quotas are created in the following ways:

- A default user quota on a FlexVol volume creates derived user quotas for every user that owns a file anywhere on the volume.
- A default user quota on a qtree creates derived user quotas for every user that owns a file in the qtree.
- A default group quota on a FlexVol volume creates derived group quotas for every group that owns a file anywhere on the volume.
- A default group quota on a qtree creates derived group quotas for every group that owns a file in the qtree.

If a user or group does not own files at the level of a default user or group quota, derived quotas are not created for the user or group. For example, if a default user quota is created for qtree proj1 and the user jsmith owns files on a different qtree, no derived user quota is created for jsmith.

The derived quotas have the same settings as the default quotas, including limits and user mapping. For example, if a default user quota has a 50-MB disk limit and has user mapping turned on, any resulting derived quotas also have a 50-MB disk limit and user mapping turned on.

However, no limits exist in derived quotas for three special users and groups. If the following users and groups own files at the level of a default user or group quota, a derived quota is created with the same user-mapping setting as the default user or group quota, but it is only a tracking quota (with no limits):

- UNIX root user (UID 0)
- UNIX root group (GID 0)
- Windows BUILTIN\Administrators group

Since quotas for Windows groups are tracked as user quotas, a derived quota for this group is a user quota that is derived from a default user quota, not a default group quota.

### Example of derived user quotas

If you have volume where three users—root, jsmith, and bob—own files, and you create a default user quota on the volume, ONTAP automatically creates three derived user quotas. Therefore, after you reinitialize quotas on the volume, four new quotas appear in the quota report:

```
cluster1::> volume quota report
  Vserver: vs1

Volume Tree      Type  ID      ----Disk----  ----Files-----  Quota
Specifier
-----
-----
vol1          user  *       0B   50MB   0      -   *
vol1          user  root    5B   -      1      -   -
vol1          user  jsmith  30B  50MB  10     -   *
vol1          user  bob     40B  50MB  15     -   *
4 entries were displayed.
```

The first new line is the default user quota that you created, which is identifiable by the asterisk (\*) as the ID. The other new lines are the derived user quotas. The derived quotas for jsmith and bob have the same 50-MB disk limit as the default quota. The derived quota for the root user is a tracking quota without limits.

### How quotas are applied to the root user

The root user (UID=0) on UNIX clients is subject to tree quotas, but not user quotas or group quotas. This allows the root user to take actions on behalf of other users that would otherwise be prevented by a quota.

When root carries out a file or directory ownership change or other operation (such as the UNIX `chown` command) on behalf of a user with less privileges, ONTAP checks the quotas based on the new owner but does not report errors or stop the operation, even if the hard quota restrictions of the new owner are exceeded. This can be useful when an administrative action, such as recovering lost data, results in temporarily exceeding quotas.



After the ownership transfer is carried out, however, a client system will report a disk space error if the user attempts to allocate more disk space while the quota is still exceeded.

### How quotas work with special Windows groups

Quotas are applied to the Everyone group and the BUILTIN\Administrators group differently than to other Windows groups.

The following list describes what happens if the quota target is a special Windows group ID:

- If the quota target is the Everyone group, a file whose ACL shows that the owner is Everyone is counted under the SID for Everyone.



- If the quota target is BUILTIN\Administrators, the entry is considered a user quota, for tracking only.

You cannot impose restrictions on BUILTIN\Administrators.

If a member of BUILTIN\Administrators creates a file, the file is owned by BUILTIN\Administrators and is counted under the SID for BUILTIN\Administrators, not the user's personal SID.



ONTAP does not support group quotas based on Windows group IDs. If you specify a Windows group ID as the quota target, the quota is considered to be a user quota.

### How quotas are applied to users with multiple IDs

A user can be represented by multiple IDs. You can set up a single user quota for such a user by specifying a list of IDs as the quota target. A file owned by any of these IDs is subject to the restriction of the user quota.

Suppose a user has the UNIX UID 20 and the Windows IDs corp\john\_smith and engineering\jsmith. For this user, you can specify a quota where the quota target is a list of the UID and Windows IDs. When this user writes to the storage system, the specified quota applies, regardless of whether the write originates from UID 20, corp\john\_smith, or engineering\jsmith.



Separate quota file entries are considered separate targets, even if the IDs belong to the same user. For example, for the same user you can specify one quota that limits UID 20 to 1 GB of disk space and another quota that limits corp\john\_smith to 2 GB of disk space, even though both IDs represent the same user. ONTAP applies quotas to UID 20 and corp\john\_smith separately.

In this case, no limits are applied to engineering\jsmith, even though limits are applied to the other IDs used by the same user.

### How ONTAP determines user IDs in a mixed environment

If you have users accessing your ONTAP storage from both Windows and UNIX clients, then both Windows and UNIX security are used to determine file ownership. Several factors determine whether ONTAP uses a UNIX or Windows ID when applying user quotas.

If the security style of the qtree or FlexVol volume that contains the file is only NTFS or only UNIX, then the security style determines the type of ID used when applying user quotas. For qtrees with the mixed security style, the type of ID used is determined by whether the file has an ACL.

The following table summarizes what type of ID is used:

Security Style	ACL	No ACL
UNIX	UNIX ID	UNIX ID
Mixed	Windows ID	UNIX ID
NTFS	Windows ID	Windows ID

## How quotas with multiple users work

When you put multiple users in the same quota target, the quota limits defined by that quota are not applied to each individual user; in this case, the quota limits are shared among all users listed in the quota target.

Unlike with commands for managing objects, such as volumes and qtrees, you cannot rename a quota target, including a multi-user quota. This means that after a multi-user quota is defined, you cannot modify the users in the quota target, and you cannot add users to a target or remove users from a target. If you want to add or remove a user from a multi-user quota, then the quota containing that user must be deleted and a new quota rule with the set of users in the target defined.



If you combine separate user quotas into one multi-user quota, you can activate the change by resizing quotas. However, if you want to remove users from a quota target with multiple users, or add users to a target that already has multiple users, you must reinitialize quotas before the change takes effect.

### Example of more than one user in a quotas file entry

In the following example, there are two users listed in the quota entry. The two users can use up to 80 MB of space combined. If one uses 75 MB, then the other one can use only 5 MB.

```
#Quota      target type      disk files thold  sdisk sfile
#-----  ----  -----  -----  -----  -----
jsmith,chen user@/vol/vol1 80M
```

## How you link UNIX and Windows names for quotas

In a mixed environment, users can log in as either Windows users or UNIX users. You can configure quotas to recognize that a user's UNIX id and Windows ID represent the same user.

Quotas for Windows user name are mapped to a UNIX user name, or vice versa, when both of the following conditions are met:

- The `user-mapping` parameter is set to "on" in the quota rule for the user.
- The user names have been mapped with the `vserver name-mapping` commands.

When a UNIX and Windows name are mapped together, they are treated as the same person for determining quota usage.

## How quotas work with qtrees

You can create quotas with a qtree as their target; these quotas are called *tree quotas*. You can also create user and group quotas for a specific qtree. In addition, quotas for a FlexVol volume are sometimes inherited by the qtrees contained by that volume.

## How tree quotas work

## How tree quotas work overview

You can create a quota with a qtree as its target to limit how large the target qtree can become. These quotas are also called *tree quotas*.

When you apply a quota to a qtree, the result is similar to a disk partition, except that you can change the qtree's maximum size at any time by changing the quota. When applying a tree quota, ONTAP limits the disk space and number of files in the qtree, regardless of their owners. No users, including root and members of the BUILTIN\Administrators group, can write to the qtree if the write operation causes the tree quota to be exceeded.



The size of the quota does not guarantee any specific amount of available space. The size of the quota can be larger than the amount of free space available to the qtree. You can use the `volume quota report` command to determine the true amount of available space in the qtree.

## How user and group quotas work with qtrees

Tree quotas limit the overall size of the qtree. To prevent individual users or groups from consuming the entire qtree, you specify a user or group quota for that qtree.

### Example user quota in a qtree

Suppose you have the following quotas file:

```
#Quota target type          disk files thold sdisk sfile
#----- ----
*          user@/vol/vol1  50M  -   45M
jsmith    user@/vol/vol1  80M  -   75M
```

It comes to your attention that a certain user, kjones, is taking up too much space in a critical qtree, qt1, which resides in vol2. You can restrict this user's space by adding the following line to the quotas file:

```
kjones          user@/vol/vol2/qt1  20M  -   15M
```

## How default tree quotas on a FlexVol volume create derived tree quotas

When you create a default tree quota on a FlexVol volume, corresponding derived tree quotas are automatically created for every qtree in that volume.

These derived tree quotas have the same limits as the default tree quota. If no additional quotas exist, the limits have the following effects:

- Users can use as much space in a qtree as they are allotted for the entire volume (provided they did not exceed the limit for the volume by using space in the root or another qtree).
- Each of the qtrees can grow to consume the entire volume.

The existence of a default tree quota on a volume continues to affect all new qtrees that are added to the volume. Each time a new qtree is created, a derived tree quota is also created.

Like all derived quotas, derived tree quotas display the following behaviors:

- Are created only if the target does not already have an explicit quota.
- Appear in quota reports but do not appear when you show quota rules with the `volume quota policy rule show` command.

### Example of derived tree quotas

You have a volume with three qtrees (proj1, proj2, and proj3) and the only tree quota is an explicit quota on the proj1 qtree limiting its disk size to 10 GB. If you create a default tree quota on the volume and reinitialize quotas on the volume, the quota report now contains four tree quotas:

Volume Specifier	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
vol1	proj1	tree	1	0B	10GB	1	-	proj1
vol1		tree	*	0B	20GB	0	-	*
vol1	proj2	tree	2	0B	20GB	1	-	proj2
vol1	proj3	tree	3	0B	20GB	1	-	proj3
...								

The first line shows the original explicit quota on the proj1 qtree. This quota remains unchanged.

The second line shows the new default tree quota on the volume. The asterisk (\*) Quota Specifier indicates it is a default quota. This quota is a result of the quota rule that you created.

The last two lines show new derived tree quotas for the proj2 and proj3 qtrees. ONTAP automatically created these quotas as a result of the default tree quota on the volume. These derived tree quotas have the same 20-GB disk limit as the default tree quota on the volume. ONTAP did not create a derived tree quota for the proj1 qtree because the proj1 qtree already had an explicit quota.

### How default user quotas on a FlexVol volume affect quotas for the qtrees in that volume

If a default user quota is defined for a FlexVol volume, a default user quota is automatically created for every qtree contained by that volume for which an explicit or derived tree quota exists.

If a default user quota on the qtree already exists, it remains unaffected when the default user quota on the volume is created.

The automatically created default user quotas on the qtrees have the same limits as the default user quota you create for the volume.

An explicit user quota for a qtree overrides (replaces the limits applied by) the automatically created default user quota, the same way as it overrides a default user quota on that qtree that was created by an administrator.

## How qtree changes affect quotas

### How qtree changes affect quotas overview

When you delete, rename, or change the security style of a qtree, the quotas applied by ONTAP might change, depending on the current quotas being applied.

### How deleting a qtree affects tree quotas

When you delete a qtree, all quotas applicable to that qtree, whether they are explicit or derived, are no longer applied by ONTAP.

Whether the quota rules persist depends on where you delete the qtree:

- If you delete a qtree using ONTAP, the quota rules for that qtree are automatically deleted, including tree quota rules and any user and group quota rules configured for that qtree.
- If you delete a qtree using your CIFS or NFS client, you must delete any quota rules for that qtree to avoid getting errors when you reinitialize quotas. If you create a new qtree with the same name as the one you deleted, the existing quota rules are not applied to the new qtree until you reinitialize quotas.

### How renaming a qtree affects quotas

When you rename a qtree using ONTAP, the quota rules for that qtree are automatically updated. If you rename a qtree using your CIFS or NFS client, you must update any quota rules for that qtree.



If you rename a qtree using your CIFS or NFS client and do not update quota rules for that qtree with the new name before you reinitialize quotas, quotas will not be applied to the qtree and explicit quotas for the qtree—including tree quotas and user or group quotas for the qtree—might be converted into derived quotas.

### How changing the security style of a qtree affects user quotas

You can apply Access Control Lists (ACLs) on qtrees by using NTFS or mixed security styles, but not by using the UNIX security style. Therefore, changing the security style of a qtree might affect how quotas are calculated. You should always reinitialize quotas after you change the security style of a qtree.

If you change the security style of a qtree from NTFS or mixed to UNIX, any ACLs on files in that qtree are ignored and the file usage is charged against the UNIX user IDs.

If you change the security style of a qtree from UNIX to either mixed or NTFS, the previously hidden ACLs become visible. In addition, any ACLs that were ignored become effective again, and the NFS user information is ignored. If no ACL existed before, the NFS information continues to be used in the quota calculation.



To make sure that quota usages for both UNIX and Windows users are properly calculated after you change the security style of a qtree, you must reinitialize quotas for the volume containing that qtree.

### Example

The following example shows how a change in the security style of a qtree results in a different user being

charged for the usage of a file in the particular qtree.

Suppose NTFS security is in effect on qtree A, and an ACL gives Windows user corp\joe ownership of a 5 MB file. User corp\joe is charged with 5 MB of disk space usage for qtree A.

Now you change the security style of qtree A from NTFS to UNIX. After quotas are reinitialized, Windows user corp\joe is no longer charged for this file; instead, the UNIX user corresponding to the UID of the file is charged for the file. The UID could be a UNIX user mapped to corp\joe or the root user.

## How quotas are activated

### How quotas are activated overview

New quotas and changes to quotas do not take effect until they are activated. Knowing how quota activation works can help you manage your quotas less disruptively.

You can activate quotas at the volume level.

Your quotas file does not need to be free of all errors to activate quotas. Invalid entries are reported and skipped. If the quotas file contains any valid entries, the quotas are activated.

Quotas are activated either by *initializing* (turning them on) or by *resizing*. Turning off quotas and turning them on again is called reinitializing.

The length of the activation process and its impact on quota enforcement depends on the type of activation:

- The initialization process involves two parts: a `quota on` job and a quota scan of the volume's entire file system. The scan begins after the `quota on` job completes successfully. The quota scan can take some time; the more files that the volume has, the longer it takes. Until the scan is finished, quota activation is not complete and quotas are not enforced.
- The resize process involves only a `quota resize` job. Because it does not involve a quota scan, resizing takes less time than a quota initialization. During a resize process, quotas are enforced.

By default, the `quota on` and `quota resize` jobs run in the background, which permits you to use other commands at the same time.

Errors and warnings from the activation process are sent to the event management system. If you use the `-foreground` parameter with the `volume quota on` or `volume quota resize` commands, the command does not return until the job is complete; this is useful if you are reinitializing from a script. To display errors and warnings later, you can use the `volume quota show` command with the `-instance` parameter.

Quota activation persists across halts and reboots. The process of quota activation does not affect the availability of the storage system data.

### When you can use resizing

Because quota resizing is faster than quota initialization, you should use resizing whenever possible. However, resizing only works for certain types of quota changes.

You can resize quotas when making the following types of changes to the quota rules:

- Changing an existing quota.

For example, changing the limits of an existing quota.

- Adding a quota for a quota target for which a default quota or a default tracking quota exists.
- Deleting a quota for which a default quota or default tracking quota entry is specified.
- Combining separate user quotas into one multi-user quota.



After you have made extensive quotas changes, you should perform a full reinitialization to ensure that all of the changes take effect.



If you attempt to resize and not all of your quota changes can be incorporated by using a resize operation, ONTAP issues a warning. You can determine from the quota report whether your storage system is tracking disk usage for a particular user, group, or qtree. If you see a quota in the quota report, it means that the storage system is tracking the disk space and the number of files owned by the quota target.

### Example quotas changes that can be made effective by resizing

Some quota rule changes can be made effective by resizing. Consider the following quotas:

```
#Quota Target type          disk  files thold  sdisk  sfile
#-----
*          user@/vol/vol2      50M   15K
*          group@/vol/vol2  750M  85K
*          tree@/vol/vol2   -      -
jdoe      user@/vol/vol2/     100M  75K
kbuck     user@/vol/vol2/     100M  75K
```

Suppose you make the following changes:

- Increase the number of files for the default user target.
- Add a new user quota for a new user, boris, that needs more disk limit than the default user quota.
- Delete the kbuck user's explicit quota entry; the new user now needs only the default quota limits.

These changes result in the following quotas:

```
#Quota Target type          disk  files thold  sdisk  sfile
#-----
*          user@/vol/vol2      50M   25K
*          group@/vol/vol2  750M  85K
*          tree@/vol/vol2   -      -
jdoe      user@/vol/vol2/     100M  75K
boris     user@/vol/vol2/     100M  75K
```

Resizing activates all of these changes; a full quota reinitialization is not necessary.

### When a full quota reinitialization is required

Although resizing quotas is faster, you must do a full quota reinitialization if you make

certain small or extensive changes to your quotas.

A full quota reinitialization is necessary in the following circumstances:

- You create a quota for a target that has not previously had a quota.
- You change user mapping in the `usermap.cfg` file and you use the `QUOTA_PERFORM_USER_MAPPING` entry in the quotas file.
- You change the security style of a qtree from UNIX to either mixed or NTFS.
- You change the security style of a qtree from mixed or NTFS to UNIX.
- You remove users from a quota target with multiple users, or add users to a target that already has multiple users.
- You make extensive changes to your quotas.

### **Example of quotas changes that require initialization**

Suppose you have a volume that contains three qtrees and the only quotas in the volume are three tree quotas. You decide to make the following changes:

- Add a new qtree and create a new tree quota for it.
- Add a default user quota for the volume.

Both of these changes require a full quota initialization. Resizing does not make the quotas effective.

### **How you can view quota information**

#### **How you can view quota information overview**

You can use quota reports to view details such as the configuration of quota rules and policies, enforced and configured quotas, and errors that occur during quota resizing and reinitialization.

Viewing quota information is useful in situations such as the following:

- Configuring quotas—for example, to configure quotas and verify the configurations
- Responding to notifications that disk space or file limits will soon be reached or that they have been reached
- Responding to requests for more space

#### **How you can use the quota report to see what quotas are in effect**

Because of the various ways that quotas interact, more quotas are in effect than just the ones you have explicitly created. To see what quotas are in effect, you can view the quota report.

The following examples show quota reports for different types of quotas applied on a FlexVol volume `vol1`, and a qtree `q1` contained in that volume:

#### **Example with no user quotas specified for the qtree**

In this example, there is one qtree, `q1`, which is contained by the volume `vol1`. The administrator has created three quotas:



- A default tree quota limit on vol1 of 400 MB
- A default user quota limit on vol1 of 100 MB
- An explicit user quota limit on vol1 of 200 MB for the user jsmith

The quotas file for these quotas looks similar to the following excerpt:

```
#Quota target type          disk files  thold sdisk  sfile
#-----
*          tree@/vol/vol1  400M
*          user@/vol/vol1  100M
jsmith    user@/vol/vol1  200M
```

The quota report for these quotas looks similar to the following excerpt:

```
cluster1::> volume quota report
Vserver: vs1

Volume  Tree      Type  ID          ----Disk----  ----Files-----  Quota
Specifier
-----
-----
vol1    -          tree  *           0B  400MB        0    -    *
vol1    -          user  *           0B  100MB        0    -    *
vol1    -          user  corp/jsmith  150B 200MB        7    -
corp/jsmith
vol1    q1         tree  1           0B  400MB        6    -    q1
vol1    q1         user  *           0B  100MB        0    -
vol1    q1         user  corp/jsmith  0B  100MB        5    -
vol1    -          user  root        0B  0MB          1    -
vol1    q1         user  root        0B  0MB          8    -
```

The first three lines of the quota report display the three quotas specified by the administrator. Since two of these quotas are default quotas, ONTAP automatically creates derived quotas.

The fourth line displays the tree quota that is derived from the default tree quota for every qtree in vol1 (in this example, only q1).

The fifth line displays the default user quota that is created for the qtree as a result of the existence of the default user quota on the volume and the qtree quota.

The sixth line displays the derived user quota that is created for jsmith on the qtree because there is a default user quota for the qtree (line 5) and the user jsmith owns files on that qtree. Note that the limit applied to the user jsmith in the qtree q1 is not determined by the explicit user quota limit (200 MB). This is because the explicit user quota limit is on the volume, so it does not affect limits for the qtree. Instead, the derived user quota limit for the qtree is determined by the default user quota for the qtree (100 MB).

The last two lines display more user quotas that are derived from the default user quotas on the volume and on the qtree. A derived user quota was created for the root user on both the volume and the qtree because the root user owned files on both the volume and the qtree. Since the root user gets special treatment in terms of quotas, its derived quotas are tracking quotas only.

### Example with user quotas specified for the qtree

This example is similar to the previous one, except that the administrator has added two quotas on the qtree.

There is still one volume, vol1, and one qtree, q1. The administrator has created the following quotas:

- A default tree quota limit on vol1 of 400 MB
- A default user quota limit on vol1 of 100 MB
- An explicit user quota limit on vol1 for the user jsmith of 200 MB
- A default user quota limit on qtree q1 of 50 MB
- An explicit user quota limit on qtree q1 for the user jsmith of 75 MB

The quotas file for these quotas looks like this:

```
#Quota target type          disk files  thold sdisk  sfile
#-----  ----  -----  ---  -----  -----
*          tree@/vol/vol1    400M
*          user@/vol/vol1    100M
jsmith     user@/vol/vol1    200M
*          user@/vol/vol1/q1  50M
jsmith     user@/vol/vol1/q1   75M
```

The quota report for these quotas looks like this:

```

cluster1::> volume quota report
Vserver: vs1

```

Volume Specifier	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
vol1	-	tree	*	0B	400MB	0	-	*
vol1	-	user	*	0B	100MB	0	-	*
vol1	-	user	corp/jsmith	2000B	200MB	7	-	
corp/jsmith								
vol1	q1	user	*	0B	50MB	0	-	*
vol1	q1	user	corp/jsmith	0B	75MB	5	-	
corp/jsmith								
vol1	q1	tree	1	0B	400MB	6	-	q1
vol1	-	user	root	0B	0MB	2	-	
vol1	q1	user	root	0B	0MB	1	-	

The first five lines of the quota report display the five quotas created by the administrator. Since some of these quotas are default quotas, ONTAP automatically creates derived quotas.

The sixth line displays the tree quota that is derived from the default tree quota for every qtree in vol1 (in this example, only q1).

The last two lines display the user quotas that are derived from the default user quotas on the volume and on the qtree. A derived user quota was created for the root user on both the volume and the qtree because the root user owned files on both the volume and the qtree. Since the root user gets special treatment in terms of quotas, its derived quotas are tracking quotas only.

No other default quotas or derived quotas were created for the following reasons:

- A derived user quota was not created for the jsmith user even though the user owns files on both the volume and the qtree because the user already has explicit quotas at both levels.
- No derived user quotas were created for other users because no other users own files on either the volume or the qtree.
- The default user quota on the volume did not create a default user quota on the qtree because the qtree already had a default user quota.

### Why enforced quotas differ from configured quotas

Enforced quotas differ from configured quotas because derived quotas are enforced without being configured but configured quotas are enforced only after they are successfully initialized. Understanding these differences can help you compare the enforced quotas that are shown in quota reports to the quotas that you configured.

Enforced quotas, which appear in quota reports, might differ from the configured quota rules for the following reasons:

- Derived quotas are enforced without being configured as quota rules; ONTAP creates derived quotas automatically in response to default quotas.
- Quotas might not have been reinitialized on a volume after quota rules were configured.
- Errors might have occurred when quotas were initialized on a volume.

### Use the quota report to determine which quotas limit writes to a specific file

You can use the volume quota report command with a specific file path to determine which quota limits affect write operations to a file. This can help you understand which quota is preventing a write operation.

#### Step

1. Use the volume quota report command with the `-path` parameter.

#### Example of showing quotas affecting a specific file

The following example shows the command and output to determine what quotas are in effect for writes to the file `file1`, which resides in the qtree `q1` in the FlexVol volume `vol2`:

```
cluster1:> volume quota report -vserver vs0 -volume vol2 -path
/vol/vol2/q1/file1
Virtual Server: vs0
```

Volume	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
vol2	q1	tree	jsmith	1MB	100MB	2	10000	q1
vol2	q1	group	eng	1MB	700MB	2	70000	
vol2		group	eng	1MB	700MB	6	70000	*
vol2		user	corp\jsmith	1MB	50MB	1	-	*
vol2	q1	user	corp\jsmith	1MB	50MB	1	-	

5 entries were displayed.

#### Commands for displaying information about quotas

You can use commands to display a quota report containing enforced quotas and resource usage, display information about quota state and errors, or about quota policies and quota rules.



You can run the following commands only on FlexVol volumes.

If you want to...	Use this command...
View information about enforced quotas	<code>volume quota report</code>
View resource usage (disk space and number of files) of quota targets	<code>volume quota report</code>
Determine which quota limits are affected when a write to a file is allowed	<code>volume quota report</code> with the <code>-path</code> parameter
Display the quota state, such as <code>on</code> , <code>off</code> , and <code>initializing</code>	<code>volume quota show</code>
View information about quota message logging	<code>volume quota show</code> with the <code>-logmsg</code> parameter
View errors that occur during quota initialization and resizing	<code>volume quota show</code> with the <code>-instance</code> parameter
View information about quota policies	<code>volume quota policy show</code>
View information about quota rules	<code>volume quota policy rule show</code>
View the name of the quota policy that is assigned to a storage virtual machine (SVM, formerly known as Vserver)	<code>vserver show</code> with the <code>-instance</code> parameter

See the man page for each command for more information.

### When to use the `volume quota policy rule show` and `volume quota report` commands

Although both commands show information about quotas, the `volume quota policy rule show` quickly displays configured quota rules while the `volume quota report` command, which consumes more time and resources, displays enforced quotas and resource usage.

The `volume quota policy rule show` command is useful for the following purposes:

- Check the configuration of quota rules before activating them

This command displays all configured quota rules regardless of whether the quotas have been initialized or resized.

- Quickly view quota rules without affecting system resources

Because it does not display disk and file usage, this command is not as resource intensive as a quota report.

- Display the quota rules in a quota policy that is not assigned to the SVM.

The `volume quota report` command is useful for the following purposes:

- View enforced quotas, including derived quotas
- View the disk space and number of files used by every quota in effect, including targets affected by derived quotas

(For default quotas, the usage appears as "0" because the usage is tracked against the resulting derived quota.)

- Determine which quota limits affect when a write to a file will be allowed

Add the `-path` parameter to the `volume quota report` command.



The quota report is resource-intensive operation. If you run it on many FlexVol volumes in the cluster, it might take a long time to complete. A more efficient way would be to view the quota report for a particular volume in an SVM.

#### **Difference in space usage displayed by a quota report and a UNIX client**

##### **Difference in space usage displayed by a quota report and a UNIX client overview**

The value of used disk space that is displayed in a quota report for a FlexVol volume or qtree can be different from the value displayed by a UNIX client for the same volume or qtree. The difference in usage values is because of the difference in methods followed by the quota report and the UNIX commands for calculating the data blocks in the volume or qtree.

For example, if a volume contains a file that has empty data blocks (to which data is not written), the quota report for the volume does not count the empty data blocks while reporting the space usage. However, when the volume is mounted on a UNIX client and the file is shown as the output of the `ls` command, the empty data blocks are also included in the space usage. Therefore, the `ls` command displays a higher file size when compared to the space usage displayed by the quota report.

Similarly, the space usage values shown in a quota report can also differ from the values shown as a result of UNIX commands such as `df` and `du`.

##### **How a quota report accounts for disk space and file usage**

The number of files used and the amount of disk space specified in a quota report for a FlexVol volume or a qtree depend on the count of the used data blocks corresponding to every inode in the volume or the qtree.

The block count includes both direct and indirect blocks used for regular and stream files. The blocks used for directories, Access Control Lists (ACLs), stream directories, and metafiles do not get accounted for in the quota report. In case of UNIX sparse files, empty data blocks are not included in the quota report.

##### **How the `ls` command accounts for space usage**

When you use the `ls` command to view the contents of a FlexVol volume mounted on a UNIX client, the file sizes displayed in the output could be lesser or more than the space

usage displayed in the quota report for the volume depending on the type of data blocks for the file.

The output of the `ls` command displays only the size of a file and does not include indirect blocks used by the file. Any empty blocks of the file also get included in the output of the command.

Therefore, if a file does not have empty blocks, the size displayed by the `ls` command might be less than the disk usage specified by a quota report because of the inclusion of indirect blocks in the quota report. Conversely, if the file has empty blocks, then the size displayed by the `ls` command might be more than the disk usage specified by the quota report.

The output of the `ls` command displays only the size of a file and does not include indirect blocks used by the file. Any empty blocks of the file also get included in the output of the command.

### Example of the difference between space usage accounted by the `ls` command and a quota report

The following quota report shows a limit of 10 MB for a qtree `q1`:

Volume Specifier	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
-----	-----	-----	-----	-----	-----	-----	-----	
-----								
vol1	q1	tree	user1	10MB	10MB	1	-	q1
...								

A file present in the same qtree can have a size exceeding the quota limit when viewed from a UNIX client by using the `ls` command, as shown in the following example:

```
[user1@lin-sys1 q1]$ ls -lh
-rwxr-xr-x 1 user1 nfsuser  **27M** Apr 09 2013 file1
```

### How the `df` command accounts for file size

The way in which in the `df` command reports the space usage depends on two conditions: whether the quotas are enabled or disabled for the volume that contains the qtree, and if quota usage within the qtree is tracked.

When quotas are enabled for the volume that contains the qtree and quota usage within the qtree is tracked, the space usage reported by the `df` command equals the value specified by the quota report. In this situation, quota usage excludes blocks used by directories, ACLs, stream directories, and metafiles.

When quotas are not enabled on the volume, or when the qtree does not have a quota rule configured, the reported space usage includes blocks used by directories, ACLs, stream directories, and metafiles for the entire volume, including other qtrees within the volume. In this situation, the space usage reported by the `df` command is greater than the expected value reported when quotas are tracked.

When you run the `df` command from the mount point of a qtree for which quota usage is tracked, the

command output shows the same space usage as the value specified by the quota report. In most cases, when the tree quota rule has a hard disk-limit, the total size reported by the `df` command equals the disk limit and the space available equals the difference between the quota disk limit and quota usage.

However, in some cases, the space available reported by the `df` command might equal the space available in the volume as a whole. This can occur when there is no hard disk limit configured for the qtree. Beginning with ONTAP 9.9.1, it can also occur when the space available in the volume as a whole is less than the remaining tree quota space. When either of these conditions occur, the total size reported by the `df` command is a synthesized number equal to the quota used within the qtree plus the space available in the FlexVol volume.



This total size is neither the qtree disk limit nor the volume configured size. It can also vary based on your write activity within other qtrees or on your background storage efficiency activity.

### Example of space usage accounted by the `df` command and a quota report

The following quota report shows a disk limit of 1 GB for qtree `alice`, 2 GB for qtree `bob`, and no limit for qtree `project1`:

```
C1_vs1m1::> quota report -vserver vs0
Vserver: vs0
```

Volume Specifier	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
vol2	alice	tree	1	502.0MB	1GB	2	-	alice
vol2	bob	tree	2	1003MB	2GB	2	-	bob
vol2	project1	tree	3	200.8MB	-	2	-	
project1								
vol2		tree	*	0B	-	0	-	*

4 entries were displayed.

In the following example, the output of the `df` command on qtrees `alice` and `bob` reports the same used space as the quota report, and the same total size (in terms of 1M blocks) as the disk limit. This is because the quota rules for qtrees `alice` and `bob` have a defined disk limit and the volume available space (1211 MB) is greater than the tree quota space remaining for qtree `alice` (523 MB) and qtree `bob` (1045 MB).

```
linux-client1 [~]$ df -m /mnt/vol2/alice
Filesystem          1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2  1024     502     523   50% /mnt/vol2

linux-client1 [~]$ df -m /mnt/vol2/bob
Filesystem          1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2  2048    1004    1045   50% /mnt/vol2
```



In the following example, the output of the `df` command on `qtree project1` reports the same used space as the quota report, but the total size is synthesized by adding the available space in the volume as a whole (1211 MB) to the quota usage of `qtree project1` (201 MB) to give a total of 1412 MB. This is because the quota rule for `qtree project1` has no disk limit.

```
linux-client1 [~]$ df -m /mnt/vol2/project1
Filesystem          1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2    1412     201     1211  15% /mnt/vol2
```

The following example shows how the output of the `df` command on the volume as a whole reports the same available space as `project1`.



```
linux-client1 [~]$ df -m /mnt/vol2
Filesystem          1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2    2919  1709     1211  59% /mnt/vol2
```

### How the `du` command accounts for space usage

When you run the `du` command to check the disk space usage for a `qtree` or `FlexVol` volume mounted on a UNIX client, the usage value might be higher than the value displayed by a quota report for the `qtree` or volume.

The output of the `du` command contains the combined space usage of all the files through the directory tree beginning at the level of the directory where the command is issued. Because the usage value displayed by the `du` command also includes the data blocks for directories, it is higher than the value displayed by a quota report.

### Example of the difference between space usage accounted by the `du` command and a quota report

The following quota report shows a limit of 10 MB for a `qtree q1`:

Volume Specifier	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
vol1	q1	tree	user1	10MB	10MB	1	-	q1
...								

In the following example, the disk space usage as the output of the `du` command shows a higher value that exceeds the quota limit:

```
[user1@lin-sys1 q1]$ du -sh
**11M**      q1
```

### Examples of quota configuration

These examples help you understand how to configure quotas and read quota reports.

For the following examples, assume that you have a storage system that includes an SVM, vs1, with one volume, vol1. To start setting up quotas, you create a new quota policy for the SVM with the following command:

```
cluster1::>volume quota policy create -vserver vs1 -policy-name
quota_policy_vs1_1
```

Since the quota policy is new, you assign it to the SVM:

```
cluster1::>vserver modify -vserver vs1 -quota-policy quota_policy_vs1_1
```

### Example 1: Default user quota

You decide to impose a hard limit of 50 MB for each user in vol1:

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type user -target "" -disk-limit 50MB
-qtrees ""
```

To activate the new rule, you initialize quotas on the volume:

```
cluster1::>volume quota on -vserver vs1 -volume vol1 -foreground
```

To view the quota report, you enter the following command:

```
cluster1::>volume quota report
```

The resulting quota report is similar to the following report:

```

Vserver: vs1

```

Volume Specifier	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
vol1		user	*	0B	50MB	0	-	*
vol1		user	jsmith	49MB	50MB	37	-	*
vol1		user	root	0B	-	1	-	

The first line shows the default user quota that you created, including the disk limit. Like all default quotas, this default user quota does not display information about disk or file usage. In addition to the quota that was created, two other quotas appear—one quota for each user that currently owns files on vol1. These additional quotas are user quotas that were derived automatically from the default user quota. The derived user quota for the user jsmith has the same 50-MB disk limit as the default user quota. The derived user quota for the root user is a tracking quota (without limits).

If any user on the system (other than the root user) tries to perform an action that would use more than 50 MB in vol1 (for example, writing to a file from an editor), the action fails.

#### Example 2: Explicit user quota overriding a default user quota

If you need to provide more space in volume vol1 to the user jsmith, then you enter the following command:

```

cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type user -target jsmith -disk-limit 80MB
-qtrees ""

```

This is an explicit user quota, because the user is explicitly listed as the target of the quota rule.

This is a change to an existing quota limit, because it changes the disk limit of the derived user quota for the user jsmith on the volume. Therefore, you do not need to reinitialize quotas on the volume to activate the change.

To resize quotas:

```

cluster1::>volume quota resize -vserver vs1 -volume vol1 -foreground

```

Quotas remain in effect while you resize, and the resizing process is short.

The resulting quota report is similar to the following report:

```

cluster1::> volume quota report
Vserver: vs1

Volume Tree      Type  ID      ----Disk----  ----Files-----  Quota
Specifier
-----
-----
vol1              user  *       0B    50MB    0      -    *
vol1              user  jsmith  50MB  80MB    37     -    jsmith
vol1              user  root    0B    -       1      -    -
3 entries were displayed.

```

The second line now shows a Disk Limit of 80 MB and a Quota Specifier of jsmith.

Therefore, jsmith can use up to 80 MB of space on vol1, even though all other users are still limited to 50 MB.

### Example 3: Thresholds

Suppose you want to receive a notification when users reach within 5 MB of their disk limits. To create a threshold of 45 MB for all users, and a threshold of 75 MB for jsmith, you change the existing quota rules:

```

cluster1::>volume quota policy rule modify -vserver vs1 -policy
quota_policy_vs1_1 -volume vol1 -type user -target "" -qtree "" -threshold
45MB
cluster1::>volume quota policy rule modify -vserver vs1 -policy
quota_policy_vs1_1 -volume vol1 -type user -target jsmith -qtree ""
-threshold 75MB

```

Since the sizes of the existing rules are changed, you resize quotas on the volume in order to activate the changes. You wait until the resize process is finished.

To see the quota report with thresholds, you add the `-thresholds` parameter to the `volume quota report` command:

```

cluster1::>volume quota report -thresholds
Vserver: vs1

Volume  Tree      Type  ID      ----Disk----  ----Files-----
Used    Limit    Used    Limit    Quota
          (Thold)
Specifier
-----
-----
vol1          user   *       0B      50MB      0        -   *
          (45MB)
vol1          user   jsmith  59MB    80MB      55       -   jsmith
          (75MB)
vol1          user   root    0B      -         1        -
          ( -)

3 entries were displayed.

```

The thresholds appear in parentheses in the Disk Limit column.

#### Example 4: Quotas on qtrees

Suppose you need to partition some space for two projects. You can create two qtrees, named proj1 and proj2, to accommodate those projects within vol1.

Currently, users can use as much space in a qtree as they are allotted for the entire volume (provided they did not exceed the limit for the volume by using space in the root or another qtree). In addition, each of the qtrees can grow to consume the entire volume. If you want to ensure that neither qtree grows beyond 20 GB, you can create default tree quota on the volume:

```

cluster1:>>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type tree -target "" -disk-limit 20GB

```

Note that the correct type is *tree*, not *qtree*.

Because this is a new quota, you cannot activate it by resizing. You reinitialize quotas on the volume:

```

cluster1:>>volume quota off -vserver vs1 -volume vol1
cluster1:>>volume quota on -vserver vs1 -volume vol1 -foreground

```



You must ensure that you wait for about five minutes before reactivating the quotas on each affected volume, as attempting to activate them almost immediately after running the `volume quota off` command might result in errors. Alternatively, you can run the commands to reinitialize the quotas for a volume from the node that contains the particular volume.

Quotas are not enforced during the reinitialization process, which takes longer than the resizing process.

When you display a quota report, it has several new lines: some lines are for tree quotas and some lines are for derived user quotas.

The following new lines are for the tree quotas:

Volume Specifier	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
.....	.....	.....	.....	.....	.....	.....	.....	
.....								
...								
vol1		tree	*	0B	20GB	0	-	*
vol1	proj1	tree	1	0B	20GB	1	-	proj1
vol1	proj2	tree	2	0B	20GB	1	-	proj2
...								

The default tree quota that you created appears in the first new line, which has an asterisk (\*) in the ID column. In response to the default tree quota on a volume, ONTAP automatically creates derived tree quotas for each qtree in the volume. These are shown in the lines where proj1 and proj2 appear in the Tree column.

The following new lines are for derived user quotas:

Volume Specifier	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
.....	.....	.....	.....	.....	.....	.....	.....	
.....								
...								
vol1	proj1	user	*	0B	50MB	0	-	
vol1	proj1	user	root	0B	-	1	-	
vol1	proj2	user	*	0B	50MB	0	-	
vol1	proj2	user	root	0B	-	1	-	
...								

Default user quotas on a volume are automatically inherited for all qtrees contained by that volume, if quotas are enabled for qtrees. When you added the first qtree quota, you enabled quotas on qtrees. Therefore, derived default user quotas were created for each qtree. These are shown in the lines where ID is asterisk (\*).

Because the root user is the owner of a file, when default user quotas were created for each of the qtrees, special tracking quotas were also created for the root user on each of the qtrees. These are shown in the lines where ID is root.

**Example 5: User quota on a qtree**

You decide to limit users to less space in the proj1 qtree than they get in the volume as a whole. You want to keep them from using any more than 10 MB in the proj1 qtree. Therefore, you create a default user quota for the qtree:

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume voll -type user -target "" -disk-limit 10MB
-qtrees proj1
```

This is a change to an existing quota, because it changes the default user quota for the proj1 qtree that was derived from the default user quota on the volume. Therefore, you activate the change by resizing quotas. When the resize process is complete, you can view the quota report.

The following new line appears in the quota report showing the new explicit user quota for the qtree:

Volume Specifier	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
----- -----	-----	-----	-----	-----	-----	-----	-----	
voll	proj1	user	*	0B	10MB	0	-	*

However, the user jsmith is being prevented from writing more data to the proj1 qtree because the quota you created to override the default user quota (to provide more space) was on the volume. As you have added a default user quota on the proj1 qtree, that quota is being applied and limiting all the users' space in that qtree, including jsmith. To provide more space to the user jsmith, you add an explicit user quota rule for the qtree with an 80 MB disk limit to override the default user quota rule for the qtree:

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume voll -type user -target jsmith -disk-limit 80MB
-qtrees proj1
```

Since this is an explicit quota for which a default quota already existed, you activate the change by resizing quotas. When the resize process is complete, you display a quota report.

The following new line appears in the quota report:

Volume Specifier	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
----- -----	-----	-----	-----	-----	-----	-----	-----	
voll	proj1	user	jsmith	61MB	80MB	57	-	jsmith

The final quota report is similar to the following report:

```

cluster1::>volume quota report
Vserver: vs1

Volume Tree      Type  ID      ----Disk----  ----Files-----  Quota
Specifier
-----
-----
vol1          tree  *       0B    20GB    0      -    *
vol1          user  *       0B    50MB    0      -    *
vol1          user  jsmith  70MB  80MB    65     -    jsmith
vol1    proj1  tree  1       0B    20GB    1      -    proj1
vol1    proj1  user  *       0B    10MB    0      -    *
vol1    proj1  user  root    0B     -      1      -
vol1    proj2  tree  2       0B    20GB    1      -    proj2
vol1    proj2  user  *       0B    50MB    0      -
vol1    proj2  user  root    0B     -      1      -
vol1          user  root    0B     -      3      -
vol1    proj1  user  jsmith  61MB  80MB    57     -    jsmith
11 entries were displayed.

```

The user `jsmith` is required to meet the following quota limits to write to a file in `proj1`:

1. The tree quota for the `proj1` qtree.
2. The user quota on the `proj1` qtree.
3. The user quota on the volume.

## Set up quotas on an SVM

To set up quotas on a new storage virtual machine (SVM, formerly known as Vserver), you must create a quota policy, add quota policy rules to the policy, assign the policy to the SVM, and initialize quotas on each FlexVol volume on the SVM.

### Steps

1. Use the `vserver show` command with the `-instance` option to display the name of the default quota policy that was automatically created when the SVM was created.

If a name was not specified when the SVM was created, the name is "default". You can also use the `vserver quota policy rename` command to give the default policy a name.



You can also create a new policy by using the `volume quota policy create` command.

2. Use the `volume quota policy rule create` command to create *any* of the following quota rules for each volume on the SVM:
  - Default quota rules for all users
  - Explicit quota rules for specific users



- Default quota rules for all groups
  - Explicit quota rules for specific groups
  - Default quota rules for all qtrees
  - Explicit quota rules for specific qtrees
3. Use the `volume quota policy rule show` command to check that the quota rules are configured correctly.
  4. If you are working on a new policy, use the `vserver modify` command to assign the new policy to the SVM.
  5. Use the `volume quota on` command to initialize the quotas on each volume on the SVM.

You can monitor the initialization process in the following ways:

- When you use the `volume quota on` command, you can add the `-foreground` parameter to run the quota on job in the foreground. (By default, the job runs in the background.)

When the job runs in the background, you can monitor its progress by using the `job show` command.

- You can use the `volume quota show` command to monitor the status of the quota initialization.

6. Use the `volume quota show -instance` command to check for initialization errors, such as quota rules that failed to initialize.
7. Use the `volume quota report` command to display a quota report so that you can ensure the enforced quotas match your expectations.

## Modify (or Resizing) quota limits

When you make changes to the size of existing quotas, you can resize the quotas on all affected volumes, which is faster than reinitializing quotas on those volumes.

### About this task

You have a storage virtual machine (SVM, formerly known as Vserver) with enforced quotas and you want either to change the size limits of existing quotas or to add or delete quotas for targets that already have derived quotas.

### Steps

1. Use the `vserver show` command with the `-instance` parameter to determine the name of the policy that is currently assigned to the SVM.
2. Modify quota rules by performing any of the following actions:
  - Use the `volume quota policy rule modify` command to modify the disk or file limits of existing quota rules.
  - Use the `volume quota policy rule create` command to create explicit quota rules for targets (users, groups, or qtrees) that currently have derived quotas.
  - Use the `volume quota policy rule delete` command to delete explicit quota rules for targets (users, groups, or qtrees) that also have default quotas.
3. Use the `volume quota policy rule show` command to check that the quota rules are configured correctly.
4. Use the `volume quota resize` command on each volume where you changed quotas, to activate the

changes on each volume.

You can monitor the resize process in either of the following ways:

- When you use the `volume quota resize` command, you can add the `-foreground` parameter to run the resize job in the foreground. (By default, the job runs in the background.)

When the job runs in the background, you can monitor its progress by using the `job show` command.

- You can use the `volume quota show` command to monitor the resize status.

5. Use the `volume quota show -instance` command to check for resize errors such as, quota rules that failed to get resized.

In particular, check for “new definition” errors, which occur when you resize quotas after adding an explicit quota for a target that does not already have a derived quota.

6. Use the `volume quota report` command to display a quota report so that you can ensure the enforced quotas match your requirements.

### Reinitialize quotas after making extensive changes

When you make extensive changes to existing quotas; for example, by adding or deleting quotas for targets that have no enforced quotas-- you must make the changes and re-initialize quotas on all affected volumes.

#### About this task

You have a storage virtual machine (SVM) with enforced quotas and you want to make changes that require a full reinitialization of quotas.

#### Steps

1. Use the `vserver show` command with the `-instance` parameter to determine the name of the policy that is currently assigned to the SVM.
2. Modify quota rules by performing any of the following actions:

If you want to...	Then...
Create new quota rules	Use the <code>volume quota policy rule create</code> command
Modify the settings of existing quota rules	Use the <code>volume quota policy rule modify</code> command
Delete existing quota rules	Use the <code>volume quota policy rule delete</code> command

3. Use the `volume quota policy rule show` command to check that the quota rules are configured correctly.
4. Re-initialize quotas on each volume where you changed quotas by turning quotas off and then turning quotas on for those volumes.

- a. Use the `volume quota off` command on each affected volume to deactivate quotas on that volume.
- b. Use the `volume quota on` command on each affected volume to activate quotas on that volume.



You must ensure that you wait for about five minutes before reactivating the quotas on each affected volume, as attempting to activate them almost immediately after running the `volume quota off` command might result in errors.

Alternatively, you can run the commands to re-initialize the quotas for a volume from the node that contains the particular volume.

You can monitor the initialization process in either of the following ways:

- When you use the `volume quota on` command, you can add the `-foreground` parameter to run the quota on job in the foreground. (By default, the job runs in the background.)

When the job runs in the background, you can monitor its progress by using the `job show` command.

- You can use the `volume quota show` command to monitor the status of the quota initialization.
5. Use the `volume quota show -instance` command to check for initialization errors, such as quota rules that failed to initialize.
  6. Use the `volume quota report` command to display a quota report so that you can ensure the enforced quotas match your expectations.

## Commands to manage quota rules and quota policies

You can use the `volume quota policy rule` commands to configure quota rules, and use the `volume quota policy` commands and some `vserver` commands to configure quota policies.



You can run the following commands only on FlexVol volumes.

### Commands for managing quota rules

If you want to...	Use this command...
Create a new quota rule	<code>volume quota policy rule create</code>
Delete an existing quota rule	<code>volume quota policy rule delete</code>
Modify an existing quota rule	<code>volume quota policy rule modify</code>
Display information about configured quota rules	<code>volume quota policy rule show</code>

### Commands for managing quota policies

If you want to...	Use this command...
Duplicate a quota policy and the quota rules it contains	<code>volume quota policy copy</code>
Create a new, blank quota policy	<code>volume quota policy create</code>
Delete an existing quota policy that is not currently assigned to a storage virtual machine (SVM)	<code>volume quota policy delete</code>
Rename a quota policy	<code>volume quota policy rename</code>
Display information about quota policies	<code>volume quota policy show</code>
Assign a quota policy to anSVM	<code>vserver modify</code>
Display the name of the quota policy assigned to anSVM	<code>vserver show</code>

See the man page for each command for more information.

### Commands to activate and modify quotas

You can use the `volume quota` commands to change the state of quotas and configure message logging of quotas.

If you want to...	Use this command...
Turn quotas on (also called <i>initializing</i> them)	<code>volume quota on</code>
Resize existing quotas	<code>volume quota resize</code>
Turn quotas off	<code>volume quota off</code>
Change the message logging of quotas, turn quotas on, turn quotas off, or resize existing quotas	<code>volume quota modify</code>

See the man page for each command for more information.

## Use deduplication, data compression, and data compaction to increase storage efficiency

### Use deduplication, data compression, and data compaction to increase storage efficiency overview

You can run deduplication, data compression, and data compaction together or independently to achieve optimal space savings on a FlexVol volume. Deduplication

eliminates duplicate data blocks. Data compression compresses the data blocks to reduce the amount of physical storage that is required. Data compaction stores more data in less space to increase storage efficiency.



Beginning with ONTAP 9.2, all inline storage efficiency features, such as inline deduplication and inline compression, are enabled by default on AFF volumes.

### Enable deduplication on a volume

You can enable deduplication on a FlexVol volume to achieve storage efficiency. You can enable postprocess deduplication on all volumes and inline deduplication on volumes that reside on AFF or Flash Pool aggregates.

If you want to enable inline deduplication on other types of volumes, see the Knowledge Base article [How to enable volume inline deduplication on Non-AFF \(All Flash FAS\) aggregates](#).

### What you'll need

For a FlexVol volume, you must have verified that enough free space exists for deduplication metadata in volumes and aggregates. The deduplication metadata requires a minimum amount of free space in the aggregate. This amount is equal to 3% of the total amount of physical data for all deduplicated FlexVol volumes or data constituents within the aggregate. Each FlexVol volume or data constituent should have 4% of the total amount of physical data's worth of free space, for a total of 7%.



Beginning with ONTAP 9.2, inline deduplication is enabled by default on AFF systems.

### Choices

- Use the `volume efficiency on` command to enable postprocess deduplication.

The following command enables postprocess deduplication on volume VolA:

```
volume efficiency on -vserver vs1 -volume VolA
```

- Use the `volume efficiency on` command followed by the `volume efficiency modify` command with the `-inline-deduplication` option set to `true` to enable both postprocess deduplication and inline deduplication.

The following commands enable both postprocess deduplication and inline deduplication on volume VolA:

```
volume efficiency on -vserver vs1 -volume VolA
```

```
volume efficiency modify -vserver vs1 -volume VolA -inline-dedupe true
```

- Use the `volume efficiency on` command followed by the `volume efficiency modify` command with the `-inline-deduplication` option set to `true` and the `-policy` option set to `inline-only` to enable only inline deduplication.

The following commands enable only inline deduplication on volume VolA:

```
volume efficiency on -vserver vs1 -volume VolA
```

```
volume efficiency modify -vserver vs1 -volume VolA -policy inline-only -inline
```

```
-dedupe true
```

### After you finish

Verify that the setting has changed by viewing the volume efficiency settings:

```
volume efficiency show -instance
```

### Disable deduplication on a volume

You can disable postprocess deduplication and inline deduplication independently on a volume.

### What you'll need

Stop any volume efficiency operation that is currently active on the volume: `volume efficiency stop`

### About this task

If you have enabled data compression on the volume, running the `volume efficiency off` command disables data compression.

### Choices

- Use the `volume efficiency off` command to disable both postprocess deduplication and inline deduplication.

The following command disable both postprocess deduplication and inline deduplication on volume VolA:

```
volume efficiency off -vserver vs1 -volume VolA
```

- Use the `volume efficiency modify` command with the `-policy` option set to `inline only` to disable postprocess deduplication, but inline deduplication remains enabled.

The following command disables postprocess deduplication, but inline deduplication remains enabled on volume VolA:

```
volume efficiency modify -vserver vs1 -volume VolA -policy inline-only
```

- Use the `volume efficiency modify` command with the `-inline-deduplication` option set to `false` to disable inline deduplication only.

The following command disables only inline deduplication on volume VolA:

```
volume efficiency modify -vserver vs1 -volume VolA -inline-deduplication false
```

### Manage automatic volume-level background deduplication on AFF systems

Beginning with ONTAP 9.3, volume-level background deduplication can be managed to run automatically using a predefined `auto` AFF policy. No manual configuration of the schedules is required. The `auto` policy performs continuous deduplication in the background.

The `auto` policy is set for all newly created volumes and for all upgraded volumes that have not been manually configured for background deduplication. You can change the policy to `default` or any other policy to disable

the feature.

If a volume moves from a non-AFF system to an AFF system, the `auto` policy is enabled on the destination node by default. If a volume moves from an AFF node to a non-AFF node, the `auto` policy on the destination node is replaced by the `inline-only` policy by default.

On AFF, the system monitors all the volumes having the `auto` policy and deprioritizes the volume that has less savings or has frequent overwrites. The deprioritized volumes no longer participate in automatic background deduplication. Change logging on deprioritized volumes is disabled and metadata on the volume is truncated.

Users can promote the deprioritized volume to re-participate in an automatic background deduplication using the `volume efficiency promote` command available at the advanced privilege level.

## Manage aggregate-level inline deduplication on AFF systems

Aggregate-level deduplication eliminates duplicate blocks across volumes belonging to the same aggregate. Beginning with ONTAP 9.2, you can perform aggregate-level deduplication inline on AFF systems. The feature is enabled by default for all newly created volumes and all upgraded volumes with volume inline deduplication turned on.

### About this task

The deduplication operation eliminates duplicate blocks before data is written to disk. Only volumes with the `space guarantee` set to `none` can participate in aggregate-level inline deduplication. This is the default setting on AFF systems.



Aggregate-level inline deduplication is sometimes referred to as cross-volume inline deduplication.

### Step

1. Manage aggregate-level inline deduplication on AFF systems:

If you want to...	Use this command
Enable aggregate-level inline deduplication	<pre>volume efficiency modify -vserver vserver_name -volume vol_name -cross -volume-inline-dedupe true</pre>
Disable aggregate-level inline deduplication	<pre>volume efficiency modify -vserver vserver_name -volume vol_name -cross -volume-inline-dedupe false</pre>
Display aggregate-level inline deduplication status	<pre>volume efficiency config -volume vol_name</pre>

### Examples

The following command displays the aggregate-level inline deduplication status:

```
wfit-8020-03-04::> volume efficiency config -volume choke0_wfit_8020_03_0
Vserver:                               vs0
Volume:                                 choke0_wfit_8020_03_0
Schedule:                               -
Policy:                                 choke_VE_policy
Compression:                            true
Inline Compression:                     true
Inline Dedupe:                          true
Data Compaction:                        true
Cross Volume Inline Deduplication:      false
```

## Manage aggregate-level background deduplication on AFF systems

Aggregate-level deduplication eliminates duplicate blocks across volumes belonging to the same aggregate. Beginning with ONTAP 9.3, you can perform aggregate-level deduplication in the background on AFF systems. The feature is enabled by default for all newly created volumes and all upgraded volumes with volume background deduplication turned on.

### About this task

The operation is triggered automatically when a large enough percentage of the change log has been populated. No schedule or policy is associated with the operation.

Beginning with ONTAP 9.4, AFF users can also run the aggregate-level deduplication scanner to eliminate duplicates of existing data across volumes in the aggregate. You can use the `storage aggregate efficiency cross-volume-dedupe start` command with the `-scan-old-data=true` option to start the scanner:

```
cluster-1::> storage aggregate efficiency cross-volume-dedupe start
-aggregate aggr1 -scan-old-data true
```

Deduplication scanning can be time-consuming. You might want to run the operation in off-peak hours.



Aggregate-level background deduplication is sometimes referred to as cross-volume background deduplication.

### Step

1. Manage aggregate-level background deduplication on AFF systems:

If you want to...	Use this command
Enable aggregate-level background deduplication	<code>volume efficiency modify -vserver &lt;vserver_name&gt; -volume &lt;vol_name&gt; -cross-volume-background-dedupe true</code>



If you want to...	Use this command
Disable aggregate-level background deduplication	<pre>volume efficiency modify -vserver &lt;vserver_name\&gt; -volume &lt;vol_name\&gt; -cross-volume-background-dedupe false</pre>
Display aggregate-level background deduplication status	<pre>aggregate efficiency cross-volume- dedupe show</pre>

## Temperature-sensitive storage efficiency overview

Temperature-sensitive storage efficiency was introduced in ONTAP 9.8 and was enabled automatically on newly created thin-provisioned AFF volumes. Beginning with ONTAP 9.10.1, new AFF volumes are created by default with 8k adaptive compression on the volume (default mode). If temperature sensitive storage efficiency is desired, it must be explicitly set to enable auto adaptive compression and inline deduplication, cross volume inline deduplication, and cross volume background deduplication on the volume (efficient mode).

Accomplishing storage efficiency depends on a correct assessment of your data's "temperature;" meaning, how frequently the data is accessed. Temperature-sensitive storage efficiency is determined by the temperature of a volume's data. For cold data, larger data blocks are compressed, and for hot data, which is overwritten more often, smaller data blocks are compressed, making the process more efficient.

Both storage efficiency modes are supported on FabricPool-enabled aggregates and with all tiering policy types.

### Upgrade considerations

When upgrading to Data ONTAP 9.10.1, existing volumes are assigned a storage efficiency mode based on the type of compression currently enabled on the volumes. During an upgrade, volumes with compression enabled are assigned the default mode, and volumes with temperature-sensitive storage efficiency enabled are assigned the efficient mode. If compression is not enabled, storage efficiency mode remains blank.

### Set storage efficiency mode during volume creation

Beginning with ONTAP 9.10.1, you can set the storage efficiency mode when creating a new AFF volume. Using the parameter `-storage-efficiency-mode`, you can specify whether the volume uses either the efficient mode or the default performance mode. The `-storage-efficiency-mode` parameter is not supported on non-AFF volumes or on data protection volumes.

#### Create a new volume using efficient mode

To set the efficiency mode when enabling storage efficiency, you can use the `-storage-efficiency-mode` parameter with the value `efficient`.

#### Step

1. Create a new volume with efficiency mode enabled:

```
volume create -vserver <vserver name> -volume <volume name> -aggregate
<aggregate name> -size <volume size> -storage-efficiency-mode efficient
```

```
volume create -vserver vs1 -volume aff_voll -aggregate aff_aggr1
-storage-efficiency-mode efficient -size 10g
```

### Create a new volume using performance modes

Performance mode is set by default when you create new AFF volumes with temperature-sensitive storage efficiency. Optionally, you can use the default value with the `-storage-efficiency-mode` parameter.

#### Step


1. Create a new volume with efficiency mode enabled:

```
volume create -vserver <vserver name> -volume <volume name> -aggregate
<aggregate name> -size <volume size> -storage-efficiency-mode default
```

```
volume create -vserver vs1 -volume aff_voll -aggregate aff_aggr1 -storage
-efficiency-mode default -size 10g
```

### System Manager procedure

Beginning with ONTAP 9.10.1, you can use System Manager to enable higher storage efficiency using the temperature-sensitive storage efficiency feature. Performance-based storage efficiency is enabled by default.

1. Click **Storage > Volumes**.
2. Locate the volume on which you want to enable or disable storage efficiency, and click .
3. Click **Edit**, and scroll to **Storage Efficiency**.
4. Select **Enable Higher Storage Efficiency**.

### Check volume efficiency mode

You can use the `volume-efficiency-show` command on an AFF volume to check whether efficiency is set and to view the current efficiency mode.

#### Step

1. Check the efficiency mode on a volume:

```
volume efficiency show -vserver <vserver name> -volume <volume name> -fields
storage-efficiency-mode
```

### Change volume efficiency mode

You can use the `volume efficiency modify` command to change the storage efficiency mode that's set on an AFF volume. You can change the mode from `default` to `efficient` or you can set an efficiency mode when volume efficiency is not already set.

## Steps

1. Change the volume efficiency mode:

```
volume efficiency modify -vserver <vserver name> -volume <volume name>
-storage-efficiency-mode <default|efficient>
```

## View temperature sensitive storage efficiency physical footprint savings

Beginning with ONTAP 9.11.1, you can view the physical footprint savings when temperature sensitive storage efficiency is set on a volume.

### Step

1. View the temperature sensitive storage efficiency footprint:

```
volume show-footprint
```

In the following example, Footprint Data Reduction and Auto Adaptive Compression display the footprint reduction or savings when temperature sensitive storage efficiency is enabled.

```
*> volume show-footprint <vol>

Vserver : vs0
Volume  : voll

Feature                                     Used          Used%
-----
Volume Data Footprint                       4.61MB         0%
Volume Guarantee                            0B             0%
Flexible Volume Metadata                    208KB          0%
Deduplication Metadata                     156KB          0%
    Deduplication                           80KB           0%
    Temporary Deduplication                  72KB           0%
    Cross Volume Deduplication                4KB            0%
Delayed Frees                               116KB          0%

Total Footprint                             5.07MB         0%

Footprint Data Reduction                     40KB           0%
    Auto Adaptive Compression                40KB           0%
Effective Total Footprint                   5.04MB         0%
```

## Enable data compression on a volume

You can enable data compression on a FlexVol volume to achieve space savings by using the `volume efficiency modify` command. You can also assign a compression type to your volume, if you do not want the default compression type.

## What you'll need

You must have enabled deduplication on the volume.



- Deduplication only needs to be enabled and does not need to be running on the volume.
- The compression scanner must be used to compress the existing data on the volumes present in AFF platforms.

## Enabling deduplication on a volume

### About this task

- In HDD aggregates and Flash Pool aggregates, you can enable both inline and postprocess compression or only postprocess compression on a volume.

If you are enabling both, then you must enable postprocess compression on the volume before enabling inline compression.

- In AFF platforms, only inline compression is supported.

Before enabling inline compression, you must enable postprocess compression on the volume. However, because postprocess compression is not supported in AFF platforms, no postprocess compression takes place on those volumes and an EMS message is generated informing you that postprocess compression was skipped.

- Temperature sensitive storage efficiency is introduced in ONTAP 9.8. With this feature, storage efficiency is applied according to whether data is hot or cold. For cold data, larger data blocks are compressed, and for hot data, which is overwritten more often, smaller data blocks are compressed, making the process more efficient. Temperature sensitive storage efficiency is enabled automatically on newly created thin-provisioned AFF volumes.
- The compression type is automatically assigned based on the aggregate's platform:

Platform/aggregates	Compression type
AFF	Adaptive compression
Flash Pool aggregates	Adaptive compression
HDD aggregates	Secondary compression

### Choices

- Use the `volume efficiency modify` command to enable data compression with the default compression type.

The following command enables postprocess compression on volume VolA of SVM vs1:

```
volume efficiency modify -vserver vs1 -volume VolA -compression true
```

The following command enables both postprocess and inline compression on volume VolA of SVM vs1:

```
volume efficiency modify -vserver vs1 -volume VolA -compression true -inline  
-compression true
```

- Use the `volume efficiency modify` command at the advanced privilege level to enable data compression with a specific compression type.
  - a. Use the `set -privilege advanced` command to change the privilege level to advanced.
  - b. Use the `volume efficiency modify` command to assign a compression type to a volume.

The following command enables postprocess compression and assigns the adaptive compression type to volume VolA of SVM vs1:

```
volume efficiency modify -vserver vs1 -volume VolA -compression true
-compression-type adaptive
```

The following command enables both postprocess and inline compression and assigns the adaptive compression type to volume VolA of SVM vs1:

```
volume efficiency modify -vserver vs1 -volume VolA -compression true
-compression-type adaptive -inline-compression true
```

- c. Use the `set -privilege admin` command to change the privilege level to admin.

### Move between secondary compression and adaptive compression

You can switch between secondary compression and adaptive compression depending on the amount of data reads. Adaptive compression is preferred when there are a high volume of random reads on the system and higher performance is required. Secondary compression is preferred when data is written sequentially and higher compression savings are required.

#### About this task

The default compression type is selected based on your aggregates and platform.

#### Steps

1. Disable data compression on the volume:

```
volume efficiency modify
```

The following command disables data compression on volume vol1:

```
volume efficiency modify -compression false -inline-compression false -volume
vol1
```

2. Change to the advanced privilege level:

```
set -privilege advanced
```

3. Decompress the compressed data:

```
volume efficiency undo
```

The following command decompresses the compressed data on volume vol1:

```
volume efficiency undo -vserver vs1 -volume vol1 -compression true
```



You must verify that you have sufficient space in the volume to accommodate the decompressed data.

4. Verify that the status of the operation is idle:

```
volume efficiency show
```

The following command displays the status of an efficiency operation on volume vol1:

```
volume efficiency show -vserver vs1 -volume voll
```

5. Enable data compression, and then set the type of compression:

```
volume efficiency modify
```

The following command enables data compression and sets the compression type as secondary compression on volume vol1:

```
volume efficiency modify -vserver vs1 -volume voll -compression true  
-compression-type secondary
```

This step only enables secondary compression on the volume; the data on the volume is not compressed.



- To compress existing data on AFF systems, you must run the background compression scanner.
- To compress existing data on Flash Pool aggregates or HDD aggregates, you must run the background compression.

6. Change to the admin privilege level:

```
set -privilege admin
```

7. Optional: Enable inline compression:

```
volume efficiency modify
```

The following command enables inline compression on volume vol1:

```
volume efficiency modify -vserver vs1 -volume voll -inline-compression true
```

## Disable data compression on a volume

You can disable data compression on a volume by using the `volume efficiency modify` command.

### About this task

If you want to disable postprocess compression, you must first disable inline compression on the volume.

### Steps

1. Stop any volume efficiency operation that is currently active on the volume:

```
volume efficiency stop
```

## 2. Disable data compression:

```
volume efficiency modify
```

Existing compressed data will remain compressed on the volume. Only new writes coming into the volume are not compressed.

### Examples

The following command disables inline compression on volume VolA:

```
volume efficiency modify -vserver vs1 -volume VolA -inline-compression false
```

The following command disables both postprocess compression and inline compression on volume VolA:

```
volume efficiency modify -vserver vs1 -volume VolA -compression false -inline  
-compression false
```

### Manage inline data compaction for AFF systems

You can control inline data compaction on AFF systems at the volume level using the `volume efficiency modify` command. Data compaction is enabled by default for all volumes on AFF systems.

#### What you'll need

Data compaction requires that the volume space guarantee be set to `none`. This is the default for AFF systems.



The default space guarantee on non-AFF data protection volumes is set to `none`.

#### Steps

##### 1. To verify the space guarantee setting for the volume:

```
volume show -vserver vserver_name -volume volume_name -fields space-guarantee
```

##### 2. To enable data compaction:

```
volume efficiency modify -vserver vserver_name -volume volume_name -data  
-compaction true
```

##### 3. To disable data compaction:

```
volume efficiency modify -vserver vserver_name -volume volume_name -data  
-compaction false
```

##### 4. To display data compaction status:

```
volume efficiency show -instance
```

### Examples

```
cluster1::> volume efficiency modify -vserver vs1 -volume voll1 -data-compaction
true cluster1::> volume efficiency modify -vserver vs1 -volume voll1 -data
-compaction false
```

## Enable inline data compaction for FAS systems

You can control inline data compaction on FAS systems with Flash Pool (hybrid) aggregates or HDD aggregates at the volume or aggregate level by using the `volume efficiency cluster shell` command. Data compaction is disabled by default for FAS systems.

### About this task

If you enable data compaction at the aggregate level, data compaction is enabled on any new volume that is created with a volume space guarantee of `none` in the aggregate. Enabling data compaction on a volume on an HDD aggregate uses additional CPU resources.

### Steps

1. Change to the advanced privilege level:  
`set -privilege advanced`
2. Check the data compaction state of the volumes and aggregates for the desired node:  
`volume efficiency show -volume volume_name +`
3. Enable data compaction on volume:  
`volume efficiency modify -volume volume_name -data-compaction true`



If data compaction is set to `false` for either an aggregate or a volume, then compaction fails. Enabling compaction does not compact existing data; only new writes to the system are compacted. The `volume efficiency start` command contains more information about how to compact existing data (in ONTAP 9.1 and later).

[ONTAP 9 Commands](#)

4. View the compaction statistics:  
`volume efficiency show -volume volume_name`

## Inline storage efficiency enabled by default on AFF systems

Storage efficiency features are currently enabled by default on all newly created volumes on AFF systems. Beginning with ONTAP 9.2, all inline storage efficiency features are enabled by default on all existing and newly created volumes on all AFF systems.

Storage efficiency features include inline deduplication, inline cross-volume deduplication and inline compression, and are enabled by default on AFF systems as shown in the table.



Data compaction behavior on AFF volumes is unchanged in ONTAP 9.2 as it is already enabled by default.



Volume conditions	Storage efficiency features enabled by default in ONTAP 9.2		
	Inline deduplication	Inline cross-volume deduplication	Inline compression
Cluster upgrade to 9.2	Yes	Yes	Yes
ONTAP 7-Mode transition to clustered ONTAP	Yes	Yes	Yes
Volume move	Yes	Yes	Yes
Thick-provisioned volumes	Yes	No	Yes
Encrypted volumes	Yes	No	Yes

The following exceptions apply to one or more inline storage efficiency features:

- Only read-write volumes can support default inline storage efficiency enablement.
- Volumes with compression savings are omitted from enabling inline compression.
- Volumes that have postprocess deduplication turned on are omitted from enabling inline compression.
- On volumes where volume efficiency is turned off, the system overrides the existing volume efficiency policy settings and sets it to enable the inline-only policy.

### Enable storage efficiency visualization

Use the `storage aggregate show-efficiency` command to display information about the storage efficiency of all the aggregates in your system.

The `storage aggregate show-efficiency` command has three different views that can be invoked by passing command options.

#### Default view

The default view displays the overall ratio for each of the aggregates.

```
cluster1::> storage aggregate show-efficiency
```

#### Detailed view

Invoke the detailed view with the `-details` command option. This view displays the following:

- Overall efficiency ratio for each of the aggregates.
- Overall ratio without Snapshot copies.
- Ratio split for the following efficiency technologies: volume deduplication, volume compression, Snapshot copies, clones, data compaction, and aggregate inline deduplication.

```
cluster1::> storage aggregate show-efficiency -details
```

## Advanced view

The advanced view is similar to the detailed view and displays the logical and physical used details. The view was enhanced to now display the efficiency technologies separately.

You must run this command at the advanced privilege level. Switch to advanced privilege by using the `set -privilege advanced` command.

The command prompt changes to `cluster::*>`.

```
cluster1::> set -privilege advanced
```

Invoke the advanced view with the `-advanced` command option.

```
cluster1::*> storage aggregate show-efficiency -advanced
```

To view ratios for a single aggregate individually invoke the `-aggregate aggregate_name` command. This command can be run at the admin level, as well as the advanced privilege level.

```
cluster1::> storage aggregate show-efficiency -aggregate aggr1
```

## Create a volume efficiency policy to run efficiency operations

### Create a volume efficiency policy to run efficiency operations

You can create a volume efficiency policy to run deduplication or data compression followed by deduplication on a volume for a specific duration, and specify the job schedule using the `volume efficiency policy create` command.

### Before you begin

You must have created a cron schedule using the `job schedule cron create` command. For more information about managing the cron schedules, see the [System administration reference](#).

### About this task

An SVM administrator with default predefined roles cannot manage the deduplication policies. However, the cluster administrator can modify the privileges assigned to an SVM administrator by using any customized roles. For more information about the SVM administrator capabilities, see [Administrator authentication and RBAC](#).



You can run deduplication or data compression operations at a scheduled time, or by creating a schedule with a specific duration, or by specifying a threshold percentage, which waits for the new data to exceed the specified percentage and then triggers the deduplication or data compression operation. This threshold value is the percentage of the total number of blocks used in the volume. You can obtain the total number of blocks used from the `df` command output.

### Steps

1. Use the `volume efficiency policy create` command to create a volume efficiency policy.

### Examples

The following command creates a volume efficiency policy named `pol1` that triggers an efficiency operation daily:

```
volume efficiency policy create -vserver vs1 -policy pol1 -schedule daily
```

The following command creates a volume efficiency policy named pol2 that triggers an efficiency operation when the threshold percentage reaches 20%:

```
volume efficiency policy create -vserver vs1 -policy pol2 -type threshold -start  
-threshold-percent 20%
```

### Assign a volume efficiency policy to a volume

You can assign an efficiency policy to a volume to run deduplication or data compression operation by using the `volume efficiency modify` command.

#### About this task

If an efficiency policy is assigned to a SnapVault secondary volume, only the volume efficiency priority attribute is considered when running volume efficiency operations. The job schedules are ignored and the deduplication operation is run when incremental updates are made to the SnapVault secondary volume.

#### Step

1. Use the `volume efficiency modify` command to assign a policy to a volume.

#### Example

The following command assigns the volume efficiency policy named `new_policy` with volume `VolA`:

```
volume efficiency modify -vserver vs1 -volume VolA -policy new_policy
```

### Modify a volume efficiency policy

You can modify a volume efficiency policy to run deduplication and data compression for a different duration or change the job schedule using the `volume efficiency policy modify` command.

#### Step

1. Use the `volume efficiency policy modify` command to modify a volume efficiency policy.

#### Examples

The following command modifies the volume efficiency policy named `policy1` to run every hour:

```
volume efficiency policy modify -vserver vs1 -policy policy1 -schedule hourly
```

The following command modifies a volume efficiency policy named `pol2` to threshold 30%:

```
volume efficiency policy modify -vserver vs1 -policy pol1 -type threshold -start  
-threshold-percent 30%
```

### View a volume efficiency policy

You can view the volume efficiency policy name, schedule, duration, and description by using the `volume efficiency policy show` command.

#### About this task

When you run the `volume efficiency policy show` command from the cluster scope, the cluster-scoped policies are not displayed. However, you can view the cluster-scoped policies in the storage virtual machine (SVM) context.

### Step

1. Use the `volume efficiency policy show` command to view information about a volume efficiency policy.

The output depends on the parameters you specify. For more information about displaying detailed view and other parameters, see the man page for this command.

### Examples

The following command displays information about the policies created for the SVM vs1: `volume efficiency policy show -vserver vs1`

The following command displays the policies for which the duration is set as 10 hours: `volume efficiency policy show -duration 10`

### Disassociate a volume efficiency policy from a volume

You can disassociate a volume efficiency policy from a volume to stop running any further schedule-based deduplication and data compression operations on the volume. Once you disassociate a volume efficiency policy, you have to trigger it manually.

### Step

1. Use the `volume efficiency modify` command to disassociate a volume efficiency policy from a volume.

### Example

The following command disassociates the volume efficiency policy from volume VolA: `volume efficiency modify -vserver vs1 -volume VolA -policy -`

### Delete a volume efficiency policy

You can delete a volume efficiency policy by using the `volume efficiency policy delete` command.

### What you'll need

You must have ensured that the policy you want to delete is not associated with any volume.



You cannot delete the *inline-only* and the *default* predefined efficiency policy.

### Step

1. Use the `volume efficiency policy delete` command to delete a volume efficiency policy.

### Example

The following command deletes a volume efficiency policy named policy1: `volume efficiency policy delete -vserver vs1 -policy policy1`

## Manage volume efficiency operations manually

### Manage volume efficiency operations manually overview

You can manage how the efficiency operations run on a volume by running efficiency operations manually.

You can also control how the efficiency operations run based on the following conditions:

- Use checkpoints or not
- Run efficiency operations on existing data or only new data
- Stop efficiency operations if required

You can use the `volume efficiency show` command with `schedule` as value for the `-fields` option to view the schedule assigned to the volumes.

### Run efficiency operations manually

You can run efficiency operations manually on a volume by using the `volume efficiency start` command.

### What you'll need

Depending on the efficiency operation you want to run manually, you must have enabled deduplication or both data compression and deduplication on a volume.

### About this task

If deduplication and data compression are enabled on a volume, data compression is run initially followed by deduplication.

Deduplication is a background process that consumes system resources while it is running. If the data does not change often in a volume, it is best to run deduplication less frequently. Multiple concurrent deduplication operations running on a storage system lead to a higher consumption of system resources.

You can run a maximum of eight concurrent deduplication or data compression operations per node. If any more efficiency operations are scheduled, the operations are queued.

### Step

1. Use the `volume efficiency start` command to start the efficiency operation on a volume.

### Example

The following command allows you to manually start only deduplication or data compression followed by deduplication on the volume `VolA`:

```
volume efficiency start -vserver vs1 -volume VolA
```

### Use checkpoints to resume efficiency operation

The checkpoints are used internally to log the execution process of an efficiency operation. When an efficiency operation is stopped for any reason (such as system halt, system disruption, reboot, or because last efficiency operation failed or stopped) and checkpoint data exists, the efficiency operation can resume from the latest checkpoint file.

A checkpoint is created:

- in each stage or substage of the operation
- when you run the `sis stop` command
- when the duration expires

### Resume a halted efficiency operation

If an efficiency operation is halted due to a system halt, system disruption, or reboot, you can resume the efficiency operation from the same point by using the `volume efficiency start` command with the `checkpoint` option. This helps in saving time and resources by not having to restart the efficiency operation from the beginning.

#### About this task

If you enabled only deduplication on the volume, deduplication runs on the data. If you enabled both deduplication and data compression on a volume, then data compression runs first, followed by deduplication.

You can view the details of the checkpoint for a volume by using the `volume efficiency show` command.

By default, the efficiency operations resume from checkpoints. However, if a checkpoint corresponding to a previous efficiency operation (the phase when the `volume efficiency start`-scan-old-data`` command is run) is older than 24 hours, then the efficiency operation does not resume from the previous checkpoint automatically. In this case, the efficiency operation starts from the beginning. However, if you know that significant changes have not occurred in the volume since the last scan, you can force continuation from the previous checkpoint by using the `-use-checkpoint` option.

#### Step

1. Use the `volume efficiency start` command with the `-use-checkpoint` option to resume an efficiency operation.

The following command enables you to resume an efficiency operation on new data on volume VolA:

```
volume efficiency start -vserver vs1 -volume VolA -use-checkpoint true
```

The following command enables you to resume an efficiency operation on existing data on volume VolA:

```
volume efficiency start -vserver vs1 -volume VolA -scan-old-data true -use-checkpoint true
```

### Run efficiency operations manually on existing data

You can run the efficiency operations manually on the data that exists in non-temperature sensitive storage efficiency volumes prior to enabling deduplication, data compression, or data compaction with ONTAP versions earlier than ONTAP 9.8. You can run these operations by using the `volume efficiency start -scan-old-data` command.

#### About this task

The `-compression` option does not work with `-scan-old-data` on temperature sensitive storage efficiency volumes. Inactive data compression runs automatically on preexisting data for temperature sensitive storage efficiency volumes in ONTAP 9.8 and later.

If you enable only deduplication on a volume, then deduplication runs on the data. If you enable deduplication, data compression, and data compaction on a volume, then data compression runs first, followed by deduplication and data compaction.

When you run data compression on existing data, by default the data compression operation skips the data blocks that are shared by deduplication and the data blocks that are locked by Snapshot copies. If you choose to run data compression on shared blocks, then optimization is turned off and the fingerprint information is captured and used for sharing again. You can change the default behavior of data compression when compressing existing data.

You can run a maximum of eight deduplication, data compression, or data compaction operations concurrently per node. The remaining operations are queued.



Postprocess compression does not run on AFF platforms. An EMS message is generated to inform you that this operation was skipped.

### Step

1. Use the `volume efficiency start -scan-old-data` command to run deduplication, data compression, or data compaction manually on the existing data.

The following command enables you to run these operations manually on the existing data in volume VolA:

```
volume efficiency start -vserver vs1 -volume VolA -scan-old-data true [-  
compression | -dedupe | -compaction ] true
```

## Manage volume efficiency operations using schedules

### Run efficiency operations depending on the amount of new data written

You can modify the efficiency operation schedule to run deduplication or data compression when the number of new blocks written to the volume after the previous efficiency operation (performed manually or scheduled) exceeds a specified threshold percentage.

#### About this task

If the `schedule` option is set to `auto`, the scheduled efficiency operation runs when the amount of new data exceeds the specified percentage. The default threshold value is 20 percent. This threshold value is the percentage of the total number of blocks already processed by the efficiency operation.

### Step

1. Use the `volume efficiency modify` command with the `auto@num` option to modify the threshold percentage value.

`num` is a two-digit number to specify the percentage.

### Example

The following command modifies the threshold percentage value to 30 percent for the volume VolA:

```
volume efficiency modify -vserver vs1 -volume -VolA -schedule auto@30
```

## Run efficiency operations using scheduling

You can modify the scheduling of deduplication or data compression operation on a volume by using the `volume efficiency modify` command. The configuration options of a schedule and volume efficiency policy are mutually exclusive.

### Step

1. Use the `volume efficiency modify` command to modify the scheduling of deduplication or data compression operations on a volume.

### Examples

The following command modifies the scheduling of efficiency operations for VolA to run at 11 p.m., Monday through Friday:

```
volume efficiency modify -vserver vs1 -volume VolA -schedule mon-fri@23
```

## Monitor volume efficiency operations

### View the status of efficiency operations

You can view whether deduplication or data compression is enabled on a volume. You can also view the status, state, type of compression, and progress of the efficiency operations on a volume by using the `volume efficiency show` command.

### Step

1. Use the `volume efficiency show` command to view the status of an efficiency operation on a volume.

The following command displays the status of an efficiency operation on volume VolA that is assigned the adaptive compression type:

```
volume efficiency show -instance -vserver vs1 -volume VolA
```

If the efficiency operation is enabled on volume VolA and the operation is idle, then you can see the following in the system output:

```
cluster1::> volume efficiency show -vserver vs1 -volume VolA

Vserver Name: vs1
Volume Name: VolA
Volume Path: /vol/VolA
    State: Enabled
    Status: Idle
    Progress: Idle for 00:03:20
```

### View efficiency space savings

You can view the amount of space savings achieved through deduplication and data compression on a volume by using the `volume show` command.



### About this task

The space savings in Snapshot copies are not included when calculating the space savings achieved on a volume. Using deduplication does not affect volume quotas. Quotas are reported at the logical level, and remain unchanged.

### Step

1. Use the `volume show` command to view space savings achieved on a volume using deduplication and data compression.

### Example

The following command enables you to view the space savings achieved by using deduplication and data compression on volume VolA: `volume show -vserver vs1 -volume VolA`

```
cluster1::> volume show -vserver vs1 -volume VolA

                                     Vserver Name: vs1
                                     Volume Name: VolA

...

    Space Saved by Storage Efficiency: 115812B
Percentage Saved by Storage Efficiency: 97%
    Space Saved by Deduplication: 13728B
Percentage Saved by Deduplication: 81%
    Space Shared by Deduplication: 1028B
    Space Saved by Compression: 102084B
Percentage Space Saved by Compression: 97%

...
```

### View efficiency statistics of a FlexVol volume

You can view the details of the efficiency operations run on a FlexVol volume by using the `volume efficiency stat` command.

### Step

1. Use the `volume efficiency stat` command to view the statistics of efficiency operations on a FlexVol volume.

### Example

The following command enables you to view the statistics of the efficiency operations on the volume VolA: `volume efficiency stat -vserver vs1 -volume VolA`

```
cluster1::> volume efficiency stat -vserver vs1 -volume VolA

Vserver Name: vs1
Volume Name: VolA
Volume Path: /vol/VolA
Inline Compression Attempts: 0
```

## Stop volume efficiency operations

You can stop a deduplication or postprocess compression operation by using the `volume efficiency stop` command. This command automatically generates a checkpoint.

### Step

1. Use the `volume efficiency stop` command to stop an active deduplication or postprocess compression operation.

If you specify the `-all` option, active and queued efficiency operations are aborted.

### Examples

The following command stops the deduplication or postprocess compression operation that is currently active on volume VolA:

```
volume efficiency stop -vserver vs1 -volume VolA
```

The following command aborts both active and queued deduplication or postprocess compression operations on volume VolA:

```
volume efficiency stop -vserver vs1 -volume VolA -all true
```

## Information about removing space savings from a volume

You can choose to remove the space savings achieved by running efficiency operations on a volume, but it must have enough space to accommodate their reversal.

See these Knowledge Base articles:

- [How to see space savings from deduplication, compression, and compaction in ONTAP 9](#)
- [How to undo the storage efficiency savings in ONTAP](#)

## Rehost a volume from one SVM to another SVM

### Rehost a volume from one SVM to another SVM overview

Volume rehost enables you to reassign NAS or SAN volumes from one storage virtual machine (SVM, formerly known as Vserver) to another SVM without requiring a SnapMirror copy. The volume rehost procedures depend upon the protocol type and the volume type. Volume rehost is a disruptive operation for data access and volume

management.

### What you'll need

Several conditions must be met before you can rehost a volume from one SVM to another:

- The volume must be online.
- Protocols: SAN or NAS

For the NAS protocol, the volume must be unmounted.

- If the volume is in a SnapMirror relationship, then the relationship must be either deleted or broken prior to volume rehost.

You can resynchronize the SnapMirror relationship after the volume rehost operation.

### Rehost CIFS volumes

You can rehost volumes that serve data over SMB protocol. After rehosting the CIFS volume, to continue accessing data over SMB protocol, you must manually configure policies and the associated rules.

### What you'll need

- Volume must be online.
- Volume management operations, such as volume move or LUN move, must not be running.
- Data access to the volume that is being rehosted must be stopped.
- The ns-switch and name services configuration of the target SVM must be configured to support data access of the rehosting volume.
- The source SVM and destination SVM must have the same Active Directory and realmDNS domain.
- The user ID and group ID of the volume must be either available in the target SVM or changed on the hosting volume.



If local users and groups are configured, and if there are files and directories on that volume with permissions set for those users or groups, these permissions are no longer effective.

### About this task

- Rehosting is a disruptive operation.
- If the rehosting operation fails, you might need to reconfigure the volume policies and the associated rules on the source volume.
- If the source SVM and destination SVM Active Directory domains differ, you might lose access to the objects on the volume.
- When the source SVM has local users and groups, the permissions for the files and directories (ACLs) that are set are no longer effective after volume rehost operation.

The same is true for audit ACLs (SACLs)

- After the rehost operation, the following volume policies, policy rules, and configurations are lost from the source volume, and must be manually reconfigured on the rehosted volume:

- Volume and qtree export policies
- Antivirus policies
- Volume efficiency policy
- Quality of service (QoS) policies
- Snapshot policies
- Quota rules
- ns-switch and name services configuration export policy and rules
- User and group IDs

## Steps

1. Record information about the CIFS shares to avoid losing information on CIFS shares in case volume rehost operation fails.
2. Unmount the volume from the parent volume:

```
volume unmount
```

3. Switch to the advanced privilege level:

```
set -privilege advanced
```

4. Rehost the volume on the destination SVM:

```
volume rehost -vserver source_svm -volume vol_name -destination-vserver
destination_svm
```

5. Mount the volume under the appropriate junction path in the destination SVM:

```
volume mount
```

6. Create CIFS shares for the rehosted volume:

```
vserver cifs share create
```

7. If the DNS domains differ between the source SVM and destination SVM, create new users and groups.
8. Update the CIFS client with the new destination SVM LIFs and junction path to the rehosted volume.

## After you finish

You must manually reconfigure the policies and the associated rules on the rehosted volume.

## [SMB configuration](#)

## [SMB and NFS multiprotocol configuration](#)

## Rehost NFS volumes

You can rehost volumes that serve data over NFS protocol. After rehosting the NFS volumes, to continue accessing data over NFS protocol, you must associate the volume with the export policy of the hosting SVM and manually configure policies and associated rules.

## What you'll need

- The volume must be online.
- Volume management operations, such as volume moves or LUN moves, must not be running.
- Data access to the volume that is being rehosted must be stopped.
- The ns-switch and name services configuration of the target SVM must be configured to support data access of the rehosting volume.
- The user ID and group ID of the volume must be either available in the target SVM or changed on the hosting volume.

## About this task

- Rehosting is a disruptive operation.
- If the rehosting operation fails, you might need to reconfigure the volume policies and the associated rules on the source volume.
- After the rehost operation, the following volume policies, policy rules, and configurations are lost from the source volume, and must be manually reconfigured on the rehosted volume:
  - Volume and qtree export policies
  - Antivirus policies
  - Volume efficiency policy
  - Quality of service (QoS) policies
  - Snapshot policies
  - Quota rules
  - ns-switch and name services configuration export policy and rules
  - User and group IDs

## Steps

1. Record information about the NFS export policies to avoid losing information on NFS policies in case volume rehost operation fails.
2. Unmount the volume from the parent volume:

```
volume unmount
```

3. Switch to the advanced privilege level:

```
set -privilege advanced
```

4. Rehost the volume on the destination SVM:

```
volume rehost -vserver source_svm -volume vol_name -destination-vserver destination_svm
```

The default export policy of the destination SVM is applied to the rehosted volume.

5. Create the export policy:

```
vserver export-policy create
```

6. Update the export policy of the rehosted volume to a user-defined export policy:

```
volume modify
```

7. Mount the volume under the appropriate junction path in the destination SVM:

```
volume mount
```

8. Verify that the NFS service is running on the destination SVM.

9. Resume NFS access to the rehosted volume.

10. Update the NFS client credentials and LIF configurations to reflect the destination SVM LIFs.

This is because the volume access path (LIFs and junction path) has undergone changes.

### After you finish

You must manually reconfigure the policies and the associated rules on the rehosted volume.

### NFS configuration

### Rehost SAN volumes

You can rehost volumes that have mapped LUNs. After re-creating the initiator group (igroup) in the destination SVM, volume rehost can automatically remap the volume on the same SVM.

### What you'll need

- The volume must be online.
- Volume management operations, such as volume moves or LUN moves, must not be running.
- There must be no active I/O on the volumes or LUNs.
- You must have verified that the destination SVM does not have igroup of the same name but different initiators.

If the igroup has the same name, then you must have renamed the igroup in either one of the SVMs (source or destination).

- You must have enabled the `force-unmap-luns` option.
  - The default value of the `force-unmap-luns` option is `false`.
  - No warning or confirmation message is displayed when you set the `force-unmap-luns` option to `true`.

### About this task

- Rehosting is a disruptive operation.
- If the rehosting operation fails, you might need to reconfigure the volume policies and the associated rules on the source volume.
- After the rehost operation, the following volume policies, policy rules, and configurations are lost from the source volume and must be manually reconfigured on the rehosted volume:
  - Antivirus policies

- Volume efficiency policy
- Quality of service (QoS) policies
- Snapshot policies
- ns-switch and name services configuration export policy and rules
- User and group IDs

### Steps

1. Record LUN mapping information on target volume:

```
lun mapping show-volume volume to be rehosted-vserver source vserver
```

This is a precautionary step to avoid losing information about LUN mapping in case the volume rehost fails.

2. Delete igroups associated with the target volume.
3. Rehost the target volume to the destination SVM:

```
volume rehost -vserver source_svm -volume vol_name -destination-vserver
destination_svm
```

4. Map LUNs on the target volume to appropriate igroups.
  - Volume rehost preserves LUNs on the target volume; however, LUNs remain unmapped.
  - Use the destination SVM port set while mapping LUNs.
  - If the `auto-remap-luns` option is set to `true`, the LUNs are mapped automatically after rehost.

### Rehost volumes in a SnapMirror relationship

You can rehost volumes in a SnapMirror relationship.

#### What you'll need

- The volume must be online.
- Volume management operations, such as volume moves or LUN moves, must not be running.
- Data access to the volume that is being rehosted must be stopped.
- The ns-switch and name services configuration of the target SVM must be configured to support data access of the rehosting volume.
- The user ID and group ID of the volume must be either available in the target SVM or changed on the hosting volume.

#### About this task

- Rehosting is a disruptive operation.
- If the rehosting operation fails, you might need to reconfigure the volume policies and the associated rules on the source volume.
- After the rehost operation, the following volume policies, policy rules, and configurations are lost from the source volume and must be manually reconfigured on the rehosted volume:
  - Volume and qtree export policies
  - Antivirus policies

- Volume efficiency policy
- Quality of service (QoS) policies
- Snapshot policies
- Quota rules
- ns-switch and name services configuration export policy and rules
- User and group IDs

## Steps

1. Record the SnapMirror relationship type:

```
snapmirror show
```

This is a precautionary step to avoid losing information about the SnapMirror relationship type in case the volume rehost fails.

2. From the destination cluster, delete the SnapMirror relationship:

```
snapmirror delete
```

You must not break the SnapMirror relationship; otherwise, the data protection capability of the destination volume is lost and the relationship cannot be reestablished after the rehosting operation.

3. From the source cluster, remove the SnapMirror relationship information:

```
snapmirror release relationship-info-only true
```

Setting the `relationship-info-only` parameter to `true` removes the source relationship information without deleting the Snapshot copies.

4. Switch to the advanced privilege level:

```
set -privilege advanced
```

5. Rehost the volume on the destination SVM:

```
volume rehost -vserver source_svm -volume vol_name -destination-vserver destination_svm
```

6. If the SVM peering relation is not present, create the SVM peer relationship between the source SVM and destination SVM:

```
vserver peer create
```

7. Create the SnapMirror relationship between the source volume and destination volume:

```
snapmirror create
```

You must run the `snapmirror create` command from the SVM that is hosting the DP volume. The rehosted volume can be the source or destination of the SnapMirror relationship.

8. Resynchronize the SnapMirror relationship.



## Features that do not support volume rehost

There are certain features that do not support volume rehost.

The following features do not support volume rehost:

- VDR setup
- MetroCluster configurations
- SnapLock volumes
- NetApp Volume Encryption (NVE) volumes

Volume encryption keys depend on SVM keys. If a volume is moved to another SVM and if multitenant key configuration is enabled on either the source or destination SVM, the volume and the SVM keys will not match.

- FlexGroup volumes
- Clone volumes

## Storage limits

There are limits for storage objects that you should consider when planning and managing your storage architecture.

Limits are often platform dependent. Refer to the [Hardware Universe](#) to learn the limits for your specific configuration.

Limits are listed in the following sections:

- [Volume limits](#)
- [FlexClone file and FlexClone LUN limits](#)

Storage limits for Cloud Volumes ONTAP are documented in the [Cloud Volumes ONTAP Release Notes](#).

### Volume limits

Storage object	Limit	Native storage	Storage arrays
<b>Array LUNs</b>	Minimum size for root volume <sup>1</sup>	N/A	Model-dependent
<b>Files</b>	Maximum size	16 TB	16 TB
	Maximum per volume <sup>3</sup>	Volume size dependent, up to 2 billion	Volume size dependent, up to 2 billion
<b>FlexClone volumes</b>	Hierarchical clone depth <sup>4</sup>	499	499

Storage object	Limit	Native storage	Storage arrays
<b>FlexVol volumes</b>	Maximum per node <sup>1</sup>	Model-dependent	Model-dependent
	Maximum per node per SVM <sup>5</sup>	Model-dependent	Model-dependent
	Minimum size	20 MB	20 MB
	Maximum size <sup>1</sup>	Model-dependent	Model-dependent
<b>FlexVol volumes for primary workloads</b>	Maximum per node <sup>2</sup>	Model-dependent	Model-dependent
<b>FlexVol root volumes</b>	Minimum size <sup>1</sup>	Model-dependent	Model-dependent
<b>LUNs</b>	Maximum per node <sup>5</sup>	Model-dependent	Model-dependent
	Maximum per cluster <sup>5</sup>	Model-dependent	Model-dependent
	Maximum per volume <sup>5</sup>	Model-dependent	Model-dependent
	Maximum size	16 TB	16 TB
<b>Qtrees</b>	Maximum per FlexVol volume	4,995	4,995
<b>Snapshot copies</b>	Maximum per volume <sup>6</sup>	255/1023	255/1023
<b>Volumes</b>	Maximum per cluster for NAS	12,000	12,000
	Maximum per cluster with SAN protocols configured	Model-dependent	Model-dependent

**Notes:**

1. In ONTAP 9.3 and earlier, a volume can contain up to 255 Snapshot copies. In ONTAP 9.4 and later, a volume can contain up to 1023 Snapshot copies.
2. Beginning with ONTAP 9.7, the maximum supported number of FlexVol volumes on AFF platforms with at least 128 GB of memory has increased to 2,500 FlexVol volumes per node; however, only 1,000 volumes per node can be active (primary workloads) at one time.

For platform-specific information and for the latest support details, see [Hardware Universe](#).

3. 2 billion =  $2 \times 10^9$ .

4. The maximum depth of a nested hierarchy of FlexClone volumes that can be created from a single FlexVol volume.

5. This limit applies only in SAN environments.

### [SAN Configuration](#)

6. You can use a SnapMirror cascade deployment to increase this limit.

## FlexClone file and FlexClone LUN limits

Limit	Native storage	Storage arrays
Maximum per file or LUN <sup>1</sup>	32,767	32,767
Maximum total shared data per FlexVol volume	640 TB	640 TB

### Note:

1. If you try to create more than 32,767 clones, ONTAP automatically creates a new physical copy of the parent file or LUN.

This limit might be lower for FlexVol volumes that use deduplication.

### Related information

[Find the Release Notes for your version of Cloud Volumes ONTAP](#)

## Recommended volume and file or LUN configuration combinations

### Recommended volume and file or LUN configuration combinations overview

There are specific combinations of FlexVol volume and file or LUN configurations you can use, depending on your application and administration requirements. Understanding the benefits and costs of these combinations can help you determine the right volume and LUN configuration combination for your environment.

The following volume and LUN configuration combinations are recommended:

- Space-reserved files or LUNs with thick volume provisioning
- Non-space-reserved files or LUNs with thin volume provisioning
- Space-reserved files or LUNs with semi-thick volume provisioning

You can use SCSI thin provisioning on your LUNs in conjunction with any of these configuration combinations.

### Space-reserved files or LUNs with thick volume provisioning

#### Benefits:

- All write operations within space-reserved files are guaranteed; they will not fail due to insufficient space.
- There are no restrictions on storage efficiency and data protection technologies on the volume.

#### Costs and limitations:

- Enough space must be set aside from the aggregate up front to support the thickly provisioned volume.
- Space equal to twice the size of the LUN is allocated from the volume at LUN creation time.

#### **Non-space-reserved files or LUNs with thin volume provisioning**

##### **Benefits:**

- There are no restrictions on storage efficiency and data protection technologies on the volume.
- Space is allocated only as it is used.

##### **Costs and restrictions:**

- Write operations are not guaranteed; they can fail if the volume runs out of free space.
- You must manage the free space in the aggregate effectively to prevent the aggregate from running out of free space.

#### **Space-reserved files or LUNs with semi-thick volume provisioning**

##### **Benefits:**

Less space is reserved up front than for thick volume provisioning, and a best-effort write guarantee is still provided.

##### **Costs and restrictions:**

- Write operations can fail with this option.

You can mitigate this risk by properly balancing free space in the volume against data volatility.

- You cannot rely on retention of data protection objects such as Snapshot copies and FlexClone files and LUNs.
- You cannot use ONTAP block-sharing storage efficiency capabilities that cannot be automatically deleted, including deduplication, compression, and ODX/Copy Offload.

#### **Determine the correct volume and LUN configuration combination for your environment**

Answering a few basic questions about your environment can help you determine the best FlexVol volume and LUN configuration for your environment.

##### **About this task**

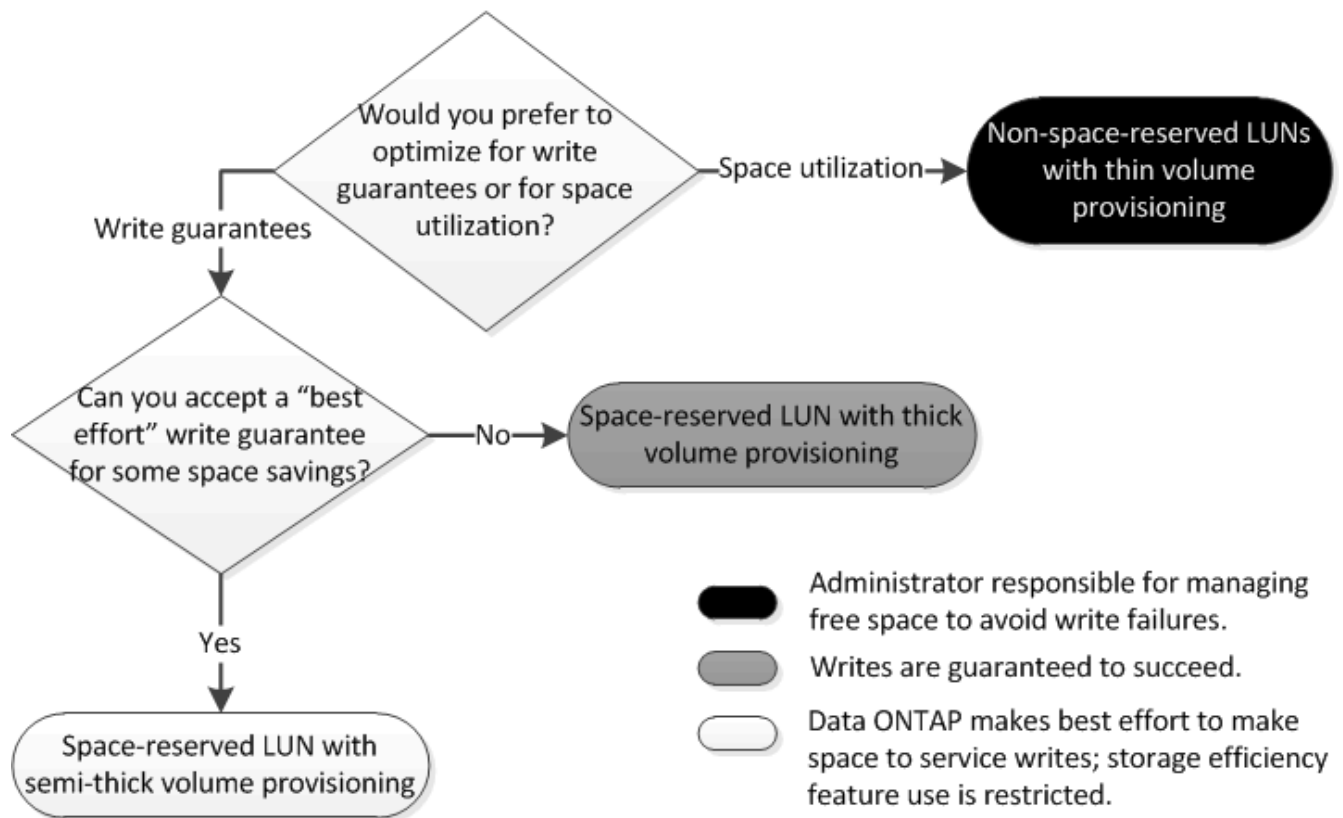
You can optimize your LUN and volume configurations for maximum storage utilization or for the security of write guarantees. Based on your requirements for storage utilization and your ability to monitor and replenish free space quickly, you must determine the FlexVol volume and LUN volumes appropriate for your installation.



You do not need a separate volume for each LUN.

##### **Step**

1. Use the following decision tree to determine the best volume and LUN configuration combination for your environment:



### Configuration settings for space-reserved files or LUNs with thick-provisioned volumes

This FlexVol volume and file or LUN configuration combination provides the ability to use storage efficiency technologies and does not require you to actively monitor your free space, because sufficient space is allocated up front.

The following settings are required to configure a space-reserved file or LUN in a volume using thick provisioning:

Volume setting	Value
Guarantee	Volume
Fractional reserve	100
Snapshot reserve	Any
Snapshot autodelete	Optional
Autogrow	Optional; if enabled, aggregate free space must be actively monitored.

File or LUN setting	Value
Space reservation	Enabled

### Configuration settings for non-space-reserved files or LUNs with thin-provisioned volumes

This FlexVol volume and file or LUN configuration combination requires the smallest amount of storage to be allocated up front, but requires active free space management to prevent errors due to lack of space.

The following settings are required to configure a non-space-reserved files or LUN in a thin-provisioned volume:

Volume setting	Value
Guarantee	None
Fractional reserve	0
Snapshot reserve	Any
Snapshot autodelete	Optional
Autogrow	Optional

File or LUN setting	Value
Space reservation	Disabled

#### Additional considerations

When the volume or aggregate runs out of space, write operations to the file or LUN can fail.

If you do not want to actively monitor free space for both the volume and the aggregate, you should enable Autogrow for the volume and set the maximum size for the volume to the size of the aggregate. In this configuration, you must monitor aggregate free space actively, but you do not need to monitor the free space in the volume.

### Configuration settings for space-reserved files or LUNs with semi-thick volume provisioning

This FlexVol volume and file or LUN configuration combination requires less storage to be allocated up front than the fully provisioned combination, but places restrictions on the efficiency technologies you can use for the volume. Overwrites are fulfilled on a best-effort basis for this configuration combination.

The following settings are required to configure a space-reserved LUN in a volume using semi-thick provisioning:

Volume setting	Value
Guarantee	Volume
Fractional reserve	0

Volume setting	Value
Snapshot reserve	0
Snapshot autodelete	On, with a commitment level of destroy, a destroy list that includes all objects, the trigger set to volume, and all FlexClone LUNs and FlexClone files enabled for automatic deletion.
Autogrow	Optional; if enabled, aggregate free space must be actively monitored.

File or LUN setting	Value
Space reservation	Enabled

### Technology restrictions

You cannot use the following volume storage efficiency technologies for this configuration combination:

- Compression
- Deduplication
- ODX and FlexClone Copy Offload
- FlexClone LUNs and FlexClone files not marked for automatic deletion (active clones)
- FlexClone subfiles
- ODX/Copy Offload

### Additional considerations

The following facts must be considered when employing this configuration combination:

- When the volume that supports that LUN runs low on space, protection data (FlexClone LUNs and files, Snapshot copies) is destroyed.
- Write operations can time out and fail when the volume runs out of free space.

Compression is enabled by default for AFF platforms. You must explicitly disable compression for any volume for which you want to use semi-thick provisioning on an AFF platform.

## Cautions and considerations for changing file or directory capacity

### Considerations for changing the maximum number of files allowed on a FlexVol volume

FlexVol volumes have a maximum number of files that they can contain. You can change the maximum number of files for a volume, but before doing so you should understand how this change affects the volume.

If your data requires a large number of files or very large directories, you can expand ONTAP file or directory capacity. However, you should understand the limitations and caveats for doing so before proceeding.

The number of files a volume can contain is determined by how many inodes it has. An *inode* is a data structure that contains information about files. Volumes have both private and public inodes. Public inodes are used for files that are visible to the user; private inodes are used for files that are used internally by ONTAP. You can change only the maximum number of public inodes for a volume. You cannot affect the number of private inodes.

ONTAP automatically sets the maximum number of public inodes for a newly created volume based on the size of the volume: 1 inode per 32 KB of volume size. When the size of a volume is increased, either directly by an administrator or automatically by ONTAP through the autosize feature, ONTAP also increases (if necessary) the maximum number of public inodes so there is at least 1 inode per 32 KB of volume size, until the volume reaches approximately 680 GB in size. Growing the volume greater than 680 GB in size does not automatically result in more inodes, because ONTAP does not automatically create more than 22,369,621 inodes. If you need more files than the default number for any size volume, you can use the volume modify command to increase the maximum number of inodes for the volume.

You can also decrease the maximum number of public inodes. This does not change the amount of space currently allocated to inodes, but it does lower the maximum amount of space the public inode file can consume. However, after space has been allocated for inodes, it is never returned to the volume. Therefore, lowering the maximum number of inodes below the number of inodes currently allocated does not return the space used by the allocated but unused inodes to the volume.

### **Cautions for increasing the maximum directory size for FlexVol volumes**

You can increase the default maximum directory size for a specific FlexVol volume by using the `-maxdir-size` option of the `volume modify` command, but doing so could impact system performance. See the Knowledge Base article [What is maxdirsize?](#)

To learn more about the model-dependent maximum directory sizes for FlexVol volumes, visit the [NetApp Hardware Universe](#).

### **Rules governing node root volumes and root aggregates**

A node's root volume contains special directories and files for that node. The root aggregate contains the root volume. A few rules govern a node's root volume and root aggregate.

A node's root volume is a FlexVol volume that is installed at the factory or by setup software. It is reserved for system files, log files, and core files. The directory name is `/mroot`, which is accessible only through the systemshell by technical support. The minimum size for a node's root volume depends on the platform model.

- The following rules govern the node's root volume:
  - Unless technical support instructs you to do so, do not modify the configuration or content of the root volume.
  - Do not store user data in the root volume.

Storing user data in the root volume increases the storage giveback time between nodes in an HA pair.

- You can move the root volume to another aggregate.

#### [Relocating root volumes to new aggregates](#)

- The root aggregate is dedicated to the node's root volume only.



ONTAP prevents you from creating other volumes in the root aggregate.

## NetApp Hardware Universe

### Relocate root volumes to new aggregates

The root replacement procedure migrates the current root aggregate to another set of disks without disruption.

#### About this task

You can change the location of the root volume to a new aggregate in the following scenarios:

- When the root aggregates are not on the disk you prefer
- When you want to rearrange the disks connected to the node
- When you are performing a shelf replacement of the EOS disk shelves

#### Steps

1. Relocate the root aggregate:

```
system node migrate-root -node node_name -disklist disk_list -raid-type  
raid_type
```

- **-node**

Specifies the node that owns the root aggregate that you want to migrate.

- **-disklist**

Specifies the list of disks on which the new root aggregate will be created. All disks must be spares and owned by the same node. The minimum number of disks required is dependent on the RAID type.

- **-raid-type**

Specifies the RAID type of the root aggregate. The default value is `raid-dp`. This is the only type supported in advanced mode.

2. Monitor the progress of the job:

```
job show -id jobid -instance
```

#### Results

If all of the pre-checks are successful, the command starts a root volume replacement job and exits.

### Features supported with FlexClone files and FlexClone LUNs

#### Features supported with FlexClone files and FlexClone LUNs

FlexClone files and FlexClone LUNs work with different ONTAP features, such as deduplication, Snapshot copies, quotas, and volume SnapMirror.

The following features are supported with FlexClone files and FlexClone LUNs:

- Deduplication
- Snapshot copies
- Access control lists
- Quotas
- FlexClone volumes
- NDMP
- Volume SnapMirror
- The `volume move` command
- Space reservation
- HA configuration

### How deduplication works with FlexClone files and FlexClone LUNs

You can efficiently use the physical storage space of the data blocks by creating a FlexClone file or FlexClone LUN of the parent file and parent LUN in a deduplication-enabled volume.

The block-sharing mechanism used by FlexClone files and LUNs is also used by deduplication. You can maximize the space savings in a FlexVol volume by enabling deduplication on the volume and then cloning the deduplication-enabled volume.



While executing the `sis undo` command on a deduplication-enabled volume, you cannot create FlexClone files and FlexClone LUNs of the parent files and parent LUNs residing in that volume.

### How Snapshot copies work with FlexClone files and FlexClone LUNs

You can create FlexClone files and FlexClone LUNs from an existing Snapshot copy of the parent files and parent LUNs contained in a FlexVol volume.

However, you cannot manually delete a Snapshot copy from which FlexClone files or FlexClone LUNs are being created until the block-sharing process between the parent and clone entities is complete. The Snapshot copy remains locked until the completion of the block-sharing process, which occurs in the background. Therefore, when you try to delete a locked Snapshot copy, the system displays a message asking you to retry the operation after some time. In such a situation, if you want to manually delete the particular Snapshot copy, you must keep retrying the deletion operation so that the Snapshot copy is deleted after the block sharing is complete.

### How access control lists work with FlexClone files and FlexClone LUNs

FlexClone files and FlexClone LUNs inherit the access control lists of their parent files and LUNs.

If the parent files contain Windows NT streams, the FlexClone files also inherit the stream information. However, parent files containing more than six streams cannot be cloned.

## How quotas work with FlexClone files and FlexClone LUNs

Quota limits are applied on the total logical size of the FlexClone files or FlexClone LUNs. Cloning operations do not fail block sharing even if it causes quotas to exceed.

When you create a FlexClone file or FlexClone LUN, quotas do not recognize any space savings. For example, if you create a FlexClone file of a parent file of 10 GB, you are only using 10 GB of physical space, but the quota utilization is recorded as 20 GB (10 GB for the parent and 10 GB for the FlexClone file).

If the creation of a FlexClone file or LUN results in the group or user quota's being exceeded, the clone operation succeeds provided the FlexVol volume has enough space to hold the metadata for the clone. However, the quota for that user or group is oversubscribed.

## How FlexClone volumes work with FlexClone files and FlexClone LUNs

You can create a FlexClone volume of a FlexVol volume that has both a FlexClone file and FlexClone LUN and its parent file or LUN in it.

FlexClone files or FlexClone LUNs and their parent files or LUNs that are present in the FlexClone volume continue to share blocks the same way they do in the parent FlexVol volume. In fact, all the FlexClone entities and their parents share the same underlying physical data blocks, minimizing physical disk space usage.

If the FlexClone volume is split from its parent volume, then the FlexClone files or FlexClone LUNs and their parent files or LUNs stop sharing the blocks in the clone of the FlexClone volume. Thereafter they exist as independent files or LUNs. This means that the clone of the volume uses more space than before the splitting operation.

## How NDMP works with FlexClone files and FlexClone LUNs

NDMP works at the logical level with FlexClone files and FlexClone LUNs. All FlexClone files or LUNs are backed up as separate files or LUNs.

When you use NDMP services to back up a qtree or a FlexVol volume that contains FlexClone files or FlexClone LUNs, block sharing between parent and clone entities is not preserved, and clone entities are backed up to tape as separate files or LUNs. The space saving is lost. Therefore, the tape onto which you are backing up should have sufficient space to store the expanded amount of data. When you restore, all the FlexClone files and FlexClone LUNs are restored as separate physical files and LUNs. You can enable deduplication on the volume to restore the block-sharing benefits.



When FlexClone files and FlexClone LUNs are being created from an existing Snapshot copy of a FlexVol volume, you cannot back up the volume to tape until the block-sharing process, which happens in the background, is complete. If you use NDMP on the volume when the block-sharing process is in progress, the system displays a message asking you to retry the operation after some time. In such a situation, you must keep retrying the tape backup operation so that it succeeds after the block sharing is complete.

## How volume SnapMirror works with FlexClone files and FlexClone LUNs

Volume SnapMirror used with FlexClone files and FlexClone LUNs helps in maintaining space savings because the cloned entities are replicated only once.

If a FlexVol volume is a volume SnapMirror source and contains FlexClone files or FlexClone LUNs, volume SnapMirror transfers only the shared physical block and a small amount of metadata to the volume SnapMirror

destination. The destination stores only one copy of the physical block, and this block is shared between the parent and cloned entities. Therefore, the destination volume is an exact copy of the source volume and all the clone files or LUNs on the destination volume share the same physical block.

### **How volume move affects FlexClone files and FlexClone LUNs**

During the cutover phase of a volume move operation, you cannot create FlexClone files or FlexClone LUNs of a FlexVol volume.

### **How space reservation works with FlexClone files and FlexClone LUNs**

FlexClone files and FlexClone LUNs inherit the space reservation attribute from the parent file and parent LUN by default. However, you can create FlexClone files and FlexClone LUNs with space reservation disabled from a parent file and parent LUN with space reservation enabled if the FlexVol volume lacks space.

If the FlexVol volume does not contain enough space to create a FlexClone file or FlexClone LUN with the same space reservation as that of the parent, then the cloning operation fails.

### **How an HA configuration works with FlexClone files and FlexClone LUNs**

FlexClone file and FlexClone LUN operations are supported in an HA configuration.

In an HA pair, you cannot create FlexClone files or FlexClone LUNs on the partner while the takeover or giveback operation is in progress. All the pending block sharing operations on the partner are resumed after the takeover or giveback operation is complete.

## **Provision NAS storage for large file systems using FlexGroup volumes**

A FlexGroup volume is a scalable NAS container that provides high performance along with automatic load distribution. FlexGroup volumes provide massive capacity (in petabytes), which considerably exceeds the FlexVol volume limits, without adding any management overhead.

The topics in this section show you how to manage FlexGroup volumes with System Manager in ONTAP 9.7 and later releases. If you are using the classic System Manager (available only in ONTAP 9.7 and earlier), see this topic:

- [Create FlexGroup volumes](#)

Beginning with ONTAP 9.9.1, SnapMirror fanout relationships of two or more FlexGroup volumes are supported, with a maximum of eight fanout legs. System Manager does not support SnapMirror cascading FlexGroup volume relationships.

ONTAP automatically selects the local tiers required for creating the FlexGroup volume.

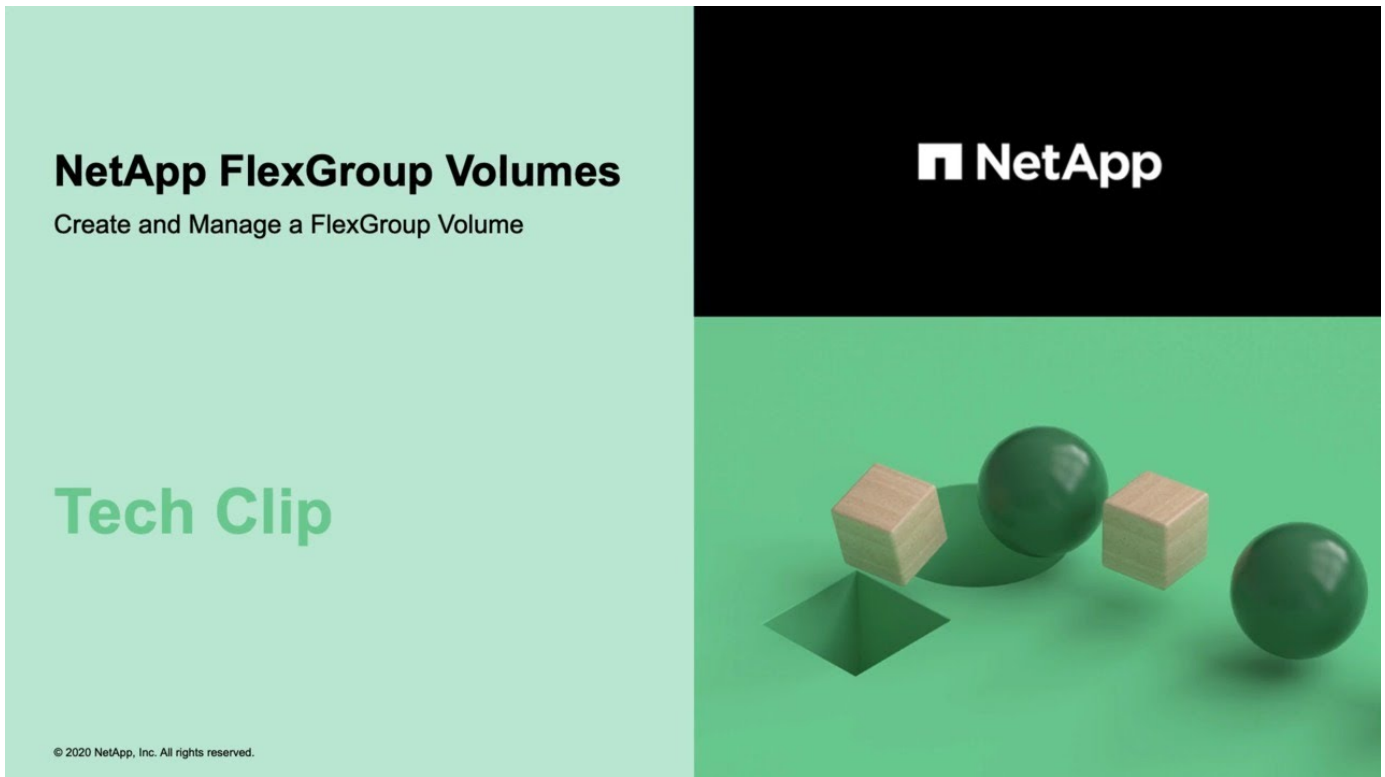
Beginning with ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

### **Steps**

1. Click **Storage > Volumes**.
2. Click **Add**.
3. Click **More Options** and then select **Distribute volume data across the cluster**.
  - a. If you are running ONTAP 9.8 or later and you want to disable QoS or choose a custom QoS policy, click **More Options** and then, under **Storage and Optimization** select **Performance Service Level**.

## Videos

### Create and manage a FlexGroup volume



### FlexGroup volumes - Do more with less

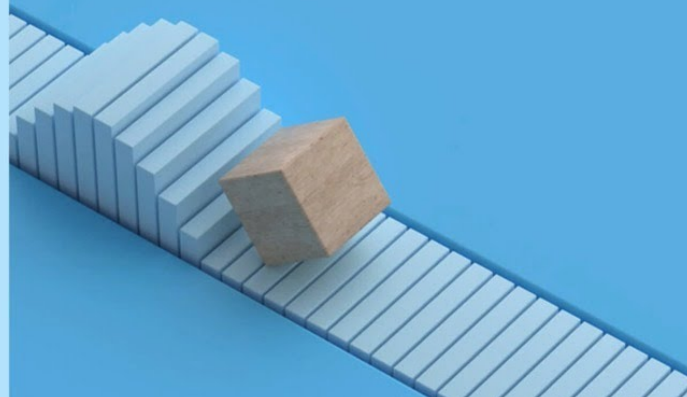
# NetApp FlexGroup Volumes

Do More with Less



## Use Case

© 2020 NetApp, Inc. All rights reserved.



## FlexGroup volumes management with the CLI

### FlexGroup volumes management overview with the CLI

You can set up, manage, and protect FlexGroup volumes for scalability and performance. A FlexGroup volume is a scale-out volume that provides high performance along with automatic load distribution.

You can configure FlexGroup volumes if the following are true:

- You are running ONTAP 9.1 or later.
- You want to use NFSv4.x, NFSv3, SMB 2.0, or SMB 2.1.
- You want to use the ONTAP command-line interface (CLI), not System Manager or an automated scripting tool.

Details about command syntax are available from the CLI help and the ONTAP man pages.

An important subset of FlexGroup functionality is available in System Manager.

- You want to use best practices, not explore every available option.
- You have cluster administrator privileges, not SVM administrator privileges.



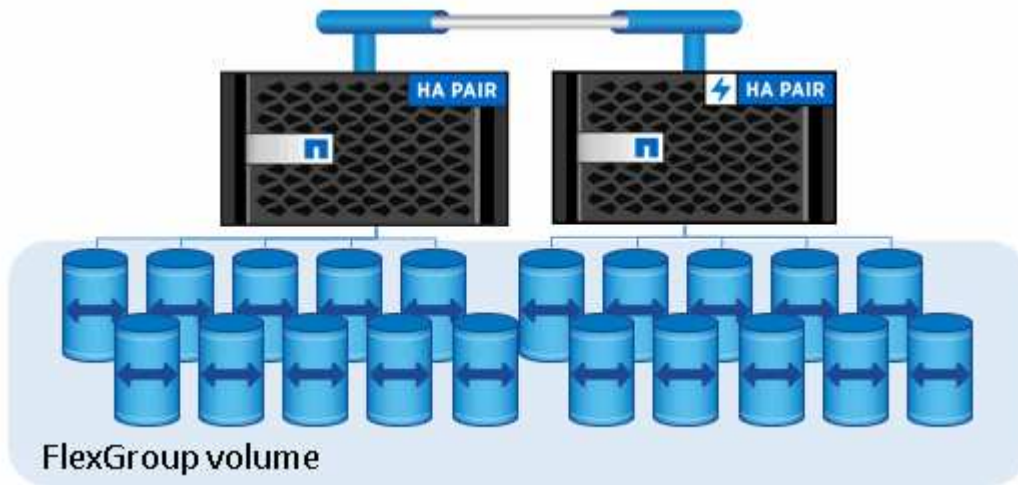
FlexGroups replace Infinite Volumes, which are not supported in newer versions of ONTAP.

### Related information

Conceptual information about FlexVol volumes is applicable to FlexGroup volumes. Information about FlexVol volumes and ONTAP technology is available in the ONTAP Reference Library and in Technical Reports (TRs).

## What a FlexGroup volume is

A FlexGroup volume is a scale-out NAS container that provides high performance along with automatic load distribution and scalability. A FlexGroup volume contains several constituents that automatically and transparently share the traffic.



FlexGroup volumes provide the following benefits:

- High scalability

The maximum size for a FlexGroup volume in ONTAP 9.1 and later is 20 PB, with 400 billion files on a 10-node cluster.

- High performance

FlexGroup volumes can utilize the resources of the cluster to serve workloads that have high throughput and low latency.

- Simplified management

A FlexGroup volume is a single namespace container that can be managed in a similar way as FlexVol volumes.

## Supported and unsupported configurations for FlexGroup volumes

You should be aware of the ONTAP features that are supported and not supported with FlexGroup volumes in ONTAP 9.

### Features supported beginning with ONTAP 9.11.1

- SnapLock volumes

SnapLock does not support the following features with FlexGroup volumes:

- Legal-hold
- Event-based retention
- SnapLock for SnapVault

You configure SnapLock at the FlexGroup level. You cannot configure SnapLock at the constituent level.

### What SnapLock is

- Client asynchronous directory delete

[Manage client rights to delete directories rapidly](#)

### Features supported beginning with ONTAP 9.10.1

- Convert FlexVol volumes to FlexGroup volumes in an SVM-DR source

[Convert a FlexVol volume to a FlexGroup volume within an SVM-DR relationship](#)

- SVM-DR FlexClone support for FlexGroup volumes

[Learn more about creating FlexClone volumes.](#)

### Features supported beginning with ONTAP 9.9.1

- SVM disaster recovery

Cloning a FlexGroup volume that is part of an SVM-DR relationship is not supported.

- SnapMirror fanout relationships of 2 or more (A to B, A to C), with a maximum of 8 fanout legs.

[Considerations for creating SnapMirror cascade and fanout relationships for FlexGroups](#)

- SnapMirror cascading relationships up to two levels (A to B to C)

[Considerations for creating SnapMirror cascade and fanout relationships for FlexGroups](#)

### Features supported beginning with ONTAP 9.8

- Restoring a single file from a FlexGroup SnapMirror vault or from a UDP destination
  - Restore can be from a FlexGroup volume of any geometry to FlexGroup volume of any geometry
  - Only one file per restore operation is supported
- Converting volumes transitioned from 7-mode systems to FlexGroup volumes

For more information, see Knowledge Base article [How To Convert a Transitioned FlexVol to FlexGroup](#).

- NFSv4.2
- Asynchronous delete of files and directories
- Files System Analytics (FSA)
- FlexGroup as a VMware vSphere datastore
- Additional support for tape backup and restore using NDMP, including the following features:
  - NDMP restartable backup extension (RBE) and Snapshot Management Extension (SSME)
  - Environment variables EXCLUDE and MULTI\_SUBTREE\_NAMES support FlexGroup backups
  - Introduction of IGNORE\_CTIME\_MTIME environment variable for FlexGroup backups



- Individual file recovery in a FlexGroup using the NDMP\_SNAP\_RECOVER message, which is part of extension 0x2050  
Dump and restore sessions are aborted during an upgrade or revert.

### Features supported beginning with ONTAP 9.7

- FlexClone volume
- NFSv4 and NFSv4.1
- pNFS
- Tape backup and restore by using NDMP

You must be aware of the following points for NDMP support on FlexGroup volumes:

- The NDMP\_SNAP\_RECOVER message in the extension class 0x2050 can be used only for recovering an entire FlexGroup volume.

Individual files in a FlexGroup volume cannot be recovered.

- NDMP restartable backup extension (RBE) is not supported for FlexGroup volumes.
- Environment variables EXCLUDE and MULTI\_SUBTREE\_NAMES are not supported for FlexGroup volumes.
- The `ndmpcopy` command is supported for data transfer between FlexVol and FlexGroup volumes.

If you revert from Data ONTAP 9.7 to an earlier version, the incremental transfer information of the previous transfers is not retained and therefore, you must perform a baseline copy after reverting.

- VMware vStorage APIs for Array Integration (VAAI)
- Conversion of a FlexVol volume to a FlexGroup volume
- FlexGroup volumes as FlexCache origin volumes

### Features supported beginning with ONTAP 9.6

- Continuously available SMB shares
- MetroCluster configurations
- Renaming a FlexGroup volume (`volume rename` command)
- Shrinking or reducing the size of a FlexGroup volume (`volume size` command)
- Elastic sizing
- NetApp aggregate encryption (NAE)
- Cloud Volumes ONTAP

### Features supported beginning with ONTAP 9.5

- ODX copy offload
- Storage-Level Access Guard
- Enhancements to change notifications for SMB shares

Change notifications are sent for changes to the parent directory on which the `changenotify` property is

set and for changes to all of the subdirectories in that parent directory.

- FabricPool
- Quota enforcement
- Qtree statistics
- Adaptive QoS for files in FlexGroup volumes
- FlexCache (cache only; FlexGroup as origin supported in ONTAP 9.7)

#### **Features supported beginning with ONTAP 9.4**

- FPolicy
- File auditing
- Throughput floor (QoS Min) and adaptive QoS for FlexGroup volumes
- Throughput ceiling (QoS Max) and throughput floor (QoS Min) for files in FlexGroup volumes

You use the `volume file modify` command to manage the QoS policy group that is associated with a file.

- Relaxed SnapMirror limits
- SMB 3.x multichannel

#### **Features supported beginning with ONTAP 9.3**

- Antivirus configuration
- Change notifications for SMB shares

Notifications are sent only for changes to the parent directory on which the `changenotify` property is set. Change notifications are not sent for changes to subdirectories in the parent directory.

- Qtrees
- Throughput ceiling (QoS Max)
- Expand the source FlexGroup volume and destination FlexGroup volume in a SnapMirror relationship
- SnapVault backup and restore
- Unified data protection relationships
- Autogrow option and autoshrink option
- Inode count factored to ingest

#### **Feature supported beginning with ONTAP 9.2**

- Volume encryption
- Aggregate inline deduplication (cross-volume deduplication)
- NetApp volume encryption (NVE)

#### **Features supported beginning with ONTAP 9.1**

FlexGroup volumes were introduced in ONTAP 9.1, with support for several ONTAP features.

- SnapMirror technology
- Snapshot copies
- Active IQ
- Inline adaptive compression
- Inline deduplication
- Inline data compaction
- AFF
- Quota reporting
- NetApp Snapshot technology
- SnapRestore software (FlexGroup level)
- Hybrid aggregates
- Constituent or member volume move
- Postprocess deduplication
- NetApp RAID-TEC technology
- Per-aggregate consistency point
- Sharing FlexGroup with FlexVol volume in the same SVM

### Unsupported configurations in ONTAP 9

Unsupported protocols	Unsupported data protection features	Other unsupported ONTAP features
<ul style="list-style-type: none"> <li>• pNFS (ONTAP 9.0 to 9.6)</li> <li>• SMB 1.0</li> <li>• SMB transparent failover (ONTAP 9.0 to 9.5)</li> <li>• SAN</li> </ul>	<ul style="list-style-type: none"> <li>• SnapLock volumes (ONTAP 9.10.1 and earlier)</li> <li>• SMTape</li> </ul>	Remote Volume Shadow Copy Service (VSS)

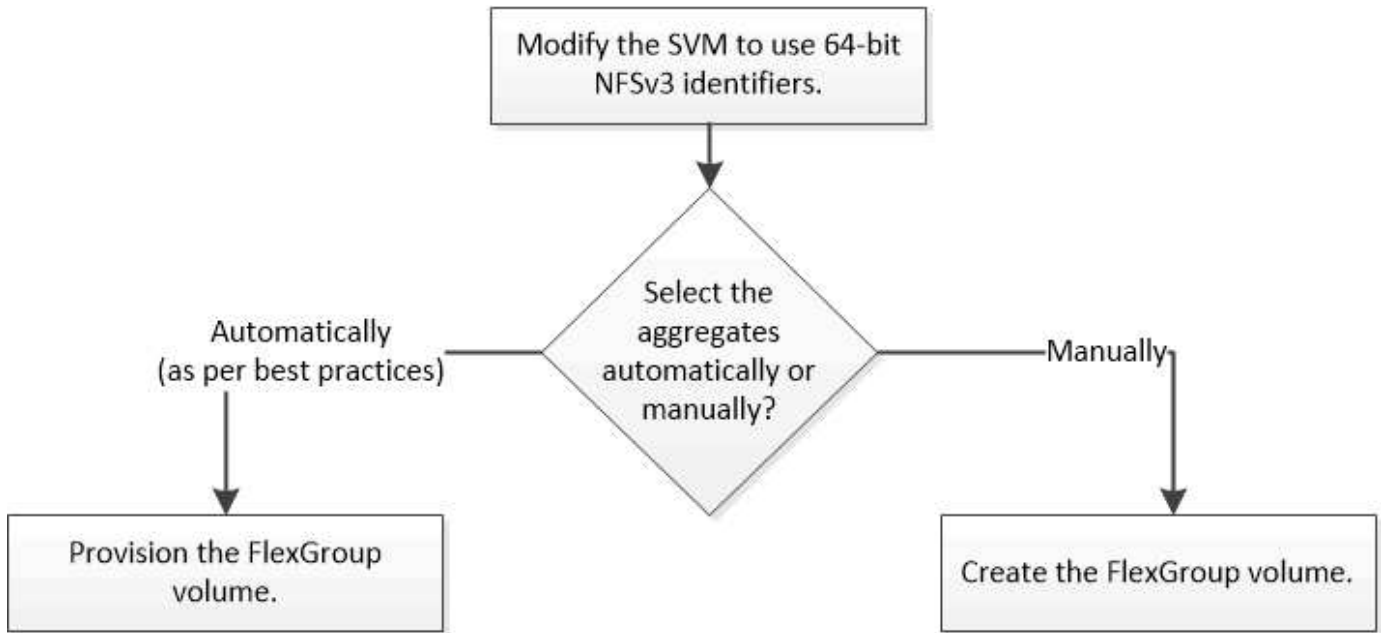
#### Related information

[ONTAP 9 Documentation Center](#)

## FlexGroup volume setup

### FlexGroup volume setup workflow

You can either provision a FlexGroup volume where ONTAP automatically selects the aggregates based on the best practices for optimum performance, or create a FlexGroup volume by manually selecting the aggregates and configuring it for data access.



### What you'll need

You must have created the SVM with NFS and SMB added to the list of allowed protocols for the SVM.

### About this task

You can automatically provision a FlexGroup volume only on clusters with four nodes or less. On clusters with more than four nodes, you must create a FlexGroup volume manually.

### Enable 64-bit NFSv3 identifiers on an SVM

To support the high file count of FlexGroup volumes and to avoid file ID collisions, you should enable 64-bit file identifiers on the SVM on which the FlexGroup volume must be created.

### Steps

1. Log in to the advanced privilege level: `set -privilege advanced`
2. Modify the SVM to use 64-bit NFSv3 FSIDs and file IDs: `vserver nfs modify -vserver svm_name -v3-64bit-identifiers enabled`

```

cluster1::*> vserver nfs modify -vserver vs0 -v3-64bit-identifiers
enabled

Warning: You are attempting to increase the number of bits used for
NFSv3
        FSIDs and File IDs from 32 to 64 on Vserver "vs0". This could
        result in older client software no longer working with the
volumes
        owned by Vserver "vs0".
Do you want to continue? {y|n}: y

Warning: Based on the changes you are making to the NFS server on
Vserver
        "vs0", it is highly recommended that you remount all NFSv3
clients
        connected to it after the command completes.
Do you want to continue? {y|n}: y

```

### After you finish

All of the clients must be remounted. This is required because the file system IDs change, and the clients might receive stale file handle messages when attempting NFS operations.

### Provision a FlexGroup volume automatically

You can automatically provision a FlexGroup volume. ONTAP creates and configures a FlexGroup volume by automatically selecting the aggregates. Aggregates are selected based on the best practices for optimum performance.

### What you'll need

Each node in the cluster must have at least one aggregate.



For creating a FlexGroup volume for FabricPool in ONTAP 9.5, each node must have at least one aggregate that is FabricPool.


### About this task

ONTAP selects two aggregates with the largest amount of usable space on each node to create the FlexGroup volume. If two aggregates are not available, ONTAP selects one aggregate per node to create the FlexGroup volume.

### Steps

1. Provision the FlexGroup volume:

If you are using...	Use this command...
---------------------	---------------------

<p>ONTAP 9.2 or later</p>	<pre>volume create -vserver svm_name -volume fg_vol_name -auto-provision-as flexgroup -size fg_size [-encrypt true] [-qos-policy-group qos_policy_group_name] [-support- tiering true]</pre> <p>Beginning with ONTAP 9.5, you can create FlexGroup volumes for FabricPool. To automatically provision a FlexGroup volume on FabricPool, you must set the <code>-support-tiering</code> parameter to <code>true</code>. The volume guarantee must be always set to <code>none</code> for FabricPool. You can also specify the tiering policy and tiering minimum cooling period for the FlexGroup volume.</p> <p><a href="#">Disk and aggregate management</a></p> <p>Beginning with ONTAP 9.3, you can specify a throughput ceiling (QoS Max) for FlexGroup volumes, which limits the performance resources that the FlexGroup volume can consume. Beginning with ONTAP 9.4, you can specify throughput floors (QoS Min) and adaptive QoS for FlexGroup volumes.</p> <p><a href="#">Performance management</a></p> <p>Beginning with ONTAP 9.2, you can set the <code>-encrypt</code> parameter to <code>true</code> if you want to enable encryption on the FlexGroup volume. For creating an encrypted volume, you must have installed the volume encryption license and the key manager.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;">  <p>You must enable encryption on FlexGroup volumes at the time of creation. You cannot enable encryption on existing FlexGroup volumes.</p> </div> <p><a href="#">Encryption of data at rest</a></p>
<p>ONTAP 9.1</p>	<pre>volume flexgroup deploy -vserver svm_name -size fg_size</pre>

The `size` parameter specifies the size of the FlexGroup volume in KB, MB, GB, TB, or PB.

The following example shows how to provision a FlexGroup volume of size 400 TB in ONTAP 9.2:

```
cluster-1::> volume create -vserver vs0 -volume fg -auto-provision-as
flexgroup -size 400TB
Warning: The FlexGroup "fg" will be created with the following number of
constituents of size 25TB: 16.
The constituents will be created on the following aggregates:
aggr1,aggr2
Do you want to continue? {y|n}: y
[Job 34] Job succeeded: Successful
```

The following example shows how to create a QoS policy group for throughput ceiling and how to apply it to a FlexGroup volume:

```
cluster1::> qos policy-group create -policy group pg-vs1 -vserver vs1
-max-throughput 5000iops
```

```
cluster-1::> volume create -vserver vs0 -volume fg -auto-provision-as
flexgroup -size 400TB -qos-policy-group pg-vs1
Warning: The FlexGroup "fg" will be created with the following number of
constituents of size 25TB: 16.
The constituents will be created on the following aggregates:
aggr1,aggr2
Do you want to continue? {y|n}: y
[Job 34] Job succeeded: Successful
```

The following example shows how to provision a FlexGroup volume of size 400 TB on aggregates in FabricPool in ONTAP 9.5:

```
cluster-1::> volume create -vserver vs0 -volume fg -auto-provision-as
flexgroup -size 400TB -support-tiering true -tiering-policy auto
Warning: The FlexGroup "fg" will be created with the following number of
constituents of size 25TB: 16.
The constituents will be created on the following aggregates:
aggr1,aggr2
Do you want to continue? {y|n}: y
[Job 34] Job succeeded: Successful
```

The FlexGroup volume is created with eight constituents on each node in the cluster. The constituents are distributed equally between the two largest aggregates on each node.

By default, the FlexGroup volume is created with the `volume space guarantee` setting except on AFF systems. For AFF systems, by default the FlexGroup volume is created with the `none` space guarantee.

2. Mount the FlexGroup volume with a junction path: `volume mount -vserver vserver_name`

```
-volume vol_name -junction-path junction_path
```

```
cluster1::> volume mount -vserver vs0 -volume fg2 -junction-path /fg2
```

### After you finish

You should mount the FlexGroup volume from the client.

If you are running ONTAP 9.6 or earlier and if the storage virtual machine (SVM) has both NFSv3 and NFSv4 configured, mounting the FlexGroup volume from the client might fail. In such cases, you must explicitly specify the NFS version when mounting the FlexGroup volume from the client.

```
# mount -t nfs -o vers=3 192.53.19.64:/fg2 /mnt/fg2
# ls /mnt/fg2
file1 file2
```

### Create a FlexGroup volume

You can create a FlexGroup volume by manually selecting the aggregates on which the FlexGroup volume must be created, and then specifying the number of constituents on each aggregate.

#### About this task

You must be aware of the space required in the aggregates for creating a FlexGroup volume.

#### [Guidelines for aggregate space when provisioning a FlexGroup volume](#)

You should also be aware of the considerations and requirements when selecting the aggregates for provisioning a FlexGroup volume.

You must consider the following guidelines when creating a FlexGroup volume for obtaining the best performance results with a FlexGroup volume:

- A FlexGroup volume should span only aggregates that are on identical hardware systems.

The use of identical hardware systems helps in providing predictable performance across the FlexGroup volume.

- A FlexGroup volume should span aggregates with the same disk type and RAID group configurations.

For consistent performance, you must ensure that all of the aggregates are made of all SSDs, all HDDs, or all hybrid aggregates. Additionally, the aggregates should have the same number of drives and RAID groups across the FlexGroup volume.

- A FlexGroup volume can span parts of a cluster.

A FlexGroup volume does not have to be configured to span the entire cluster, but doing so can take greater advantage of the hardware resources that are available.

- When creating a FlexGroup volume, it is best if the aggregates on which the FlexGroup volume is deployed have the following characteristics:



- Approximately the same amount of free space should be available across multiple aggregates, especially when using thin provisioning.
- Approximately 3 percent of the free space should be reserved for aggregate metadata after creation of the FlexGroup volume.
- For FAS systems, it is best to have two aggregates per node and for AFF systems, you must have one aggregate per node for the FlexGroup volume.
- For each FlexGroup volume, you should create at least eight constituents that are distributed over two or more aggregates on FAS systems, and over one or more aggregates on AFF systems.

## Steps

1. Create the FlexGroup volume: `volume create -vserver svm_name -volume flexgroup_name -aggr-list aggr1,aggr2,.. -aggr-list-multiplier constituents_per_aggr -size fg_size [-encrypt true] [-qos-policy-group qos_policy_group_name]`

- The `-aggr-list` parameter specifies the list of aggregates to be used for FlexGroup volume constituents.

Each entry in the list creates a constituent on the specified aggregate. You can specify an aggregate multiple times to have multiple constituents created on the aggregate.

For consistent performance across the FlexGroup volume, all of the aggregates must use the same disk type and RAID group configurations.

- The `-aggr-list-multiplier` parameter specifies the number of times to iterate over the aggregates that are listed with the `-aggr-list` parameter when creating a FlexGroup volume.

The default value of the `-aggr-list-multiplier` parameter is 4.

- The `size` parameter specifies the size of the FlexGroup volume in KB, MB, GB, TB, or PB.
- Beginning with ONTAP 9.5, you can create FlexGroup volumes for FabricPool, which use only all SSD aggregates.

To create a FlexGroup volume for FabricPool, all the aggregates specified with the `-aggr-list` parameter must be FabricPool. The volume guarantee must be always set to `none` for FabricPool. You can also specify the tiering policy and tiering minimum cooling period for the FlexGroup volume.

### Disk and aggregate management

- Beginning with ONTAP 9.4, you can specify throughput floors (QoS Min) and adaptive QoS for FlexGroup volumes.

### Performance management

- Beginning with ONTAP 9.3, you can specify a throughput ceiling (QoS Max) for FlexGroup volumes, which limits the performance resources that the FlexGroup volume can consume.
- Beginning with ONTAP 9.2, you can set the `-encrypt` parameter to `true` if you want to enable encryption on the FlexGroup volume.

For creating an encrypted volume, you must have installed the volume encryption license and the key manager.



You must enable encryption on FlexGroup volumes at the time of creation. You cannot enable encryption on existing FlexGroup volumes.

### Encryption of data at rest

```
cluster-1::> volume create -vserver vs0 -volume fg2 -aggr-list
aggr1,aggr2,aggr3,aggr1 -aggr-list-multiplier 2 -size 500TB

Warning: A FlexGroup "fg2" will be created with the following number of
constituents of size 62.50TB: 8.
Do you want to continue? {y|n}: y

[Job 43] Job succeeded: Successful
```

In the previous example, if you want to create the FlexGroup volume for FabricPool, all aggregates (aggr1, aggr2, and aggr3) must be aggregates in FabricPool.

. Mount the FlexGroup volume with a junction path: `volume mount -vserver vserver_name -volume vol_name -junction-path junction_path`

```
cluster1::> volume mount -vserver vs0 -volume fg2 -junction-path /fg
```

### After you finish

You should mount the FlexGroup volume from the client.

If you are running ONTAP 9.6 or earlier and if the storage virtual machine (SVM) has both NFSv3 and NFSv4 configured, mounting the FlexGroup volume from the client might fail. In such cases, you must explicitly specify the NFS version when you are mounting the FlexGroup volume from the client.

```
# mount -t nfs -o vers=3 192.53.19.64:/fg /mnt/fg2
# ls /mnt/fg2
file1  file2
```

### Related information

[NetApp Technical Report 4571: NetApp FlexGroup Best Practices and Implementation Guide](#)

## Manage FlexGroup volumes

### Monitor the space usage of a FlexGroup volume

You can view a FlexGroup volume and its constituents, and monitor the space used by the FlexGroup volume.

### About this task

Beginning with ONTAP 9.6, elastic sizing is supported. ONTAP automatically grows a constituent of a FlexGroup volume if it is running out of space by shrinking any other constituent in the FlexGroup volume that

has free space by an equivalent amount. Elastic sizing avoids any out-of-space errors that are generated because of one or more FlexGroup constituent volumes running out of space.



Beginning with ONTAP 9.9.1, logical space reporting and enforcement is also available for FlexGroup volumes. For more information, see [Logical space reporting and enforcement for volumes](#).

**Step**

1. View the space used by the FlexGroup volume and its constituents: `volume show -vserver vs1 -volume-style-extended flexgroup`

```
cluster-2::> volume show -vserver vs1 -volume-style-extended flexgroup
Vserver   Volume      Aggregate   State      Type      Size
Available Used%
-----
vs1       fg1         -           online     RW        500GB
207.5GB  56%
```

```

ccluster-2::> volume show -vserver vs1 -volume-style-extended flexgroup-
constituent
Vserver    Volume           Aggregate    State    Type    Size
Available Used%
-----
-----
vs1        fg1__0001       aggr3       online   RW      31.25GB
12.97GB   56%
vs1        fg1__0002       aggr1       online   RW      31.25GB
12.98GB   56%
vs1        fg1__0003       aggr1       online   RW      31.25GB
13.00GB   56%
vs1        fg1__0004       aggr3       online   RW      31.25GB
12.88GB   56%
vs1        fg1__0005       aggr1       online   RW      31.25GB
13.00GB   56%
vs1        fg1__0006       aggr3       online   RW      31.25GB
12.97GB   56%
vs1        fg1__0007       aggr1       online   RW      31.25GB
13.01GB   56%
vs1        fg1__0008       aggr1       online   RW      31.25GB
13.01GB   56%
vs1        fg1__0009       aggr3       online   RW      31.25GB
12.88GB   56%
vs1        fg1__0010       aggr1       online   RW      31.25GB
13.01GB   56%
vs1        fg1__0011       aggr3       online   RW      31.25GB
12.97GB   56%
vs1        fg1__0012       aggr1       online   RW      31.25GB
13.01GB   56%
vs1        fg1__0013       aggr3       online   RW      31.25GB
12.95GB   56%
vs1        fg1__0014       aggr3       online   RW      31.25GB
12.97GB   56%
vs1        fg1__0015       aggr3       online   RW      31.25GB
12.88GB   56%
vs1        fg1__0016       aggr1       online   RW      31.25GB
13.01GB   56%
16 entries were displayed.

```

You can use the available space and percentage space used to monitor the space usage of the FlexGroup volume.

## Increase the size of a FlexGroup volume

You can increase the size of a FlexGroup volume either by adding more capacity to the existing constituents of the FlexGroup volume or by expanding the FlexGroup volume with new constituents.

### What you'll need

Sufficient space must be available in the aggregates.

### About this task

If you want to add more space, you can increase the collective size of the FlexGroup volume. Increasing the size of a FlexGroup volume resizes the existing constituents of the FlexGroup volume.

If you want to improve performance, you can expand the FlexGroup volume. You might want to expand a FlexGroup volume and add new constituents in the following situations:

- New nodes have been added to the cluster.
- New aggregates have been created on the existing nodes.
- The existing constituents of the FlexGroup volume have reached the maximum FlexVol size for the hardware, and therefore the FlexGroup volume cannot be resized.

In releases earlier than ONTAP 9.3, you must not expand FlexGroup volumes after a SnapMirror relationship is established. If you expand the source FlexGroup volume after breaking the SnapMirror relationship in releases earlier than ONTAP 9.3, you must perform a baseline transfer to the destination FlexGroup volume once again. Beginning with ONTAP 9.3, you can expand FlexGroup volumes that are in a SnapMirror relationship.

### Step

1. Increase the size of the FlexGroup volume by increasing the capacity or performance of the FlexGroup volume, as required:

If you want to increase the...	Then do this...
Capacity of the FlexGroup volume	Resize the constituents of the FlexGroup volume:  <pre>volume modify -vserver vs_server_name -volume fg_name -size new_size</pre>
Performance to the FlexGroup volume	Expand the FlexGroup volume by adding new constituents:  <pre>volume expand -vserver vs_server_name -volume fg_name -aggr-list aggregate name,... [-aggr-list-multiplier constituents_per_aggr]</pre> <p>The default value of the <code>-aggr-list-multiplier</code> parameter is 1.</p> <p>To expand a FlexGroup volume for FabricPool in ONTAP 9.5, any new aggregates used must be FabricPool.</p>

Whenever possible, you should increase the capacity of a FlexGroup volume. If you must expand a FlexGroup volume, you should add constituents in the same multiples as the constituents of the existing FlexGroup volume to ensure consistent performance. For example, if the existing FlexGroup volume has 16 constituents with eight constituents per node, you can expand the existing FlexGroup volume by 8 or 16 constituents.

## Examples

### Example of increasing the capacity of the existing constituents

The following example shows how to add 20 TB space to a FlexGroup volume volX:

```
cluster1::> volume modify -vserver svml -volume volX -size +20TB
```

If the FlexGroup volume has 16 constituents, the space of each constituent is increased by 1.25 TB.

### Example of improving performance by adding new constituents

The following example shows how to add two more constituents to the FlexGroup volume volX:

```
cluster1::> volume expand -vserver vs1 -volume volX -aggr-list aggr1,aggr2
```

The size of the new constituents is the same as that of the existing constituents.

## Reduce the size of a FlexGroup volume

Beginning with ONTAP 9.6, you can resize a FlexGroup volume to a value lower than its current size to free up the unused space from the volume. When you reduce the size of a FlexGroup volume, ONTAP automatically resizes all of the FlexGroup constituents.

### Step

1. Reduce the size of the FlexGroup volume: `volume size -vserver vserver_name -volume fg_name -size new_size`

`new_size` is the size of the FlexGroup volume. You can either specify a lower value than the current size or a negative value by which the current size of the FlexGroup volume is reduced.



If automatic shrinking is enabled for the volume (`volume autosize` command), the minimum autosize is set to the new size of the volume.

```
cluster1::> volume size -vserver svml -volume volX -size 10TB
```

```
cluster1::> volume size -vserver svml -volume volX -size -5TB
```

## Configure FlexGroup volumes to automatically grow and shrink their size

Beginning with ONTAP 9.3, you can configure FlexGroup volumes to automatically grow

and shrink according to how much space they currently require.

### What you'll need

The FlexGroup volume must be online.

### About this task

You can autosize FlexGroup volumes in two modes:

- Increase the size of the volume automatically (`grow` mode)

Automatic growing helps prevent a FlexGroup volume from running out of space, if the aggregate can supply more space. You can configure the maximum size for the volume. The increase is automatically triggered based on the amount of data being written to the volume in relation to the current amount of used space and any thresholds set.

By default, the maximum size a volume can grow to is 120% of the size at which autogrow is enabled. If you need to ensure that the volume can grow to be larger than that, you must set the maximum size for the volume accordingly.

- Shrink the size of the volume automatically (`grow_shrink` mode)

Automatic shrinking prevents a volume from being larger than needed, freeing space in the aggregate for use by other volumes.

Autoshrink can only be used in combination with autogrow to meet changing space demands and is not available alone. When autoshrink is enabled, ONTAP automatically manages the shrinking behavior of a volume to prevent an endless loop of autogrow and autoshrink actions.

As a volume grows, the maximum number of files it can contain might be automatically increased. When a volume is shrunk, the maximum number of files it can contain is left unchanged, and a volume cannot be automatically shrunk below the size that corresponds to its current maximum number of files. For this reason, it might not be possible to automatically shrink a volume all the way to its original size.

### Step

1. Configure the volume to grow and shrink its size automatically: `volume autosize -vserver vs_server_name -volume vol_name -mode [grow | grow_shrink]`

You can also specify the maximum size, minimum size, and thresholds for growing or shrinking the volume.

The following command enables automatic size changes for a volume called `fg1`. The volume is configured to grow to a maximum size of 5 TB when it is 70% full.

```
cluster1::> volume autosize -volume fg1 -mode grow -maximum-size 5TB
-grow-threshold-percent 70
vol autosize: volume "vs_src:fg1" autosize settings UPDATED.
```

### Delete directories rapidly on the cluster

Beginning with ONTAP 9.8, you can use low-latency *fast-directory delete* functionality to delete directories from Linux and Windows client shares asynchronously (that is, in the

background). Cluster and SVM administrators can perform asynchronous delete operations on both FlexVol and FlexGroup volumes.

If you are using a version of ONTAP earlier than ONTAP 9.11.1, you must be a cluster administrator or a SVM administrator using the advanced privilege mode.

Beginning with ONTAP 9.11.1, a storage administrator can grant rights on a volume to allow NFS and SMB clients to perform asynchronous delete operations. For more information, see [Manage client rights to delete directories rapidly](#).

Beginning with ONTAP 9.8, you can use fast directory delete functionality using the ONTAP CLI. Beginning with ONTAP 9.9.1, you can use this functionality with System Manager. For more information about this process, see [Take corrective action based on analytics](#).



## System Manager

For more information, see [Take corrective action based on analytics](#).

### CLI

#### Use the CLI to perform a fast directory delete

1. Enter advanced privilege mode:

```
-privilege advance
```

2. Delete files or directories on a FlexVol or FlexGroup volume:

```
volume file async-delete start -vserver vserver_name -volume volume_name  
-path file_path -throttle throttle
```

The minimum throttle value is 10, the maximum is 100,000, and the default is 5000.

The following example deletes the directory named d2, which is located in the directory named d1.

```
cluster::*>volume file async-delete start -vserver vs1 -volume vol1  
-path d1/d2
```

3. Verify that the directory was deleted:

```
event log show
```

The following example shows output for the event log when the directory is successfully deleted.

```
cluster-cli::*> event log show  
Time                Node                Severity           Event  
-----  
-----  
MM/DD/YYYY 00:11:11 cluster-vsim        INFORMATIONAL  
asyncDelete.message.success: Async delete job on path d1/d2 of  
volume (MSID: 2162149232) was completed.
```

#### Cancel a directory delete job

1. Enter advanced privilege mode:

```
set -privilege advanced
```

2. Verify that the directory delete is in progress:

```
volume file async-delete show
```

If the SVM, volume, JobID, and path of your directory is displayed, you can cancel the job.

### 3. Cancel the directory delete:

```
volume file async-delete cancel -vserver SVM_name -volume volume_name
-jobid job_id
```

## Manage client rights to delete directories rapidly

Beginning with ONTAP 9.11.1, storage administrators can grant rights on a volume to allow NFS and SMB clients to perform low latency *fast-directory delete* operations themselves. When asynchronous delete is enabled on the cluster, Linux client users can use the `mv` command and Windows client users can use the `rename` command to delete a directory rapidly on the specified volume by moving it to a hidden directory that by default is named `.ontaptrashbin`.

### Enable client asynchronous directory delete

#### Steps

1. From the cluster CLI, enter advanced privilege mode: `-privilege advance`
2. Enable client asynchronous delete and, if desired, provide an alternate name for the trashbin directory:

```
volume file async-delete client enable volume volname vserver vserverName
trashbinname name
```

Example using the default trashbin name:

```
cluster1::*> volume file async-delete client enable -volume v1 -vserver
vs0

Info: Async directory delete from the client has been enabled on volume
"v1" in
      Vserver "vs0".
```

Example specifying an alternate trashbin name:

```
cluster1::*> volume file async-delete client enable -volume test
-trashbin ntaptrash -vserver vs1

Success: Async directory delete from the client is enabled on volume
"v1" in
      Vserver "vs0".
```

3. Verify client asynchronous delete is enabled:

```
volume file async-delete client show
```

Example:

```
cluster1::*> volume file async-delete client show
```

```
Vserver Volume          async-delete client TrashBinName
```

```
-----  
vs1         vol1           Enabled           .ntaptrash
```

```
vs2         vol2           Disabled          -
```

```
2 entries were displayed.
```

### Disable client asynchronous directory delete

#### Steps

1. From the cluster CLI, disable client asynchronous directory delete:

```
volume file async-delete client disable volume volname vserver vserverName
```

Example:

```
cluster1::*> volume file async-delete client disable -volume vol1  
-vserver vs1
```

```
Success: Asynchronous directory delete client disabled  
successfully on volume.
```

2. Verify client asynchronous delete is disabled:

```
volume file async-delete client show
```

Example:

```
cluster1::*> volume file async-delete client show
```

```
Vserver      Volume          async-delete client      TrashBinName
```

```
-----  
vs1         vol1           Disabled          -
```

```
vs2         vol2           Disabled          -
```

```
2 entries were displayed.
```

### Create qtrees with FlexGroup volumes

Beginning with ONTAP 9.3, you can create qtrees with FlexGroup volumes. Qtrees enable you to partition your FlexGroup volumes into smaller segments that you can

manage individually.

### About this task

- If you want to revert to ONTAP 9.2 or earlier and if you have created one or more qtrees in the FlexGroup volume or modified the attributes (security style and SMB oplocks) of the default qtree, you must delete all of the non-default qtrees and then disable the qtree functionality on each FlexGroup volume before reverting to ONTAP 9.2 or earlier.

#### [Disable qtree functionality in FlexGroup volumes before reverting](#)

- If the source FlexGroup volume has qtrees in a SnapMirror relationship, the destination cluster must be running ONTAP 9.3 or later (a version of ONTAP software that supports qtrees).
- Beginning with ONTAP 9.5, qtree statistics are supported for FlexGroup volumes.

### Steps

1. Create a qtree in the FlexGroup volume: `volume qtree create -vserver vs0 -volume fg1 -qtree qtree1 -security-style mixed`

You can optionally specify the security style, SMB oplocks, UNIX permissions, and export policy for the qtree.

```
cluster1::> volume qtree create -vserver vs0 -volume fg1 -qtree qtree1
-security-style mixed
```

### Related information

[Logical storage management](#)

### Use quotas for FlexGroup volumes

In ONTAP 9.4 and earlier, you can apply quotas rules to FlexGroup volumes only for reporting purposes, but not for enforcing quota limits. Beginning with ONTAP 9.5, you can enforce limits on quota rules that are applied to FlexGroup volumes.

### About this task

- Beginning with ONTAP 9.5, you can specify hard, soft, and threshold limit quotas for FlexGroup volumes.

You can specify these limits to constrain the amount of space, the number of files that a specific user, group, or qtree can create, or both. Quota limits generate warning messages in the following scenarios:

- When usage exceeds a configured soft limit, ONTAP issues a warning message, but further traffic is still allowed.

If usage later drops below the configured soft limit again, an all-clear message is issued.

- When usage exceeds a configured threshold limit, ONTAP issues a second warning message.

No all-clear administrative message is issued when usage later drops below a configured threshold limit.

- If usage reaches a configured hard limit, ONTAP prevents further resource consumption by rejecting

traffic.


- In ONTAP 9.5, quota rules cannot be created or activated on the destination FlexGroup volume of a SnapMirror relationship.
- During quota initialization, quotas are not enforced, and there are no notifications of breached quotas following quota initialization.

To check if quotas were breached during quota initialization, you can use the `volume quota report` command.

### Quota targets and types

Quotas have a type: they can be either user, group, or tree. Quota targets specify the user, group, or qtree for which the quota limits are applied.

The following table lists the kinds of quota targets, what types of quotas each quota target is associated with, and how each quota target is represented:

Quota target	Quota type	How target is represented	Notes
user	user quota	UNIX user name UNIX UID  Windows user name in pre-Windows 2000 format  Windows SID	User quotas can be applied for a specific volume or qtree.
group	group quota	UNIX group name UNIX GID	Group quotas can be applied for a specific volume or qtree.   ONTAP does not apply group quotas based on Windows IDs.
qtree	tree quota	qtree name	Tree quotas are applied to a particular volume and do not affect qtrees in other volumes.
""	user quotagroup quota  tree quota	Double quotation marks ("" )	A quota target of "" denotes a <i>default quota</i> . For default quotas, the quota type is determined by the value of the type field.

## Behavior of FlexGroup volumes when quota limits are exceeded

Beginning with ONTAP 9.5, quota limits are supported on FlexGroup volumes. There are some differences in the way quota limits are enforced on a FlexGroup volume when compared to a FlexVol volume.

FlexGroup volumes might show the following behaviors when the quota limits are exceeded:

- The space and file usage in a FlexGroup volume might reach up to 5 percent higher than the configured hard limit before the quota limit is enforced by rejecting further traffic.

To provide the best performance, ONTAP might allow the space consumption to exceed the configured hard limit by a small margin before the quota enforcement begins. This additional space consumption does not exceed 5 percent of the configured hard limits, 1 GB, or 65536 files, whichever is lower.

- After the quota limit is reached, if a user or administrator deletes some files or directories such that the quota usage is now below the limit, the subsequent quota-consuming file operation might resume with a delay (might take up to 5 seconds to resume).
- When the total space and file usage of a FlexGroup volume exceed the configured quota limits, there might be a slight delay in logging an event log message.
- You might get “no space” errors if some constituents of the FlexGroup volume get full, but the quota limits are not reached.
- Operations, such as renaming a file or directory or moving files between qtrees, on quota targets, for which quota hard limits are configured, might take longer when compared to similar operations on FlexVol volumes.

## Examples of quota enforcement for FlexGroup volumes

You can use the examples to understand how to configure quotas with limits in ONTAP 9.5 and later.

### Example 1: Enforcing a quota rule with disk limits

1. You should create a quota policy rule of type `user` with both an achievable soft disk limit and hard disk limit.

```
cluster1::> volume quota policy rule create -vserver vs0 -policy-name
default -volume FG -type user -target "" -qtree "" -disk-limit 1T -soft
-disk-limit 800G
```

2. You can view the quota policy rule:

```
cluster1::> volume quota policy rule show -vserver vs0 -policy-name
default -volume FG
```

```
Vserver: vs0                Policy: default                Volume: FG

                                User          Disk          Soft          Soft
                                Mapping       Limit         Disk         Files         Files
Type   Target   Qtree      Mapping      Limit        Limit        Limit        Limit
-----
-----
user   ""       ""         off          1TB          800GB        -           -
-
```

3. To activate the new quota rule, you initialize quotas on the volume:

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

4. You can view the disk usage and file usage information of the FlexGroup volume by using the quota report.

```
cluster1::> volume quota report -vserver vs0 -volume FG
Vserver: vs0

                                ----Disk----  ----Files-----  Quota
Volume  Tree      Type   ID          Used  Limit   Used  Limit
Specifier
-----
-----
FG      user      root   50GB        -     1       -
FG      user      *      800GB      1TB   0       -   *
2 entries were displayed.
```

After the hard disk limit is reached, the quota policy rule target (user, in this case) is blocked from writing more data to the files.

### Example 2: Enforcing a quota rule for multiple users

1. You should create a quota policy rule of type `user`, where multiple users are specified in the quota target (UNIX users, SMB users, or a combination of both) and where the rule has both an achievable soft disk limit and hard disk limit.

```
cluster1::> quota policy rule create -vserver vs0 -policy-name default
-volume FG -type user -target "rdavis,ABCCORP\RobertDavis" -qtree ""
-disk-limit 1TB -soft-disk-limit 800GB
```

2. You can view the quota policy rule:

```
cluster1::> quota policy rule show -vserver vs0 -policy-name default
-volume FG
```

Vserver: vs0			Policy: default			Volume: FG	
Type	Target	Qtree	User Mapping	Disk Limit	Soft Disk Limit	Files Limit	Soft Files Limit
user	"rdavis,ABCCORP\RobertDavis"	""	off	1TB	800GB	-	-

3. To activate the new quota rule, you initialize quotas on the volume:

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

4. You can verify that the quota state is active:

```
cluster1::> volume quota show -vserver vs0 -volume FG
Vserver Name: vs0
Volume Name: FG
Quota State: on
Scan Status: -
Logging Messages: on
Logging Interval: 1h
Sub Quota Status: none
Last Quota Error Message: -
Collection of Quota Errors: -
```

5. You can view the disk usage and file usage information of the FlexGroup volume by using the quota report.



```

cluster1::> quota report -vserver vs0 -volume FG
Vserver: vs0

Volume      Tree      Type      ID      ----Disk----  ----Files-----  Quota
Specifier
-----
FG          user      rdavis,ABCCORP\RobertDavis  0B  1TB  0  -
rdavis,ABCCORP\RobertDavis

```

The quota limit is shared among all users listed in the quota target.

After the hard disk limit is reached, users listed in the quota target are blocked from writing more data to the files.

### Example 3: Enforcing quota with user mapping enabled

1. You should create a quota policy rule of type `user`, specify a UNIX user or a Windows user as the quota target with `user-mapping` set to `on`, and create the rule with both an achievable soft disk limit and hard disk limit.

The mapping between UNIX and Windows users must be configured earlier by using the `vserver name-mapping create` command.

```

cluster1::> quota policy rule create -vserver vs0 -policy-name default
-volume FG -type user -target rdavis -qtree "" -disk-limit 1TB -soft
-disk-limit 800GB -user-mapping on

```

2. You can view the quota policy rule:

```

cluster1::> quota policy rule show -vserver vs0 -policy-name default
-volume FG

Vserver: vs0          Policy: default          Volume: FG

Type  Target  Qtree  User      Disk      Soft      Soft
Threshold  Mapping  Limit  Limit  Limit  Files  Files
-----
user  rdavis  ""     on        1TB      800GB    -      -
-

```

3. To activate the new quota rule, you initialize quotas on the volume:

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

4. You can verify that the quota state is active:

```
cluster1::> volume quota show -vserver vs0 -volume FG
      Vserver Name: vs0
      Volume Name: FG
      Quota State: on
      Scan Status: -
      Logging Messages: on
      Logging Interval: 1h
      Sub Quota Status: none
      Last Quota Error Message: -
      Collection of Quota Errors: -
```

5. You can view the disk usage and file usage information of the FlexGroup volume by using the quota report.

```
cluster1::> quota report -vserver vs0 -volume FG
Vserver: vs0

Volume  Tree      Type  ID          ----Disk----  ----Files-----  Quota
Specifier                                     Used  Limit      Used  Limit
-----  -
FG      rdavis      user  rdavis,ABCCORP\RobertDavis  0B  1TB  0  -
```

The quota limit is shared between the user listed in the quota target and its corresponding Windows or UNIX user.

After the hard disk limit is reached, both the user listed in the quota target and its corresponding Windows or UNIX user is blocked from writing more data to the files.

#### Example 4: Verifying the qtree size when quota is enabled

1. You should create a quota policy rule of type `tree` and where the rule has both an achievable soft disk limit and hard disk limit.

```
cluster1::> quota policy rule create -vserver vs0 -policy-name default
-volume FG -type tree -target tree_4118314302 -qtree "" -disk-limit 48GB
-soft-disk-limit 30GB
```

2. You can view the quota policy rule:

```
cluster1::> quota policy rule show -vserver vs0
```

Vserver: vs0			Policy: default			Volume: FG	
Type	Target	Qtree	User Mapping	Disk Limit	Soft Disk Limit	Files Limit	Soft Files Limit
tree	tree_4118314302	""	-	48GB	-	20	-

3. To activate the new quota rule, you initialize quotas on the volume:

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

a. You can view the disk usage and file usage information of the FlexGroup volume by using the quota report.

```
cluster1::> quota report -vserver vs0
```

Vserver: vs0		Quota		Specifier	
Volume	Tree	Type	ID	Used	Limit
FG	tree_4118314302	tree	1	30.35GB	48GB

The quota limit is shared between the user listed in the quota target and its corresponding Windows or UNIX user.

4. From an NFS client, use the `df` command to view the total space usage, available space, and the used space.

```
scsps0472342001# df -m /t/10.53.2.189/FG-3/tree_4118314302
```

Filesystem	1M-blocks	Used	Available	Use%	Mounted on
10.53.2.189/FG-3	49152	31078	18074	63%	/t/10.53.2.189/FG-3

With hard limit, the space usage is calculated from an NFS client as follows:

- Total space usage = hard limit for tree
  - Free space = Hard limit minus qtree space usage
- Without hard limit, the space usage is calculated from an NFS client as follows:

- Space usage = quota usage
- Total space = Sum of quota usage and physical free space in the volume

5. From the SMB share, use Windows Explorer to view the total space usage, available space, and the used space.

From an SMB share, you should be aware of the following considerations for calculating the space usage:

- The user quota hard limit for the user and group is taken into consideration for calculating the total available space.
- The minimum value among the free space of the tree quota rule, the user quota rule, and the group quota rule is considered as the free space for the SMB share.
- The total space usage is variable for SMB and depends on the hard limit that corresponds to the minimum free space among the tree, user, and group.

## Apply rules and limits on the FlexGroups volume

### Steps

1. Create quota rules for targets: `volume quota policy rule create -vserver vs0 -policy-name quota_policy_of_the_rule -volume flexgroup_vol -type {tree|user|group} -target target_for_rule -qtree qtree_name [-disk-limit hard_disk_limit_size] [-file-limit hard_limit_number_of_files] [-threshold threshold_disk_limit_size] [-soft-disk-limit soft_disk_limit_size] [-soft-file-limit soft_limit_number_of_files]`

- In ONTAP 9.2 and ONTAP 9.1, the quota target type can be only `user` or `group` for FlexGroup volumes.

Tree quota type is not supported for FlexGroup volumes in ONTAP 9.2 and ONTAP 9.1.

- In ONTAP 9.3 and later, the quota target type can be `user`, `group`, or `tree` for FlexGroup volumes.
- A path is not supported as the target when creating quota rules for FlexGroup volumes.
- Beginning with ONTAP 9.5, you can specify hard disk limit, hard file limit, soft disk limit, soft file limit, and threshold limit quotas for FlexGroup volumes.

In ONTAP 9.4 and earlier, you cannot specify the disk limit, file limit, threshold for disk limit, soft disk limit, or soft file limit when you create quota rules for FlexGroup volumes.

The following example shows a default quota rule being created for the user target type:

```
cluster1::> volume quota policy rule create -vserver vs0 -policy-name
quota_policy_vs0_1 -volume fg1 -type user -target "" -qtree ""
```

The following example shows a tree quota rule being created for the qtree named qtree1:

```
cluster1::> volume quota policy rule create -policy-name default -vserver
vs0 -volume fg1 -type tree -target "qtree1"
```

1. Activate the quotas for the specified FlexGroup volume: `volume quota on -vserver svm_name -volume flexgroup_vol -foreground true`

```
cluster1::> volume quota on -vserver vs0 -volume fg1 -foreground true
```

1. Monitor the state of quota initialization: `volume quota show -vserver svm_name`

FlexGroup volumes might show the mixed state, which indicates that all of the constituent volumes are not in the same state yet.

```
cluster1::> volume quota show -vserver vs0
```

Vserver	Volume	State	Scan Status
vs0	fg1	initializing	95%
vs0	vol1	off	-

2 entries were displayed.

1. View the quota report for the FlexGroup volume with active quotas: `volume quota report -vserver svm_name -volume flexgroup_vol`

You cannot specify a path with the `volume quota report` command for FlexGroup volumes.

The following example shows the user quota for the FlexGroup volume fg1:

```
cluster1::> volume quota report -vserver vs0 -volume fg1
```

Vserver: vs0

Quota				----Disk----		----Files----	
Volume	Tree	Type	ID	Used	Limit	Used	Limit
Specifier							
fg1		user	*	0B	-	0	- *
fg1		user	root	1GB	-	1	- *

2 entries were displayed.

The following example shows the tree quota for the FlexGroup volume fg1:

```

cluster1::> volume quota report -vserver vs0 -volume fg1
Vserver: vs0

Volume      Tree      Type      ID      ----Disk----  ----Files-----  Quota
Specifier
-----
fg1         qtree1   tree      1       68KB          -                18          -
qtree1
fg1         tree     *         *       0B            -                0           -   *
2 entries were displayed.

```

## Results

The quota rules and limits are applied on the FlexGroups volume.

The usage might reach up to 5 percent higher than a configured hard limit before ONTAP enforces the quota by rejecting further traffic.

## Related information

[ONTAP 9 Commands](#)

## Enable storage efficiency on a FlexGroup volume

You can run deduplication and data compression together or independently on a FlexGroup volume to achieve optimal space savings.

### What you'll need

The FlexGroup volume must be online.

### Steps

1. Enable storage efficiency on the FlexGroup volume: `volume efficiency on -vserver svm_name -volume volume_name`

Storage efficiency operations are enabled on all the constituents of the FlexGroup volume.

If a FlexGroup volume is expanded after storage efficiency is enabled on the volume, storage efficiency is automatically enabled on the new constituents.

2. Enable the required storage efficiency operation on the FlexGroup volume by using the `volume efficiency modify` command.

You can enable inline deduplication, postprocess deduplication, inline compression, and postprocess compression on FlexGroup volumes. You can also set the type of compression (secondary or adaptive) and specify a schedule or efficiency policy for the FlexGroup volume.

3. If you are not using schedules or efficiency policies for running the storage efficiency operations, start the efficiency operation: `volume efficiency start -vserver svm_name -volume volume_name`

If deduplication and data compression are enabled on a volume, data compression is run initially followed by deduplication. This command fails if any efficiency operation is already active on the FlexGroup volume.

4. Verify the efficiency operations that are enabled on the FlexGroup volume: `volume efficiency show -vserver svm_name -volume volume_name`

```
cluster1::> volume efficiency show -vserver vs1 -volume fg1
      Vserver Name: vs1
      Volume Name: fg1
      Volume Path: /vol/fg1
      State: Enabled
      Status: Idle
      Progress: Idle for 17:07:25
      Type: Regular
      Schedule: sun-sat@0

...

      Compression: true
      Inline Compression: true
      Incompressible Data Detection: false
      Constituent Volume: false
      Compression Quick Check File Size: 524288000
      Inline Dedupe: true
      Data Compaction: false
```

## Protect FlexGroup volumes using Snapshot copies

You can create Snapshot policies that automatically manage the creation of Snapshot copies or you can manually create Snapshot copies for FlexGroup volumes. A valid Snapshot copy is created for a FlexGroup volume only after ONTAP can successfully create a Snapshot copy for each constituent of the FlexGroup volume.

### About this task



- If you have multiple FlexGroup volumes associated with a Snapshot policy, you should ensure that the FlexGroup volumes schedules do not overlap.
- Beginning with ONTAP 9.8, the maximum number of Snapshot copies supported on a FlexGroup volume is 1023.



Beginning with ONTAP 9.8, the `volume snapshot show` command for FlexGroup volumes reports Snapshot copy size using logical blocks, rather than calculating the youngest owned blocks. This new size calculation method might make the Snapshot copy size appear larger than calculations in earlier versions of ONTAP.

### Steps

1. Create a Snapshot policy or manually create a Snapshot copy:

If you want to create a...	Enter this command...
Snapshot policy	<pre>volume snapshot policy create</pre> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  The schedules that are associated with the Snapshot policy of a FlexGroup volume must have an interval greater than 30 minutes. </div> <p>When you create a FlexGroup volume, the default Snapshot policy is applied to the FlexGroup volume.</p>
Snapshot copy manually	<pre>volume snapshot create</pre> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  After you create a Snapshot copy for a FlexGroup volume, you cannot modify the attributes of the Snapshot copy. If you want to modify the attributes, you must delete and then re-create the Snapshot copy. </div>

Client access to the FlexGroup volume is briefly quiesced when a Snapshot copy is created.

1. Verify that a valid Snapshot copy is created for the FlexGroup volume: `volume snapshot show -volume volume_name -fields state`

```
cluster1::> volume snapshot show -volume fg -fields state
vserver volume snapshot                state
-----
fg_vs   fg      hourly.2016-08-23_0505 valid
```

2. View the Snapshot copies for the constituents of the FlexGroup volume: `volume snapshot show -is -constituent true`



```

cluster1::> volume snapshot show -is-constituent true

---Blocks---
Vserver  Volume      Snapshot                               Size Total%
Used%
-----
fg_vs    fg__0001
        hourly.2016-08-23_0505                72MB    0%
27%
        fg__0002
        hourly.2016-08-23_0505                72MB    0%
27%
        fg__0003
        hourly.2016-08-23_0505                72MB    0%
27%
...
        fg__0016
        hourly.2016-08-23_0505                72MB    0%
27%

```

## Move the constituents of a FlexGroup volume

You can move the constituents of a FlexGroup volume from one aggregate to another for balancing the load when certain constituents experience more traffic. Moving constituents also helps in freeing up space on an aggregate for resizing the existing constituents.

### What you'll need

To move a FlexGroup volume constituent that is in a SnapMirror relationship, you must have initialized the SnapMirror relationship.

### About this task

You cannot perform a volume move operation while the constituents of the FlexGroup volume are being expanded.

### Steps

1. Identify the FlexGroup volume constituent that you want to move: `volume show -vserver svm_name -is-constituent *`

```
cluster1::> volume show -vserver vs2 -is-constituent *
```

Vserver	Volume	Aggregate	State	Type	Size
vs2	fg1	-	online	RW	400TB
15.12TB	62%				
vs2	fg1__0001	aggr1	online	RW	25TB
8.12MB	59%				
vs2	fg1__0002	aggr2	online	RW	25TB
2.50TB	90%				
...					

2. Identify an aggregate to which you can move the FlexGroup volume constituent: `volume move target-aggr show -vserver svm_name -volume vol_constituent_name`

The available space in the aggregate that you select must be greater than the size of the FlexGroup volume constituent that you are moving.

```
cluster1::> volume move target-aggr show -vserver vs2 -volume fg1_0002
```

Aggregate Name	Available Size	Storage Type
aggr2	467.9TB	hdd
node12a_aggr3	100.34TB	hdd
node12a_aggr2	100.36TB	hdd
node12a_aggr1	100.36TB	hdd
node12a_aggr4	100.36TB	hdd

5 entries were displayed.

3. Verify that the FlexGroup volume constituent can be moved to the intended aggregate: `volume move start -vserver svm_name -volume vol_constituent_name -perform-validation-only true`

```
cluster1::> volume move start -vserver vs2 -volume fg1_0002 -destination
-aggregate node12a_aggr3 -perform-validation-only true
Validation succeeded.
```

4. Move the FlexGroup volume constituent: `volume move start -vserver svm_name -volume vol_constituent_name -destination-aggregate aggr_name [-allow-mixed-aggr-types {true|false}]`

The volume move operation runs as a background process.

Beginning with ONTAP 9.5, you can move FlexGroup volume constituents from a Fabric Pool to a non-Fabric Pool, or vice versa by setting the `-allow-mixed-aggr-types` parameter to `true`. By default, the

`-allow-mixed-aggr-types` option is set to `false`.



You cannot use the `volume move` command for enabling encryption on FlexGroup volumes.

```
cluster1::> volume move start -vserver vs2 -volume fg1_002 -destination
-aggregate node12a_aggr3
```



If the volume move operation fails due to an active SnapMirror operation, you should abort the SnapMirror operation by using the `snapmirror abort -h` command. In some cases, the SnapMirror abort operation might also fail. In such situations, you should abort the volume move operation and retry later.

5. Verify the state of the volume move operation: `volume move show -volume vol_constituent_name`

The following example shows the state of a FlexGroup constituent volume that completed the replication phase and is in the cutover phase of the volume move operation:

```
cluster1::> volume move show -volume fg1_002
Vserver    Volume      State      Move Phase  Percent-Complete  Time-To-
Complete
-----
vs2        fg1_002    healthy    cutover     -                  -
```

## Use aggregates in FabricPool for existing FlexGroup volumes

Beginning with ONTAP 9.5, FabricPool is supported for FlexGroup volumes. If you want to use aggregates in FabricPool for your existing FlexGroup volumes, you can either convert the aggregates on which the FlexGroup volume resides to aggregates in FabricPool or migrate the FlexGroup volume constituents to aggregates in FabricPool.

### What you'll need

- The FlexGroup volume must have `space-guarantee` set to `none`.
- If you want to convert the aggregates on which the FlexGroup volume resides to aggregates in FabricPool, the aggregates must be using all SSD disks.

### About this task

If an existing FlexGroup volume resides on non-SSD aggregates, you must migrate the FlexGroup volume constituents to aggregates in FabricPool.

### Choices

- To convert the aggregates on which the FlexGroup volume resides to aggregates in FabricPool, perform the following steps:

- a. Set the tiering policy on the existing FlexGroup volume: `volume modify -volume flexgroup_name -tiering-policy [auto|snapshot|none|backup]`

```
cluster-2::> volume modify -volume fg1 -tiering-policy auto
```

- b. Identify the aggregates on which the FlexGroup volume resides: `volume show -volume flexgroup_name -fields aggr-list`

```
cluster-2::> volume show -volume fg1 -fields aggr-list
vserver volume aggr-list
-----
vs1      fg1      aggr1,aggr3
```

- c. Attach an object store to each aggregate listed in the aggregate list: `storage aggregate object-store attach -aggregate aggregate name -name object-store-name -allow -flexgroup true`

You must attach all of the aggregates to an object store.

```
cluster-2::> storage aggregate object-store attach -aggregate aggr1
-object-store-name Amazon01B1
```

- To migrate the FlexGroup volume constituents to aggregates in FabricPool, perform the following steps:

- a. Set the tiering policy on the existing FlexGroup volume: `volume modify -volume flexgroup_name -tiering-policy [auto|snapshot|none|backup]`

```
cluster-2::> volume modify -volume fg1 -tiering-policy auto
```

- b. Move each constituent of the FlexGroup volume to an aggregate in FabricPool in the same cluster:

```
volume move start -volume constituent-volume -destination-aggregate
FabricPool_aggregate -allow-mixed-aggr-types true
```

You must move all FlexGroup volume constituents to aggregates in FabricPool (in case the FlexGroup volume constituents are on mixed aggregate types) and ensure that all the constituents are balanced across the nodes in the cluster.

```
cluster-2::> volume move start -volume fg1_001 -destination-aggregate
FP_aggr1 -allow-mixed-aggr-types true
```

## Related information

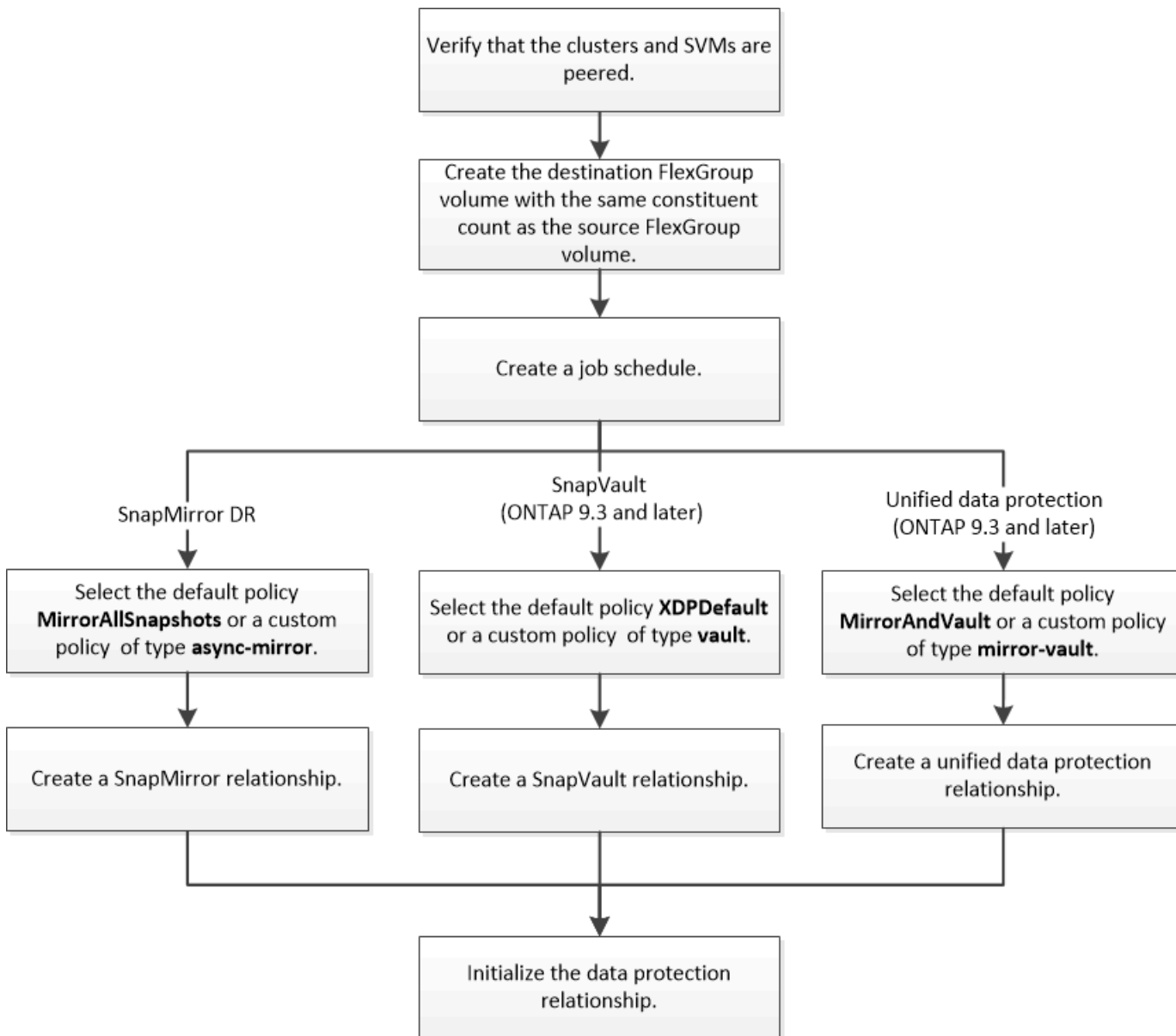
[Disk and aggregate management](#)

## Data protection for FlexGroup volumes

### Data protection workflow for FlexGroup volumes

You can create SnapMirror disaster recovery (DR) relationships for FlexGroup volumes. Beginning with ONTAP 9.3, you can also backup and restore FlexGroup volumes by using SnapVault technology, and you can create a unified data protection relationship that uses the same destination for backup and DR.

The data protection workflow consists of verifying the cluster and SVM peer relationships, creating a destination volume, creating a job schedule, specifying a policy, creating a data protection relationship, and initializing the relationship.



#### About this task

The SnapMirror relationship type is always XDP for FlexGroup volumes. The type of data protection that is provided by a SnapMirror relationship is determined by the replication policy that you use. You can use either the default policy or a custom policy of the required type for the replication relationship that you want to create.

The following table shows the default policy types and supported custom policy types for different types of data protection relationships.

Relationship type	Default Policy	Custom policy type
SnapMirror DR	MirrorAllSnapshots	async-mirror
SnapVault backup	XDPDefault	vault
Unified data protection	MirrorAndVault	mirror-vault

The MirrorLatest policy is not supported with FlexGroup volumes.

### Create a SnapMirror relationship for FlexGroup volumes

You can create a SnapMirror relationship between the source FlexGroup volume and the destination FlexGroup volume on a peered SVM for replicating data for disaster recovery. You can use the mirror copies of the FlexGroup volume to recover data when a disaster occurs.

#### What you'll need

You must have created the cluster peering relationship and SVM peering relationship.

#### [Cluster and SVM peering](#)

#### About this task

- You can create both intercluster SnapMirror relationships and intracluster SnapMirror relationships for FlexGroup volumes.
- Beginning with ONTAP 9.3, you can expand FlexGroup volumes that are in a SnapMirror relationship.

If you are using a version of ONTAP earlier than ONTAP 9.3, you must not expand FlexGroup volumes after a SnapMirror relationship is established; however, you can increase the capacity of FlexGroup volumes after establishing a SnapMirror relationship. If you expand the source FlexGroup volume after breaking the SnapMirror relationship in releases earlier than ONTAP 9.3, you must perform a baseline transfer to the destination FlexGroup volume.

#### Steps

1. Create a destination FlexGroup volume of type DP that has the same number of constituents as that of the source FlexGroup volume:
  - a. From the source cluster, determine the number of constituents in the source FlexGroup volume:

```
volume show -volume volume_name* -is-constituent true
```

```

cluster1::> volume show -volume srcFG* -is-constituent true
Vserver    Volume          Aggregate      State      Type      Size
Available Used%
-----
vss        srcFG           -              online     RW        400TB
172.86GB  56%
vss        srcFG__0001    Aggr_cmode    online     RW        25GB
10.86TB   56%
vss        srcFG__0002    aggr1         online     RW        25TB
10.86TB   56%
vss        srcFG__0003    Aggr_cmode    online     RW        25TB
10.72TB   57%
vss        srcFG__0004    aggr1         online     RW        25TB
10.73TB   57%
vss        srcFG__0005    Aggr_cmode    online     RW        25TB
10.67TB   57%
vss        srcFG__0006    aggr1         online     RW        25TB
10.64TB   57%
vss        srcFG__0007    Aggr_cmode    online     RW        25TB
10.63TB   57%
...

```

- b. From the destination cluster, create a destination FlexGroup volume of type DP with the same number of constituents as that of the source FlexGroup volume.

```

cluster2::> volume create -vserver vsd -aggr-list aggr1,aggr2 -aggr
-list-multiplier 8 -size 400TB -type DP dstFG

Warning: The FlexGroup volume "dstFG" will be created with the
following number of constituents of size 25TB: 16.
Do you want to continue? {y|n}: y
[Job 766] Job succeeded: Successful

```

- c. From the destination cluster, verify the number of constituents in the destination FlexGroup volume:  
 volume show -volume volume\_name\* -is-constituent true

```
cluster2::> volume show -volume dstFG* -is-constituent true
Vserver    Volume                Aggregate    State    Type    Size
Available  Used%
-----
vsd        dstFG                 -           online   DP      400TB
172.86GB  56%
vsd        dstFG__0001          Aggr_cmode  online   DP      25GB
10.86TB   56%
vsd        dstFG__0002          aggr1       online   DP      25TB
10.86TB   56%
vsd        dstFG__0003          Aggr_cmode  online   DP      25TB
10.72TB   57%
vsd        dstFG__0004          aggr1       online   DP      25TB
10.73TB   57%
vsd        dstFG__0005          Aggr_cmode  online   DP      25TB
10.67TB   57%
vsd        dstFG__0006          aggr1       online   DP      25TB
10.64TB   57%
vsd        dstFG__0007          Aggr_cmode  online   DP      25TB
10.63TB   57%
...
```

2. Create a job schedule: `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

For the `-month`, `-dayofweek`, and `-hour` options, you can specify `all` to run the job every month, every day of the week, and every hour, respectively.

The following example creates a job schedule named `my_weekly` that runs on Saturdays at 3:00 a.m.:

```
cluster1::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

3. Create a custom policy of type `async-mirror` for the SnapMirror relationship: `snapmirror policy create -vserver SVM -policy snapmirror_policy -type async-mirror`

If you do not create a custom policy, you should specify the `MirrorAllSnapshots` policy for SnapMirror relationships.

4. From the destination cluster, create a SnapMirror relationship between the source FlexGroup volume and the destination FlexGroup volume: `snapmirror create -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -type XDP -policy snapmirror_policy -schedule sched_name`

SnapMirror relationships for FlexGroup volumes must be of type `XDP`.



If you specify a throttle value for the SnapMirror relationship for the FlexGroup volume, each constituent uses the same throttle value. The throttle value is not divided among the constituents.



You cannot use SnapMirror labels of Snapshot copies for FlexGroup volumes.

In ONTAP 9.4 and earlier, if the policy is not specified with the `snapmirror create` command, the `MirrorAllSnapshots` policy is used by default. In ONTAP 9.5, if the policy is not specified with the `snapmirror create` command, the `MirrorAndVault` policy is used by default.

```
cluster2::> snapmirror create -source-path vss:srcFG -destination-path
vsd:dstFG -type XDP -policy MirrorAllSnapshots -schedule hourly
Operation succeeded: snapmirror create for the relationship with
destination "vsd:dstFG".
```

5. From the destination cluster, initialize the SnapMirror relationship by performing a baseline transfer:

```
snapmirror initialize -destination-path dest_svm:dest_flexgroup
```

After the baseline transfer is completed, the destination FlexGroup volume is updated periodically based on the schedule of the SnapMirror relationship.

```
cluster2::> snapmirror initialize -destination-path vsd:dstFG
Operation is queued: snapmirror initialize of destination "vsd:dstFG".
```



If you have created any SnapMirror relationship between FlexGroup volumes with the source cluster running ONTAP 9.3 and the destination cluster running ONTAP 9.2 or earlier, and if you create any qtrees in the source FlexGroup volume, the SnapMirror updates fail. To recover from this situation, you must delete all of the non-default qtrees in the FlexGroup volume, disable the qtree functionality on the FlexGroup volume, and then delete all of the Snapshot copies that are enabled with the qtree functionality. You must also perform these steps before reverting from ONTAP 9.3 to an earlier version of ONTAP, if you have the qtree functionality enabled on the FlexGroup volumes. [Disable qtree functionality in FlexGroup volumes before reverting](#)

### After you finish

You should set up the destination SVM for data access by setting up required configurations such as LIFs and export policies.

### Create a SnapVault relationship for FlexGroup volumes

You can configure a SnapVault relationship and assign a SnapVault policy to the relationship to create a SnapVault backup.

### What you'll need

You must be aware of the considerations for creating a SnapVault relationship for FlexGroup volumes.

### Steps

1. Create a destination FlexGroup volume of type `DP` that has the same number of constituents as that of the

source FlexGroup volume:

- a. From the source cluster, determine the number of constituents in the source FlexGroup volume:

```
volume show -volume volume_name* -is-constituent true
```

```
cluster1::> volume show -volume src* -is-constituent true
Vserver   Volume           Aggregate      State      Type      Size
Available Used%
-----
-----
vss       src              -              online    RW        400TB
172.86GB  56%
vss       src__0001        Aggr_cmode    online    RW        25GB
10.86TB   56%
vss       src__0002        aggr1         online    RW        25TB
10.86TB   56%
vss       src__0003        Aggr_cmode    online    RW        25TB
10.72TB   57%
vss       src__0004        aggr1         online    RW        25TB
10.73TB   57%
vss       src__0005        Aggr_cmode    online    RW        25TB
10.67TB   57%
vss       src__0006        aggr1         online    RW        25TB
10.64TB   57%
vss       src__0007        Aggr_cmode    online    RW        25TB
10.63TB   57%
...
```

- b. From the destination cluster, create a destination FlexGroup volume of type DP with the same number of constituents as that of the source FlexGroup volume.

```
cluster2::> volume create -vserver vsd -aggr-list aggr1,aggr2 -aggr
-list-multiplier 8 -size 400TB -type DP dst
```

```
Warning: The FlexGroup volume "dst" will be created with the
following number of constituents of size 25TB: 16.
```

```
Do you want to continue? {y|n}: y
```

```
[Job 766] Job succeeded: Successful
```

- c. From the destination cluster, verify the number of constituents in the destination FlexGroup volume:

```
volume show -volume volume_name* -is-constituent true
```

```

cluster2::> volume show -volume dst* -is-constituent true
Vserver    Volume          Aggregate      State    Type    Size
Available Used%
-----
vsd        dst              -              online   RW      400TB
172.86GB  56%
vsd        dst__0001       Aggr_cmode    online   RW      25GB
10.86TB   56%
vsd        dst__0002       aggr1         online   RW      25TB
10.86TB   56%
vsd        dst__0003       Aggr_cmode    online   RW      25TB
10.72TB   57%
vsd        dst__0004       aggr1         online   RW      25TB
10.73TB   57%
vsd        dst__0005       Aggr_cmode    online   RW      25TB
10.67TB   57%
vsd        dst__0006       aggr1         online   RW      25TB
10.64TB   57%
vsd        dst__0007       Aggr_cmode    online   RW      25TB
10.63TB   57%
...

```

2. Create a job schedule: `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

For `-month`, `-dayofweek`, and `-hour`, you can specify `all` to run the job every month, day of the week, and hour, respectively.

The following example creates a job schedule named `my_weekly` that runs on Saturdays at 3:00 a.m.:

```

cluster1::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0

```

3. Create a SnapVault policy, and then define a rule for the SnapVault policy:
  - a. Create a custom policy of type `vault` for the SnapVault relationship: `snapmirror policy create -vserver svm_name -policy policy_name -type vault`
  - b. Define a rule for the SnapVault policy that determines which Snapshot copies are transferred during initialization and update operations: `snapmirror policy add-rule -vserver svm_name -policy policy_for_rule -snapmirror-label snapmirror-label -keep retention_count -schedule schedule`

If you do not create a custom policy, you should specify the `XDPDefault` policy for SnapVault relationships.

4. Create a SnapVault relationship: `snapmirror create -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -type XDP -schedule schedule_name -policy XDPDefault`

In ONTAP 9.4 and earlier, if the policy is not specified with the `snapmirror create` command, the `MirrorAllSnapshots` policy is used by default. In ONTAP 9.5, if the policy is not specified with the `snapmirror create` command, the `MirrorAndVault` policy is used by default.

```
cluster2::> snapmirror create -source-path vss:srcFG -destination-path vsd:dstFG -type XDP -schedule Daily -policy XDPDefault
```

5. From the destination cluster, initialize the SnapVault relationship by performing a baseline transfer: `snapmirror initialize -destination-path dest_svm:dest_flexgroup`

```
cluster2::> snapmirror initialize -destination-path vsd:dst
Operation is queued: snapmirror initialize of destination "vsd:dst".
```

## Create a unified data protection relationship for FlexGroup volumes

Beginning with ONTAP 9.3, you can create and configure SnapMirror unified data protection relationships to configure disaster recovery and archiving on the same destination volume.

### What you'll need

You must be aware of the considerations for creating unified data protection relationships for FlexGroup volumes.

[Considerations for creating a SnapVault backup relationship and a unified data protection relationship for FlexGroup volumes](#)

### Steps

1. Create a destination FlexGroup volume of type `DP` that has the same number of constituents as that of the source FlexGroup volume:
  - a. From the source cluster, determine the number of constituents in the source FlexGroup volume:

```
volume show -volume volume_name* -is-constituent true
```

```

cluster1::> volume show -volume srcFG* -is-constituent true
Vserver    Volume                Aggregate    State    Type    Size
Available  Used%
-----
vss        srcFG                  -           online   RW      400TB
172.86GB   56%
vss        srcFG__0001           Aggr_cmode  online   RW      25GB
10.86TB    56%
vss        srcFG__0002           aggr1       online   RW      25TB
10.86TB    56%
vss        srcFG__0003           Aggr_cmode  online   RW      25TB
10.72TB    57%
vss        srcFG__0004           aggr1       online   RW      25TB
10.73TB    57%
vss        srcFG__0005           Aggr_cmode  online   RW      25TB
10.67TB    57%
vss        srcFG__0006           aggr1       online   RW      25TB
10.64TB    57%
vss        srcFG__0007           Aggr_cmode  online   RW      25TB
10.63TB    57%
...

```

- b. From the destination cluster, create a destination FlexGroup volume of type DP with the same number of constituents as that of the source FlexGroup volume.

```

cluster2::> volume create -vserver vsd -aggr-list aggr1,aggr2 -aggr
-list-multiplier 8 -size 400TB -type DP dstFG

Warning: The FlexGroup volume "dstFG" will be created with the
following number of constituents of size 25TB: 16.
Do you want to continue? {y|n}: y
[Job 766] Job succeeded: Successful

```

- c. From the destination cluster, verify the number of constituents in the destination FlexGroup volume:  
 volume show -volume volume\_name\* -is-constituent true

```
cluster2::> volume show -volume dstFG* -is-constituent true
Vserver    Volume          Aggregate      State      Type      Size
Available Used%
-----
vsd        dstFG            -              online     RW        400TB
172.86GB  56%
vsd        dstFG__0001     Aggr_cmode    online     RW        25GB
10.86TB   56%
vsd        dstFG__0002     aggr1         online     RW        25TB
10.86TB   56%
vsd        dstFG__0003     Aggr_cmode    online     RW        25TB
10.72TB   57%
vsd        dstFG__0004     aggr1         online     RW        25TB
10.73TB   57%
vsd        dstFG__0005     Aggr_cmode    online     RW        25TB
10.67TB   57%
vsd        dstFG__0006     aggr1         online     RW        25TB
10.64TB   57%
vsd        dstFG__0007     Aggr_cmode    online     RW        25TB
10.63TB   57%
...
```

2. Create a job schedule: `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

For the `-month`, `-dayofweek`, and `-hour` options, you can specify `all` to run the job every month, every day of the week, and every hour, respectively.

The following example creates a job schedule named `my_weekly` that runs on Saturdays at 3:00 a.m.:

```
cluster1::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

3. Create a custom policy of type `mirror-vault`, and then define a rule for the mirror and vault policy:
  - a. Create a custom policy of type `mirror-vault` for the unified data protection relationship:

```
snapmirror policy create -vserver svm_name -policy policy_name -type mirror-vault
```
  - b. Define a rule for the mirror and vault policy that determines which Snapshot copies are transferred during initialization and update operations:

```
snapmirror policy add-rule -vserver svm_name -policy policy_for_rule - snapmirror-label snapmirror-label -keep retention_count -schedule schedule
```

If you do not specify a custom policy, the `MirrorAndVault` policy is used for unified data protection relationships.

4. Create a unified data protection relationship: `snapmirror create -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -type XDP -schedule schedule_name -policy MirrorAndVault`

In ONTAP 9.4 and earlier, if the policy is not specified with the `snapmirror create` command, the `MirrorAllSnapshots` policy is used by default. In ONTAP 9.5, if the policy is not specified with the `snapmirror create` command, the `MirrorAndVault` policy is used by default.

```
cluster2::> snapmirror create -source-path vss:srcFG -destination-path vsd:dstFG -type XDP -schedule Daily -policy MirrorAndVault
```

5. From the destination cluster, initialize the unified data protection relationship by performing a baseline transfer: `snapmirror initialize -destination-path dest_svm:dest_flexgroup`

```
cluster2::> snapmirror initialize -destination-path vsd:dstFG
Operation is queued: snapmirror initialize of destination "vsd:dstFG".
```

## Create an SVM disaster recovery relationship for FlexGroup volumes

Beginning with ONTAP 9.9.1, you can create SVM disaster recovery (SVM DR) relationships using FlexGroup volumes. An SVM DR relationship provides redundancy and the ability to recover FlexGroups in the event of a disaster by synchronizing and replicating the SVM configuration and its data. A SnapMirror license is required for SVM DR.

### Before you begin

You should be aware of the conditions when you cannot create a FlexGroup SVM DR relationship.

- A FlexClone FlexGroup configuration exists
- A FlexGroup volume contains a FabricPool configuration
- The FlexGroup volume is part of a fanout or cascading relationship

### About this task

- All nodes in both clusters must be running the same ONTAP version as the node on which SVM DR support was added (ONTAP 9.9.1 or later).
- The SVM DR relationship between the primary and secondary sites should be healthy and should have enough space on both the primary and secondary SVMs to support the FlexGroup volumes.

For information about creating an SVM DR relationship, see [Manage SnapMirror SVM replication](#).

### Steps

1. Create an SVM DR relationship, or use an existing relationship.

#### [Replicate an entire SVM configuration](#)

2. Create a FlexGroup volume on the primary site with the required number of constituents.

## Creating a FlexGroup volume.

Wait until FlexGroup and all of its constituents are created before proceeding.

3. To replicate the FlexGroup volume, update the SVM at the secondary site: `snapmirror update -destination-path destination_svm_name: -source-path source_svm_name:`  
+ You can also check if a scheduled SnapMirror update already exists by entering `snapmirror show -fields schedule`
4. From the secondary site, verify that the SnapMirror relationship is healthy: `snapmirror show`

```
cluster2::> snapmirror show
```

Progress	Source	Destination	Mirror	Relationship	Total		
Last	Path	Type	Path	State	Status	Progress	Healthy
Updated							
	vs1:	XDP	vs1_dst:	Snapmirrored			
				Idle	-	true	-

5. From the secondary site, verify that the new FlexGroup volume and its constituents exist: `snapmirror show -expand`



```
cluster2::> snapmirror show -expand
```

Progress

Source		Destination	Mirror	Relationship	Total		
Last							
Path	Type	Path	State	Status	Progress	Healthy	
Updated							
-----	----	-----	-----	-----	-----	-----	-----
-----							
vs1:	XDP	vs1_dst:	Snapmirrored	Idle	-	true	-
vs1:fg_src	XDP	vs1_dst:fg_src	Snapmirrored	Idle	-	true	-
vs1:fg_src__0001	XDP	vs1_dst:fg_src__0001	Snapmirrored	Idle	-	true	-
vs1:fg_src__0002	XDP	vs1_dst:fg_src__0002	Snapmirrored	Idle	-	true	-
vs1:fg_src__0003	XDP	vs1_dst:fg_src__0003	Snapmirrored	Idle	-	true	-
vs1:fg_src__0004	XDP	vs1_dst:fg_src__0004	Snapmirrored	Idle	-	true	-

6 entries were displayed.

## Transition an existing FlexGroup SnapMirror relationship to SVM DR

You can create a FlexGroup SVM DR relationship by transitioning an existing FlexGroup volume SnapMirror relationship.

### What you'll need

- The FlexGroup volume SnapMirror relationship is in a healthy state.
- The source and destination FlexGroup volumes have the same name.

### Steps

1. From the SnapMirror destination, resynchronize the FlexGroup level SnapMirror relationship: `snapmirror resync`

2. Create the FlexGroup SVM DR SnapMirror relationship. Use the same SnapMirror policy which is configured on the FlexGroup volume SnapMirror relationships: `snapmirror create -destination -path dest_svm: -source-path src_svm: -identity-preserve true -policy MirrorAllSnapshots`

You must use the `-identity-preserve true` option of the `snapmirror create` command when you create your replication relationship.

1. Verify the relationship is broken off: `snapmirror show -destination-path dest_svm: -source -path src_svm:`

```
snapmirror show -destination-path fg_vs_renamed: -source-path fg_vs:
```

Progress

Source	Destination	Mirror	Relationship	Total		
Last Path	Type	Path	State	Status	Progress	Healthy
Updated						
fg_vs:	XDP	fg_vs1_renamed:	Broken-off	Idle	-	true -

2. Stop the destination SVM: `vserver stop -vserver vs_name`

```
vserver stop -vserver fg_vs_renamed
[Job 245] Job is queued: Vserver Stop fg_vs_renamed.
[Job 245] Done
```

3. Resynchronize the SVM SnapMirror relationship: `snapmirror resync -destination-path dest_svm: -source-path src_svm:`

```
snapmirror resync -destination-path fg_vs_renamed: -source-path fg_vs:
Warning: This Vserver has volumes which are the destination of FlexVol
or FlexGroup SnapMirror relationships. A resync on the Vserver
SnapMirror relationship will cause disruptions in data access
```

4. Verify that the SVM DR level SnapMirror relationship reaches a healthy idle state: `snapmirror show -expand`
5. Verify that the FlexGroup SnapMirror relationship is in a healthy state: `snapmirror show`

## Convert a FlexVol volume to a FlexGroup volume within an SVM-DR relationship

Beginning with ONTAP 9.10.1, you can convert a FlexVol volume to a FlexGroup volume on an SVM-DR source.

### What you'll need

- The FlexVol volume that is being converted must be online.
- The operations and configurations on the FlexVol volume must be compatible with the conversion process.

An error message is generated if the FlexVol volume has any incompatibility, and the volume conversion is cancelled. You can take corrective actions and retry the conversion.

For more details, see [Considerations for converting FlexVol volumes to FlexGroup volumes](#)

### Steps

1. From the destination, update the SVM-DR relationship:

```
snapmirror update -destination-path destination_svm_name: -source-path source_svm_name:
```

2. Ensure that the SVM-DR relationship is in a SnapMirrored state and is not broken-off:

```
snapmirror show
```

3. From the destination SVM, verify that the FlexVol volume is ready for conversion:

```
volume conversion start -vserver svm_name -volume vol_name -check-only true
```

4. From the destination, disable transfers on the SVM-DR relationship:

```
snapmirror quiesce -destination-path dest_svm:
```

5. Start the conversion:

```
volume conversion start -vserver svm_name -volume vol_name
```

6. Verify that the conversion is successful:

```
volume show vol_name -fields -volume-style-extended,state
```

```
cluster-1::*> volume show my_volume -fields volume-style-extended,state

vserver   volume      state      volume-style-extended
-----
vs0       my_volume  online    flexgroup
```

7. From the destination cluster, resume transfers for the relationship:

```
snapmirror resume -destination-path dest_svm:
```

8. From the destination cluster, perform an update to propagate the conversion to the destination:

```
snapmirror update -destination-path dest_svm:
```

9. Ensure that the SVM-DR relationship is in a SnapMirrored state and is not broken off:

```
snapmirror show
```

10. Ensure the conversion occurred on the destination:

```
volume show vol_name -fields -volume-style-extended,state
```

```
cluster-2::*> volume show my_volume -fields volume-style-extended,state

vserver      volume      state      volume-style-extended
-----      -
vs0_dst      my_volume   online     flexgroup
```

### Considerations for creating SnapMirror cascade and fanout relationships for FlexGroups

There are support considerations and limitations you should keep in mind when creating SnapMirror cascade and fanout relationships for FlexGroup volumes.

#### Considerations for creating cascading relationships

- Each relationship can be either an inter cluster or intra cluster relationship.
- All asynchronous policy types, including async-mirror, mirror-vault, and vault, are supported for both relationships.
- Only "MirrorAllSnapshots," not "MirrorLatest" async-mirror policies are supported.
- Concurrent updates of cascaded XDP relationships is supported.
- Supports removing A to B and B to C and resync A to C or resync C to A
- A and B FlexGroup volumes also support fanout when all nodes are running ONTAP 9.9.1 or later.
- Restore operations from B or C FlexGroup volumes are supported.
- Transfers on FlexGroup relationships are not support while the destination is the source of a restore relationship.
- The destination of a FlexGroup restore cannot be the destination of any other FlexGroup relationship.
- FlexGroup file restore operations have the same restrictions as regular FlexGroup restore operations.
- All nodes in the cluster where the B and C FlexGroup volumes reside must be running ONTAP 9.9.1 or later.
- All expand and auto expand functionality is supported.
- In a cascade configuration such as A to B to C, if A to B and B to C have different numbers of constituent SnapMirror relationships, then an abort operation from the source is not supported for the B to C SnapMirror relationship.
- System Manager does not support cascading relationships in ONTAP 9.9.1.
- When converting an A to B to C set of FlexVol relationship to a FlexGroup relationship, you must convert the B to C hop first.

- All FlexGroup cascade configurations for relationships with policy types supported by REST are also supported by REST APIs in cascading FlexGroup configurations.
- As with FlexVol relationships, FlexGroup cascading is not supported by the `snapmirror protect` command.

#### Considerations for creating fanout relationships

- Two or more FlexGroup fanout relationships are supported; for example, A to B, A to C, with a maximum of 8 fanout legs.
- Each relationship can be either intercluster or intracluster.
- Concurrent updates are supported for the two relationships.
- All expand and auto expand functionality is supported.
- If the fanout legs of the relationship have different numbers of constituent SnapMirror relationships, then an abort operation from the source is not supported for the A to B and A to C relationships.
- All nodes in the cluster where the source and destination FlexGroups reside must be running ONTAP 9.9.1 or later.
- All asynchronous policy types currently supported for FlexGroup SnapMirror are supported in fanout relationships.
- You can perform restore operations from B to C FlexGroups.
- All fanout configurations with policy types supported by rest are also supported for REST APIs in FlexGroup fanout configurations.

#### Considerations for creating a SnapVault backup relationship and a unified data protection relationship for FlexGroup volumes

You must be aware of the considerations for creating a SnapVault backup relationship and unified data protection relationship for FlexGroup volumes.

- You can resynchronize a SnapVault backup relationship and a unified data protection relationship by using the `-preserve` option that enables you to preserve Snapshot copies on the destination volume that are newer than the latest common Snapshot copy.
- Long-term retention is not supported with FlexGroup volumes.

Long-term retention enables creating Snapshot copies directly on the destination volume without requiring to store the Snapshot copies on the source volume.

- The `snapshot expiry-time` option is not supported for FlexGroup volumes.
- Storage efficiency cannot be configured on the destination FlexGroup volume of a SnapVault backup relationship and unified data protection relationship.
- You cannot rename Snapshot copies of a SnapVault backup relationship and unified data protection relationship for FlexGroup volumes.
- A FlexGroup volume can be the source volume of only one backup relationship or restore relationship.

A FlexGroup volume cannot be the source of two SnapVault relationships, two restore relationships, or a SnapVault backup relationship and a restore relationship.

- If you delete a Snapshot copy on the source FlexGroup volume and re-create a Snapshot copy with the same name, the next update transfer to the destination FlexGroup volume fails if the destination volume

has a Snapshot copy of the same name.

This is because Snapshot copies cannot be renamed for FlexGroup volumes.

### Monitor SnapMirror data transfers for FlexGroup volumes

You should periodically monitor the status of the FlexGroup volume SnapMirror relationships to verify that the destination FlexGroup volume is updated periodically as per the specified schedule.

#### About this task

You must perform this task from the destination cluster.

#### Steps

1. View the SnapMirror relationship status of all FlexGroup volume relationships: `snapmirror show -relationship-group-type flexgroup`

```
cluster2::> snapmirror show -relationship-group-type flexgroup

Progress
Source          Destination Mirror  Relationship  Total
Last
Path           Type  Path           State  Status           Progress  Healthy
Updated
-----
-----
vss:s          XDP  vsd:d          Snapmirrored
                               Idle           -         true  -
vss:s2         XDP  vsd:d2         Uninitialized
                               Idle           -         true  -
2 entries were displayed.
```

2. View the SnapMirror relationship status for each constituent in the FlexGroup volume: `snapmirror show -expand`

```
cluster2::> snapmirror show -expand
```

Progress

Source		Destination	Mirror	Relationship	Total		
Last							
Path	Type	Path	State	Status	Progress	Healthy	
Updated							
-----	----	-----	-----	-----	-----	-----	-----
vss:s	XDP	vsd:d	Snapmirrored	Idle	-	true	-
vss:s__0001	XDP	vsd:d__0001	Snapmirrored	Idle	-	true	-
vss:s__0002	XDP	vsd:d__0002	Snapmirrored	Idle	-	true	-
vss:s__0003	XDP	vsd:d__0003	Snapmirrored	Idle	-	true	-
vss:s__0004	XDP	vsd:d__0004	Snapmirrored	Idle	-	true	-
vss:s__0005	XDP	vsd:d__0005	Snapmirrored	Idle	-	true	-
vss:s__0006	XDP	vsd:d__0006	Snapmirrored	Idle	-	true	-
vss:s__0007	XDP	vsd:d__0007	Snapmirrored	Idle	-	true	-
vss:s__0008	XDP	vsd:d__0008	Snapmirrored	Idle	-	true	-
...							

3. If the SnapMirror transfer fails, identify the FlexGroup volume constituent for which the transfer failed and the reason for the error: `snapmirror show -fields last-transfer-error -expand`

```

cluster2::> snapmirror show -fields last-transfer-error -expand
source-path destination-path last-transfer-error
-----
-----
vss:s          vsd:d          Group Update failed (Failed to complete
update operation on one or more item relationships.)
vss:s__0001 vsd:d__0001      -
vss:s__0002 vsd:d__0002      -
vss:s__0003 vsd:d__0003      Failed to get information for source volume
"vss:s__0003" for setup of transfer. (Failed to get volume attributes
for e2de028c-8049-11e6-96ea-005056851ca2:s__0003. (Volume is offline))
vss:s__0004 vsd:d__0004      -
vss:s__0005 vsd:d__0005      -
vss:s__0006 vsd:d__0006      -
vss:s__0007 vsd:d__0007      -
vss:s__0008 vsd:d__0008      -
9 entries were displayed.

```

After rectifying the issue, you must rerun the SnapMirror operation.

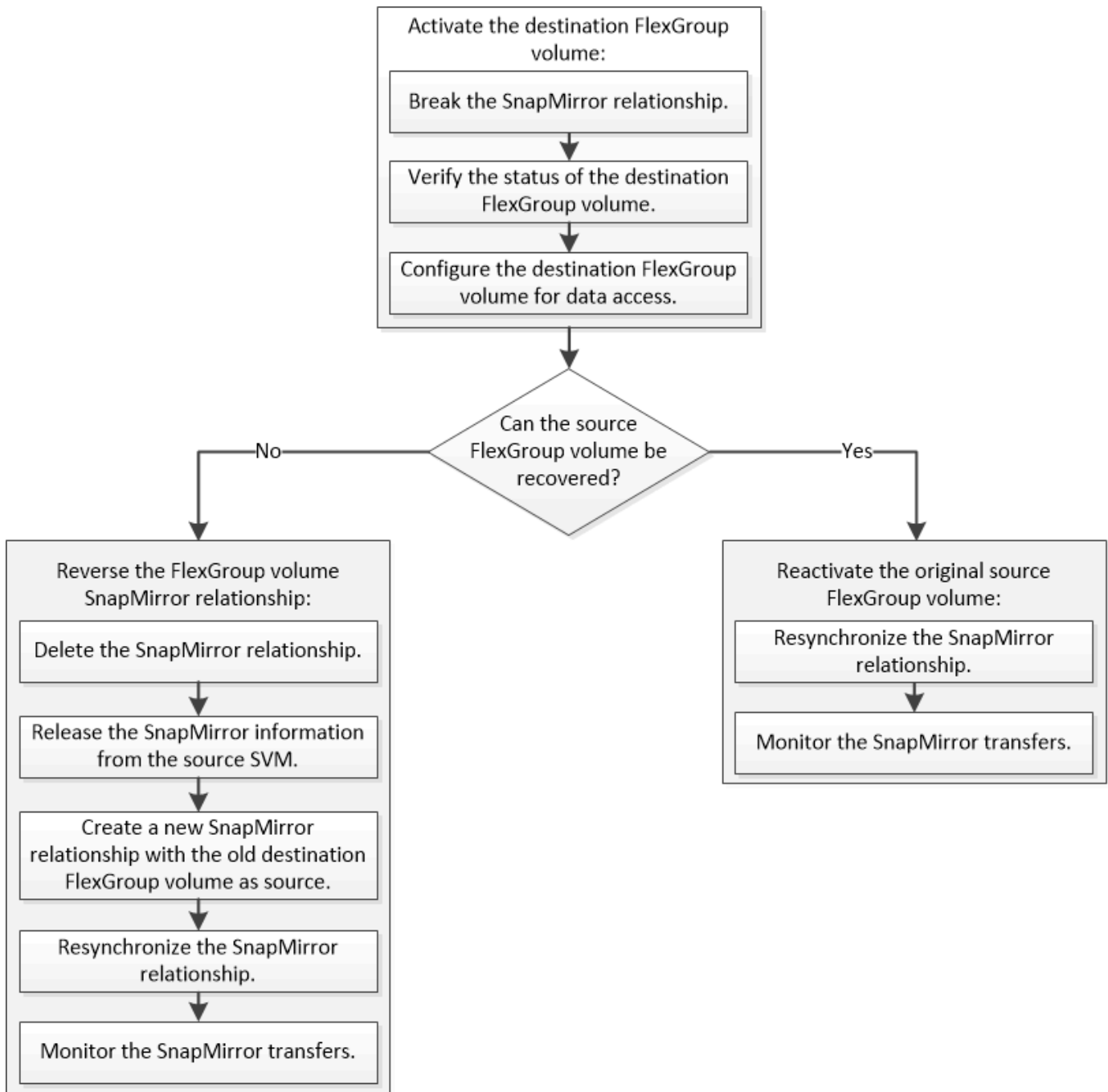
## Manage data protection operations for FlexGroup volumes

### Disaster recovery for FlexGroup volumes

#### Disaster recovery workflow for FlexGroup volumes

When a disaster strikes on the source FlexGroup volume, you should activate the destination FlexGroup volume and redirect client access. Depending on whether the source FlexGroup volume can be recovered, you should either reactivate the source FlexGroup volume or reverse the SnapMirror relationship.





### About this task

Client access to the destination FlexGroup volume is blocked for a brief period when some SnapMirror operations, such as SnapMirror break and resynchronization, are running. If the SnapMirror operation fails, it is possible that some of the constituents remain in this state and access to the FlexGroup volume is denied. In such cases, you must retry the SnapMirror operation.

### Activate the destination FlexGroup volume

When the source FlexGroup volume is unable to serve data due to events such as data corruption, accidental deletion or an offline state, you must activate the destination FlexGroup volume to provide data access until you recover the data on the source FlexGroup volume. Activation involves stopping future SnapMirror data transfers and breaking the SnapMirror relationship.

## About this task

You must perform this task from the destination cluster.

### Steps

1. Disable future transfers for the FlexGroup volume SnapMirror relationship: `snapmirror quiesce dest_svm:dest_flexgroup`

```
cluster2::> snapmirror quiesce -destination-path vsd:dst
```

2. Break the FlexGroup volume SnapMirror relationship: `snapmirror break dest_svm:dest_flexgroup`

```
cluster2::> snapmirror break -destination-path vsd:dst
```

3. View the status of the SnapMirror relationship: `snapmirror show -expand`

```
cluster2::> snapmirror show -expand
```

```
Progress
Source          Destination Mirror Relationship Total
Last
Path           Type Path           State Status           Progress Healthy
Updated
-----
-----
vss:s           XDP vsd:dst           Broken-off
                  Idle              -              true -
vss:s__0001    XDP vsd:dst__0001    Broken-off
                  Idle              -              true -
vss:s__0002    XDP vsd:dst__0002    Broken-off
                  Idle              -              true -
vss:s__0003    XDP vsd:dst__0003    Broken-off
                  Idle              -              true -
vss:s__0004    XDP vsd:dst__0004    Broken-off
                  Idle              -              true -
vss:s__0005    XDP vsd:dst__0005    Broken-off
                  Idle              -              true -
vss:s__0006    XDP vsd:dst__0006    Broken-off
                  Idle              -              true -
vss:s__0007    XDP vsd:dst__0007    Broken-off
                  Idle              -              true -
vss:s__0008    XDP vsd:dst__0008    Broken-off
                  Idle              -              true -
...

```

The SnapMirror relationship status of each constituent is Broken-off.

4. Verify that the destination FlexGroup volume is read/write: `volume show -vserver svm_name`

```

cluster2::> volume show -vserver vsd
Vserver   Volume           Aggregate      State      Type      Size
Available Used%
-----
vsd       dst              -             online    **RW**    2GB
1.54GB   22%
vsd       d2               -             online    DP         2GB
1.55GB   22%
vsd       root_vs0        aggr1         online    RW         100MB
94.02MB  5%
3 entries were displayed.

```

5. Redirect clients to the destination FlexGroup volume.

#### Reactivate the original source FlexGroup volume after disaster

When the source FlexGroup volume becomes available, you can resynchronize the original source and original destination FlexGroup volumes. Any new data on the destination FlexGroup volume is lost.

#### About this task

Any active quota rules on the destination volume are deactivated and the quota rules are deleted before resynchronization is performed.

You can use the `volume quota policy rule create` and `volume quota modify` commands to create and reactivate quota rules after the resynchronization operation is complete.

#### Steps

1. From the destination cluster, resynchronize the FlexGroup volume SnapMirror relationship: `snapmirror resync -destination-path dst_svm:dest_flexgroup`
2. View the status of the SnapMirror relationship: `snapmirror show -expand`

```
cluster2::> snapmirror show -expand
```

Progress

Source		Destination	Mirror	Relationship	Total		
Last							
Path	Type	Path	State	Status	Progress	Healthy	
Updated							
vss:s	XDP	vsd:dst	Snapmirrored	Idle	-	true	-
vss:s__0001	XDP	vsd:dst__0001	Snapmirrored	Idle	-	true	-
vss:s__0002	XDP	vsd:dst__0002	Snapmirrored	Idle	-	true	-
vss:s__0003	XDP	vsd:dst__0003	Snapmirrored	Idle	-	true	-
vss:s__0004	XDP	vsd:dst__0004	Snapmirrored	Idle	-	true	-
vss:s__0005	XDP	vsd:dst__0005	Snapmirrored	Idle	-	true	-
vss:s__0006	XDP	vsd:dst__0006	Snapmirrored	Idle	-	true	-
vss:s__0007	XDP	vsd:dst__0007	Snapmirrored	Idle	-	true	-
vss:s__0008	XDP	vsd:dst__0008	Snapmirrored	Idle	-	true	-
...							

The SnapMirror relationship status of each constituent is Snapmirrored.

### Reverse a SnapMirror relationship between FlexGroup volumes during disaster recovery

When a disaster disables the source FlexGroup volume of a SnapMirror relationship, you can use the destination FlexGroup volume to serve data while you repair or replace the source FlexGroup volume. After the source FlexGroup volume is online, you can make the original source FlexGroup volume a read-only destination and reverse the SnapMirror relationship.

#### About this task

Any active quota rules on the destination volume are deactivated and the quota rules are deleted before resynchronization is performed.

You can use the `volume quota policy rule create` and `volume quota modify` commands to create and reactivate quota rules after the resynchronization operation is complete.

## Steps

1. On the original destination FlexGroup volume, remove the data protection mirror relationship between the source FlexGroup volume and the destination FlexGroup volume: `snapmirror delete -destination -path svm_name:volume_name`

```
cluster2::> snapmirror delete -destination-path vsd:dst
```

2. On the original source FlexGroup volume, remove the relationship information from the source FlexGroup volume: `snapmirror release -destination-path svm_name:volume_name -relationship -info-only`

After deleting a SnapMirror relationship, you must remove the relationship information from the source FlexGroup volume before attempting a resynchronization operation.

```
cluster1::> snapmirror release -destination-path vsd:dst -relationship -info-only true
```

3. On the new destination FlexGroup volume, create the mirror relationship: `snapmirror create -source-path src_svm_name:volume_name -destination-path dst_svm_name:volume_name -type XDP -policy MirrorAllSnapshots`

```
cluster1::> snapmirror create -source-path vsd:dst -destination-path vss:src -type XDP -policy MirrorAllSnapshots
```

4. On the new destination FlexGroup volume, resynchronize the source FlexGroup: `snapmirror resync -source-path svm_name:volume_name`

```
cluster1::> snapmirror resync -source-path vsd:dst
```

5. Monitor the SnapMirror transfers: `snapmirror show -expand`

```
cluster2::> snapmirror show -expand
```

Progress

Source		Destination	Mirror	Relationship	Total		
Last							
Path	Type	Path	State	Status	Progress	Healthy	
Updated							
-----	----	-----	-----	-----	-----	-----	-----
vsd:dst	XDP	vss:src		Snapmirrored			
				Idle	-	true	-
vss:dst__0001	XDP	vss:src__0001		Snapmirrored			
				Idle	-	true	-
vsd:dst__0002	XDP	vss:src__0002		Snapmirrored			
				Idle	-	true	-
vsd:dst__0003	XDP	vss:src__0003		Snapmirrored			
				Idle	-	true	-
vsd:dst__0004	XDP	vss:src__0004		Snapmirrored			
				Idle	-	true	-
vsd:dst__0005	XDP	vss:src__0005		Snapmirrored			
				Idle	-	true	-
vsd:dst__0006	XDP	vss:src__0006		Snapmirrored			
				Idle	-	true	-
vsd:dst__0007	XDP	vss:src__0007		Snapmirrored			
				Idle	-	true	-
vsd:dst__0008	XDP	vss:src__0008		Snapmirrored			
				Idle	-	true	-
...							

The SnapMirror relationship status of each constituent shows as `Snapmirrored` that indicates that the resynchronization was successful.

## Expand FlexGroup volumes in a SnapMirror relationship

### Expand FlexGroup volumes in a SnapMirror relationship

Beginning with ONTAP 9.3, you can expand the source FlexGroup volume and destination FlexGroup volume that are in a SnapMirror relationship by adding new constituents to the volumes. You can expand the destination volumes either manually or automatically.

#### About this task

- After expansion, the number of constituents in the source FlexGroup volume and destination FlexGroup volume of a SnapMirror relationship must match.

If the number of constituents in the volumes does not match, the SnapMirror transfers fail.

- You should not perform any SnapMirror operation when the expansion process is in progress.
- If a disaster strikes before the expansion process is complete, you must break the SnapMirror relationship and wait until the operation succeeds.



You should break the SnapMirror relationship when the expansion process is in progress only in the case of a disaster. In the case of a disaster, the break operation can take some time to complete. You should wait for the break operation to get completed successfully before performing a resync operation. If the break operation fails, you must retry the break operation. If the break operation fails, some of the new constituents might remain in the destination FlexGroup volume after the break operation. It is best to delete these constituents manually before proceeding further.

### Expand the source FlexGroup volume of a SnapMirror relationship

Beginning with ONTAP 9.3, you can expand the source FlexGroup volume of a SnapMirror relationship by adding new constituents to the source volume. You can expand the source volume in the same way that you expand a regular FlexGroup volume (read-write volume).

#### Steps

1. Expand the source FlexGroup volume: `volume expand -vserver vs_server_name -volume fg_src -aggr-list aggregate name,... [-aggr-list-multiplier constituents_per_aggr]`

```
cluster1::> volume expand -volume src_fg -aggr-list aggr1 -aggr-list
-multiplier 2 -vserver vs_src
```

```
Warning: The following number of constituents of size 50GB will be added
to FlexGroup "src_fg": 2.
```

```
Expanding the FlexGroup will cause the state of all Snapshot copies to
be set to "partial".
```

```
Partial Snapshot copies cannot be restored.
```

```
Do you want to continue? {y|n}: Y
```

```
[Job 146] Job succeeded: Successful
```

The state of all of the Snapshot copies that are taken before the volume is expanded changes to partial.

### Expand the destination FlexGroup volume of a SnapMirror relationship

You can expand the destination FlexGroup volume and reestablish the SnapMirror relationship either automatically or manually. By default, the SnapMirror relationship is set for automatic expansion, and the destination FlexGroup volume expands automatically if the source volume expands.

#### What you'll need

- The source FlexGroup volume must have been expanded.
- The SnapMirror relationship must be in the `SnapMirrored` state.



The SnapMirror relationship must not be broken or deleted.

### About this task

- When the destination FlexGroup volume is created, the volume is set up for automatic expansion by default.

You can modify the destination FlexGroup volume for manual expansion, if required.



The best practice is to expand the destination FlexGroup volume automatically.

- All SnapMirror operations fail until both the source FlexGroup volume and destination FlexGroup volume have expanded and have the same number of constituents.
- If you expand the destination FlexGroup volume after the SnapMirror relationship is broken or deleted, you cannot resync the original relationship again.

If you intend to reuse the destination FlexGroup volume, you must not expand the volume after deleting the SnapMirror relationship.

### Choices

- Perform an update transfer to expand the destination FlexGroup volume automatically:
  - a. Perform a SnapMirror update transfer: `snapmirror update -destination-path svm:vol_name`
  - b. Verify that the status of the SnapMirror relationship is in the SnapMirrored state: `snapmirror show`

```
cluster2::> snapmirror show

Progress
Source          Destination Mirror Relationship Total
Last
Path           Type Path           State Status Progress
Healthy Updated
-----
vs_src:src_fg
                XDP vs_dst:dst_fg
                               Snapmirrored
                               Idle           -           true
-
```

Based on the size and availability of aggregates, the aggregates are automatically selected, and new constituents that match the constituents of the source FlexGroup volume are added to the destination FlexGroup volume. After expansion, a resynchronization operation is automatically triggered.

- Expand the destination FlexGroup volume manually:
  - a. If the SnapMirror relationship is in the auto-expand mode, set the SnapMirror relationship to the manual expand mode: `snapmirror modify -destination-path svm:vol_name -is-auto-expand`

-enabled false

```
cluster2::> snapmirror modify -destination-path vs_dst:dst_fg -is
-auto-expand-enabled false
Operation succeeded: snapmirror modify for the relationship with
destination "vs_dst:dst_fg".
```

- b. Quiesce the SnapMirror relationship: `snapmirror quiesce -destination-path svm:vol_name`

```
cluster2::> snapmirror quiesce -destination-path vs_dst:dst_fg
Operation succeeded: snapmirror quiesce for destination
"vs_dst:dst_fg".
```

- c. Expand the destination FlexGroup volume: `volume expand -vserver vs_server_name -volume fg_name -aggr-list aggregate name,... [-aggr-list-multiplier constituents_per_aggr]`

```
cluster2::> volume expand -volume dst_fg -aggr-list aggr1 -aggr-list
-multiplier 2 -vserver vs_dst

Warning: The following number of constituents of size 50GB will be
added to FlexGroup "dst_fg": 2.
Do you want to continue? {y|n}: y
[Job 68] Job succeeded: Successful
```

- d. Resynchronize the SnapMirror relationship: `snapmirror resync -destination-path svm:vol_name`

```
cluster2::> snapmirror resync -destination-path vs_dst:dst_fg
Operation is queued: snapmirror resync to destination
"vs_dst:dst_fg".
```

- e. Verify that the status of the SnapMirror relationship is SnapMirrored: `snapmirror show`

```

cluster2::> snapmirror show

Progress
Source          Destination Mirror Relationship Total
Last
Path           Type Path           State Status Progress
Healthy Updated
-----
vs_src:src_fg
                XDP vs_dst:dst_fg
                               Snapmirrored
                               Idle           -           true
-

```

## Perform a SnapMirror single file restore from a FlexGroup volume

Beginning with ONTAP 9.8, you can restore a single file from a FlexGroup SnapMirror vault or from a UDP destination.

### About this task

- You can restore from a FlexGroup volume of any geometry to FlexGroup volume of any geometry
- Only one file per restore operation is supported
- You can restore to either the original source FlexGroup volume or to a new FlexGroup volume
- Remote fenced file lookup is not supported.

Single file restore fails if the source file is fenced.

- You can restart or clean up an aborted single file restore
- You should clean up a failed single file restore transfer by using the `clean-up-failure` option of the `snapmirror restore` command
- Expansion of FlexGroup volumes is supported when a FlexGroup single file restore is in progress or in an aborted state

### Steps

1. Restore a file from a FlexGroup volume: `snapmirror restore -destination-path destination_path -source-path source_path -file-list /f1 -throttle throttle -source-snapshot snapshot`

The following is an example of a FlexGroup volume single file restore operation.

```

vserverA::> snapmirror restore -destination-path vs0:fg2 -source-path
vs0:fgd -file-list /f1 -throttle 5 -source-snapshot snapmirror.81072ce1-
d57b-11e9-94c0-005056a7e422_2159190496.2019-09-19_062631
[Job 135] Job is queued: snapmirror restore from source "vs0:fgd" for

```

```
the snapshot snapmirror.81072ce1-d57b-11e9-94c0-005056a7e422_2159190496.2019-09-19_062631.
```

```
vserverA::> snapmirror show
```

Source		Destination	Mirror	Relationship		
Total	Last					
Path	Type	Path	State	Status		Progress
Healthy	Updated					
vs0:v1d	RST	vs0:v2	-	Transferring	Idle	83.12KB
true	09/19 11:38:42					

```
vserverA::*> snapmirror show vs0:fg2
```

```
Source Path: vs0:fgd
Source Cluster: -
Source Vserver: vs0
Source Volume: fgd
Destination Path: vs0:fg2
Destination Cluster: -
Destination Vserver: vs0
Destination Volume: fg2
Relationship Type: RST
Relationship Group Type: none
Managing Vserver: vs0
SnapMirror Schedule: -
SnapMirror Policy Type: -
SnapMirror Policy: -
Tries Limit: -
Throttle (KB/sec): unlimited
Current Transfer Throttle (KB/sec): 2
Mirror State: -
Relationship Status: Transferring
File Restore File Count: 1
File Restore File List: f1
Transfer Snapshot: snapmirror.81072ce1-d57b-11e9-94c0-005056a7e422_2159190496.2019-09-19_062631
Snapshot Progress: 2.87MB
Total Progress: 2.87MB
Network Compression Ratio: 1:1
Snapshot Checkpoint: 2.97KB
Newest Snapshot: -
Newest Snapshot Timestamp: -
Exported Snapshot: -
Exported Snapshot Timestamp: -
```

```
Healthy: true
Physical Replica: -
Relationship ID: e6081667-dacb-11e9-94c0-005056a7e422
Source Vserver UUID: 81072ce1-d57b-11e9-94c0-005056a7e422
Destination Vserver UUID: 81072ce1-d57b-11e9-94c0-005056a7e422
Current Operation ID: 138f12e6-dacc-11e9-94c0-005056a7e422
Transfer Type: cg_file_restore
Transfer Error: -
Last Transfer Type: -
Last Transfer Error: -
Last Transfer Error Codes: -
Last Transfer Size: -
Last Transfer Network Compression Ratio: -
Last Transfer Duration: -
Last Transfer From: -
Last Transfer End Timestamp: -
Unhealthy Reason: -
Progress Last Updated: 09/19 07:07:36
Relationship Capability: 8.2 and above
Lag Time: -
Current Transfer Priority: normal
SMTape Operation: -
Constituent Relationship: false
Destination Volume Node Name: vserverA
Identity Preserve Vserver DR: -
Number of Successful Updates: 0
Number of Failed Updates: 0
Number of Successful Resyncs: 0
Number of Failed Resyncs: 0
Number of Successful Breaks: 0
Number of Failed Breaks: 0
Total Transfer Bytes: 0
Total Transfer Time in Seconds: 0
Source Volume MSIDs Preserved: -
OpMask: ffffffffffffffff
Is Auto Expand Enabled: -
Source Endpoint UUID: -
Destination Endpoint UUID: -
Is Catalog Enabled: false
```

### Restore a FlexGroup volume from a SnapVault backup

You can perform a full-volume restore operation of FlexGroup volumes from a Snapshot copy in the SnapVault secondary volume. You can restore the FlexGroup volume either to the original source volume or to a new FlexGroup volume.

## Before you begin

You must be aware of certain considerations when you restore from SnapVault backups for FlexGroup volumes.

- Only baseline restore is supported with partial Snapshot copies from a SnapVault backup. The number of constituents in the destination volume must match the number of constituents in the source volume when the Snapshot copy was taken.
- If a restore operation fails, no other operations are allowed until the restore operation is complete. You can either retry the restore operation or run the restore operation with the `cleanup` parameter.
- A FlexGroup volume can be the source volume of only one backup relationship or restore relationship. A FlexGroup volume cannot be the source of two SnapVault relationships, two restore relationships, or a SnapVault relationship and a restore relationship.
- SnapVault backup and restore operations cannot run in parallel. When either a baseline restore operation or an incremental restore operation is in progress, you should quiesce the backup operations.
- You must abort a restore operation of a partial Snapshot copy from the destination FlexGroup volume. You cannot abort the restore operation of a partial Snapshot copy from the source volume.
- If you abort a restore operation, you must restart the restore operation with the same Snapshot copy that was used for the previous restore operation.

## About this task

Any active quota rules on the destination FlexGroup volume are deactivated before the restore is performed.

You can use the `volume quota modify` command to reactivate quota rules after the restore operation is complete.

## Steps

1. Restore the FlexGroup volume: `snapmirror restore -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -snapshot snapshot_name`  
`snapshot_name` is the Snapshot copy that is to be restored from the source volume to the destination volume. If the Snapshot copy is not specified, the destination volume is restored from the latest Snapshot copy.

```
vserverA::> snapmirror restore -source-path vserverB:dstFG -destination
-path vserverA:newFG -snapshot daily.2016-07-15_0010
Warning: This is a disruptive operation and the volume vserverA:newFG
will be read-only until the operation completes
Do you want to continue? {y|n}: y
```

## Disable SVM protection on a FlexGroup volume

When the SVM DR flag is set to `protected` on a FlexGroup volume, you can set the flag to `unprotected` to disable SVM DR protection on a FlexGroup volume.

## What you'll need

- The SVM DR relationship between the primary and secondary is healthy.

- SVM DR protection parameter is set to `protected`.

### Steps

1. Disable protection by using the `volume modify` command to change the `vserver-dr-protection` parameter for the FlexGroup volume to `unprotected`.

```
cluster2::> volume modify -vserver vs1 -volume fg_src -vserver-dr
-protection unprotected
[Job 5384] Job is queued: Modify fg_src.
[Job 5384] Steps completed: 4 of 4.
cluster2::>
```

2. Update the SVM at the secondary site: `snapmirror update -destination-path destination_svm_name: -source-path Source_svm_name:`
3. Verify that the SnapMirror relationship is healthy: `snapmirror show`
4. Verify that the FlexGroup SnapMirror relationship has been removed: `snapmirror show -expand`

### Enable SVM protection on a FlexGroup volume

When the SVM DR protection flag is set to `unprotected` on a FlexGroup volume, you can set the flag to `protected` to enable SVM DR protection.

### What you'll need

- The SVM DR relationship between the primary and secondary is healthy.
- SVM DR protection parameter is set to `unprotected`.

### Steps

1. Enable protection by using the `volume modify` to change the `vserver-dr-protection` parameter for the FlexGroup volume to `protected`.

```
cluster2::> volume modify -vserver vs1 -volume fg_src -vserver-dr
-protection protected
[Job 5384] Job is queued: Modify fg_src.
[Job 5384] Steps completed: 4 of 4.
cluster2::>
```

2. Update the SVM at the secondary site: `snapmirror update -destination-path destination_svm_name -source-path source_svm_name`

```
snapmirror update -destination-path vs1_dst: -source-path vs1:
```

3. Verify that the SnapMirror relationship is healthy: `snapmirror show`

```
cluster2::> snapmirror show
```

```
Progress
```

```
Source          Destination Mirror Relationship Total
```

```
Last
```

```
Path           Type Path           State Status           Progress Healthy
```

```
Updated
```

```
-----
```

```
-----
```

```
vs1:           XDP vs1_dst: Snapmirrored  
                                     Idle           -           true  -
```

4. Verify that the FlexGroup SnapMirror relationship is healthy: `snapmirror show -expand`



```
cluster2::> snapmirror show -expand
```

```
Progress
Source          Destination Mirror Relationship Total
Last
Path           Type Path           State Status           Progress Healthy
Updated
-----
-----
vs1:            XDP vs1_dst:       Snapmirrored
                Idle           -               true  -
vs1:fg_src     XDP vs1_dst:fg_src Snapmirrored
                Idle           -               true  -
vs1:fg_src__0001
                XDP vs1_dst:fg_src__0001 Snapmirrored
                Idle           -               true  -
vs1:fg_src__0002
                XDP vs1_dst:fg_src__0002 Snapmirrored
                Idle           -               true  -
vs1:fg_src__0003
                XDP vs1_dst:fg_src__0003 Snapmirrored
                Idle           -               true  -
vs1:fg_src__0004
                XDP vs1_dst:fg_src__0004 Snapmirrored
                Idle           -               true  -
6 entries were displayed.
```

## Convert FlexVol volumes to FlexGroup volumes

### Converting FlexVol volumes to FlexGroup volumes overview

If you want to expand a FlexVol volume beyond its space limit, you can convert the FlexVol volume to a FlexGroup volume. Beginning with ONTAP 9.7, you can convert standalone FlexVol volumes or FlexVol volumes that are in a SnapMirror relationship to FlexGroup volumes.

### Considerations for converting FlexVol volumes to FlexGroup volumes

You should be aware of the features and operations that are supported before you decide to convert FlexVol volumes to FlexGroup volumes.

## Operations not supported during conversion

The following operations are not allowed when volume conversion is in progress:

- Volume move
- Aggregate autobalance
- Aggregate relocation
- Planned takeover and giveback in a high-availability configuration
- Manual and automatic giveback in an high-availability configuration
- Cluster upgrade and revert
- FlexClone volume split
- Volume rehost
- Volume modify and autosize
- Volume rename
- Attaching an object store to an aggregate
- Negotiated switchover in MetroCluster configuration
- SnapMirror operations
- Restoring from a Snapshot copy
- Quota operations
- Storage efficiency operations

You can perform these operations on the FlexGroup volume after successful conversion.

## Configurations that are not supported with FlexGroup volumes

- Offline or restricted volume
- SVM root volume
- SnapLock volumes
- SAN
- SMB 1.0
- NVMe namespaces
- Remote Volume Shadow Copy Service (VSS)

## Convert a FlexVol volume to a FlexGroup volume

Beginning with ONTAP 9.7, you can perform an in-place conversion of a FlexVol volume to a FlexGroup volume without requiring a data copy or additional disk space.

### What you'll need

- Transitioned volumes can be converted to FlexGroup volumes beginning in ONTAP 9.8. If you are converting a transitioned volume to FlexGroup, see Knowledge Base article [How To Convert a Transitioned FlexVol to FlexGroup](#) for more information.
- The FlexVol volume that is being converted must be online.

- The operations and configurations on the FlexVol volume must be compatible with the conversion process.

An error message is generated if the FlexVol volume has any incompatibility and the volume conversion is aborted. You can take corrective actions and retry the conversion.

- If a FlexVol volume is very large (for example, 80 to 100 TB) and very full (80 to 100 percent), you should copy the data rather than convert it.



Converting a very large FlexGroup volume results in a very full FlexGroup volume member constituent, which can create performance issues. For more information, see the section called "When not to create a FlexGroup volume" in the TR [FlexGroup volumes - Best Practices and Implementation Guide](#).

## Steps

1. Verify that the FlexVol volume is online: `volume show vol_name -volume-style-extended,state`

```
cluster-1::> volume show my_volume -fields volume-style-extended,state
vserver volume      state  volume-style-extended
-----
vs0      my_volume online flexvol
```

2. Verify whether the FlexVol volume can be converted without issues:

- a. Log in to the advance privilege mode: `set -privilege advanced`

- b. Verify the conversion process: `volume conversion start -vserver vs1 -volume flexvol -check-only true`

You must rectify all errors before converting the volume.



You cannot convert a FlexGroup volume back to a FlexVol volume.

3. Start the conversion: `volume conversion start -vserver svm_name -volume vol_name`

```
cluster-1::*> volume conversion start -vserver vs0 -volume my_volume

Warning: Converting flexible volume "my_volume" in Vserver "vs0" to a
FlexGroup
        will cause the state of all Snapshot copies from the volume to
be set
        to "pre-conversion". Pre-conversion Snapshot copies cannot be
restored.
Do you want to continue? {y|n}: y
[Job 57] Job succeeded: success
```

4. Verify that the conversion is successful: `volume show vol_name -fields -volume-style-extended,state`

```
cluster-1::*> volume show my_volume -fields volume-style-extended,state
vserver volume      state  volume-style-extended
-----
vs0      my_volume online flexgroup
```

## Results

The FlexVol volume is converted to a single-member FlexGroup volume.

## After you finish

You can expand the FlexGroup volume, as required.

## Convert a FlexVol volume SnapMirror relationship to a FlexGroup volume SnapMirror relationship

To convert a FlexVol volume SnapMirror relationship to a FlexGroup volume SnapMirror relationship in ONTAP, you must first convert the destination FlexVol volume followed by the source FlexVol volume.

## What you'll need

- The FlexVol volume that is being converted must be online.
- The source FlexVol volume in the SnapMirror relationship must not be the source volume for multiple SnapMirror relationships.

Fan-out SnapMirror relationships are not supported for FlexGroup volumes.

- The operations and configurations on the FlexVol volume must be compatible with the conversion process.

An error message is generated if the FlexVol volume has any incompatibility and the volume conversion is aborted. You can take corrective actions and retry the conversion.

## About this task

FlexGroup conversion is supported only for asynchronous SnapMirror relationships.

## Steps

1. Verify that the SnapMirror relationship is healthy: `snapmirror show`

Only XDP type mirror relationships can be converted.

```
cluster2::> snapmirror show
```

```
Progress
Source          Destination Mirror Relationship Total
Last
Path           Type Path           State Status           Progress Healthy
Updated
-----
-----
vs0:src_dpv DP   vs2:dst_dpv Snapmirrored
                        Idle              -             true  -
vs0:src_xdp XDP  vs2:dst_xdp Snapmirrored
                        Idle              -             true  -
```

2. Verify whether the source volume is compatible for conversion:

- a. Log in to the advance privilege mode: `set -privilege advanced`
- b. Verify the conversion process: `volume conversion start -vserver vs1 -volume src_vol -check-only true`

You must rectify all errors before converting the volume.

3. Convert the destination FlexVol volume to FlexGroup volume.

- a. Quiesce the FlexVol SnapMirror relationship: `snapmirror quiesce -destination-path dest_svm:dest_volume`

```
cluster2::> snapmirror quiesce -destination-path vs2:dst_xdp
```

- b. Start the conversion: `volume conversion start -vserver dest_svm -volume dest_volume`

```
cluster-1::> volume conversion start -vserver vs2 -volume dst_xdp
```

```
Warning: After the volume is converted to a FlexGroup, it will not be possible
```

```
to change it back to a flexible volume.
```

```
Do you want to continue? {y|n}: y
```

```
[Job 510] Job succeeded: SnapMirror destination volume "dst_xdp" has been successfully converted to a FlexGroup volume.
```

```
You must now convert the relationship's source volume, "vs0:src_xdp", to a FlexGroup.
```

```
Then, re-establish the SnapMirror relationship using the "snapmirror resync" command.
```

4. Convert the source FlexVol volume to FlexGroup volume: `volume conversion start -vserver src_svm_name -volume src_vol_name`

```
cluster-1::> volume conversion start -vserver vs0 -volume src_xdp

Warning: Converting flexible volume "src_xdp" in Vserver "vs0" to a
FlexGroup
        will cause the state of all Snapshot copies from the volume to
be set
        to "pre-conversion". Pre-conversion Snapshot copies cannot be
restored.
Do you want to continue? {y|n}: y
[Job 57] Job succeeded: success
```

5. Resync the relationship: `snapmirror resync -destination-path dest_svm_name:dest_volume`

```
cluster2::> snapmirror resync -destination-path vs2:dst_xdp
```

### After you finish

You must ensure that when the source FlexGroup volume is expanded to include more constituents, the destination volume is also expanded.

## Improve performance for multiple clients with FlexCache

You can use FlexCache volumes to speed up access to data or to offload traffic from heavily accessed volumes. FlexCache volumes are ideal for read-intensive workloads, especially where clients need to access the same data repeatedly.

The topics in this section show you how to manage FlexCache volumes with System Manager in ONTAP 9.7 and later releases. If you are using the classic System Manager (available only in ONTAP 9.7 and earlier), see this topic:

- [Create FlexCache volumes](#)

The FlexCache volume can be on the same cluster as or on a different cluster than that of the remote volume. If the remote volume is on a different cluster, you need to have already peered the clusters and storage VMs.



If an HA pair is using [encrypting SAS or NVMe drives \(SED, NSE, FIPS\)](#), you must follow the instructions in the topic [Returning a FIPS drive or SED to unprotected mode](#) for all drives within the HA pair prior to initializing the system (boot options 4 or 9). Failure to do this may result in future data loss if the drives are repurposed.

### Steps

1. Click **Storage > Volumes**.
2. Click **Add**.

3. Click **More Options** and then select **Add as cache for a remote volume**.
  - a. If you are running ONTAP 9.8 or later and you want to disable QoS or choose a custom QoS policy, click **More Options** and then, under **Storage and Optimization** select **Performance Service Level**.

For any new data requests, the FlexCache volume requests the data from the remote volume and stores it. All the subsequent read requests for the data are then served directly from the FlexCache volume.

## Videos

### How FlexCache can reduce WAN latency and read times for global data



**Learn about the performance benefits of ONTAP FlexCache!**

## ONTAP FlexCache

Data Access Where You Need It



## Tech Clip

© 2020 NetApp, Inc. All rights reserved.



## FlexCache volumes management with the CLI

### FlexCache volumes management overview with the CLI

You can configure and manage FlexCache volumes for accelerating data access.

Use these procedures to configure FlexCache volumes if the following are true:

- You are running ONTAP 9.5 or later.
- You want to use the ONTAP command-line interface (CLI), not System Manager or an automated scripting tool.
- You want to use best practices, not explore every available option.

Details about command syntax are available from the CLI help and the ONTAP man pages.

- You have cluster administrator privileges, not SVM administrator privileges.

### Use FlexCache volumes to accelerate data access overview

A FlexCache volume is a sparsely populated volume that is backed by an origin volume. The FlexCache volume can be on the same cluster as or on a different cluster than that of the origin volume. The FlexCache volume provides access to data in the origin volume without requiring that all of the data be in the FlexCache volume.

In ONTAP 9.5, the origin volume is a FlexVol volume and the FlexCache volume is a FlexGroup volume. An origin volume supports NFSv3, NFSv4, and SMB protocols. A FlexCache volume supports only NFSv3 protocol in ONTAP 9.5. Beginning with ONTAP 9.8, a FlexCache volume also supports SMB protocol. Beginning with ONTAP 9.10.1, a FlexCache volume supports the NFSv4 protocol. For a table summary of



supported features in FlexCache volumes, refer to [Supported and unsupported features for FlexCache volumes](#).

Beginning with ONTAP 9.7, FlexGroup volumes are also supported as source volumes.



In ONTAP 9 releases earlier than 9.5, origin FlexVol volumes can only serve data to FlexCache volumes created on systems running Data ONTAP 8.2.x operating in 7-Mode. Beginning with ONTAP 9.5, origin FlexVol volumes can also serve data to FlexCache volumes on ONTAP 9 systems. For information about migrating from 7-mode FlexCache to ONTAP 9 FlexCache, [NetApp Technical Report 4743: FlexCache Volumes in NetApp ONTAP](#).

A FlexCache volume directly serves read requests if the volume contains the data requested by the client. Otherwise, the FlexCache volume requests the data from the origin volume and stores the data before serving the client request. Subsequent read requests for the data are then served directly from the FlexCache volume. This improves performance when the same data is accessed repeatedly, because after the first request, the data no longer has to travel across the network, or be served from an overloaded system.

Beginning with ONTAP 9.9.1, FlexCache volumes cache a directory listing for "file not found" errors that occur when a file no longer exists on the origin volume. This helps reduce network traffic by removing the need to send multiple calls to the origin when clients search for non-existent files.

Beginning with ONTAP 9.10.1, global file locking can be enabled across FlexCache volumes to favor consistency, ensuring modifications to an origin volume are distributed simultaneously to FlexCache volumes. Global file locking can only be enabled from the CLI.

You can use FlexCache volumes to speed up access to data or to offload traffic from heavily accessed volumes. FlexCache volumes help improve performance, especially when clients need to access the same data repeatedly, because the data can be served directly without having to access the origin volume. Therefore, you can use FlexCache volumes to handle system workloads that are read-intensive.

Any write operation is applied at the origin volume.

## Typical FlexCache deployments

FlexCache volumes are typically used for read-intensive workloads. You can have a FlexCache volume in the same cluster to accelerate performance for frequently accessed data or "hot objects". You can also have FlexCache volumes to distribute data across multiple clusters to reduce WAN latencies.

You can have FlexCache deployments with AFF, FAS, or ONTAP Select systems. Beginning with ONTAP 9.6, FlexCache deployments are also supported with Cloud Volumes ONTAP.

### Performance acceleration for hot volumes

In a LAN deployment, the FlexCache volume is in the same cluster as the origin cluster. The FlexCache volume can be located in the same SVM as or in a different SVM than that of the origin volume.

The FlexCache volume is used for CPU-intensive workloads to offload work from busy file servers and to free system resources. You can use multiple mount points corresponding to different FlexCache volumes for reducing network latency because the data access load is shared among all of the caching systems. This type of LAN deployment reduces the workload of an overloaded storage system.

## Cross-cluster data distribution

In a WAN deployment, the FlexCache volume is remote from the data center and is in a different cluster than the origin volume. When clients request data, the FlexCache volume caches popular data, giving the end user faster access to information. This type of WAN deployment decreases the average access time for remote clients.


The FlexCache volume is placed as close as possible to the remote office. Client requests are then explicitly directed to the FlexCache volume. If valid data exists in the cache, that data is served directly to the client. If the data does not exist in the cache, the data is retrieved across the WAN from the origin system, cached in the FlexCache volume, and then served to the client.

## Supported and unsupported features for FlexCache volumes

You must be aware of the features that are supported by FlexCache volumes and their origin volumes.

Feature	Supported at the origin volume?	Supported at the FlexCache volume?
Anti-ransomware protection	Yes  Supported for FlexVol origin volumes beginning with ONTAP 9.10.1, not supported for FlexGroup origin volumes.	No
Antivirus	Yes  Supported beginning with ONTAP 9.7	Not applicable
Auditing	Yes  Supported beginning with ONTAP 9.7 You can audit NFS file access events in FlexCache relationships using native ONTAP auditing. For more information, see <a href="#">Considerations for auditing FlexCache volumes</a>	Yes  Supported beginning with ONTAP 9.7 You can audit NFS file access events in FlexCache relationships using native ONTAP auditing. For more information, see <a href="#">Considerations for auditing FlexCache volumes</a>
Cloud Volumes ONTAP	Yes  Supported beginning with ONTAP 9.6	Yes  Supported beginning with ONTAP 9.6
Compaction	Yes  Supported beginning with ONTAP 9.6	Yes  Supported beginning with ONTAP 9.7

Compression	Yes  Supported beginning with ONTAP 9.6	Yes  Supported beginning with ONTAP 9.6
Deduplication	Yes	Yes  Inline deduplication is supported on FlexCache volumes beginning with ONTAP 9.6. Cross-volume deduplication is supported on FlexCache volumes beginning with ONTAP 9.7.
FabricPool	Yes	Yes  Supported beginning with ONTAP 9.7
FlexCache DR	Yes	Yes  Supported beginning with ONTAP 9.9.1, with NFSv3 protocol, only. FlexCache volumes must be in separate SVMs or in separate clusters.
FlexGroup volume	Yes  Supported beginning with ONTAP 9.7	Yes
FlexVol volume	Yes	No
FPolicy	Yes  Supported beginning with ONTAP 9.7	Yes  Supported for NFS beginning with ONTAP 9.7
MetroCluster configuration	Yes  Supported beginning with ONTAP 9.7	Yes  Supported beginning with ONTAP 9.7
Microsoft Offloaded Data Transfer (ODX)	No	No

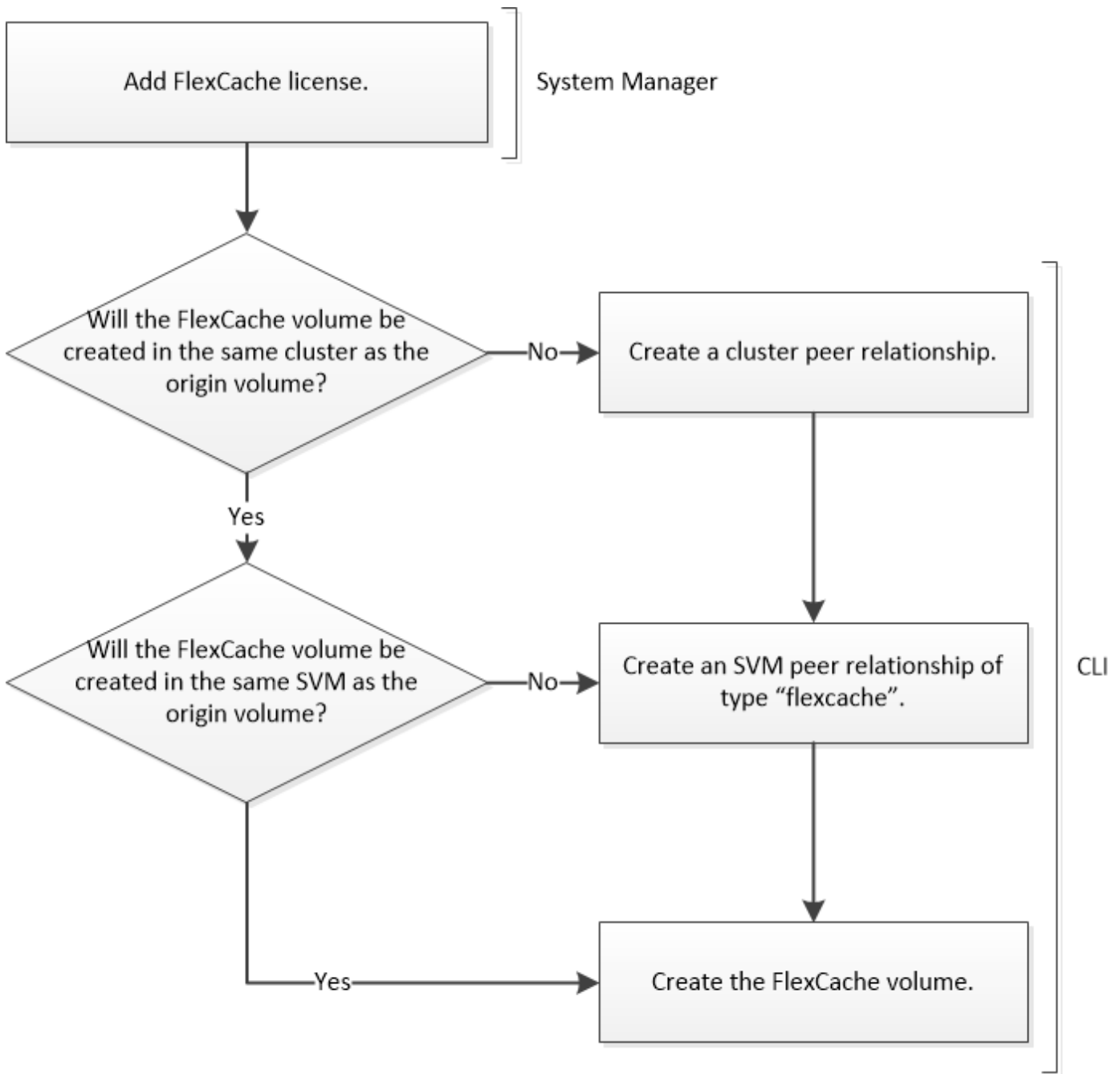
NetApp Volume Encryption (NVE)	Yes Supported beginning with ONTAP 9.6	Yes Supported beginning with ONTAP 9.6
NFSv3	Yes	Yes
NFSv4	Yes	Yes Supported beginning with ONTAP 9.10.1
QoS	Yes	Yes NOTE: File-level QoS is not supported for FlexCache volumes.
Qtrees	Yes Supported beginning with ONTAP 9.6	No
Quotas	Yes	No   Beginning with ONTAP 9.6, remote quota (rquota) is supported at FlexCache volumes.
SMB	Yes	Yes Supported beginning with ONTAP 9.8.
SnapLock volumes	No	No
SnapMirror Asynchronous relationships	Yes	No  <ul style="list-style-type: none"> <li>• You can have a FlexCache volume from an origin primary volume in SnapMirror relationship.</li> <li>• Beginning with ONTAP 9.8, a SnapMirror secondary volume can be a FlexCache origin volume.</li> </ul>
SnapMirror Synchronous relationships	No	No

SnapRestore	Yes	No
Snapshot copies	Yes	No
SVM DR configuration	Yes  Supported beginning with ONTAP 9.5. The primary SVM of an SVM DR relationship can have the origin volume; however, if the SVM DR relationship is broken, the FlexCache relationship must be re-created with a new origin volume.	No  You can have FlexCache volumes in primary SVMs, but not in secondary SVMs. Any FlexCache volume in the primary SVM is not replicated as part of the SVM DR relationship.
Storage-level Access Guard (SLAG)	No	No
Thin provisioning	Yes	Yes  Supported beginning with ONTAP 9.7
Volume cloning	Yes  Cloning of an origin volume and the files in the origin volume is supported beginning with ONTAP 9.6.	No
Volume move	Yes	Yes (only for volume constituents)  Moving volume constituents of a FlexCache volume is supported from ONTAP 9.6 onwards.
Volume rehost	No	No

## FlexCache volume creation

### FlexCache volume creation workflow

You must first install the FlexCache license from System Manager. You can then create a FlexCache volume in the same cluster or in a remote cluster by using the CLI.



You must be running ONTAP 9.5 or later.

You can use FlexCache volumes in the same cluster for accelerated performance when accessing hot volumes. You can use FlexCache volumes in different clusters for improving the performance of cross-cluster data distribution.

### Add a FlexCache license

If you are running ONTAP 9.6 or earlier, you must install a FlexCache license, which is a capacity-based and term-based license, by using System Manager.

### About this task

The FlexCache license is a cluster-wide license. The license includes an entitled usage limit that you purchase for using FlexCache volumes in the cluster. The space usage by FlexCache volumes across the cluster must

not exceed the capacity of the entitled usage limit. If you need to increase the usage limit of the license, you should contact your sales representative.

Beginning with ONTAP 9.7, the capacity-based license is not required. The FlexCache license is bundled with the ONTAP package.

### Steps

1. Download the NetApp License File for the FlexCache license from the NetApp Support Site.

[NetApp Support](#)

2. Use System Manager to upload the FlexCache license to the cluster:
  - a. Click the **Configurations > Cluster > Licenses** tab.
  - b. In the **Packages** window, click **Add**.
  - c. In the **Add License Packages** dialog box, click **Choose Files** to select the NetApp License File that you downloaded, and then click **Add** to upload the file to the cluster.

### Process to create a FlexCache volume

#### Create a FlexCache volume

You can create a FlexCache volume in the same cluster for improving performance when accessing a hot object. If you have data centers in different locations, you can create FlexCache volumes on remote clusters for accelerating data access.

#### About this task

The FlexCache volume is always a FlexGroup volume, and not a FlexVol volume.

Beginning with ONTAP 9.7, FlexGroup volumes are also supported at the origin of the FlexCache relationship.

### Steps

1. If the FlexCache volume to be created is in a different cluster, create a cluster peer relationship:
  - a. On the destination cluster, create a peer relationship with the data protection source cluster:

```
cluster peer create -generate-passphrase -offer-expiration MM/DD/YYYY  
HH:MM:SS|1...7days|1...168hours -peer-addr peer_LIF_IPs -initial-allowed  
-vserver-peers svm_name,..|* -ip-space ip-space_name
```

Beginning with ONTAP 9.6, TLS encryption is enabled by default when creating a cluster peer relationship. TLS encryption is supported for the intercluster communication between the origin and FlexCache volumes. You can also disable TLS encryption for the cluster peer relationship, if required.

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers *
```

Passphrase: UCa+6lRVICXeL/gq1WrK7ShR  
Expiration Time: 6/7/2017 08:16:10 EST  
Initial Allowed Vserver Peers: \*

Intercluster LIF IP: 192.140.112.101  
Peer Cluster Name: Clus\_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed again.

- b. On the source cluster, authenticate the source cluster to the destination cluster:

```
cluster peer create -peer-addr peer_LIF_IPs -ip-space ip-space
```

```
cluster01::> cluster peer create -peer-addr
192.140.112.101,192.140.112.102
```

Notice: Use a generated passphrase or choose a passphrase of 8 or more characters.

To ensure the authenticity of the peering relationship, use a phrase or sequence of characters that would be hard to guess.

Enter the passphrase:

Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.

2. If the FlexCache volume is in a different SVM than that of the origin volume, create an SVM peer relationship with flexcache as the application:

- a. If the SVM is in a different cluster, create an SVM permission for the peering SVMs:

```
vserver peer permission create -peer-cluster cluster_name -vserver svm-name
-applications flexcache
```

The following example illustrates how to create an SVM peer permission that applies for all of the local SVMs:



```
cluster1::> vserver peer permission create -peer-cluster cluster2
-vserver "*" -applications flexcache
```

Warning: This Vserver peer permission applies to all local Vservers. After that no explicit "vserver peer accept" command required for Vserver peer relationship creation request from peer cluster "cluster2" with any of the local Vservers. Do you want to continue? {y|n}: y

b. Create the SVM peer relationship:

```
vserver peer create -vserver local_SVM -peer-vserver remote_SVM -peer
-cluster cluster_name -applications flexcache
```

3. Create a FlexCache volume:

```
volume flexcache create -vserver cache_svm -volume cache_vol_name -auto
-provision-as flexgroup -size vol_size -origin-vserver origin_svm -origin
-volume origin_vol_name
```

The following example creates a FlexCache volume and automatically selects existing aggregates for provisioning:

```
cluster1::> volume flexcache create -vserver vs_1 -volume fc1 -auto
-provision-as flexgroup -origin-volume vol_1 -size 160MB -origin-vserver
vs_1
[Job 443] Job succeeded: Successful
```

The following example creates a FlexCache volume and sets the junction path:

```
cluster1::> flexcache create -vserver vs34 -volume fc4 -aggr-list
aggr34,aggr43 -origin-volume origin1 -size 400m -junction-path /fc4
[Job 903] Job succeeded: Successful
```

4. Verify the FlexCache relationship from the FlexCache volume and the origin volume.

a. View the FlexCache relationship in the cluster:

```
volume flexcache show
```

```

cluster1::> volume flexcache show
Vserver Volume      Size      Origin-Vserver Origin-Volume Origin-
Cluster
-----
vs_1    fc1          160MB    vs_1          vol_1
cluster1

```

b. View all of the FlexCache relationships in the origin cluster:

```

volume flexcache origin show-caches

```

```

cluster::> volume flexcache origin show-caches
Origin-Vserver Origin-Volume  Cache-Vserver  Cache-Volume  Cache-
Cluster
-----
vs0            ovol1         vs1            cfg1           clusA
vs0            ovol1         vs2            cfg2           clusB
vs_1          vol_1         vs_1           fc1
cluster1

```

**Result**

The FlexCache volume is successfully created. Clients can mount the volume by using the junction path of the FlexCache volume.

**Related information**

[Cluster and SVM peering](#)

[ONTAP 9 Commands](#)

**Guidelines for sizing a FlexCache volume**

You must be aware of the limits for FlexCache volumes before you start provisioning the volumes.

The size limit of a FlexVol volume is applicable to an origin volume. The size of a FlexCache volume can be less than or equal to the origin volume. The best practice for the size of a FlexCache volume is to be at least 10 percent of the size of the origin volume.

You must also be aware of the following additional limits on FlexCache volumes:

Limit	ONTAP 9.5-9.6	ONTAP 9.7	ONTAP 9.8 and later

Maximum number of FlexCache volumes that you can create from an origin volume	10	10	100
Recommended maximum number of origin volumes per node	10	100	100
Recommended maximum number of FlexCache volumes per node	10	100	100
Recommended maximum number of FlexGroup constituents in a FlexCache volume per node	40	800	800
Maximum number of constituents per FlexCache volume per node	32	32	32

## Related information

[NetApp Interoperability](#)

### Considerations for auditing FlexCache volumes

Beginning with ONTAP 9.7, you can audit NFS file access events in FlexCache relationships using native ONTAP auditing and file policy management with FPolicy. FPolicy is not supported for FlexCache volumes with SMB. Native auditing and FPolicy are configured and managed with the same CLI commands used for FlexVol volumes. However, there is some different behavior with FlexCache volumes.

- **Native auditing**

- You can't use a FlexCache volume as the destination for audit logs.
- If you want to audit read and writes on FlexCache volumes, you must configure auditing on both the cache SVM as well as on the origin SVM.

This is because file system operations are audited where they are processed. That is, reads are audited on the cache SVM and writes are audited on the origin SVM.

- To track the origin of write operations, the SVM UUID and MSID are appended in the audit log to identify the FlexCache volume from which the write originated.
- Although system access control lists (SACLs) can be set on a file using NFSv4 or SMB protocols, FlexCache volumes support only NFSv3. Therefore, SACLs can only be set on the origin volume.

- **FPolicy**

- Although writes to a FlexCache volume are committed on the origin volume, FPolicy configurations monitor the writes on the cache volume. This is unlike native auditing, in which the writes are audited on the origin volume.
- While ONTAP does not require the same FPolicy configuration on cache and origin SVMs, it is recommended that you deploy two similar configurations. You can do so by creating a new FPolicy policy for the cache, configured like that of the origin SVM but with the scope of the new policy limited to the cache SVM.

## Manage a FlexCache relationship

## View the connection status of a FlexCache relationship

Beginning with ONTAP 9.6, you can view the connection status of a FlexCache relationship and take any corrective action if the connection status between the origin and FlexCache volumes goes to the disconnected mode.

### About this task

A FlexCache relationship can have one of the following connection status:

- connected
- disconnected
- unknown

### Steps

1. Log in to the advanced privilege mode:

```
set -privilege advanced
```

2. Verify the connection status of all the FlexCache relationships in the cluster:

```
volume flexcache connection-status show
```

```
cluster::*> volume flexcache connection-status show
```

```
Node: cluster-01
```

		Remote	Remote	
Connection				
+Vserver	Volume	Vserver	Remote Volume	Endpoint
Status				
+-----	-----	-----	-----	-----
-----				
vs_1 connected	vol_origin	vs_2	fc_11__0001	cache
vs_1 connected	vol_origin	vs_2	fc_11__0002	cache
vs_1 connected	vol_origin	vs_2	fc_11__0003	cache
vs_1 connected	vol_origin	vs_2	fc_11__0004	cache
vs_2 connected	fc_11	vs_1	vol_origin	origin

### Synchronize properties of a FlexCache volume from an origin volume

Some of the volume properties of the FlexCache volume must always be synchronized with those of the origin volume. If the volume properties of a FlexCache volume fail to synchronize automatically after the properties are modified at the origin volume, you can manually synchronize the properties.

#### About this task

The following volume properties of a FlexCache volume must always be synchronized with those of the origin volume:

- Security style (-security-style)
- Volume name (-volume-name)
- Maximum directory size (-maxdir-size)
- Minimum read ahead (-min-readahead)

## Step

1. From the FlexCache volume, synchronize the volume properties:

```
volume flexcache sync-properties -vserver svm_name -volume flexcache_volume
```

```
cluster1::> volume flexcache sync-properties -vserver vs1 -volume fc1
```

## Update the configurations of a FlexCache relationship

After events such as volume move, aggregate relocation, or storage failover, the volume configuration information on the origin volume and FlexCache volume is updated automatically. In case the automatic updates fail, an EMS message is generated and then you must manually update the configuration for the FlexCache relationship.

If the origin volume and the FlexCache volume are in the disconnected mode, you might need to perform some additional operations to update a FlexCache relationship manually.

### About this task

If you want to update the configurations of a FlexCache volume, you must run the command from the origin volume. If you want to update the configurations of an origin volume, you must run the command from the FlexCache volume.

## Step

1. Update the configuration of the FlexCache relationship:

```
volume flexcache config-refresh -peer-vserver peer_svm -peer-volume  
peer_volume_to_update -peer-endpoint-type [origin | cache]
```

## Enable file access time updates

Beginning with ONTAP 9.11.1, you can enable the `-atime-update` field on the FlexCache volume to permit file access time updates. You can also set an access time update period with the `-atime-update-period` attribute. The `-atime-update-period` attribute controls how often access time updates can take place and when they can propagate to the origin volume.

### Overview

ONTAP provides a volume-level field called `-atime-update`, to manage access time updates on files and directories that are read using `READ`, `READLINK`, and `REaddir`. Atime is used for data lifecycle decisions for files and directories that are infrequently accessed. The infrequently accessed files are eventually migrated to archive storage and are often later moved to tape.

The `atime-update` field is disabled by default on existing and newly created FlexCache volumes. If you are using FlexCache volumes with ONTAP releases earlier than 9.11.1, you should leave the `atime-update` field disabled so caches aren't unnecessarily evicted when a read operation is performed on the origin volume. With large FlexCache caches, however, administrators use special tools to manage data and help to ensure that hot data remains in the cache and cold data is purged. This is not possible when `atime-update` is disabled.

However, beginning with ONTAP 9.11.1, you can enable `-atime-update` and `-atime-update-period`, and use the tools required to manage the cached data.

### Before you begin

All FlexCache volumes must be running ONTAP 9.11.1 or later.

### About this task

Setting `-atime-update-period` to 86400 seconds allows no more than one access time update per 24-hour period, regardless of the number of read-like operations performed on a file.

Setting the `-atime-update-period` to 0 sends messages to the origin for each read access. The origin then informs each FlexCache volume that the atime is outdated, which impacts performance.

### Steps

1. Enable file access time updates and set the update frequency:

```
volume modify -volume vol_name -vserver SVM_name -atime-update true -atime
-update-period seconds
```

The following example enables `-atime-update` and sets `-atime-update-period` to 86400 seconds, or 24 hours:

```
c1: volume modify -volume origin1 vs1_c1 -atime-update true -atime
-update-period 86400
```

2. Verify that `-atime-update` is enabled:

```
volume show -volume vol_name -fields atime-update,atime-update-period
```

```
c1::*> volume show -volume cache1_origin1 -fields atime-update,atime-
update-period
vserver volume          atime-update atime-update-period
-----
vs2_c1  cache1_origin1 true           86400
```

### Enable global file locking

Beginning with ONTAP 9.10.1, global file locking can be applied to prevent reads across all related cached files.

### About this task

By default, FlexCache volumes favor availability over consistency. Without global file locking, any modification to an origin will be distributed to FlexCache volumes, but they might not be updated simultaneously. Global file locking favors consistency across volumes over availability. With global file locking enabled, modifications to the origin will be suspended until all FlexCache volumes are online.



You should only enable global file locking when you have control over the reliability of the connections between cache and origin due to suspension and possible timeouts of modifications when FlexCache volumes are offline.

Global file locking requires the clusters containing the origin and all associated caches to be running ONTAP 9.9.1 or later. Global file locking can be enabled on new or existing FlexCache volumes. The command can be run on one volume and will apply to all associated volumes.

You must be in the advanced privilege level to enable global file locking.

The process to enable global file locking depends on whether the origin has existing caches.

- [Enable global file locking on new FlexCache volumes](#)
- [Enable global file locking on existing FlexCache volumes](#)

### Enable global file locking on new FlexCache volumes

#### Steps

1. Create the FlexCache volume with `-is-global-file-locking` set to true:

```
volume flexcache create volume volume_name -is-global-file-locking-enabled true
```

The default value of `-is-global-file-locking` is “false”. When any subsequent `volume flexcache create` commands are run on a volume, they must be passed with `-is-global-file-locking enabled` set to “true”.

### Enable global file locking on existing FlexCache volumes

#### Steps

1. Global file locking must be set from the origin volume.
2. The origin cannot have any other existing relationships (for example, SnapMirror). Any existing relationships must be dissociated. All caches and volumes must be connected at the time of running the command. To check the connection status, run:

```
volume flexcache connection-status show
```

The status for all the listed volumes should display as “connected.” For more information, see [View the status of a FlexCache relationship](#) or [Synchronize properties of a FlexCache volume from an origin](#).

3. Enable global file locking on the caches:

```
volume flexcache origin config show/modify -volume volume_name -is-global-file-locking-enabled true
```

If reverting to a version of ONTAP earlier than 9.9.1, global file lock must first be disabled on the origin and associated caches. This can be managed by running:

```
volume flexcache prepare-to-downgrade -disable-feature-set 9.10.0
```



## Prepopulate a FlexCache volume

You can prepopulate a FlexCache volume to reduce the time it takes to access cached data.

### What you'll need

- You must be a cluster administrator at the advanced privilege level
- The paths you pass for prepopulation must be valid or the prepopulate operation fails.

### About this task

- Prepopulate reads files only and crawls through directories
- The `is-recursion` flag applies to the entire list of directories passed to prepopulate

### Steps

1. Prepopulate a FlexCache volume:

```
volume flexcache prepopulate -cache-vserver vs1 -cache-volume -path  
-list path_list -is-recursion true|false
```

This example includes a single directory path for prepopulation:

```
cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache  
-volume fg_cachevol_1 -path-list /dir1  
(volume flexcache prepopulate start)  
[JobId 207]: FlexCache prepopulate job queued.
```

This example includes a list of several paths for prepopulation:

```
cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache  
-volume fg_cachevol_1 -path-list /dir1,/dir2,/dir3,/dir4  
(volume flexcache prepopulate start)  
[JobId 208]: FlexCache prepopulate job queued.
```

2. Display the number of files read:

```
job show -id job_ID -ins
```

## Delete a FlexCache relationship

You can delete a FlexCache relationship and the FlexCache volume if you no longer require the FlexCache volume.

### Steps

1. From the cluster that has the FlexCache volume, take the FlexCache volume offline:

```
volume offline -vserver svm_name -volume volume_name
```

## 2. Delete the FlexCache volume:

```
volume flexcache delete -vserver svm_name -volume volume_name
```

The FlexCache relationship details are removed from the origin volume and the FlexCache volume.



If the `volume flexcache delete` command fails to clean up the origin side configuration, you are prompted to run the `volume flexcache origin cleanup-cache-relationship` command. In this scenario, go to Step 3.

## 3. From the origin cluster, clean up the FlexCache relationship details from the origin volume:

```
volume flexcache origin cleanup-cache-relationship -origin-volume  
origin_volume -origin-vserver origin_svm -cache-vserver flexcache_svm -cache  
-volume flexcache_vol
```



If you run the `volume flexcache origin cleanup-cache-relationship` command, the FlexCache relationship is deleted and cannot be reestablished.

```
cluster1::> volume flexcache origin cleanup-cache-relationship -origin  
-volume origin1 -origin-vserver vs34 -cache-vserver vs56 -cache-volume  
fc1
```

```
Warning: This command only needs to be run if "volume flexcache delete"  
fails on
```

```
the FlexCache cluster and prompts you to run this command. The  
cache
```

```
configuration will be deleted and cannot be reestablished for  
the
```

```
cache relationship between origin of a FlexCache volume  
"origin1" in Vserver "vs34" and FlexCache volume  
"fc1" in Vserver "vs56".
```

```
Do you want to continue? {y|n}: y
```

# Network Management

## Manage your network with System Manager

### Network management overview with System Manager

The topics in this section show you how to manage your storage system network – including IPspaces, broadcast domains, subnets, network interfaces, and Ethernet ports — with System Manager in ONTAP 9.7 and later releases.

If you are using the classic System Manager (available only in ONTAP 9.7 and earlier), see this topic:

- [Managing the network](#)

### Viewing and managing your network

Beginning with ONTAP 9.8, you can use System Manager to display a graphic that shows the components and configuration of your network. Beginning with ONTAP 9.12.0, you can view the LIF and subnet association on the Network Interfaces grid.

The new network visualization feature enables users to see the network connections path across hosts, ports, SVMs, volumes, etc. in a graphical interface.

The graphic displays when you select **Network > Overview** or when you select  from the **Network** section of the Dashboard.


The following categories of components are shown in the graphic:

- Hosts
- Storage ports
- Network interfaces
- Storage VMs
- Data access components

Each section shows additional details that you can hover your mouse over or select to perform network management and configuration tasks.

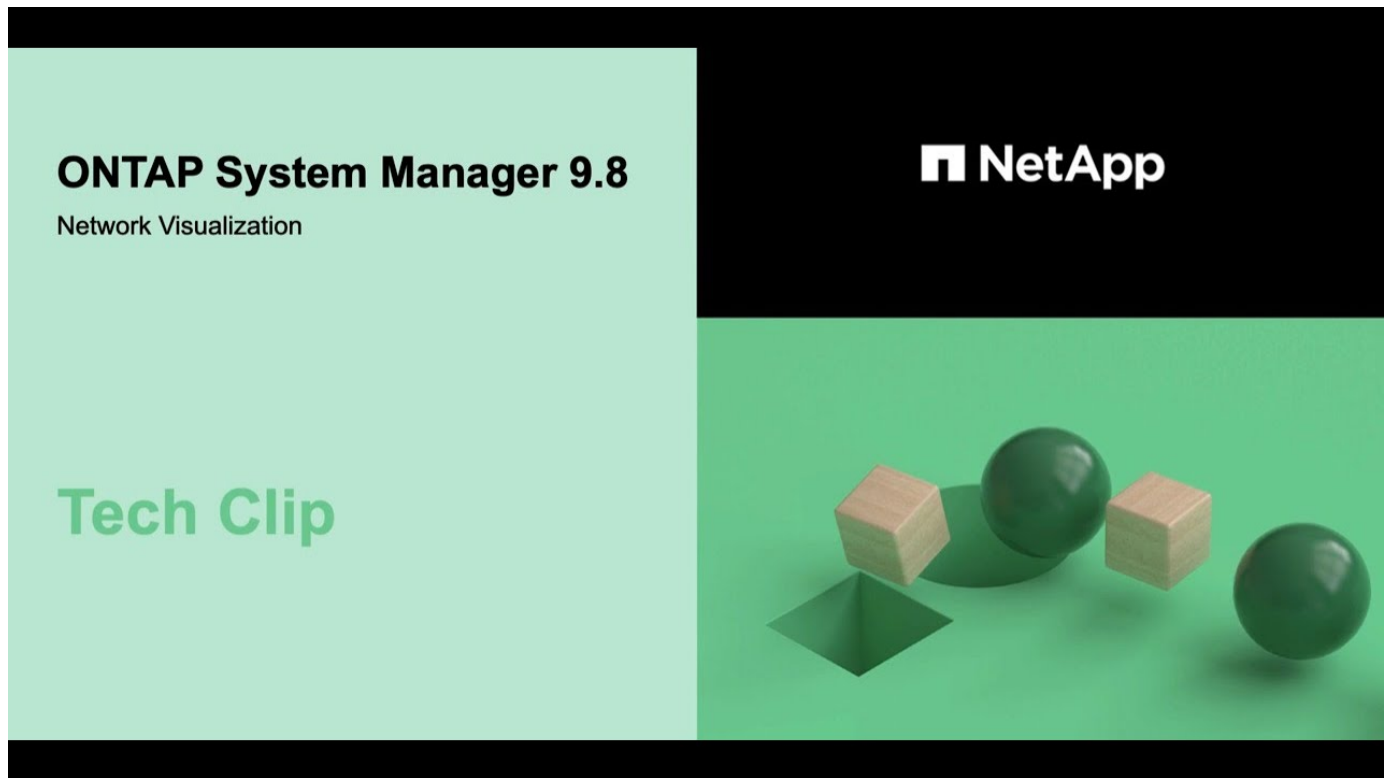
### Examples

The following are some examples of the many ways you can interact with the graphic to view details about each component or initiate actions to manage your network:

- Click on a host to see its configuration: the ports, network interfaces, storage VMs, and data access components associated with it.
- Hover the mouse over the number of volumes in a storage VM to select a volume to view its details.
- Select an iSCSI interface to view its performance over the last week.
- Click on  next to a component to initiate actions to modify that component.
- Quickly determine where problems might occur in your network, indicated by an "X" next to unhealthy

components.

## System Manager Network Visualization video



### Automatic detection and repair recommendations for network wiring issues

ONTAP can automatically detect and recommend solutions to network wiring issues based on a broadcast domain constituent's (ethernet ports) layer-2 reachability.

Incorrect wiring during cluster setup or when a new node joins an existing cluster might cause an unexpected broadcast domain port assignment. Beginning with ONTAP 9.10.1, the cluster automatically checks for network wiring issues by verifying port reachability after cluster setup or when a new node joins an existing cluster.

If a port reachability issue is detected, System Manager recommends a repair operation to resolve the issue.

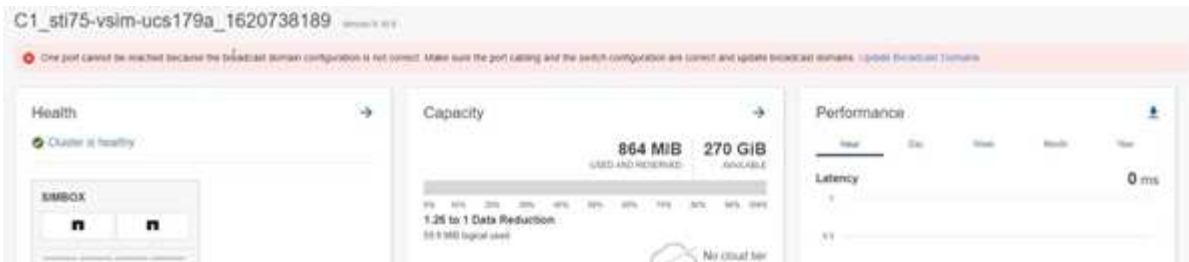
After you set up the cluster, network wiring issues are reported on the Dashboard.

After joining a new node to a cluster, network wiring issues appear on the Nodes page.

You can also view network wiring health on the network diagram. Port reachability issues are indicated on the network diagram by a red error icon.

### Post cluster setup

After you set up the cluster, if the system detects a network wiring issue, a message appears on the Dashboard.



## Steps

1. Correct the wiring as suggested in the message.
2. Click the link to launch the Update Broadcast Domains dialog. The Update Broadcast Domains dialog opens.



3. Review the information about the port, including the node, the issues, the current broadcast domain, and the expected broadcast domain.
4. Select the ports that you want to repair and click **Fix**. The system will move the ports from the current broadcast domain into the expected broadcast domain.

## Post node join

After joining a new node to a cluster, if the system detects a network wiring issue, a message appears on the Nodes page.

## Steps

1. Correct the wiring as suggested in the message.
2. Click the link to launch the Update Broadcast Domains dialog. The Update Broadcast Domains dialog opens.

3. Review the information about the port, including the node, the issues, the current broadcast domain, and the expected broadcast domain.
4. Select the ports you want to repair and click **Fix**. The system will move the ports from the current broadcast domain into the expected broadcast domain.

## Downloading network data for reporting

Beginning with ONTAP 9.8, you can download the data that is displayed in System Manager about your network.

When you display information in a *List View*, you can click **Download**, and the list of objects displayed is downloaded.

- The list is downloaded in comma-separated values (CSV) format.

- Only the data in the visible columns is downloaded.
- The CSV filename is formatted with the object name and a time stamp.

## Set up NAS path failover with the CLI

### ONTAP 9.8 and later

#### About NAS path failover for ONTAP 9.8 and later CLI

This workflow guides you through the networking configuration steps to set up NAS path failover for ONTAP 9.8 and later. This workflow assumes the following:

- You want to use NAS path failover best practices in a workflow that simplifies network configuration.
- You want to use the CLI, not System Manager.
- You are configuring networking on a new system running ONTAP 9.8 or later.

If you are running an ONTAP release earlier than 9.8, you should use the following NAS path failover procedure for ONTAP 9.0 to 9.7:

- [ONTAP 9.0-9.7 NAS path failover workflow](#)

If you want network management details, you should use the network management reference material:

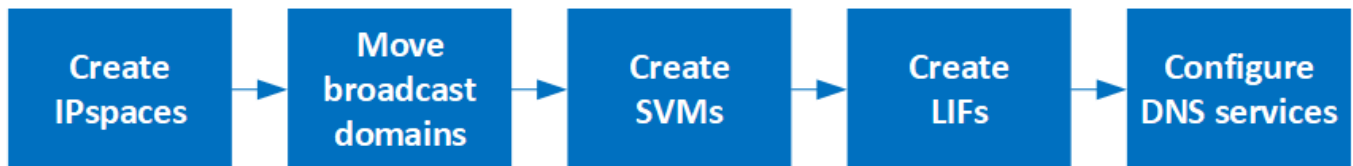
- [Network management overview](#)

#### Workflow NAS path failover

##### Overview

If you are already familiar with basic networking concepts, you might be able to save time setting up your network by reviewing this "hands on" workflow for NAS path failover configuration.

A NAS LIF automatically migrates to a surviving network port after a link failure on its current port. You can rely on the ONTAP defaults to manage path failover.



A SAN LIF does not migrate (unless you move it manually after the link failure). Instead, multipathing technology on the host diverts traffic to a different LIF. For more information, see [SAN administration](#).

#### Worksheet for NAS path failover configuration for ONTAP 9.8 and later

You should complete all sections of the worksheet before configuring NAS path failover.

## IPspace configuration

You can use an IPspace to create a distinct IP address space for each SVM in a cluster. Doing so enables clients in administratively separate network domains to access cluster data while using overlapping IP addresses from the same IP address subnet range.

Information	Required?	Your values
IPspace name The unique identifier of the IPspace.	Yes	

## Broadcast domain configuration

A broadcast domain groups ports that belong in the same Layer 2 network and sets the MTU for the broadcast domain ports.

Broadcast domains are assigned to an IPspace. An IPspace can contain one or more broadcast domains.



The port to which a LIF fails over must be a member of the failover group for the LIF. For each broadcast domain created by ONTAP, a failover group with the same name is also created that contains all the ports in the broadcast domain.

Information	Required?	Your values
IPspace name The IPspace to which the broadcast domain is assigned.  This IPspace must exist.	Yes	
Broadcast domain name The name of the broadcast domain.  This name must be unique in the IPspace.	Yes	
MTU The maximum transmission unit value for the broadcast domain, commonly set to either <b>1500</b> or <b>9000</b> .  The MTU value is applied to all ports in the broadcast domain and to any ports that are later added to the broadcast domain.  The MTU value should match all the devices connected to that network. Note that the e0M port handling management and service processor traffic should have the MTU set to no more than 1500 bytes.	Yes	



<p>Ports</p> <p>Ports are assigned to broadcast domains based on reachability. After port assignment is complete, check reachability by running the <code>network port reachability show</code> command.</p> <p>These ports can be physical ports, VLANs, or interface groups.</p>	Yes	
--	-----	--

**Subnet configuration**

A subnet contains pools of IP addresses and a default gateway that can be assigned to LIFs used by SVMs residing in the IPspace.

- When creating a LIF on an SVM, you can specify the name of the subnet instead of supplying an IP address and a subnet.
- Since a subnet can be configured with a default gateway, you do not have to create the default gateway in a separate step when creating an SVM.
- A broadcast domain can contain one or more subnets.
- You can configure SVM LIFs that are on different subnets by associating more than one subnet with the IPspace’s broadcast domain.
- Each subnet must contain IP addresses that do not overlap with IP addresses assigned to other subnets in the same IPspace.
- You can assign specific IP addresses to SVM data LIFs and create a default gateway for the SVM instead of using a subnet.

Information	Required?	Your values
<p>IPspace name</p> <p>The IPspace to which the subnet will be assigned.</p> <p>This IPspace must exist.</p>	Yes	
<p>Subnet name</p> <p>The name of the subnet.</p> <p>This name must be unique in the IPspace.</p>	Yes	
<p>Broadcast domain name</p> <p>The broadcast domain to which the subnet will be assigned.</p> <p>This broadcast domain must reside in the specified IPspace.</p>	Yes	

<p>Subnet name and mask The subnet and mask in which the IP addresses reside.</p>	Yes	
<p>Gateway You can specify a default gateway for the subnet.</p> <p>If you do not assign a gateway when you create the subnet, you can assign one later.</p>	No	
<p>IP address ranges You can specify a range of IP addresses or specific IP addresses.</p> <p>For example, you can specify a range such as:</p> <p>192.168.1.1-192.168.1.100, 192.168.1.112, 192.168.1.145</p> <p>If you do not specify an IP address range, the entire range of IP addresses in the specified subnet are available to assign to LIFs.</p>	No	
<p>Force update of LIF associations Specifies whether to force the update of existing LIF associations.</p> <p>By default, subnet creation fails if any service processor interfaces or network interfaces are using the IP addresses in the ranges provided.</p> <p>Using this parameter associates any manually addressed interfaces with the subnet and allows the command to succeed.</p>	No	

## SVM configuration

You use SVMs to serve data to clients and hosts.

The values you record are for creating a default data SVM. If you are creating a MetroCluster source SVM, see the [Fabric-attached MetroCluster Installation and Configuration Guide](#) or the [Stretch MetroCluster Installation and Configuration Guide](#).

Information	Required?	Your values
-------------	-----------	-------------

SVM name The fully qualified domain name (FQDN) of the SVM.  This name must be unique across cluster leagues.	Yes	
Root volume name The name of the SVM root volume.	Yes	
Aggregate name The name of the aggregate that holds the SVM root volume.  This aggregate must exist.	Yes	
Security style The security style for the SVM root volume.  Possible values are <b>ntfs</b> , <b>unix</b> , and <b>mixed</b> .	Yes	
IPspace name The IPspace to which the SVM is assigned.  This IPspace must exist.	No	
SVM language setting The default language to use for the SVM and its volumes.  If you do not specify a default language, the default SVM language is set to <b>C.UTF-8</b> .  The SVM language setting determines the character set used to display file names and data for all NAS volumes in the SVM.  You can modify The language after the SVM is created.	No	

### LIF configuration

An SVM serves data to clients and hosts through one or more network logical interfaces (LIFs).

Information	Required?	Your values
SVM name The name of the SVM for the LIF.	Yes	

<p>LIF name The name of the LIF.</p> <p>You can assign multiple data LIFs per node, and you can assign LIFs to any node in the cluster, provided that the node has available data ports.</p> <p>To provide redundancy, you should create at least two data LIFs for each data subnet, and the LIFs assigned to a particular subnet should be assigned home ports on different nodes.</p> <p><b>Important:</b> If you are configuring a SMB server to host Hyper-V or SQL Server over SMB for nondisruptive operation solutions, the SVM must have at least one data LIF on every node in the cluster.</p>	<p>Yes</p>	
<p>Service policy Service policy for the LIF.</p> <p>The service policy defines which network services can use the LIF. Built-in services and service policies are available for managing data and management traffic on both data and system SVMs.</p>	<p>Yes</p>	
<p>Allowed protocols IP-based LIFs do not require allowed protocols, use the service policy row instead.</p> <p>Specify allowed protocols for SAN LIFs on FibreChannel ports. These are the protocols that can use that LIF. The protocols that use the LIF cannot be modified after the LIF is created. You should specify all protocols when you configure the LIF.</p>	<p>No</p>	
<p>Home node The node to which the LIF returns when the LIF is reverted to its home port.</p> <p>You should record a home node for each data LIF.</p>	<p>Yes</p>	

<p>Home port or broadcast domain Chose one of the following:</p> <p><b>Port:</b> Specify the port to which the logical interface returns when the LIF is reverted to its home port. This is only done for the first LIF in the subnet of an IPspace, otherwise it is not required.</p> <p><b>Broadcast Domain:</b> Specify the broadcast domain, and the system will select the appropriate port to which the logical interface returns when the LIF is reverted to its home port.</p>	Yes	
<p>Subnet name The subnet to assign to the SVM.</p> <p>All data LIFs used to create continuously available SMB connections to application servers must be on the same subnet.</p>	Yes (if using a subnet)	

### DNS configuration

You must configure DNS on the SVM before creating an NFS or SMB server.

Information	Required?	Your values
<p>SVM name The name of the SVM on which you want to create an NFS or SMB server.</p>	Yes	
<p>DNS domain name A list of domain names to append to a host name when performing host- to-IP name resolution.</p> <p>List the local domain first, followed by the domain names for which DNS queries are most often made.</p>	Yes	

<p>IP addresses of the DNS servers List of IP addresses for the DNS servers that will provide name resolution for the NFS or SMB server.</p> <p>The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the SMB server will join.</p> <p>The SRV record is used to map the name of a service to the DNS computer name of a server that offers that service. SMB server creation fails if ONTAP cannot obtain the service location records through local DNS queries.</p> <p>The simplest way to ensure that ONTAP can locate the Active Directory SRV records is to configure Active Directory-integrated DNS servers as the SVM DNS servers.</p> <p>You can use non-Active Directory-integrated DNS servers provided that the DNS administrator has manually added the SRV records to the DNS zone that contains information about the Active Directory domain controllers.</p> <p>For information about the Active Directory-integrated SRV records, see the topic <a href="#">How DNS Support for Active Directory Works on Microsoft TechNet</a>.</p>	<p>Yes</p>	
--	------------	--

**Dynamic DNS configuration**

Before you can use dynamic DNS to automatically add DNS entries to your Active Directory- integrated DNS servers, you must configure dynamic DNS (DDNS) on the SVM.

DNS records are created for every data LIF on the SVM. By creating multiple data LIFS on the SVM, you can load-balance client connections to the assigned data IP addresses. DNS load balances connections that are made using the host name to the assigned IP addresses in a round- robin fashion.

Information	Required?	Your values
<p>SVM name The SVM on which you want to create an NFS or SMB server.</p>	<p>Yes</p>	
<p>Whether to use DDNS Specifies whether to use DDNS.</p> <p>The DNS servers configured on the SVM must support DDNS. By default, DDNS is disabled.</p>	<p>Yes</p>	

<p>Whether to use secure DDNS Secure DDNS is supported only with Active Directory-integrated DNS.</p> <p>If your Active Directory-integrated DNS allows only secure DDNS updates, the value for this parameter must be true.</p> <p>By default, secure DDNS is disabled.</p> <p>Secure DDNS can be enabled only after a SMB server or an Active Directory account has been created for the SVM.</p>	No	
<p>FQDN of the DNS domain The FQDN of the DNS domain.</p> <p>You must use the same domain name configured for DNS name services on the SVM.</p>	No	

### Create IPspaces

You can use an IPspace to create a distinct IP address space for each SVM in a cluster. Doing so enables clients in administratively separate network domains to access cluster data while using overlapping IP addresses from the same IP address subnet range.

### Before you begin

You must be a cluster administrator to perform this task.

### Step

Create an IPspace.

```
network ipspace create -ipspace ipspacel
```

```
network ipspace show
```

IPspace	Vserver List	Broadcast Domains
Cluster	Cluster	Cluster
Default	Cluster1	Default
ipspacel	ipspacel	-

The IPspace is created, along with the system SVM for the IPspace. The system SVM carries management traffic.

### Move broadcast domains into IPspaces

Move the broadcast domains that the system created based on layer 2 reachability into the IPspaces you created.

Before you move the broadcast domain, you must verify the reachability of the ports in your broadcast domains.

The automatic scanning of ports can determine which ports can reach each other and place them in the same broadcast domain, but this scanning is unable to determine the appropriate IPspace. If the broadcast domain belongs in a non-default IPspace, then you must move it manually using the steps in this section.

### Before you begin

Broadcast domains are automatically configured as part of cluster create and join operations. ONTAP defines the "Default" broadcast domain to be the set of ports that have layer 2 connectivity to the home port of the management interface on the first node created in the cluster. Other broadcast domains are created, if necessary, and are named **Default-1**, **Default-2**, and so forth.

When a node joins an existing cluster, their network ports automatically join existing broadcast domains based on their layer 2 reachability. If they do not have reachability to an existing broadcast domain, the ports are placed into one or more new broadcast domains.

### About this task

- Ports with cluster LIFs are automatically placed into the "Cluster" IPspace.
- Ports with reachability to the home port of the node-management LIF are placed into the "Default" broadcast domain.
- Other broadcast domains are created by ONTAP automatically as part of the cluster create or join operation.
- As you add VLANs and interface groups, they are automatically placed into the appropriate broadcast domain about a minute after they are created.

### Steps

1. Verify the reachability of the ports in your broadcast domains. ONTAP automatically monitors layer 2 reachability. Use the following command to verify each port has been added to a broadcast domain and has "ok" reachability.

```
network port reachability show -detail
```

2. If necessary, move broadcast domains into other IPspaces:

```
network port broadcast-domain move
```

For example, if you want to move a broadcast domain from "Default" to "ips1":

```
network port broadcast-domain move -ip-space Default -broadcast-domain Default  
-to-ip-space ips1
```

### Repair port reachability

Broadcast domains are automatically created. However, if a port is recabled, or the switch configuration changes, a port might need to be repaired into a different broadcast domain (new or existing).

### Before you begin

You must be a cluster administrator to perform this task.



### About this task

A command is available to automatically repair the broadcast domain configuration for a port based on the layer 2 reachability detected by ONTAP.

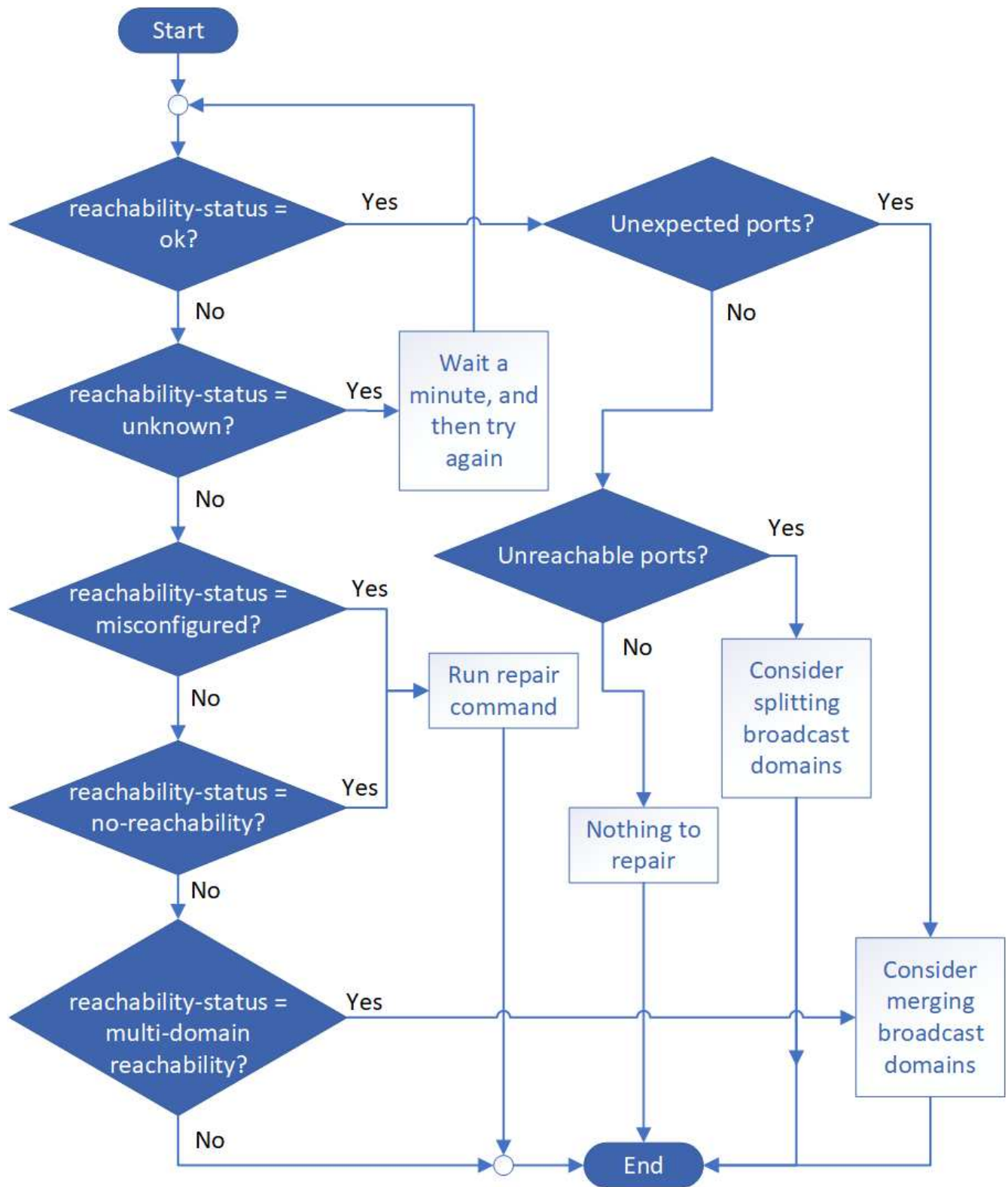
### Steps

1. Check your switch configuration and cabling.
2. Check the reachability of the port:

```
network port reachability show -detail -node -port
```

The command output contains reachability results.

3. Use the following decision tree and table to understand the reachability results and determine what, if anything, to do next.



Reachability-status	Description
---------------------	-------------

ok	<p>The port has layer 2 reachability to its assigned broadcast domain.</p> <p>If the reachability-status is "ok", but there are "unexpected ports", consider merging one or more broadcast domains. For more information, see the following <i>Unexpected ports</i> row.</p> <p>If the reachability-status is "ok", but there are "unreachable ports", consider splitting one or more broadcast domains. For more information, see the following <i>Unreachable ports</i> row.</p> <p>If the reachability-status is "ok", and there are no unexpected or unreachable ports, your configuration is correct.</p>
Unexpected ports	<p>The port has layer 2 reachability to its assigned broadcast domain; however, it also has layer 2 reachability to at least one other broadcast domain.</p> <p>Examine the physical connectivity and switch configuration to determine if it is incorrect or if the port's assigned broadcast domain needs to be merged with one or more broadcast domains.</p> <p>For more information, see <a href="#">Merge broadcast domains</a>.</p>
Unreachable ports	<p>If a single broadcast domain has become partitioned into two different reachability sets, you can split a broadcast domain to synchronize the ONTAP configuration with the physical network topology.</p> <p>Typically, the list of unreachable ports defines the set of ports that should be split into another broadcast domain after you have verified that the physical and switch configuration is accurate.</p> <p>For more information, see <a href="#">Split broadcast domains</a>.</p>
misconfigured-reachability	<p>The port does not have layer 2 reachability to its assigned broadcast domain; however, the port does have layer 2 reachability to a different broadcast domain.</p> <p>You can repair the port reachability. When you run the following command, the system will assign the port to the broadcast domain to which it has reachability:</p> <pre>network port reachability repair -node -port</pre>
no-reachability	<p>The port does not have layer 2 reachability to any existing broadcast domain.</p> <p>You can repair the port reachability. When you run the following command, the system will assign the port to a new automatically created broadcast domain in the Default IPspace:</p> <pre>network port reachability repair -node -port</pre>

multi-domain-reachability	<p>The port has layer 2 reachability to its assigned broadcast domain; however, it also has layer 2 reachability to at least one other broadcast domain.</p> <p>Examine the physical connectivity and switch configuration to determine if it is incorrect or if the port's assigned broadcast domain needs to be merged with one or more broadcast domains.</p> <p>For more information, see <a href="#">Merge broadcast domains</a>.</p>
unknown	<p>If the reachability-status is "unknown", then wait a few minutes and try the command again.</p>

After you repair a port, check for displaced LIFs and VLANs. If the port was part of an interface group, you also need to understand what happened to that interface group.

## LIFs

When a port is repaired and moved into a different broadcast domain, any LIFs that were configured on the repaired port will be automatically assigned a new home port. That home port is selected from the same broadcast domain on the same node, if possible. Alternatively, a home port from another node is selected, or, if no suitable home ports exist, the home port will be cleared.

If a LIF's home port is moved to another node, or is cleared, then the LIF is considered to have been "displaced". You can view these displaced LIFs with the following command:

```
displaced-interface show
```

If there are any displaced LIFs, you must either:

- Restore the home of the displaced LIF:

```
displaced-interface restore
```

- Set the home of the LIF manually:

```
network interface modify -home-port -home-node
```

- Remove the entry from the "displaced-interface" table if you are satisfied with the LIF's currently configured home:

```
displaced-interface delete
```

## VLANs

If the repaired port had VLANs, those VLANs are automatically deleted but are also recorded as having been "displaced". You can view these displaced VLANs:

```
displaced-vlans show
```

If there are any displaced VLANs, you must either:

- Restore the VLANs to another port:

```
displaced-vlans restore
```

- Remove the entry from the "displaced-vlans" table:

```
displaced-vlans delete
```

## Interface groups

If the repaired port was part of an interface group, it is removed from that interface group. If it was the only member port assigned to the interface group, the interface group itself is removed.

## Related topics

[Verify your network configuration after upgrading](#)

[Monitor the reachability of network ports](#)

## Create SVMs

You must create an SVM to serve data to clients.

### Before you begin

- You must be a cluster administrator to perform this task.
- You must know which security style the SVM root volume will have.

If you plan to implement a Hyper-V or SQL Server over SMB solution on this SVM, you should use NTFS security style for the root volume. Volumes that contain Hyper-V files or SQL database files must be set to NTFS security at the time they are created. By setting the root volume security style to NTFS, you ensure that you do not inadvertently create UNIX or mixed security-style data volumes.

### Steps

1. Determine which aggregates are candidates for containing the SVM root volume.

```
storage aggregate show -has-mroot false
```

You must choose an aggregate that has at least 1 GB of free space to contain the root volume. If you intend to configure NAS auditing on the SVM, you must have a minimum of 3 GB of extra free space on the root aggregate, with the extra space being used to create the auditing staging volume when auditing is enabled.



If NAS auditing is already enabled on an existing SVM, the aggregate's staging volume is created immediately after aggregate creation is successfully completed.

2. Record the name of the aggregate on which you want to create the SVM root volume.
3. If you plan on specifying a language when you create the SVM and do not know the value to use, identify and record the value of the language you want to specify:

```
vserver create -language ?
```

4. If you plan on specifying a Snapshot policy when you create the SVM and do not know the name of the policy, list the available policies and identify and record the name of the Snapshot policy you want to use:

```
volume snapshot policy show -vserver vserver_name
```

5. If you plan on specifying a quota policy when you create the SVM and do not know the name of the policy, list the available policies and identify and record the name of the quota policy you want to use:

```
volume quota policy show -vserver vserver_name
```

6. Create an SVM:

```
vserver create -vserver vserver_name -aggregate aggregate_name -rootvolume  
root_volume_name -rootvolume-security-style {unix|ntfs|mixed} [-ipspace  
IPspace_name] [-language <language>] [-snapshot-policy snapshot_policy_name]  
[-quota-policy quota_policy_name] [-comment comment]
```

```
vserver create -vserver vs1 -aggregate aggr3 -rootvolume vs1_root  
-rootvolume-security-style ntfs -ipspace ipspace1 -language en_US.UTF-8
```

```
[Job 72] Job succeeded: Vserver creation completed
```

7. Verify that the SVM configuration is correct.

```
vserver show -vserver vs1
```

```
Vserver: vs1
Vserver Type: data
Vserver Subtype: default
Vserver UUID: 11111111-1111-1111-1111-111111111111
Root Volume: vs1_root
Aggregate: aggr3
NIS Domain: -
Root Volume Security Style: ntfs
LDAP Client: -
Default Volume Language Code: en_US.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, ndmp
Disallowed Protocols: fcp, iscsi
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspace1
Is Vserver Protected: false
```

In this example, the command creates the SVM named "vs1" in IPspace "ipspace1". The root volume is named "vs1\_root" and is created on aggr3 with NTFS security style.

## Create LIFs

An SVM serves data to clients through one or more network logical interfaces (LIFs). You must create LIFs on the ports you want to use to access data.

### Before you begin

You must be a cluster administrator to perform this task.

### About this task

Beginning with ONTAP 9.7, ONTAP automatically chooses the home port of a LIF, as long as at least one LIF already exists in the same subnet in that IPspace. ONTAP chooses a home-port in the same broadcast domain as other LIFs in that subnet. You can still specify a home port, but it is no longer required (unless no LIFs yet exist in that subnet in the specified IPspace).

You should not configure LIFs that carry SMB traffic to automatically revert to their home nodes. This recommendation is mandatory if the SMB server is to host a solution for nondisruptive operations with Hyper-V or SQL Server over SMB.

## Steps

1. Determine which broadcast domain ports you want to use for the LIF.

```
network port broadcast-domain show -ipspace ipspace1
```

IPspace Name	Broadcast Domain name	MTU	Port List	Update Status	Details
ipspace1	default	1500	node1:e0d node1:e0e node2:e0d node2:e0e	complete complete complete complete	

2. Verify that the subnet you want to use for the LIFs contains sufficient unused IP addresses.

```
network subnet show -ipspace ipspace1
```

3. Create one or more LIFs on the ports you want to use to access data.

```
network interface create -vserver vs1 -lif lif1 -home-node node1 -home-port e0d -service-policy default-data-files -subnet-name ipspace1
```

4. Verify that the LIF interface configuration is correct.

```
network interface show -vserver vs1
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
vs1	lif1	up/up	10.0.0.128/24	node1	e0d	true

5. Verify that the failover group configuration is as desired.

```
network interface show -failover -vserver vs1
```

Vserver	Logical interface	Home Node:Port	Failover Policy	Failover Group
vs1	lif1	node1:e0d	system-defined	ipspace1

Failover Targets: node1:e0d, node1:e0e, node2:e0d, node2:e0e



## Configure DNS services

You must configure DNS services for the SVM before creating an NFS or SMB server. Generally, the DNS name servers are the Active Directory-integrated DNS servers for the domain that the NFS or SMB server will join.

### About this task

Active Directory-integrated DNS servers contain the service location records (SRV) for the domain LDAP and domain controller servers. If the SVM cannot find the Active Directory LDAP servers and domain controllers, NFS or SMB server setup fails.

SVMs use the hosts name services ns-switch database to determine which name services to use and in which order when looking up information about hosts. The two supported name services for the hosts database are files and dns.

You must ensure that dns is one of the sources before you create the SMB server.



To view the statistics for DNS name services for the mgwd process and SecD process, use the Statistics UI.

### Steps

1. Determine what the current configuration is for the hosts name services database. In this example, the hosts name service database uses the default settings.

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

```
Vserver: vs1
Name Service Switch Database: hosts
Vserver: vs1 Name Service Switch Database: hosts
Name Service Source Order: files, dns
```

2. Perform the following actions, if required.

- a. Add the DNS name service to the hosts name service database in the desired order, or reorder the sources.

In this example, the hosts database is configured to use DNS and local files in that order.

```
vserver services name-service ns-switch modify -vserver vs1 -database hosts
-sources dns,files
```

- b. Verify that the name services configuration is correct.

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

```
Vserver: vs1
Name Service Switch Database: hosts
Name Service Source Order: dns, files
```

### 3. Configure DNS services.

```
vserver services name-service dns create -vserver vs1 -domains
example.com,example2.com -name-servers 10.0.0.50,10.0.0.51
```



The `vserver services name-service dns create` command performs an automatic configuration validation and reports an error message if ONTAP is unable to contact the name server.

### 4. Verify that the DNS configuration is correct and that the service is enabled.

```
Vserver: vs1
Domains: example.com, example2.com Name Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled Timeout (secs): 2
Maximum Attempts: 1
```

### 5. Validate the status of the name servers.

```
vserver services name-service dns check -vserver vs1
```

Vserver	Name Server	Status	Status Details
vs1	10.0.0.50	up	Response time (msec): 2
vs1	10.0.0.51	up	Response time (msec): 2

## Configure dynamic DNS on the SVM

If you want the Active Directory-integrated DNS server to dynamically register the DNS records of an NFS or SMB server in DNS, you must configure dynamic DNS (DDNS) on the SVM.

### Before you begin

DNS name services must be configured on the SVM. If you are using secure DDNS, you must use Active Directory-integrated DNS name servers and you must have created either an NFS or SMB server or an Active Directory account for the SVM.

### About this task

The specified fully qualified domain name (FQDN) must be unique:

The specified fully qualified domain name (FQDN) must be unique:

- For NFS, the value specified in `-vserver-fqdn` as part of the `vserver services name-service dns dynamic-update` command becomes the registered FQDN for the LIFs.
- For SMB, the values specified as the CIFS server NetBIOS name and the CIFS server fully qualified domain name become the registered FQDN for the LIFs. This is not configurable in ONTAP. In the following scenario, the LIF FQDN is "CIFS\_VS1.EXAMPLE.COM":

```
cluster1::> cifs server show -vserver vs1
```

```

                                Vserver: vs1
                                CIFS Server NetBIOS Name: CIFS_VS1
                                NetBIOS Domain/Workgroup Name: EXAMPLE
                                Fully Qualified Domain Name: EXAMPLE.COM
                                Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
                                Workgroup Name: -
                                Kerberos Realm: -
                                Authentication Style: domain
                                CIFS Server Administrative Status: up
                                CIFS Server Description:
                                List of NetBIOS Aliases: -
```



To avoid a configuration failure of an SVM FQDN that is not compliant to RFC rules for DDNS updates, use an FQDN name that is RFC compliant. For more information, see [RFC 1123](#).

## Steps

1. Configure DDNS on the SVM:

```
vserver services name-service dns dynamic-update modify -vserver vserver_name
-is-enabled true [-use-secure {true|false} -vserver-fqdn
FQDN_used_for_DNS_updates
```

```
vserver services name-service dns dynamic-update modify -vserver vs1 -is
-enabled true - use-secure true -vserver-fqdn vs1.example.com
```

Asterisks cannot be used as part of the customized FQDN. For example, \*.netapp.com is not valid.

2. Verify that the DDNS configuration is correct:

```
vserver services name-service dns dynamic-update show
```

Vserver	Is-Enabled	Use-Secure	Vserver FQDN	TTL
vs1	true	true	vs1.example.com	24h

## ONTAP 9.7 and earlier

### Set up NAS path failover with the CLI (ONTAP 9.0-9.7)

This workflow guides you through the networking configuration steps to set up NAS path failover for ONTAP 9.0 - 9.7. This workflow assumes the following:

- You want to use NAS path failover best practices that simplify network configuration.
- You want to use the CLI, not System Manager.
- You are configuring networking on a new system running ONTAP 9.0 to 9.7.

If you are running an ONTAP release later than 9.7, you should use the NAS path failover procedure for ONTAP 9.8 or later:

- [ONTAP 9.8 and later NAS path failover workflow](#)

If you want details about network components and management, you should use the network management reference material:

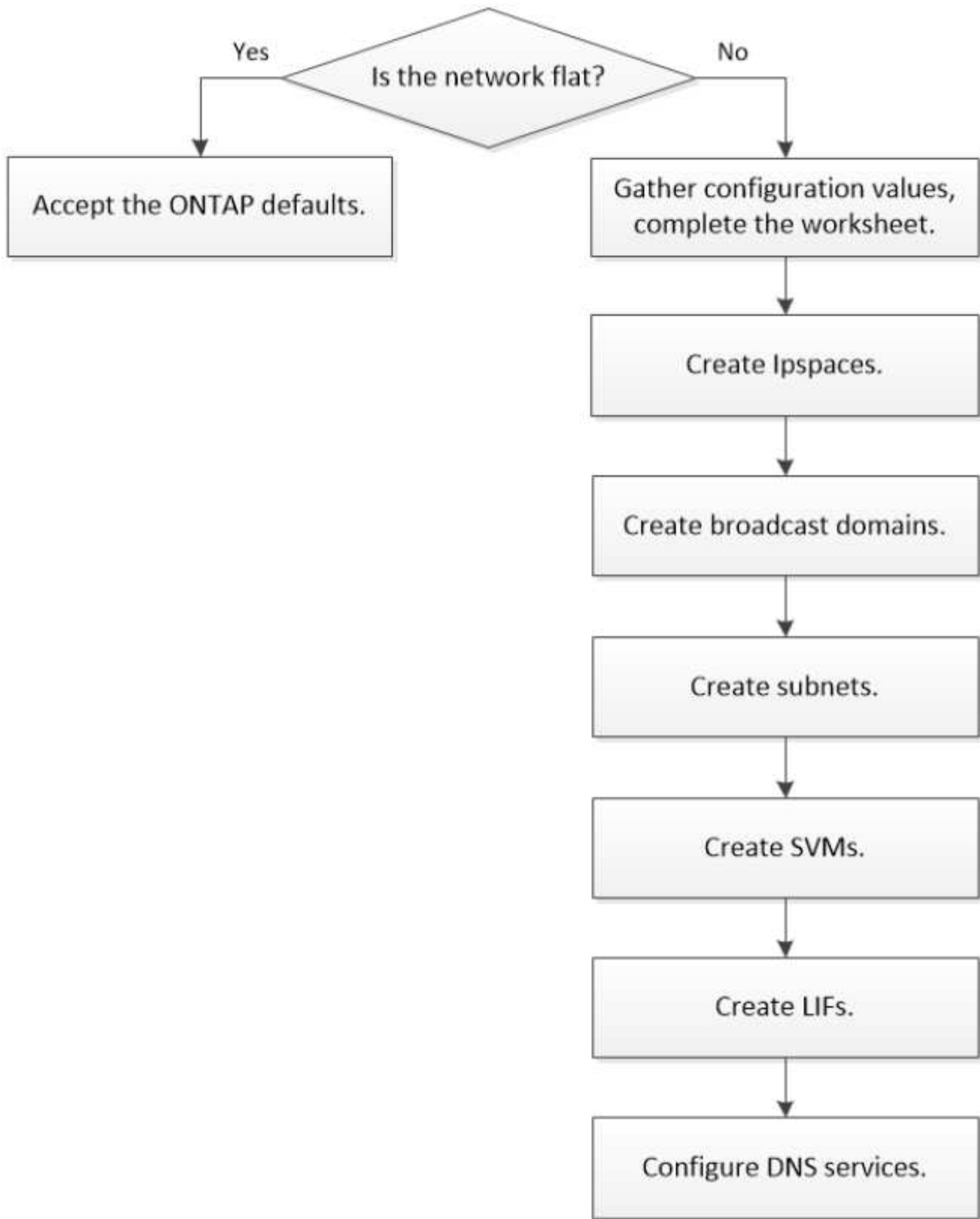
- [Network management overview](#)

## **Workflow NAS path failover**

### **Overview**

If you are already familiar with basic networking concepts, you might be able to save time setting up your network by reviewing this "hands on" workflow for NAS path failover configuration.

A NAS LIF automatically migrates to a surviving network port after a link failure on its current port. If your network is flat, you can rely on the ONTAP defaults to manage path failover. Otherwise, you should configure path failover following the steps in this workflow.



A SAN LIF does not migrate (unless you move it manually after the link failure). Instead, multipathing technology on the host diverts traffic to a different LIF. For more information, see [SAN administration](#).

You should complete all sections of the worksheet before configuring NAS path failover.

### IPspace configuration

You can use an IPspace to create a distinct IP address space for each SVM in a cluster. Doing so enables clients in administratively separate network domains to access cluster data while using overlapping IP addresses from the same IP address subnet range.

Information	Required?	Your values
IPspace name <ul style="list-style-type: none"> <li>• The name of the IPspace.</li> <li>• The name must be unique in the cluster.</li> </ul>	Yes	

### Broadcast domain configuration


A broadcast domain groups ports that belong in the same Layer 2 network and sets the MTU for the broadcast domain ports.

Broadcast domains are assigned to an IPspace. An IPspace can contain one or more broadcast domains.



The port to which a LIF fails over must be a member of the failover group for the LIF. When you create a broadcast domain, ONTAP automatically creates a failover group with the same name. The failover group contains all the ports assigned to the broadcast domain.

Information	Required?	Your values
IPspace name <ul style="list-style-type: none"> <li>• The IPspace to which the broadcast domain is assigned.</li> <li>• The IPspace must exist.</li> </ul>	Yes	
Broadcast domain name <ul style="list-style-type: none"> <li>• The name of the broadcast domain.</li> <li>• This name must be unique in the IPspace.</li> </ul>	Yes	

<p>MTU</p> <ul style="list-style-type: none"> <li>• The MTU of the broadcast domain.</li> <li>• Commonly set to either <b>1500</b> or <b>9000</b>.</li> <li>• The MTU value is applied to all ports in the broadcast domain and to any ports that are later added to the broadcast domain.</li> </ul> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;"> <p> The MTU value should match all the devices connected to that network. Note that the e0M port handling management and service processor traffic should have the MTU set to no more than 1500 bytes.</p> </div>	<p>Yes</p>	
<p>Ports</p> <ul style="list-style-type: none"> <li>• The network ports to add to the broadcast domain.</li> <li>• The ports assigned to the broadcast domain can be physical ports, VLANs, or interface groups (ifgroups).</li> <li>• If a port is in another broadcast domain, it must be removed before it can be added to the broadcast domain.</li> <li>• Ports are assigned by specifying both the node name and port: for example, node1:e0d.</li> </ul>	<p>Yes</p>	

### Subnet configuration

A subnet contains pools of IP addresses and a default gateway that can be assigned to LIFs used by SVMs residing in the IPspace.

- When creating a LIF on an SVM, you can specify the name of the subnet instead of supplying an IP address and a subnet.
- Since a subnet can be configured with a default gateway, you do not have to create the default gateway in

a separate step when creating an SVM.

- A broadcast domain can contain one or more subnets.  
You can configure SVM LIFs that are on different subnets by associating more than one subnet with the IPspace's broadcast domain.
- Each subnet must contain IP addresses that do not overlap with IP addresses assigned to other subnets in the same IPspace.
- You can assign specific IP addresses to SVM data LIFs and create a default gateway for the SVM instead of using a subnet.

Information	Required?	Your values
IPspace name <ul style="list-style-type: none"> <li>• The IPspace to which the subnet will be assigned.</li> <li>• The IPspace must exist.</li> </ul>	Yes	
Subnet name <ul style="list-style-type: none"> <li>• The name of the subnet.</li> <li>• The name must be unique in the IPspace.</li> </ul>	Yes	
Broadcast domain name <ul style="list-style-type: none"> <li>• The broadcast domain to which the subnet will be assigned.</li> <li>• The broadcast domain must reside in the specified IPspace.</li> </ul>	Yes	
Subnet name and mask <ul style="list-style-type: none"> <li>• The subnet and mask in which the IP addresses reside.</li> </ul>	Yes	
Gateway <ul style="list-style-type: none"> <li>• You can specify a default gateway for the subnet.</li> <li>• If you do not assign a gateway when you create the subnet, you can assign one to the subnet at any time.</li> </ul>	No	



<p>IP address ranges</p> <ul style="list-style-type: none"> <li>You can specify a range of IP addresses or specific IP addresses. For example, you can specify a range such as: 192.168.1.1– 192.168.1.100, 192.168.1.112, 192.168.1.145</li> <li>If you do not specify an IP address range, the entire range of IP addresses in the specified subnet are available to assign to LIFs.</li> </ul>	No	
<p>Force update of LIF associations</p> <ul style="list-style-type: none"> <li>Specifies whether to force the update of existing LIF associations.</li> <li>By default, subnet creation fails if any service processor interfaces or network interfaces are using the IP addresses in the ranges provided.</li> <li>Using this parameter associates any manually addressed interfaces with the subnet and allows the command to succeed.</li> </ul>	No	

### SVM configuration

You use SVMs to serve data to clients and hosts.

The values you record are for creating a default data SVM. If you are creating a MetroCluster source SVM, see the [Fabric-attached MetroCluster Installation and Configuration Guide](#) or the [Stretch MetroCluster Installation and Configuration Guide](#).

Information	Required?	Your values
<p>SVM name</p> <ul style="list-style-type: none"> <li>The name of the SVM.</li> <li>You should use a fully qualified domain name (FQDN) to ensure unique SVM names across cluster leagues.</li> </ul>	Yes	


<p>Root volume name</p> <ul style="list-style-type: none"> <li>• The name of the SVM root volume.</li> </ul>	Yes	
<p>Aggregate name</p> <ul style="list-style-type: none"> <li>• The name of the aggregate that holds the SVM root volume.</li> <li>• This aggregate must exist.</li> </ul>	Yes	
<p>Security style</p> <ul style="list-style-type: none"> <li>• The security style for the SVM root volume.</li> <li>• Possible values are <b>ntfs</b>, <b>unix</b>, and <b>mixed</b>.</li> </ul>	Yes	
<p>IPspace name</p> <ul style="list-style-type: none"> <li>• The IPspace to which the SVM is assigned.</li> <li>• This IPspace must exist.</li> </ul>	No	
<p>SVM language setting</p> <ul style="list-style-type: none"> <li>• The default language to use for the SVM and its volumes.</li> <li>• If you do not specify a default language, the default SVM language is set to <b>C.UTF-8</b>.</li> <li>• The SVM language setting determines the character set used to display file names and data for all NAS volumes in the SVM. You can modify The language after the SVM is created.</li> </ul>	No	

## LIF configuration

An SVM serves data to clients and hosts through one or more network logical interfaces (LIFs).

Information	Required?	Your values
<p>SVM name</p> <ul style="list-style-type: none"> <li>• The name of the SVM for the LIF.</li> </ul>	Yes	

<p>LIF name</p> <ul style="list-style-type: none"> <li>• The name of the LIF.</li> <li>• You can assign multiple data LIFs per node, and you can assign LIFs to any node in the cluster, provided that the node has available data ports.</li> <li>• To provide redundancy, you should create at least two data LIFs for each data subnet, and the LIFs assigned to a particular subnet should be assigned home ports on different nodes.</li> </ul> <p><b>Important:</b> If you are configuring a SMB server to host Hyper-V or SQL Server over SMB for nondisruptive operation solutions, the SVM must have at least one data LIF on every node in the cluster.</p>	<p>Yes</p>	
<p>LIF role</p> <ul style="list-style-type: none"> <li>• The role of the LIF.</li> <li>• Data LIFs are assigned the data role.</li> </ul>	<p>Yes Deprecated from ONTAP 9.6</p>	<p>data</p>
<p>Service policy Service policy for the LIF.</p> <p>The service policy defines which network services can use the LIF. Built-in services and service policies are available for managing data and management traffic on both data and system SVMs.</p>	<p>Yes Beginning with ONTAP 9.6</p>	

<p>Allowed protocols</p> <ul style="list-style-type: none"> <li>• The protocols that can use the LIF.</li> <li>• By default, SMB, NFS, and FlexCache are allowed. The FlexCache protocol enables a volume to be used as an origin volume for a FlexCache volume on a system running Data ONTAP operating in 7-Mode.</li> </ul> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  <p>The protocols that use the LIF cannot be modified after the LIF is created. You should specify all protocols when you configure the LIF.</p> </div>	No	
<p>Home node</p> <ul style="list-style-type: none"> <li>• The node to which the LIF returns when the LIF is reverted to its home port.</li> <li>• You should record a home node for each data LIF.</li> </ul>	Yes	
<p>Home port or broadcast domain</p> <ul style="list-style-type: none"> <li>• The port to which the logical interface returns when the LIF is reverted to its home port.</li> <li>• You should record a home port for each data LIF.</li> </ul>	Yes	
<p>Subnet name</p> <ul style="list-style-type: none"> <li>• The subnet to assign to the SVM.</li> <li>• All data LIFs used to create continuously available SMB connections to application servers must be on the same subnet.</li> </ul>	Yes (if using a subnet)	

## DNS configuration

You must configure DNS on the SVM before creating an NFS or SMB server.

Information	Required?	Your values
<p>SVM name</p> <ul style="list-style-type: none"><li>• The name of the SVM on which you want to create an NFS or SMB server.</li></ul>	Yes	
<p>DNS domain name</p> <ul style="list-style-type: none"><li>• A list of domain names to append to a host name when performing host- to-IP name resolution.</li><li>• List the local domain first, followed by the domain names for which DNS queries are most often made.</li></ul>	Yes	

<p>IP addresses of the DNS servers</p> <p>* List of IP addresses for the DNS servers that will provide name resolution for the NFS or SMB server.</p> <p>* The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the SMB server will join. The SRV record is used to map the name of a service to the DNS computer name of a server that offers that service. SMB server creation fails if ONTAP cannot obtain the service location records through local DNS queries. The simplest way to ensure that ONTAP can locate the Active Directory SRV records is to configure Active Directory-integrated DNS servers as the SVM DNS servers. You can use non-Active Directory-integrated DNS servers provided that the DNS administrator has manually added the SRV records to the DNS zone that contains information about the Active Directory domain controllers.</p> <p>* For information about the Active Directory-integrated SRV records, see the topic <a href="#">How DNS Support for Active Directory Works on Microsoft TechNet</a>.</p>	<p>Yes</p>	
--	------------	--

**Dynamic DNS configuration**

Before you can use dynamic DNS to automatically add DNS entries to your Active Directory- integrated DNS servers, you must configure dynamic DNS (DDNS) on the SVM.

DNS records are created for every data LIF on the SVM. By creating multiple data LIFS on the SVM, you can load-balance client connections to the assigned data IP addresses. DNS load balances connections that are made using the host name to the assigned IP addresses in a round- robin fashion.

Information	Required?	Your values
<p>SVM name</p> <ul style="list-style-type: none"> <li>The SVM on which you want to create an NFS or SMB server.</li> </ul>	<p>Yes</p>	

<p>Whether to use DDNS</p> <ul style="list-style-type: none"> <li>• Specifies whether to use DDNS.</li> <li>• The DNS servers configured on the SVM must support DDNS. By default, DDNS is disabled.</li> </ul>	Yes	
<p>Whether to use secure DDNS</p> <ul style="list-style-type: none"> <li>• Secure DDNS is supported only with Active Directory-integrated DNS.</li> <li>• If your Active Directory-integrated DNS allows only secure DDNS updates, the value for this parameter must be true.</li> <li>• By default, secure DDNS is disabled.</li> <li>• Secure DDNS can be enabled only after a SMB server or an Active Directory account has been created for the SVM.</li> </ul>	No	
<p>FQDN of the DNS domain</p> <ul style="list-style-type: none"> <li>• The FQDN of the DNS domain.</li> <li>• You must use the same domain name configured for DNS name services on the SVM.</li> </ul>	No	

### Create IPspaces

You can use an IPspace to create a distinct IP address space for each SVM in a cluster. Doing so enables clients in administratively separate network domains to access cluster data while using overlapping IP addresses from the same IP address subnet range.

### Before you begin

You must be a cluster administrator to perform this task.

### Step

Create an IPspace.

```
network ipspace create -ipspace ipspace1
```

```
network ipspace show
```

IPspace	Vserver List	Broadcast Domains
Cluster	Cluster	Cluster
Default	Cluster1	Default
ipspacel	ipspacel	-

The IPspace is created, along with the system SVM for the IPspace. The system SVM carries management traffic.

**Determining which ports can be used for a broadcast domain**

Before you can configure a broadcast domain to add to the new IPspace, you must determine what ports are available for the broadcast domain.



This task is relevant for ONTAP 9.0 - 9.7, not ONTAP 9.8.

**Before you begin**

You must be a cluster administrator to perform this task.

**About this task**

- Ports can be physical ports, VLANs, or interface groups (ifgroups).
- The ports that you want to add to the new broadcast domain cannot be assigned to an existing broadcast domain.
- If the ports that you want to add to the broadcast domain are already in another broadcast domain (for example, the Default broadcast domain in the Default IPspace), you must remove the ports from that broadcast domain before assigning them to the new broadcast domain.
- Ports that have LIFs assigned to them cannot be removed from a broadcast domain.
- Because the cluster management and node management LIFs are assigned to the Default broadcast domain in the Default IPspace, the ports assigned to these LIFs cannot be removed from the Default broadcast domain.

**Steps**

1. Determine the current port assignments.

```
network port show
```



Node	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper
node1						
	e0a	Cluster	Cluster	up	9000	auto/1000
	e0b	Cluster	Cluster	up	9000	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	Default	up	1500	auto/1000
	e0f	Default	Default	up	1500	auto/1000
	e0g	Default	Default	up	1500	auto/1000
node2						
	e0a	Cluster	Cluster	up	9000	auto/1000
	e0b	Cluster	Cluster	up	9000	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	Default	up	1500	auto/1000
	e0f	Default	Default	up	1500	auto/1000
	e0g	Default	Default	up	1500	auto/1000

In this example, the output from the command provides the following information:

- Ports e0c, e0d, e0e, e0f, and e0g on each node are assigned to the Default broadcast domain.
- These ports are potentially available to use in the broadcast domain of the IPspace that you want to create.

2. Determine which ports in the Default broadcast domain are assigned to LIF interfaces, and therefore cannot be moved to a new broadcast domain.

network interface show

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
Cluster						
	node1_clus1	up/up	10.0.2.40/24	node1	e0a	true
	node1_clus2	up/up	10.0.2.41/24	node1	e0b	true
	node2_clus1	up/up	10.0.2.42/24	node2	e0a	true
	node2_clus2	up/up	10.0.2.43/24	node2	e0b	true
cluster1						
	cluster_mgmt	up/up	10.0.1.41/24	node1	e0c	true
	node1_mgmt	up/up	10.0.1.42/24	node1	e0c	true
	node2_mgmt	up/up	10.0.1.43/24	node2	e0c	true

In the following example, the output from the command provides the following information:

- The node ports are assigned to port `e0c` on each node and the cluster administrative LIF's home node is on `e0c` on `node1`.
- Ports `e0d`, `e0e`, `e0f`, and `e0g` on each node are not hosting LIFs and can be removed from the Default broadcast domain and then added to a new broadcast domain for the new IPspace.

### Remove ports from a broadcast domain

If the ports that you want to add to the new broadcast domain are already in another broadcast domain, you must remove the ports from that broadcast domain before assigning them to the new broadcast domain.



This task is relevant for ONTAP 9.0 - 9.7, not ONTAP 9.8.

### Before you begin

You must be a cluster administrator to perform this task.

### Steps

1. Remove ports from the broadcast domain specifying the following:
  - IPspace, `Default` in the following sample.
  - Broadcast domain, `Default` in the following sample.
  - Ports, using the node and port syntax, `node1:e0d,node1:e0e,node2:e0d,node2:e0e` in the following sample.

```
network port broadcast-domain remove-ports -ipspace Default
-broadcast-domain Default -ports
node1:e0d,node1:e0e,node2:e0d,node2:e0e
```

2. Verify that the ports were removed from the broadcast domain:

```
network port show
```

### Create a broadcast domain

You must create a broadcast domain for a custom IPspace. The SVMs created in the IPspace use the ports in the broadcast domain.



This task is relevant for ONTAP 9.0 - 9.7, not ONTAP 9.8.

### Before you begin

You must be a cluster administrator to perform this task.

### About this task

The port to which a LIF fails over must be a member of the failover group for the LIF. When you create a broadcast domain, ONTAP automatically creates a failover group with the same name. The failover group contains all the ports assigned to the broadcast domain.

## Steps

1. Create a broadcast domain.

```
network port broadcast-domain create -ip-space ip-space1 -broadcast-domain  
-ip-space1 -mtu 1500 -ports node1:e0d,node1:e0e,node2:e0d,node2:e0e
```

2. Verify that the broadcast domain configuration is correct.

- a. Verify the broadcast domain is correct:

```
network port broadcast-domain show
```

- b. Verify the network port is correct:

```
network port show
```

- c. Verify the failover group names and failover targets are correct:

```
network interface failover-groups show
```

## Create a subnet

You can create a subnet to allocate specific blocks of IPv4 or IPv6 addresses to be used later when you create LIFs for the SVM.

This enables you to create LIFs more easily by specifying a subnet name instead of having to specify IP address and network mask values for each LIF.

## Before you begin

You must be a cluster administrator to perform this task.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

## System Manager

Beginning with ONTAP 9.12.0, you can use System Manager to create a subnet

### Steps

1. Select **Network > Overview > Subnets**.
2. Click **+ Add** to create a subnet.
3. Name the subnet.
4. Specify the subnet IP address.
5. Set the subnet mask.
6. Define the range of IP addresses that comprise the subnet.
7. If useful, specify a gateway.
8. Select the broadcast domain to which the subnet belongs.
9. Save your changes.
  - a. If the IP address or range entered is already used by an interface, the following message is displayed:  
An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?
  - b. When you click **OK**, the existing LIF will be associated with the subnet.

## CLI

Use the CLI to create a subnet

### Steps

1. Create a subnet.

```
network subnet create -broadcast-domain ipspace1 -ip-space ipspace1 -subnet
-name ipspace1 -subnets 10.0.0.0/24 -gateway 10.0.0.1 -ip-ranges
"10.0.0.128-10.0.0.130,10.0.0.132"
```

The subnet name can be either a subnet IP value such as 192.0.2.0/24 or a string such as ipspace1 like the one used in this example.

2. Verify that the subnet configuration is correct.

The output from this example shows information about the subnet named ipspace1 in the ipspace1 IPspace. The subnet belongs to the broadcast domain name ipspace1. You can assign the IP addresses in this subnet to data LIFs for SVMs created in the ipspace1 IPspace.

```
network subnet show -ip-space ipspace1
```

## Create SVMs

You must create an SVM to serve data to clients.

### Before you begin

- You must be a cluster administrator to perform this task.

- You must know which security style the SVM root volume will have.

If you plan to implement a Hyper-V or SQL Server over SMB solution on this SVM, you should use NTFS security style for the root volume. Volumes that contain Hyper-V files or SQL database files must be set to NTFS security at the time they are created. By setting the root volume security style to NTFS, you ensure that you do not inadvertently create UNIX or mixed security-style data volumes.

## Steps

1. Determine which aggregates are candidates for containing the SVM root volume.

```
storage aggregate show -has-mroot false
```

You must choose an aggregate that has at least 1 GB of free space to contain the root volume. If you intend to configure NAS auditing on the SVM, you must have a minimum of 3 GB of extra free space on the root aggregate, with the extra space being used to create the auditing staging volume when auditing is enabled.



If NAS auditing is already enabled on an existing SVM, the aggregate's staging volume is created immediately after aggregate creation is successfully completed.

2. Record the name of the aggregate on which you want to create the SVM root volume.
3. If you plan on specifying a language when you create the SVM and do not know the value to use, identify and record the value of the language you want to specify:

```
vserver create -language ?
```

4. If you plan on specifying a Snapshot policy when you create the SVM and do not know the name of the policy, list the available policies and identify and record the name of the Snapshot policy you want to use:

```
volume snapshot policy show -vserver vserver_name
```

5. If you plan on specifying a quota policy when you create the SVM and do not know the name of the policy, list the available policies and identify and record the name of the quota policy you want to use:

```
volume quota policy show -vserver vserver_name
```

6. Create an SVM:

```
vserver create -vserver vserver_name -aggregate aggregate_name -rootvolume  
root_volume_name -rootvolume-security-style {unix|ntfs|mixed} [-ipspace  
IPspace_name] [-language <language>] [-snapshot-policy snapshot_policy_name]  
[-quota-policy quota_policy_name] [-comment comment]
```

```
vserver create -vserver vs1 -aggregate aggr3 -rootvolume vs1_root  
-rootvolume-security-style ntfs -ipspace ipspace1 -language en_US.UTF-8
```

```
[Job 72] Job succeeded: Vserver creation completed
```

7. Verify that the SVM configuration is correct.

```
vserver show -vserver vs1
```

```
Vserver: vs1
Vserver Type: data
Vserver Subtype: default
Vserver UUID: 11111111-1111-1111-1111-111111111111
Root Volume: vs1_root
Aggregate: aggr3
NIS Domain: -
Root Volume Security Style: ntfs
LDAP Client: -
Default Volume Language Code: en_US.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, ndmp
Disallowed Protocols: fcp, iscsi
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspace1
Is Vserver Protected: false
```

In this example, the command creates the SVM named "vs1" in IPspace "ipspace1". The root volume is named "vs1\_root" and is created on aggr3 with NTFS security style.

### Create LIFs

An SVM serves data to clients through one or more network logical interfaces (LIFs). You must create LIFs on the ports you want to use to access data.

### Before you begin

You must be a cluster administrator to perform this task.

### About this task

Beginning with ONTAP 9.7, ONTAP automatically chooses the home port of a LIF, as long as at least one LIF already exists in the same subnet in that IPspace. ONTAP chooses a home-port in the same broadcast domain as other LIFs in that subnet. You can still specify a home port, but it is no longer required (unless no LIFs yet exist in that subnet in the specified IPspace).

You should not configure LIFs that carry SMB traffic to automatically revert to their home nodes. This recommendation is mandatory if the SMB server is to host a solution for nondisruptive operations with Hyper-V or SQL Server over SMB.

## Steps

1. Determine which broadcast domain ports you want to use for the LIF.

```
network port broadcast-domain show -ipspace ipspace1
```

IPspace Name	Broadcast Domain name	MTU	Port List	Update Status	Details
ipspace1	default	1500	node1:e0d node1:e0e node2:e0d node2:e0e	complete complete complete complete	

2. Verify that the subnet you want to use for the LIFs contains sufficient unused IP addresses.

```
network subnet show -ipspace ipspace1
```

3. Create one or more LIFs on the ports you want to use to access data.

```
network interface create -vserver vs1 -lif lif1 -home-node node1 -home-port e0d -service-policy default-data-files -subnet-name ipspace1
```

4. Verify that the LIF interface configuration is correct.

```
network interface show -vserver vs1
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
vs1	lif1	up/up	10.0.0.128/24	node1	e0d	true

5. Verify that the failover group configuration is as desired.

```
network interface show -failover -vserver vs1
```

Vserver	Logical interface	Home Node:Port	Failover Policy	Failover Group
vs1	lif1	node1:e0d	system-defined	ipspace1

Failover Targets: node1:e0d, node1:e0e, node2:e0d, node2:e0e

## Configure DNS services

You must configure DNS services for the SVM before creating an NFS or SMB server. Generally, the DNS name servers are the Active Directory-integrated DNS servers for the domain that the NFS or SMB server will join.

### About this task

Active Directory-integrated DNS servers contain the service location records (SRV) for the domain LDAP and domain controller servers. If the SVM cannot find the Active Directory LDAP servers and domain controllers, NFS or SMB server setup fails.

SVMs use the hosts name services ns-switch database to determine which name services to use and in which order when looking up information about hosts. The two supported name services for the hosts database are `files` and `dns`.

You must ensure that `dns` is one of the sources before you create the SMB server.



To view the statistics for DNS name services for the `mgwd` process and `SecD` process, use the Statistics UI.

### Steps

1. Determine what the current configuration is for the `hosts` name services database.

In this example, the hosts name service database uses the default settings.

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

```
Vserver: vs1
Name Service Switch Database: hosts
Name Service Source Order: files, dns
```

2. Perform the following actions, if required.
  - a. Add the DNS name service to the hosts name service database in the desired order, or reorder the sources.

In this example, the hosts database is configured to use DNS and local files in that order.

```
vserver services name-service ns-switch modify -vserver vs1 -database hosts
-sources dns,files
```

- b. Verify that the name services configuration is correct.

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

3. Configure DNS services.

```
vserver services name-service dns create -vserver vs1 -domains
example.com,example2.com -name-servers 10.0.0.50,10.0.0.51
```





The `vserver services name-service dns create` command performs an automatic configuration validation and reports an error message if ONTAP is unable to contact the name server.

4. Verify that the DNS configuration is correct and that the service is enabled.

```
Vserver: vs1
Domains: example.com, example2.com Name
Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled Timeout (secs): 2
Maximum Attempts: 1
```

5. Validate the status of the name servers.

```
vserver services name-service dns check -vserver vs1
```

Vserver	Name Server	Status	Status Details
vs1	10.0.0.50	up	Response time (msec): 2
vs1	10.0.0.51	up	Response time (msec): 2

## Configure dynamic DNS on the SVM

If you want the Active Directory-integrated DNS server to dynamically register the DNS records of an NFS or SMB server in DNS, you must configure dynamic DNS (DDNS) on the SVM.

### Before you begin

DNS name services must be configured on the SVM. If you are using secure DDNS, you must use Active Directory-integrated DNS name servers and you must have created either an NFS or SMB server or an Active Directory account for the SVM.

### About this task

The specified fully qualified domain name (FQDN) must be unique:

- For NFS, the value specified in `-vserver-fqdn` as part of the `vserver services name-service dns dynamic-update` command becomes the registered FQDN for the LIFs.
- For SMB, the values specified as the CIFS server NetBIOS name and the CIFS server fully qualified domain name become the registered FQDN for the LIFs. This is not configurable in ONTAP. In the following scenario, the LIF FQDN is "CIFS\_VS1.EXAMPLE.COM":

```
cluster1::> cifs server show -vserver vs1
```

```

                                Vserver: vs1
                                CIFS Server NetBIOS Name: CIFS_VS1
                                NetBIOS Domain/Workgroup Name: EXAMPLE
                                Fully Qualified Domain Name: EXAMPLE.COM
                                Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
                                Workgroup Name: -
                                Kerberos Realm: -
                                Authentication Style: domain
                                CIFS Server Administrative Status: up
                                CIFS Server Description:
                                List of NetBIOS Aliases: -
```



To avoid a configuration failure of an SVM FQDN that is not compliant to RFC rules for DDNS updates, use an FQDN name that is RFC compliant. For more information, see [RFC 1123](#).

## Steps

1. Configure DDNS on the SVM:

```
vserver services name-service dns dynamic-update modify -vserver vserver_name
-is-enabled true [-use-secure {true|false} -vserver-fqdn
FQDN_used_for_DNS_updates
```

```
vserver services name-service dns dynamic-update modify -vserver vs1 -is
-enabled true - use-secure true -vserver-fqdn vs1.example.com
```

Asterisks cannot be used as part of the customized FQDN. For example, \*.netapp.com is not valid.

2. Verify that the DDNS configuration is correct:

```
vserver services name-service dns dynamic-update show
```

Vserver	Is-Enabled	Use-Secure	Vserver FQDN	TTL
vs1	true	true	vs1.example.com	24h

## Configure dynamic DNS services

If you want the Active Directory-integrated DNS server to dynamically register the DNS records of an NFS or SMB server in DNS, you must configure dynamic DNS (DDNS) on the SVM.

## Before you begin

DNS name services must be configured on the SVM. If you are using secure DDNS, you must use Active Directory-integrated DNS name servers and you must have created either an NFS or SMB server or an Active Directory account for the SVM.

### About this task

The specified FQDN must be unique.



To avoid a configuration failure of an SVM FQDN that is not compliant to RFC rules for DDNS updates, use an FQDN name that is RFC compliant.

### Steps

1. Configure DDNS on the SVM:

```
vserver services name-service dns dynamic-update modify -vserver vserver_name  
-is-enabled true [-use-secure {true|false} -vserver-fqdn  
FQDN_used_for_DNS_updates
```

```
vserver services name-service dns dynamic-update modify -vserver vs1 -is-  
-enabled true - use-secure true -vserver-fqdn vs1.example.com
```

Asterisks cannot be used as part of the customized FQDN. For example, \*.netapp.com is not valid.

2. Verify that the DDNS configuration is correct:

```
vserver services name-service dns dynamic-update show
```

Vserver	Is-Enabled	Use-Secure	Vserver FQDN	TTL
vs1	true	true	vs1.example.com	24h

## Manage your network with the CLI

### Network management overview

You can use the following information to perform basic storage network administration. You can configure physical and virtual network ports (VLANs and interface groups), create LIFs using IPv4 and IPv6, manage routing and host-resolution services in clusters, use load balancing to optimize network traffic, and monitor a cluster using SNMP.

Unless otherwise stated, these procedures apply to all versions of ONTAP 9.

You should use these procedures under the following circumstances:

- You want to understand the range of ONTAP network management capabilities.
- You want to use the CLI, not System Manager.

## Upgrade considerations

### Network features by release

Analyze the impact of network features available with each ONTAP 9 release.

Available beginning	Feature	Description
ONTAP 9.12.0	System Manager networking enhancements	<p>System Manager offers more control over networking functions, including the following:</p> <ul style="list-style-type: none"><li>• Link Aggregation Groups (LAGs)</li><li>• VLANs</li><li>• Broadcast domains</li><li>• Subnets</li><li>• Network interfaces</li></ul> <p><a href="#">Combine physical ports to create interface groups</a></p> <p><a href="#">Configure VLANs over physical ports</a></p> <p><a href="#">Add a broadcast domain</a></p> <p><a href="#">Delete a broadcast domain</a></p> <p><a href="#">Display subnets</a></p> <p><a href="#">Create a subnet</a></p> <p><a href="#">Delete a subnet</a></p> <p><a href="#">Add or remove IP addresses from a subnet</a></p> <p><a href="#">Change subnet properties</a></p> <p><a href="#">Create a LIF</a></p> <p><a href="#">Modify a LIF</a></p> <p><a href="#">Migrate a LIF</a></p> <p><a href="#">Revert a LIF to its home port</a></p> <p><a href="#">Viewing and managing your network</a></p>

ONTAP 9.11.1	iSCSI LIF Failover	<p>The new iSCSI LIF failover feature supports automatic and manual migration of iSCSI LIFs in an SFO partner failover and in a local failover.</p> <p>It is available for All SAN Array (ASA) platforms.</p> <p><a href="#">iSCSI LIF failover for ASA platforms</a></p>
ONTAP 9.11.1	LIF Services	<p>New client-side LIF services provide more control over which LIFs are used for outbound AD, DNS, LDAP, and NIS requests.</p> <p><a href="#">LIFs and service policies in ONTAP 9.6 and later</a></p>
ONTAP 9.11.1	Link Layer Discovery Protocol (LLDP)	<p>The cluster network supports LLDP to allow ONTAP to work with cluster switches that do not support Cisco Discovery Protocol (CDP).</p> <p><a href="#">Display network connectivity with neighbor discovery protocols</a></p>
ONTAP 9.10.1	Automatic detection and repair recommendations for network wiring issues	<p>ONTAP can automatically detect and recommend corrections for network wiring issues based on a broadcast domain constituent's (ethernet ports) layer-2 reachability.</p> <p>When a port reachability issue is detected, System Manager recommends a repair operation to resolve the issue.</p> <p><a href="#">Automatic detection and repair recommendations for network wiring issues</a></p>
ONTAP 9.10.1	Internet Protocol security (IPsec) certificate authentication	<p>IPsec policies now support pre-shared keys (PSKs) and certificates for authentication.</p> <ul style="list-style-type: none"> <li>• Policies configured with PSKs require sharing of the key among all clients in the policy.</li> <li>• Policies configured with certificates do not require sharing of the key among clients because each client can have its own unique certificate for authentication.</li> </ul> <p><a href="#">Configure IP security (IPsec) over wire encryption</a></p>
ONTAP 9.10.1	LIF services	<p>Firewall policies are deprecated and wholly replaced with LIF service policies.</p> <p>A new NTP LIF service provides more control over which LIFs are used for outbound NTP requests.</p> <p><a href="#">LIFs and service policies in ONTAP 9.6 and later</a></p>

ONTAP 9.10.1	NFS over RDMA	<p>ONTAP offers support for NFS over RDMA, a higher performance realization of NFSv4.0 for customers with the NVIDIA GDX ecosystem. Utilizing RDMA adapters allows memory to be copied directly from storage to the GPU, circumventing the CPU overhead.</p> <p><a href="#">NFS over RDMA</a></p>
ONTAP 9.9.1	Cluster resiliency	<p>The following cluster resiliency and diagnostic improvements improve the customer experience:</p> <ul style="list-style-type: none"> <li>• Port monitoring and avoidance: <ul style="list-style-type: none"> <li>◦ In two-node switchless cluster configurations, the system avoids ports that experience total packet loss (connectivity loss). Previously this functionality was only available in switched configurations.</li> </ul> </li> <li>• Automatic node failover: <ul style="list-style-type: none"> <li>◦ If a node cannot serve data across its cluster network, that node should not own any disks. Instead its HA partner should take over, if the partner is healthy.</li> </ul> </li> <li>• Commands to analyze connectivity issues: <ul style="list-style-type: none"> <li>◦ Use the following command to display which cluster paths are experiencing packet loss:  <pre>network interface check cluster- connectivity show</pre> </li> </ul> </li> </ul>

<p>ONTAP 9.9.1</p>	<p>VIP LIF enhancements</p>	<p>The following fields have been added to extend virtual IP (VIP) border gateway protocol (BGP) functionality:</p> <ul style="list-style-type: none"> <li>• <code>-asn</code> or <code>-peer-asn</code> (4-byte value) The attribute itself is not new, but it now uses a 4-byte integer.</li> <li>• <code>-med</code></li> <li>• <code>-use-peer-as-next-hop</code></li> </ul> <p>The <code>asn_integer</code> parameter specifies the autonomous system number (ASN) or peer ASN.</p> <ul style="list-style-type: none"> <li>• Beginning with ONTAP 9.8, ASN for BGP supports a 2-byte non-negative integer. This is a 16-bit number (0 - 64511 available values).</li> <li>• Beginning with ONTAP 9.9.1, ASN for BGP supports a 4-byte non-negative integer (65536 - 4294967295). The default ASN is 65501. ASN 23456 is reserved for ONTAP session establishment with peers that do not announce 4-byte ASN capability.</li> </ul> <p>You can make advanced route selections with Multi-Exit Discriminator (MED) support for path prioritization. MED is an optional attribute in the BGP update message that tells routers to select the best route for the traffic. The MED is an unsigned 32-bit integer (0 - 4294967295); lower values are preferred.</p> <p>VIP BGP provides default route automation using BGP peer grouping to simplify configuration. ONTAP has a simple way to learn default routes using the BGP peers as next-hop routers when the BGP peer is on the same subnet. To use the feature, set the <code>-use-peer-as-next-hop</code> attribute to <code>true</code>. By default, this attribute is <code>false</code>.</p> <p><a href="#">Configure virtual IP (VIP) LIFs</a></p>
--------------------	-----------------------------	--

<p>ONTAP 9.8</p>	<p>Auto port placement</p>	<p>ONTAP can automatically configure broadcast domains, select ports, and help configure network interfaces (LIFs), virtual LANs (VLANs), and link aggregation groups (LAGs) based on reachability and network topology detection.</p> <p>When you first create a cluster, ONTAP automatically discovers the networks connected to ports and configures the needed broadcast domains based on layer 2 reachability. You no longer have to configure broadcast domains manually.</p> <p>A new cluster will continue to be created with two IPspaces:</p> <p><b>Cluster IPspace:</b> Containing one broadcast domain for the cluster interconnect. You should never touch this configuration.</p> <p><b>Default IPspace:</b> Containing one or more broadcast domains for the remaining ports. Depending on your network topology, ONTAP configures additional broadcast domains as needed: Default-1, Default-2, and so on. You can rename these broadcast domains if desired, but do not modify which ports are configured in these broadcast domains.</p> <p>When you configure network interfaces, the home port selection is optional. If you do not manually select a home port, ONTAP will attempt to assign an appropriate home port in the same broadcast domain as other network interfaces in the same subnet.</p> <p>When creating a VLAN or adding the first port to a newly created LAG, ONTAP will attempt to automatically assign the VLAN or LAG to the appropriate broadcast domain based on its layer 2 reachability.</p> <p>By automatically configuring broadcast domains and ports, ONTAP helps to ensure that clients maintain access to their data during failover to another port or node in the cluster.</p> <p>Finally, ONTAP sends EMS messages when it detects that the port reachability is incorrect and provides the "network port reachability repair" command to automatically repair common misconfigurations.</p>
<p>ONTAP 9.8</p>	<p>Internet Protocol security (IPsec) over wire encryption</p>	<p>To ensure data is continuously secure and encrypted, even while in transit, ONTAP uses the IPsec protocol in transport mode. IPsec offers data encryption for all IP traffic including the NFS, iSCSI, and SMB protocols. IPsec provides the only encryption in flight option for iSCSI traffic.</p> <p>Once IPsec is configured, network traffic between the client and ONTAP is protected with preventive measures to combat replay and man-in-the-middle (MITM) attacks.</p> <p><a href="#">Configure IP security (IPsec) over wire encryption</a></p>



ONTAP 9.8	Virtual IP (VIP) expansion	<p>New fields have been added to the <code>network bgp peer-group</code> command. This expansion allows you to configure two additional Border Gateway Protocol (BGP) attributes for Virtual IP (VIP).</p> <p><b>AS path prepend:</b> Other factors being equal, BGP prefers to select the route with shortest AS (autonomous system) Path. You can use the optional AS path prepend attribute to repeat an autonomous system number (ASN), which increases the length of the AS path attribute. The route update with the shortest AS path will be selected by the receiver.</p> <p><b>BGP community:</b> The BGP community attribute is a 32-bit tag that can be assigned to the route updates. Each route update can have one or more BGP community tags. The neighbors receiving the prefix can examine the community value and take actions like filtering or applying specific routing policies for redistribution.</p>
ONTAP 9.8	Switch CLI simplification	<p>To simplify switch commands, the cluster and storage switch CLIs are consolidated. The consolidated switch CLIs include Ethernet switches, FC switches, and ATTO protocol bridges.</p> <p>Instead of using separate "system cluster-switch" and "system storage-switch" commands, you now use "system switch". For the ATTO protocol bridge, instead of using "storage bridge", use "system bridge".</p> <p>Switch health monitoring has similarly expanded to monitor the storage switches as well as the cluster interconnect switch. You can view health information for the cluster interconnect under "cluster_network" in the "client_device" table. You can view health information for a storage switch under "storage_network" in the "client_device" table.</p>
ONTAP 9.8	IPv6 variable length	<p>The supported IPv6 variable prefix length range has increased from 64 to 1 through 127 bits. A value of bit 128 remains reserved for virtual IP (VIP).</p> <p>When upgrading, non-VIP LIF lengths other than 64 bits are blocked until the last node is updated.</p> <p>When reverting an upgrade, the revert checks any non-VIP LIFs for any prefix other than 64 bits. If found, the check blocks the revert until you delete or modify the offending LIF. VIP LIFs are not checked.</p>

ONTAP 9.7	Automatic portmap service	<p>The portmap service maps RPC services to the ports on which they listen.</p> <p>The portmap service is always accessible in ONTAP 9.3 and earlier, is configurable in ONTAP 9.4 through ONTAP 9.6, and is managed automatically beginning with ONTAP 9.7.</p> <p><b>In ONTAP 9.3 and earlier:</b> The portmap service (rpcbind) is always accessible on port 111 in network configurations that rely on the built-in ONTAP firewall rather than a third-party firewall.</p> <p><b>From ONTAP 9.4 through ONTAP 9.6:</b> You can modify firewall policies to control whether the portmap service is accessible on particular LIFs.</p> <p><b>Beginning with ONTAP 9.7:</b> The portmap firewall service is eliminated. Instead, the portmap port is opened automatically for all LIFs that support the NFS service.</p> <p><a href="#">Portmap service configuration</a></p>
ONTAP 9.7	Cache search	<p>You can cache NIS <code>netgroup.byhost</code> entries using the <code>vserver services name-service nis-domain netgroup-database</code> commands.</p>
ONTAP 9.6	CUBIC	<p>CUBIC is the default TCP congestion control algorithm for ONTAP hardware. CUBIC replaced the ONTAP 9.5 and earlier default TCP congestion control algorithm, NewReno.</p> <p>CUBIC addresses the problems of long, fat networks (LFNs), including high round trip times (RTTs). CUBIC detects and avoids congestion. CUBIC improves performance for most environments.</p>
ONTAP 9.6	LIF service policies replace LIF roles	<p>You can assign service policies (instead of LIF roles) to LIFs that determine the kind of traffic that is supported for the LIFs. Service policies define a collection of network services supported by a LIF. ONTAP provides a set of built-in service policies that can be associated with a LIF.</p> <p>ONTAP supports service policies beginning with ONTAP 9.5; however, service policies can only be used to configure a limited number of services. Beginning with with ONTAP 9.6, LIF roles are deprecated and service policies are supported for all types of services.</p> <p><a href="#">LIFs and service policies</a></p>
ONTAP 9.5	NTPv3 support	<p>Network Time Protocol (NTP) version 3 includes symmetric authentication using SHA-1 keys, which increases network security.</p>

ONTAP 9.5	SSH login security alerts	When you log in as a Secure Shell (SSH) admin user, you can view information about previous logins, unsuccessful attempts to log in, and changes to your role and privileges since your last successful login.
ONTAP 9.5	LIF service policies	You can create new service policies or use a built-in policy. You can assign a service policy to one or more LIFs; thereby allowing the LIF to carry traffic for a single service or a list of services.  <a href="#">LIFs and service policies</a>
ONTAP 9.5	VIP LIFs and BGP support	A VIP data LIF is a LIF that is not part of any subnet and is reachable from all ports that host a border gateway protocol (BGP) LIF in the same IPspace. A VIP data LIF eliminates the dependency of a host on individual network interfaces.  <a href="#">Create a virtual IP (VIP) data LIF</a>
ONTAP 9.5	Multipath routing	Multipath routing provides load balancing by utilizing all the available routes to a destination.  <a href="#">Enable multipath routing</a>
ONTAP 9.4	Portmap service	The portmap service maps remote procedure call (RPC) services to the ports on which they listen.  The portmap service is always accessible in ONTAP 9.3 and earlier. Beginning with ONTAP 9.4, the portmap service is configurable.  You can modify firewall policies to control whether the portmap service is accessible on particular LIFs.  <a href="#">Portmap service configuration</a>
ONTAP 9.4	SSH MFA for LDAP or NIS	SSH multi-factor authentication (MFA) for LDAP or NIS uses a public key and nsswitch to authenticate remote users.
ONTAP 9.3	SSH MFA	SSH MFA for local administrator accounts use a public key and a password to authenticate local users.
ONTAP 9.3	SAML authentication	You can use Security Assertion Markup Language (SAML) authentication to configure MFA for web services such as Service Processor Infrastructure (spi), ONTAP APIs, and OnCommand System Manager.
ONTAP 9.2	SSH login attempts	You can configure the maximum number of unsuccessful SSH login attempts to protect against brute force attacks.

ONTAP 9.2	Digital security certificates	ONTAP provides enhanced support for digital certificate security with Online Certificate Status Protocol (OCSP) and pre-installed default security certificates.
ONTAP 9.2	Fastpath	<p>As part of a networking stack update for improved performance and resiliency, fast path routing support was removed in ONTAP 9.2 and later releases because it made it difficult to identify problems with improper routing tables. Therefore, it is no longer possible to set the following option in the nodeshell, and existing fast path configurations are disabled when upgrading to ONTAP 9.2 and later:</p> <pre>ip.fastpath.enable</pre> <p><a href="#">Network traffic not sent or sent out of an unexpected interface after upgrade to 9.2 due to elimination of IP Fastpath</a></p>
ONTAP 9.1	Security with SNMPv3 traphosts	<p>You can configure SNMPv3 traphosts with the User-based Security Model (USM) security. With this enhancement, SNMPv3 traps can be generated by using a predefined USM user's authentication and privacy credentials.</p> <p><a href="#">Configure traphosts to receive SNMP notifications</a></p>
ONTAP 9.0	IPv6	<p>Dynamic DNS (DDNS) name service is available on IPv6 LIFs.</p> <p><a href="#">Create a LIF</a></p>
ONTAP 9.0	LIFs per node	<p>The supported number of LIFs per node has increased for some systems. See the Hardware Universe for the number of LIFs supported on each platform for a specified ONTAP release.</p> <p><a href="#">Create a LIF</a></p> <p><a href="#">NetApp hardware universe</a></p>
ONTAP 9.0	LIF management	<p>ONTAP and System Manager automatically detect and isolate network port failures. LIFs are automatically migrated from degraded ports to healthy ports.</p> <p><a href="#">Monitor the health of network ports</a></p>
ONTAP 9.0	LLDP	<p>Link Layer Discovery Protocol (LLDP) provides a vendor-neutral interface for verifying and troubleshooting cabling between an ONTAP system and a switch or router. It is an alternative to Cisco Discovery Protocol (CDP), a proprietary link layer protocol developed by Cisco Systems.</p> <p><a href="#">Enable or Disable LLDP</a></p>

ONTAP 9.0	UC compliance with DSCP marking	<p>Unified Capability (UC) compliance with Differentiated Services Code Point (DSCP) marking.</p> <p>Differentiated Services Code Point (DSCP) marking is a mechanism for classifying and managing network traffic and is a component of Unified Capability (UC) compliance. You can enable DSCP marking on outgoing (egress) IP packet traffic for a given protocol with a default or user-provided DSCP code.</p> <p>If you do not provide a DSCP value when enabling DSCP marking for a given protocol, a default is used:</p> <p><b>0x0A (10):</b> The default value for data protocols/traffic.</p> <p><b>0x30 (48):</b> The default value for control protocols/traffic.</p> <p><a href="#">DSCP marking for US compliance</a></p>
ONTAP 9.0	SHA-2 password hash function	<p>To enhance password security, ONTAP 9 supports the SHA-2 password hash function and uses SHA-512 by default for hashing newly created or changed passwords.</p> <p>Existing user accounts with unchanged passwords continue to use the MD5 hash function after the upgrade to ONTAP 9 or later, and users can continue to access their accounts. However, it is strongly recommended that you migrate MD5 accounts to SHA-512 by having users change their passwords.</p>
ONTAP 9.0	FIPS 140-2 support	<p>You can enable the Federal Information Processing Standard (FIPS) 140-2 compliance mode for cluster-wide control plane web service interfaces.</p> <p>By default, the FIPS 140-2 only mode is disabled.</p> <p><a href="#">Configure network security using Federal Information Processing Standards (FIPS)</a></p>

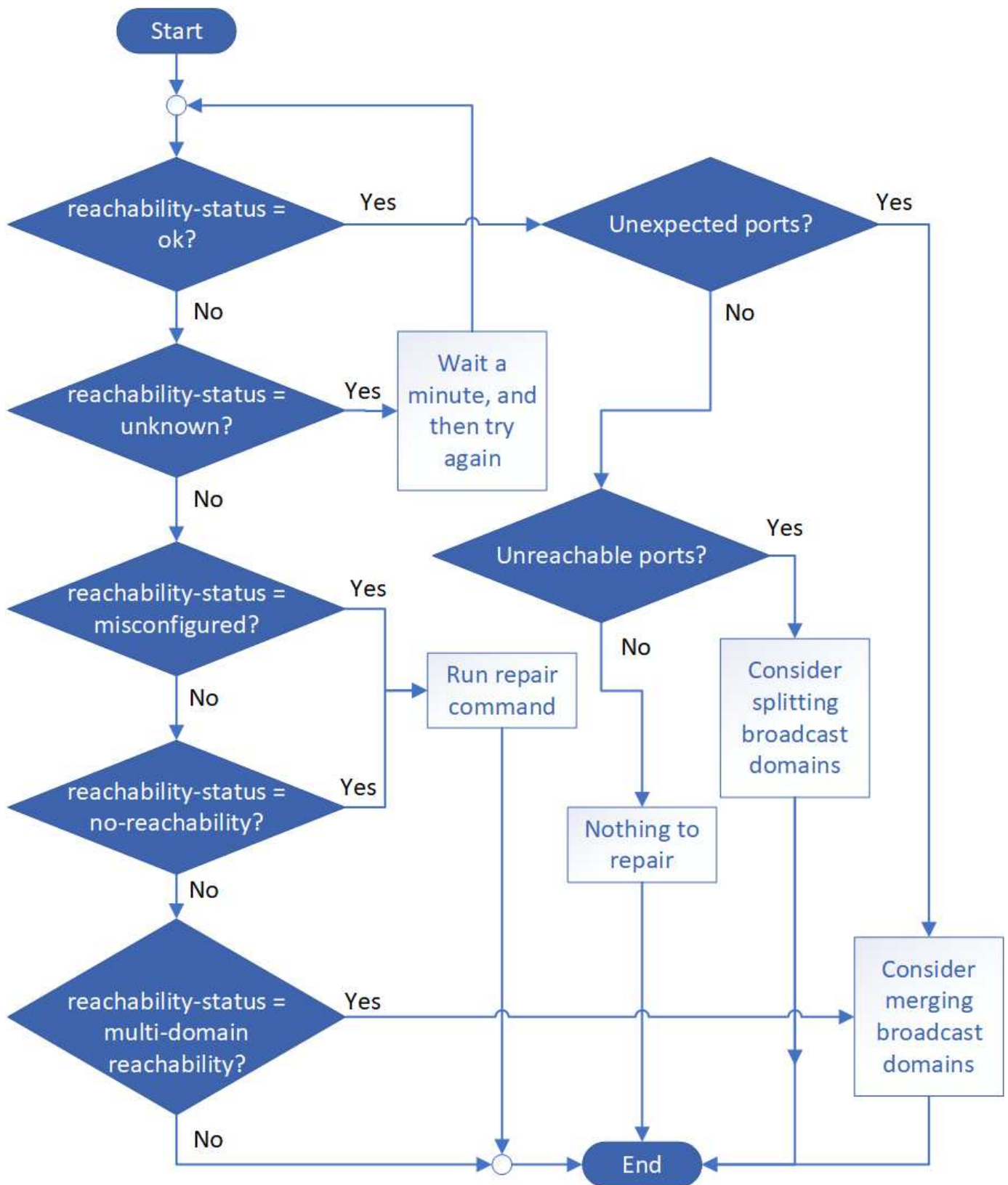
### Verify your networking configuration after upgrading to ONTAP 9.8 or later

After an upgrade to ONTAP 9.8, you should verify your network configuration. After the upgrade, ONTAP automatically monitors layer 2 reachability.

Use the following command to verify each port has reachability to its expected broadcast domain:

```
network port reachability show -detail
```

The command output contains reachability results. Use the following decision tree and table to understand the reachability results (reachability-status) and determine what, if anything, to do next.



reachability-status	Description
---------------------	-------------

ok	<p>The port has layer 2 reachability to its assigned broadcast domain.</p> <p>If the reachability-status is "ok", but there are "unexpected ports", consider merging one or more broadcast domains. For more information, see <a href="#">Merge broadcast domains</a>.</p> <p>If the reachability-status is "ok", but there are "unreachable ports", consider splitting one or more broadcast domains. For more information, see <a href="#">Split broadcast domains</a>.</p> <p>If the reachability-status is "ok", and there are no unexpected or unreachable ports, your configuration is correct.</p>
misconfigured-reachability	<p>The port does not have layer 2 reachability to its assigned broadcast domain; however, the port does have layer 2 reachability to a different broadcast domain.</p> <p>You can repair the port reachability. When you run the following command, the system will assign the port to the broadcast domain to which it has reachability:</p> <pre>network port reachability repair -node -port</pre> <p>For more information, see <a href="#">Repair port reachability</a>.</p>
no-reachability	<p>The port does not have layer 2 reachability to any existing broadcast domain.</p> <p>You can repair the port reachability. When you run the following command, the system will assign the port to a new automatically created broadcast domain in the Default IPspace:</p> <pre>network port reachability repair -node -port</pre> <p>For more information, see <a href="#">Repair port reachability</a>.</p>
multi-domain-reachability	<p>The port has layer 2 reachability to its assigned broadcast domain; however, it also has layer 2 reachability to at least one other broadcast domain.</p> <p>Examine the physical connectivity and switch configuration to determine if it is incorrect or if the port's assigned broadcast domain needs to be merged with one or more broadcast domains.</p> <p>For more information, see <a href="#">Merge broadcast domains</a> or <a href="#">Repair port reachability</a>.</p>
unknown	<p>If the reachability-status is "unknown", then wait a few minutes and try the command again.</p>

After you repair a port, you need to check for and resolve displaced LIFs and VLANs. If the port was part of an interface group, you also need to understand what happened to that interface group. For more information, see [Repair port reachability](#).

## Networking components of a cluster

## Overview

You should familiarize yourself with the networking components of a cluster before setting up the cluster. Configuring the physical networking components of a cluster into logical components provides the flexibility and multi-tenancy functionality in ONTAP.

The various networking components in a cluster are as follows:

- Physical ports

Network interface cards (NICs) and host bus adapters (HBAs) provide physical (Ethernet and Fibre Channel) connections from each node to the physical networks (management and data networks).

For site requirements, switch information, port cabling information, and controller onboard port cabling, see the Hardware Universe at [hwu.netapp.com](http://hwu.netapp.com).

- Logical ports

Virtual local area networks (VLANs) and interface groups constitute the logical ports. Interface groups treat several physical ports as a single port, while VLANs subdivide a physical port into multiple separate ports.

- IPspaces

You can use an IPspace to create a distinct IP address space for each SVM in a cluster. Doing so enables clients in administratively separate network domains to access cluster data while using overlapping IP addresses from the same IP address subnet range.

- Broadcast domains

A broadcast domain resides in an IPspace and contains a group of network ports, potentially from many nodes in the cluster, that belong to the same layer 2 network. The ports in the group are used in an SVM for data traffic.

- Subnets

A subnet is created within a broadcast domain and contains a pool of IP addresses that belong to the same layer 3 subnet. This pool of IP addresses simplifies IP address allocation during LIF creation.

- Logical interfaces

A logical interface (LIF) is an IP address or a worldwide port name (WWPN) that is associated with a port. It is associated with attributes such as failover groups, failover rules, and firewall rules. A LIF communicates over the network through the port (physical or logical) to which it is currently bound.

The different types of LIFs in a cluster are data LIFs, cluster-scoped management LIFs, node-scoped management LIFs, intercluster LIFs, and cluster LIFs. The ownership of the LIFs depends on the SVM where the LIF resides. Data LIFs are owned by data SVMs, node-scoped management LIFs, cluster-scoped management, and intercluster LIFs are owned by the admin SVMs, and cluster LIFs are owned by the cluster SVM.

- DNS zones

DNS zone can be specified during the LIF creation, providing a name for the LIF to be exported through the cluster's DNS server. Multiple LIFs can share the same name, allowing the DNS load balancing feature to distribute IP addresses for the name according to load.

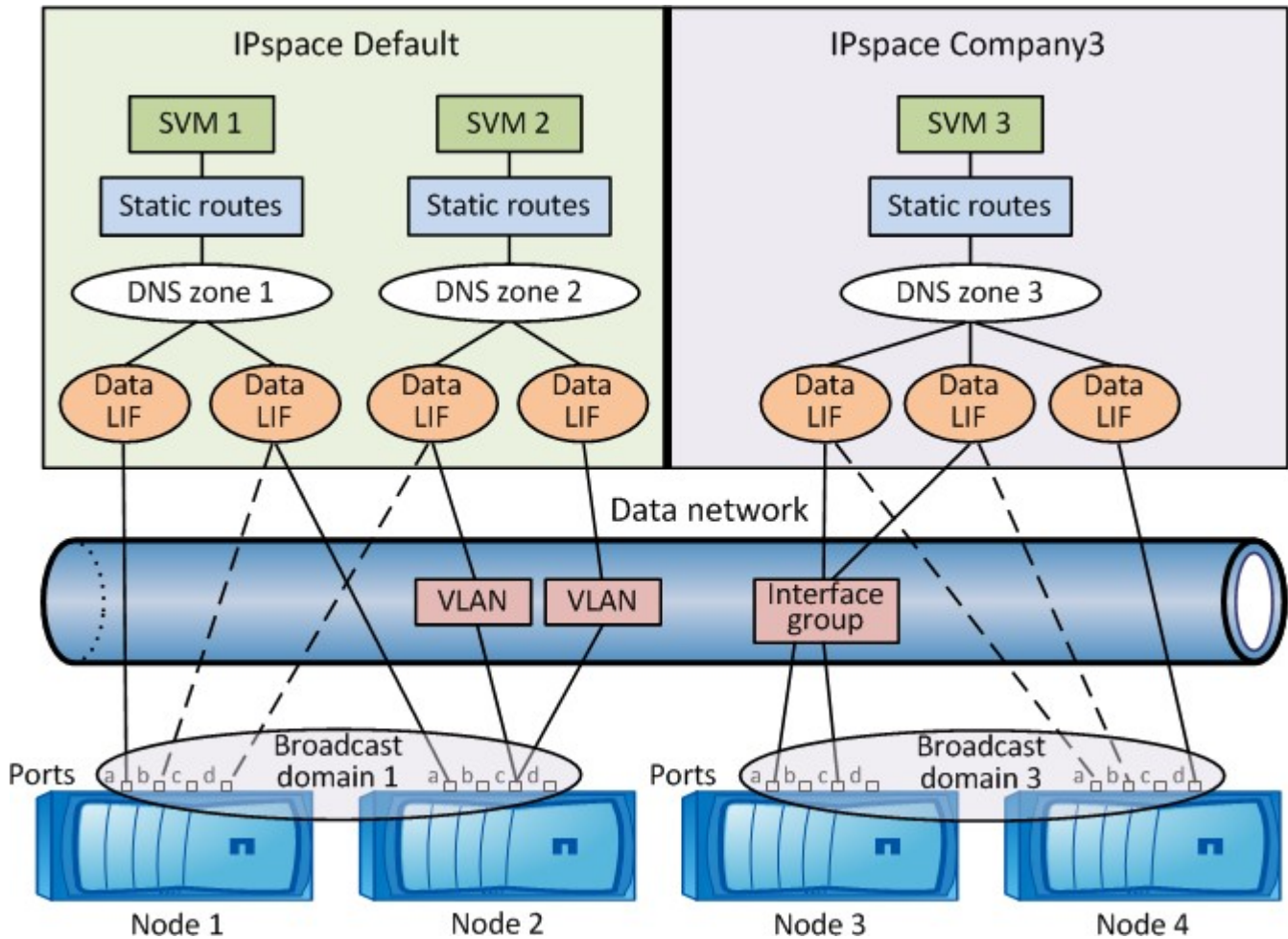


SVMs can have multiple DNS zones.

- Routing

Each SVM is self-sufficient with respect to networking. An SVM owns LIFs and routes that can reach each of the configured external servers.

The following figure illustrates how the different networking components are associated in a four-node cluster:

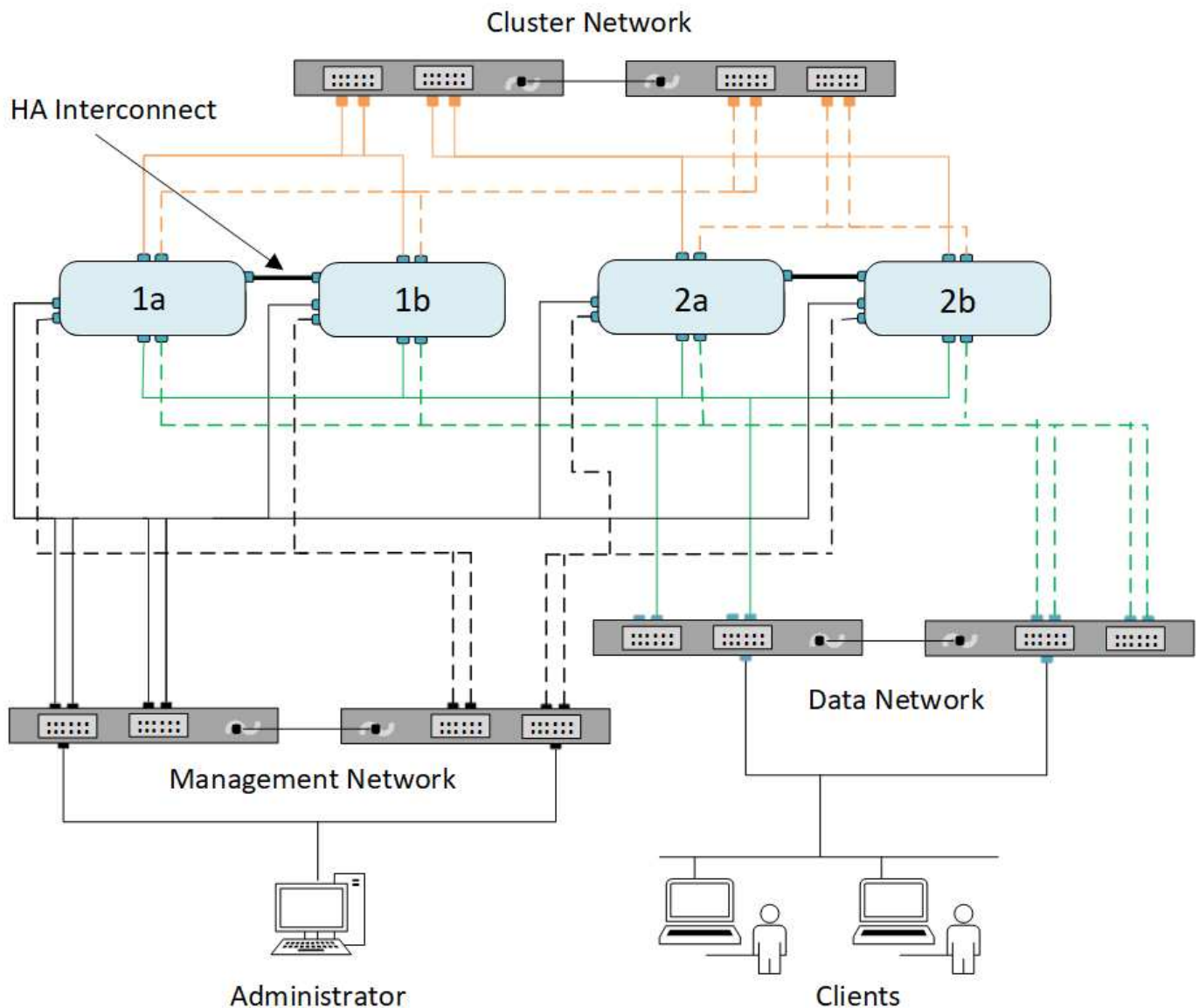


### Network cabling guidelines

Network cabling best practices separate traffic into the following networks: cluster, management, and data.

You should cable a cluster so that the cluster traffic is on a separate network from all other traffic. It is an optional, but recommended practice to have network management traffic separated from data and intracluster traffic. By maintaining separate networks, you can achieve better performance, ease of administration, and improved security and management access to the nodes.

The following diagram illustrates the network cabling of a four-node HA cluster that includes three separate networks:



You should follow certain guidelines when cabling network connections:

- Each node should be connected to three distinct networks.

One network is for management, one is for data access, and one is for intracluster communication. The management and data networks can be logically separated.

- You can have more than one data network connection to each node for improving the client (data) traffic flow.
- A cluster can be created without data network connections, but it must include a cluster interconnect connection.
- There should always be two or more cluster connections to each node, but nodes on FAS22xx systems can be configured with a single 10-GbE cluster port.

For more information on network cabling, see the [AFF and FAS System Documentation Center](#) and the [Hardware Universe](#).

## Relationship between broadcast domains, failover groups, and failover policies

Broadcast domains, failover groups, and failover policies work together to determine which port will take over when the node or port on which a LIF is configured fails.

A broadcast domain lists all the ports reachable in the same layer 2 Ethernet network. An Ethernet broadcast packet sent from one of the ports is seen by all other ports in the broadcast domain. This common-reachability characteristic of a broadcast domain is important to LIFs because if a LIF were to fail over to any other port in the broadcast domain, it could still reach every local and remote host that was reachable from the original port.

Failover groups define the ports within a broadcast domain that provide LIF failover coverage for each other. Each broadcast domain has one failover group that includes all its ports. This failover group containing all ports in the broadcast domain is the default and recommended failover group for the LIF. You can create failover groups with smaller subsets that you define, such as a failover group of ports that have the same link speed within a broadcast domain.

A failover policy dictates how a LIF uses the ports of a failover group when a node or port goes down. Consider the failover policy as a type of filter that is applied to a failover group. The failover targets for a LIF (the set of ports to which a LIF can failover) is determined by applying the LIF's failover policy to the LIF's failover group in the broadcast domain.

You can view the failover targets for a LIF using the following CLI command:

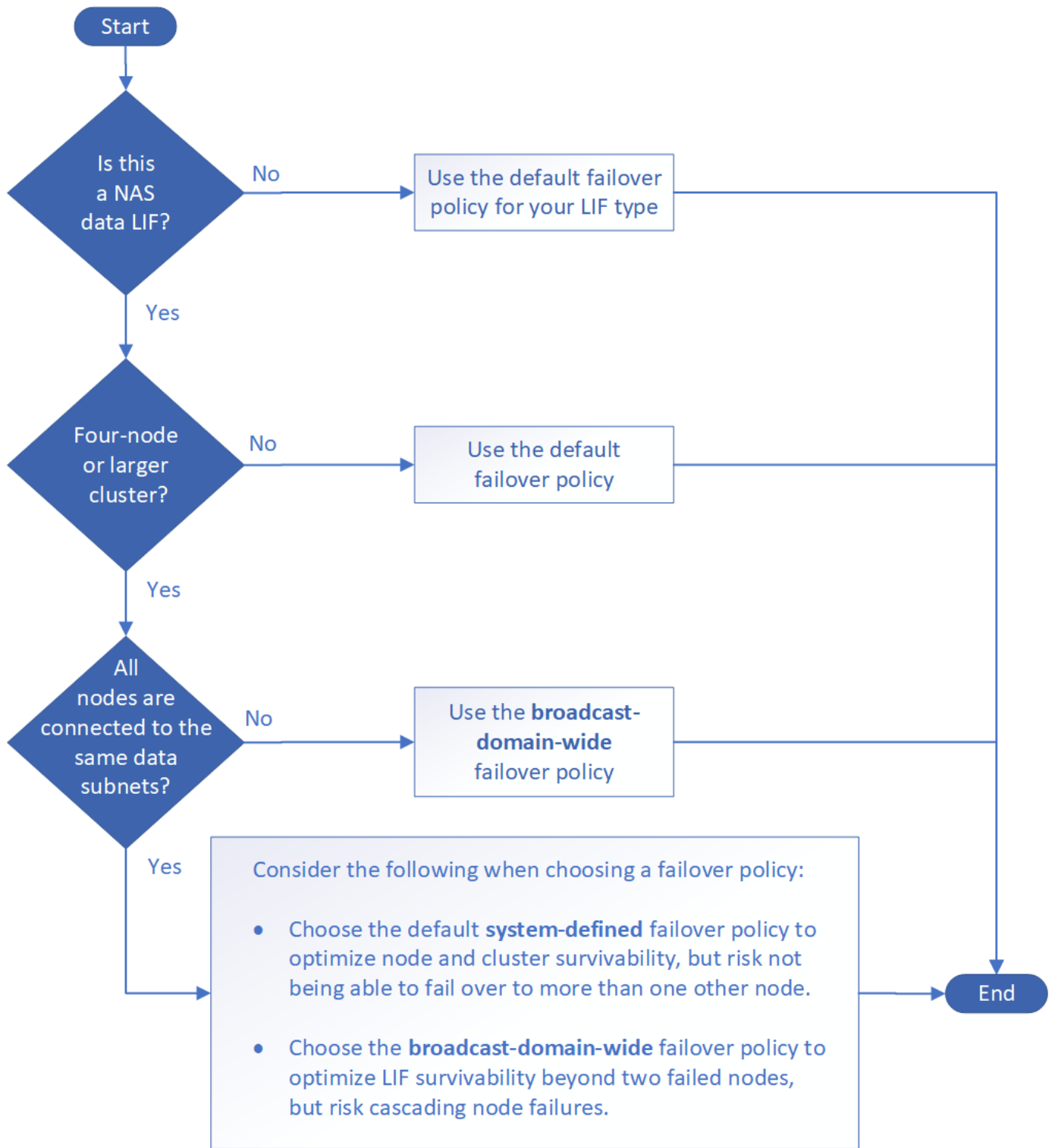
```
network interface show -failover
```

NetApp strongly recommends using the default failover policy for your LIF type.

### Decide which LIF failover policy to use

Decide whether to use the recommended, default failover policy or whether to change it based on your LIF type and environment.

### Failover policy decision tree



### Default failover policies by LIF type

LIF type	Default failover policy	Description
BGP LIFs	disabled	LIF does not fail over to another port.
Cluster LIFs	local-only	LIF fails over to ports on the same node only.
Cluster-mgmt LIF	broadcast-domain-wide	LIF fails over to ports in the same broadcast domain, on any and every node in the cluster.

Intercluster LIFs	local-only	LIF fails over to ports on the same node only.
NAS data LIFs	system-defined	LIF fails over to one other node that is not the HA partner.
Node management LIFs	local-only	LIF fails over to ports on the same node only.
SAN data LIFs	disabled	LIF does not fail over to another port.

The `sfo-partner-only` failover policy is not a default, but can be used when you want the LIF to fail over to a port on the home node or SFO partner only.

## Configure network ports (cluster administrators only)

### Overview

Ports are either physical ports (NICs) or virtualized ports, such as interface groups or VLANs.

Virtual local area networks (VLANs) and interface groups constitute the virtual ports. Interface groups treat several physical ports as a single port, while VLANs subdivide a physical port into multiple separate logical ports.

- Physical ports: LIFs can be configured directly on physical ports.
- Interface group: A port aggregate containing two or more physical ports that act as a single trunk port. An interface group can be single-mode, multimode, or dynamic multimode.
- VLAN: A logical port that receives and sends VLAN-tagged (IEEE 802.1Q standard) traffic. VLAN port characteristics include the VLAN ID for the port. The underlying physical port or interface group ports are considered VLAN trunk ports, and the connected switch ports must be configured to trunk the VLAN IDs.

The underlying physical port or interface group ports for a VLAN port can continue to host LIFs, which transmit and receive untagged traffic.

- Virtual IP (VIP) port: A logical port that is used as the home port for a VIP LIF. VIP ports are created automatically by the system and support only a limited number of operations. VIP ports are supported beginning with ONTAP 9.5.

The port naming convention is *enumberletter*:

- The first character describes the port type.  
"e" represents Ethernet.
- The second character indicates the numbered slot in which the port adapter is located.
- The third character indicates the port's position on a multiport adapter.  
"a" indicates the first port, "b" indicates the second port, and so on.

For example, `e0b` indicates that an Ethernet port is the second port on the node's motherboard.

VLANs must be named by using the syntax `port_name-vlan-id`.

`port_name` specifies the physical port or interface group.

`vlan-id` specifies the VLAN identification on the network. For example, `e1c-80` is a valid VLAN name.

## Combine physical ports to create interface groups

An interface group, also known as a Link Aggregation Group (LAG), is created by combining two or more physical ports into a single logical port. The logical port provides increased resiliency, increased availability, and load sharing.

### Interface group types

Three types of interface groups are supported on the storage system: single-mode, static multimode, and dynamic multimode. Each interface group provides different levels of fault tolerance. Multimode interface groups provide methods for load balancing network traffic.

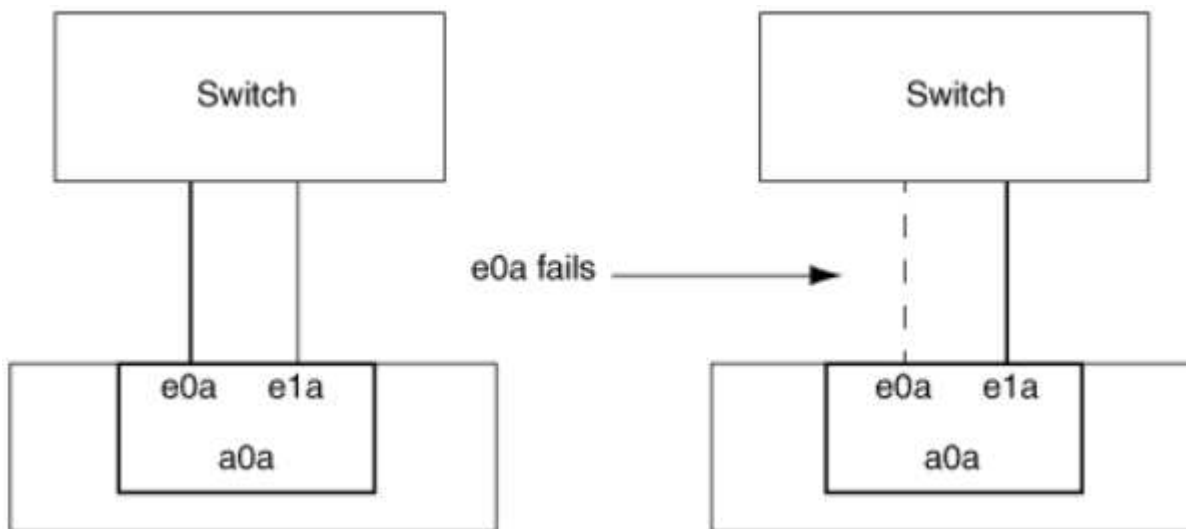
### Characteristics of single-mode interface groups

In a single-mode interface group, only one of the interfaces in the interface group is active. The other interfaces are on standby, ready to take over if the active interface fails.

Characteristics of a single-mode interface groups:

- For failover, the cluster monitors the active link and controls failover. Because the cluster monitors the active link, there is no switch configuration required.
- There can be more than one interface on standby in a single-mode interface group.
- If a single-mode interface group spans multiple switches, you must connect the switches with an Inter-Switch link (ISL).
- For a single-mode interface group, the switch ports must be in the same broadcast domain.
- Link-monitoring ARP packets, which have a source address of 0.0.0.0, are sent over the ports to verify that the ports are in the same broadcast domain.

The following figure is an example of a single-mode interface group. In the figure, e0a and e1a are part of the a0a single-mode interface group. If the active interface, e0a, fails, the standby e1a interface takes over and maintains the connection to the switch.





To accomplish single-mode functionality, the recommended approach is to instead use failover groups. By using a failover group, the second port can still be used for other LIFs and need not remain unused. Additionally, failover groups can span more than two ports and can span ports on multiple nodes.

### Characteristics of static multimode interface groups

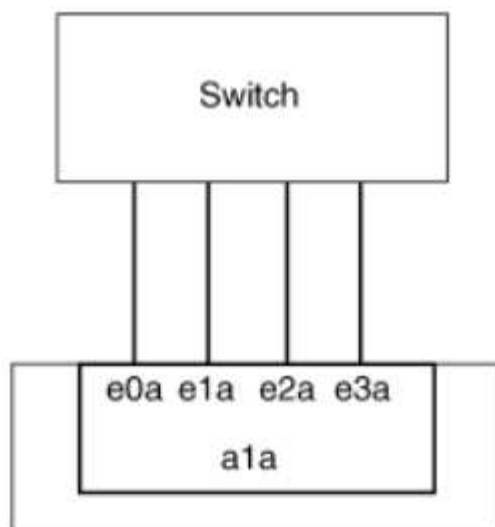
The static multimode interface group implementation in ONTAP complies with IEEE 802.3ad (static). Any switch that supports aggregates, but does not have control packet exchange for configuring an aggregate, can be used with static multimode interface groups.

Static multimode interface groups do not comply with IEEE 802.3ad (dynamic), also known as Link Aggregation Control Protocol (LACP). LACP is equivalent to Port Aggregation Protocol (PAgP), the proprietary link aggregation protocol from Cisco.

The following are characteristics of a static multimode interface group:

- All interfaces in the interface group are active and share a single MAC address.
  - Multiple individual connections are distributed among the interfaces in the interface group.
  - Each connection or session uses one interface within the interface group.  
When you use the sequential load balancing scheme, all sessions are distributed across available links on a packet-by-packet basis, and are not bound to a particular interface from the interface group.
- Static multimode interface groups can recover from a failure of up to "n-1" interfaces, where n is the total number of interfaces that form the interface group.
- If a port fails or is unplugged, the traffic that was traversing the failed link is automatically redistributed to one of the remaining interfaces.
- Static multimode interface groups can detect a loss of link, but they cannot detect a loss of connectivity to the client or switch misconfigurations that might impact connectivity and performance.
- A static multimode interface group requires a switch that supports link aggregation over multiple switch ports.  
The switch is configured so that all ports to which links of an interface group are connected are part of a single logical port. Some switches might not support link aggregation of ports configured for jumbo frames. For more information, see your switch vendor's documentation.
- Several load balancing options are available to distribute traffic among the interfaces of a static multimode interface group.

The following figure is an example of a static multimode interface group. Interfaces e0a, e1a, e2a, and e3a are part of the a1a multimode interface group. All four interfaces in the a1a multimode interface group are active.



Several technologies exist that enable traffic in a single aggregated link to be distributed across multiple physical switches. The technologies used to enable this capability vary among networking products. Static multimode interface groups in ONTAP conform to the IEEE 802.3 standards. If a particular multiple switch link aggregation technology is said to interoperate with or conform to the IEEE 802.3 standards, it should operate with ONTAP.

The IEEE 802.3 standard states that the transmitting device in an aggregated link determines the physical interface for transmission. Therefore, ONTAP is only responsible for distributing outbound traffic, and cannot control how inbound frames arrive. If you want to manage or control the transmission of inbound traffic on an aggregated link, that transmission must be modified on the directly connected network device.

### Dynamic multimode interface group

Dynamic multimode interface groups implement Link Aggregation Control Protocol (LACP) to communicate group membership to the directly attached switch. LACP enables you to detect the loss of link status and the inability of the node to communicate with the direct-attached switch port.

Dynamic multimode interface group implementation in ONTAP complies with IEEE 802.3 AD (802.1 AX). ONTAP does not support Port Aggregation Protocol (PAgP), which is a proprietary link aggregation protocol from Cisco.

A dynamic multimode interface group requires a switch that supports LACP.

ONTAP implements LACP in nonconfigurable active mode that works well with switches that are configured in either active or passive mode. ONTAP implements the long and short LACP timers (for use with nonconfigurable values 3 seconds and 90 seconds), as specified in IEEE 802.3 AD (802.1AX).

The ONTAP load balancing algorithm determines the member port to be used to transmit outbound traffic, and does not control how inbound frames are received. The switch determines the member (individual physical port) of its port channel group to be used for transmission, based on the load balancing algorithm configured in the switch's port channel group. Therefore, the switch configuration determines the member port (individual physical port) of the storage system to receive traffic. For more information about configuring the switch, see the documentation from your switch vendor.

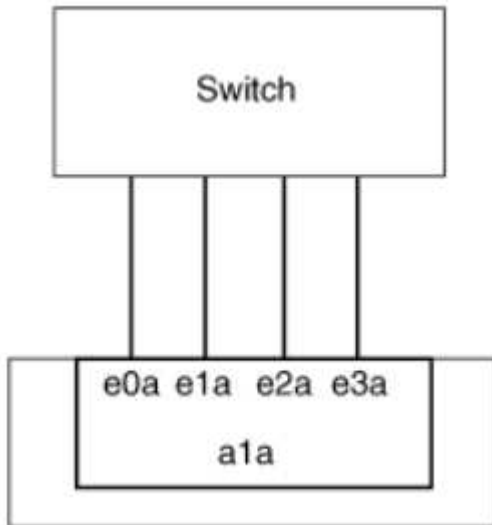
If an individual interface fails to receive successive LACP protocol packets, then that individual interface is marked as "lag\_inactive" in the output of "ifgrp status" command. Existing traffic is automatically rerouted to any remaining active interfaces.



The following rules apply when using dynamic multimode interface groups:

- Dynamic multimode interface groups should be configured to use the port-based, IP-based, MAC-based, or round robin load balancing methods.
- In a dynamic multimode interface group, all interfaces must be active and share a single MAC address.

The following figure is an example of a dynamic multimode interface group. Interfaces e0a, e1a, e2a, and e3a are part of the a1a multimode interface group. All four interfaces in the a1a dynamic multimode interface group are active.



### Load balancing in multimode interface groups

You can ensure that all interfaces of a multimode interface group are equally utilized for outgoing traffic by using the IP address, MAC address, sequential, or port-based load balancing methods to distribute network traffic equally over the network ports of a multimode interface group.

The load balancing method for a multimode interface group can be specified only when the interface group is created.

**Best Practice:** Port-based load balancing is recommended whenever possible. Use port-based load balancing unless there is a specific reason or limitation in the network that prevents it.

### Port-based load balancing

Port-based load balancing is the recommended method.

You can equalize traffic on a multimode interface group based on the transport layer (TCP/UDP) ports by using the port-based load balancing method.

The port-based load balancing method uses a fast hashing algorithm on the source and destination IP addresses along with the transport layer port number.

### IP address and MAC address load balancing

IP address and MAC address load balancing are the methods for equalizing traffic on multimode interface groups.

These load balancing methods use a fast hashing algorithm on the source and destination addresses (IP

address and MAC address). If the result of the hashing algorithm maps to an interface that is not in the UP link-state, the next active interface is used.



Do not select the MAC address load balancing method when creating interface groups on a system that connects directly to a router. In such a setup, for every outgoing IP frame, the destination MAC address is the MAC address of the router. As a result, only one interface of the interface group is used.

IP address load balancing works in the same way for both IPv4 and IPv6 addresses.

### **Sequential load balancing**

You can use sequential load balancing to equally distribute packets among multiple links using a round robin algorithm. You can use the sequential option for load balancing a single connection's traffic across multiple links to increase single connection throughput.

However, because sequential load balancing may cause out-of-order packet delivery, extremely poor performance can result. Therefore, sequential load balancing is generally not recommended.

### **Create an interface group or LAG**

You can create an interface group or LAG—single-mode, static multimode, or dynamic multimode (LACP)—to present a single interface to clients by combining the capabilities of the aggregated network ports.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

## System Manager

### Use System Manager to create a LAG

#### Steps

1. Select **Network > Ethernet port > + Link Aggregation Group** to create a LAG.
2. Select the node from the drop-down list.
3. Choose from the following:
  - a. ONTAP to **Automatically select broadcast domain (recommended)**.
  - b. To manually select a broadcast domain.
4. Select the ports to form the LAG.
5. Select the mode:
  - a. Single: Only one port is used at a time.
  - b. Multiple: All ports can be used simultaneously.
  - c. LACP: The LACP protocol determines the ports that can be used.
6. Select the load balancing:
  - a. IP based
  - b. MAC based
  - c. Port
  - d. Sequential
7. Save your changes.

The screenshot displays the ONTAP System Manager web interface. The left sidebar contains a navigation menu with categories: DASHBOARD, INSIGHTS, STORAGE, NETWORK, EVENTS & JOBS, PROTECTION, HOSTS, and CLUSTER. The 'NETWORK' section is expanded, showing 'Ethernet Ports' as the active page. The main content area is titled 'Add Link Aggregation Group' and includes the following configuration options:

- NODE:** A dropdown menu showing 'sti47-vs1im-uc5521e'.
- BROADCAST DOMAIN:** A dropdown menu with 'Automatically select broadcast domain (Recommended)' selected. A red arrow points to this dropdown with a note: 'Note: Instead of a global switch or checkbox, what if we expose BD dropdown with "Automatic" as a default selection?'.
- PORTS TO INCLUDE:** Two checkboxes, 'e0e' and 'e0f', both of which are unchecked.
- MODE:** Three radio button options: 'Single' (selected), 'Multiple', and 'LACP'. Below 'Single' is the text 'Only one port is used at a time.' Below 'Multiple' is 'All ports can be used simultaneously.' Below 'LACP' is 'The LACP protocol determines the ports that can be used.'
- LOAD DISTRIBUTION:** Three radio button options: 'IP based' (selected), 'MAC based', and 'Port'. Below 'IP based' is the text 'Network traffic is distributed based on the destination IP address.' Below 'MAC based' is 'Network traffic is distributed based on the next-hop MAC addresses.'

#### CLI

### Use the CLI to create an interface group

For a complete list of configuration restrictions that apply to port interface groups, see the `network port ifgrp add-port` man page.

When creating a multimode interface group, you can specify any of the following load-balancing methods:

- `port`: Network traffic is distributed on the basis of the transport layer (TCP/UDP) ports. This is the recommended load-balancing method.
- `mac`: Network traffic is distributed on the basis of MAC addresses.
- `ip`: Network traffic is distributed on the basis of IP addresses.
- `sequential`: Network traffic is distributed as it is received.



The MAC address of an interface group is determined by the order of the underlying ports and how these ports initialize during bootup. You should therefore not assume that the ifgrp MAC address is persistent across reboots or ONTAP upgrades.

### Step

Use the `network port ifgrp create` command to create an interface group.

Interface groups must be named using the syntax `a<number><letter>`. For example, `a0a`, `a0b`, `a1c`, and `a2a` are valid interface group names.

For more information about this command, see [ONTAP 9 commands](#).

The following example shows how to create an interface group named `a0a` with a distribution function of `port` and a mode of `multimode`:

```
network port ifgrp create -node cluster-1-01 -ifgrp a0a -distr-func port -mode multimode
```

### Add a port to an interface group or LAG

You can add up to 16 physical ports to an interface group or LAG for all port speeds.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

## System Manager

### Use System Manager to add a port to a LAG

#### Steps

1. Select **Network > Ethernet port > LAG** to edit a LAG.
2. Select additional ports on the same node to add to the LAG.
3. Save your changes.

#### CLI

### Use the CLI to add ports to an interface group

#### Step

Add network ports to the interface group:

```
network port ifgrp add-port
```

For more information about this command, see [ONTAP 9 commands](#).

The following example shows how to add port e0c to an interface group named a0a:

```
network port ifgrp add-port -node cluster-1-01 -ifgrp a0a -port e0c
```

Beginning with ONTAP 9.8, interface groups are automatically placed into an appropriate broadcast domain about one minute after the first physical port is added to the interface group. If you do not want ONTAP to do this, and prefer to manually place the ifgrp into a broadcast domain, then specify the `-skip -broadcast-domain-placement` parameter as part of the `ifgrp add-port` command.

### Remove a port from an interface group or LAG

You can remove a port from an interface group that hosts LIFs, as long as it is not the last port in the interface group. There is no requirement that the interface group must not host LIFs or that the interface group must not be the home port of a LIF considering that you are not removing the last port from the interface group. However, if you are removing the last port, then you must migrate or move the LIFs from the interface group first.

#### About this task

You can remove up to 16 ports (physical interfaces) from an interface group or LAG.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

## System Manager

### Use System Manager to remove a port from a LAG

#### Steps

1. Select **Network > Ethernet port > LAG** to edit a LAG.
2. Select the ports to remove from the LAG.
3. Save your changes.

#### CLI

### Use the CLI to remove ports from an interface group

#### Step

Remove network ports from an interface group:

```
network port ifgrp remove-port
```

The following example shows how to remove port e0c from an interface group named a0a:

```
network port ifgrp remove-port -node cluster-1-01 -ifgrp a0a -port e0c
```

## Delete an interface group or LAG

You can delete interface groups or LAGs if you want to configure LIFs directly on the underlying physical ports or decide to change the interface group or LAG mode or distribution function.

### Before you begin

- The interface group or LAG must not be hosting a LIF.
- The interface group or LAG must be neither the home port nor the failover target of a LIF.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

## System Manager

### Use System Manager to delete a LAG

#### Steps

1. Select **Network > Ethernet port > LAG** to delete a LAG.
2. Select the LAG you want to remove.
3. Delete the LAG.

#### CLI

### Use the CLI to delete an interface group

#### Step

Use the `network port ifgrp delete` command to delete an interface group.

For more information about this command, see [ONTAP 9 commands](#).

The following example shows how to delete an interface group named `a0b`:

```
network port ifgrp delete -node cluster-1-01 -ifgrp a0b
```

## Configure VLANs over physical ports

VLANs provide logical segmentation of networks by creating separate broadcast domains that are defined on a switch port basis as opposed to the traditional broadcast domains, defined on physical boundaries.

A VLAN can span multiple physical network segments. The end-stations belonging to a VLAN are related by function or application.

For example, end-stations in a VLAN might be grouped by departments, such as engineering and accounting, or by projects, such as `release1` and `release2`. Because physical proximity of the end-stations is not essential in a VLAN, you can disperse the end-stations geographically and still contain the broadcast domain in a switched network.

You can manage VLANs by creating, deleting, or displaying information about them.



You should not create a VLAN on a network interface with the same identifier as the native VLAN of the switch. For example, if the network interface `e0b` is on native VLAN 10, you should not create a VLAN `e0b-10` on that interface.

### Create a VLAN

You can create a VLAN for maintaining separate broadcast domains within the same network domain by using System Manager or the `network port vlan create` command.

### Before you begin

Confirm that the following requirements have been met:

- The switches deployed in the network must either comply with IEEE 802.1Q standards or have a vendor-

specific implementation of VLANs.

- For supporting multiple VLANs, an end-station must be statically configured to belong to one or more VLANs.
- The VLAN is not attached to a port hosting a cluster LIF.
- The VLAN is not attached to ports assigned to the Cluster IPspace.
- The VLAN is not created on an interface group port that contains no member ports.

#### **About this task**

Creating a VLAN attaches the VLAN to the network port on a specified node in a cluster.

When you configure a VLAN over a port for the first time, the port might go down, resulting in a temporary disconnection of the network. Subsequent VLAN additions to the same port do not affect the port state.



You should not create a VLAN on a network interface with the same identifier as the native VLAN of the switch. For example, if the network interface e0b is on native VLAN 10, you should not create a VLAN e0b-10 on that interface.

The procedure you follow depends on the interface that you use—System Manager or the CLI:



## System Manager

### Use System Manager to create a VLAN

Beginning with ONTAP 9.12.0, you can automatically select the broadcast domain or manually select one from the list. Previously, broadcast domains were always automatically selected based on layer 2 connectivity. If you manually select a broadcast domain, a warning appears indicating that manually selecting a broadcast domain could result in loss of connectivity.

#### Steps

1. Select **Network > Ethernet port > + VLAN**.
2. Select the node from the drop-down list.
3. Choose from the following:
  - a. ONTAP to **Automatically select broadcast domain (recommended)**.
  - b. To manually select a broadcast domain from the list.
4. Select the ports to form the VLAN.
5. Specify the VLAN ID.
6. Save your changes.

#### CLI

### Use the CLI to create a VLAN

In certain circumstances, if you want to create the VLAN port on a degraded port without correcting the hardware issue or any software misconfiguration, then you can set the `-ignore-health-status` parameter of the `network port modify` command as `true`.

#### Steps

1. Use the `network port vlan create` command to create a VLAN.
2. You must specify either the `vlan-name` or the `port` and `vlan-id` options when creating a VLAN. The VLAN name is a combination of the name of the port (or interface group) and the network switch VLAN identifier, with a hyphen in between. For example, `e0c-24` and `e1c-80` are valid VLAN names.

The following example shows how to create a VLAN `e1c-80` attached to network port `e1c` on the node `cluster-1-01`:

```
network port vlan create -node cluster-1-01 -vlan-name e1c-80
```

Beginning with ONTAP 9.8, VLANs are automatically placed into appropriate broadcast domains about one minute after their creation. If you do not want ONTAP to do this, and prefer to manually place the VLAN into a broadcast domain, then specify the `-skip-broadcast-domain-placement` parameter as part of the `vlan create` command.

For more information about this command, see [ONTAP 9 commands](#).

## Edit a VLAN

You can change the broadcast domain or disable a VLAN.

### Use System Manager to edit a VLAN

Beginning with ONTAP 9.12.0, you can automatically select the broadcast domain or manually select one from the list. Previously broadcast domains were always automatically selected based on layer 2 connectivity. If you manually select a broadcast domain, a warning appears indicating that manually selecting a broadcast domain could result in loss of connectivity.

### Steps

1. Select **Network > Ethernet port > VLAN**.
2. Select the edit icon.
3. Do one of the following:
  - Change the broadcast domain by selecting a different one from the list.
  - Clear the **Enabled** check box.
4. Save your changes.

## Delete a VLAN

You might have to delete a VLAN before removing a NIC from its slot. When you delete a VLAN, it is automatically removed from all of the failover rules and groups that use it.

### Before you begin

Make sure there are no LIFs associated with the VLAN.

### About this task

Deletion of the last VLAN from a port might cause a temporary disconnection of the network from the port.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

## System Manager

### Use System Manager to delete a VLAN

#### Steps

1. Select **Network > Ethernet port > VLAN**.
2. Select the VLAN you want to remove.
3. Click **Delete**.

#### CLI

### Use the CLI to delete a VLAN

#### Step

Use the `network port vlan delete` command to delete a VLAN.

The following example shows how to delete VLAN `e1c-80` from network port `e1c` on the node `cluster-1-01`:

```
network port vlan delete -node cluster-1-01 -vlan-name e1c-80
```

## Modify network port attributes

You can modify the autonegotiation, duplex, flow control, speed, and health settings of a physical network port.

### Before you begin

The port that you want to modify must not be hosting any LIFs.

### About this task

- It is not recommended to modify the administrative settings of the 100 GbE, 40 GbE, 10 GbE or 1 GbE network interfaces.

The values that you set for duplex mode and port speed are referred to as administrative settings.

Depending on network limitations, the administrative settings can differ from the operational settings (that is, the duplex mode and speed that the port actually uses).

- It is not recommended to modify the administrative settings of the underlying physical ports in an interface group.

The `-up-admin` parameter (available at the advanced privilege level) modifies the administrative settings of the port.

- It is not recommended to set the `-up-admin` administrative setting to false for all ports on a node, or for the port that hosts the last operational cluster LIF on a node.
- It is not recommended to modify the MTU size of the management port, `e0M`.
- The MTU size of a port in a broadcast domain cannot be changed from the MTU value that is set for the broadcast domain.

- The MTU size of a VLAN cannot exceed the value of the MTU size of its base port.

### Steps

1. Modify the attributes of a network port:

```
network port modify
```

2. You can set the `-ignore-health-status` field to true for specifying that the system can ignore the network port health status of a specified port.

The network port health status is automatically changed from degraded to healthy, and this port can now be used for hosting LIFs. You should set the flow control of cluster ports to `none`. By default, the flow control is set to `full`.

The following command disables the flow control on port e0b by setting the flow control to `none`:

```
network port modify -node cluster-1-01 -port e0b -flowcontrol-admin none
```

### Modify MTU setting for interface group ports

To modify the MTU setting for interface groups, you must modify the MTU of the broadcast domain.

VLAN MTU size should match the broadcast domain MTU of the underlying interface groups and physical ports. If a different VLAN setting is needed for a VLAN, it must not exceed the size specified by the underlying broadcast domain.

### Steps

1. Modify the broadcast domain settings:

```
broadcast-domain modify -broadcast-domain broadcast_domain_name -mtu  
mtu_setting
```

The following warning message is displayed:

```
Warning: Changing broadcast domain settings will cause a momentary data-  
serving interruption.  
Do you want to continue? {y|n}: y
```

2. Enter `y` to continue.
3. Verify that the MTU setting were modified correctly:

```
network port show
```

```

network port show
(network port show)
Node: vsim-01

```

Port	IPspace	Broadcast	Domain	Link	MTU	Speed (Mbps) Admin/Oper	Health Status	Ignore Health Status
a0a	Default	Default-1		up	1300	auto/1000	healthy	false
e0a	Default	Default-1		up	1300	auto/1000	healthy	false
e0b	Default	Default		up	1500	auto/1000	healthy	false
e0c	Default	Default		up	1500	auto/1000	healthy	false
e0d	Default	Default		up	1500	auto/1000	healthy	false

5 entries were displayed.

## Monitor the health of network ports

ONTAP management of network ports includes automatic health monitoring and a set of health monitors to help you identify network ports that might not be suitable for hosting LIFs.

### About this task

If a health monitor determines that a network port is unhealthy, it warns administrators through an EMS message or marks the port as degraded. ONTAP avoids hosting LIFs on degraded network ports if there are healthy alternative failover targets for that LIF. A port can become degraded because of a soft failure event, such as link flapping (links bouncing quickly between up and down) or network partitioning:

- Network ports in the cluster IPspace are marked as degraded when they experience link flapping or loss of layer 2 (L2) reachability to other network ports in the broadcast domain.
- Network ports in non-cluster IPspaces are marked as degraded when they experience link flapping.

You must be aware of the following behaviors of a degraded port:

- A degraded port cannot be included in a VLAN or an interface group.

If a member port of an interface group is marked as degraded, but the interface group is still marked as healthy, LIFs can be hosted on that interface group.

- LIFs are automatically migrated from degraded ports to healthy ports.
- During a failover event, a degraded port is not considered as the failover target. If no healthy ports are available, degraded ports host LIFs according to the normal failover policy.
- You cannot create, migrate, or revert a LIF to a degraded port.

You can modify the `ignore-health-status` setting of the network port to `true`. You can then host a LIF on the healthy ports.

## Steps

1. Log in to the advanced privilege mode:

```
set -privilege advanced
```

2. Check which health monitors are enabled for monitoring network port health:

```
network options port-health-monitor show
```

The health status of a port is determined by the value of health monitors.

The following health monitors are available and enabled by default in ONTAP:

- Link-flapping health monitor: Monitors link flapping

If a port has link flapping more than once in five minutes, this port is marked as degraded.

- L2 reachability health monitor: Monitors whether all ports configured in the same broadcast domain have L2 reachability to each other

This health monitor reports L2 reachability issues in all IPspaces; however, it marks only the ports in the cluster IPspace as degraded.

- CRC monitor: Monitors the CRC statistics on the ports

This health monitor does not mark a port as degraded but generates an EMS message when a very high CRC failure rate is observed.

3. Enable or disable any of the health monitors for an IPspace as desired by using the `network options port-health-monitor modify` command.

4. View the detailed health of a port:

```
network port show -health
```

The command output displays the health status of the port, `ignore health status setting`, and list of reasons the port is marked as degraded.

A port health status can be `healthy` or `degraded`.

If the `ignore health status setting` is `true`, it indicates that the port health status has been modified from `degraded` to `healthy` by the administrator.

If the `ignore health status setting` is `false`, the port health status is determined automatically by the system.

### Monitor the reachability of network ports in ONTAP 9.8 and later

Reachability monitoring is built into ONTAP 9.8 and later. Use this monitoring to identify when the physical network topology does not match the ONTAP configuration. In some cases, ONTAP can repair port reachability. In other cases, additional steps are required.

**About this task**

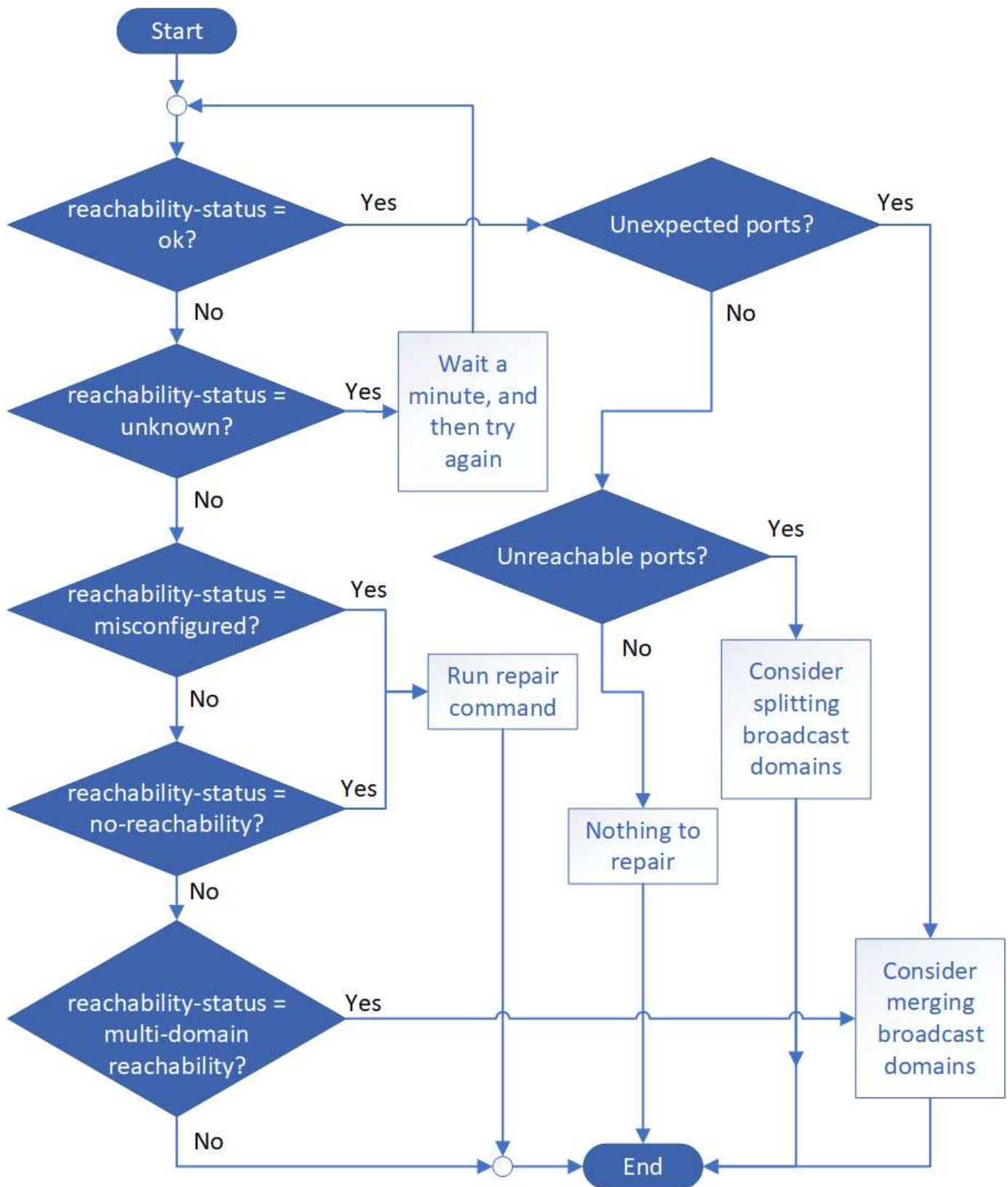
Use these commands to verify, diagnose, and repair network misconfigurations that stem from the ONTAP configuration not matching either the physical cabling or the network switch configuration.

**Step**

1. View port reachability:

```
network port reachability show
```

2. Use the following decision tree and table to determine the next step, if any.



Reachability-status	Description
---------------------	-------------



ok	<p>The port has layer 2 reachability to its assigned broadcast domain.</p> <p>If the reachability-status is "ok", but there are "unexpected ports", consider merging one or more broadcast domains. For more information, see the following <i>Unexpected ports</i> row.</p> <p>If the reachability-status is "ok", but there are "unreachable ports", consider splitting one or more broadcast domains. For more information, see the following <i>Unreachable ports</i> row.</p> <p>If the reachability-status is "ok", and there are no unexpected or unreachable ports, your configuration is correct.</p>
Unexpected ports	<p>The port has layer 2 reachability to its assigned broadcast domain; however, it also has layer 2 reachability to at least one other broadcast domain.</p> <p>Examine the physical connectivity and switch configuration to determine if it is incorrect or if the port's assigned broadcast domain needs to be merged with one or more broadcast domains.</p> <p>For more information, see <a href="#">Merge broadcast domains</a>.</p>
Unreachable ports	<p>If a single broadcast domain has become partitioned into two different reachability sets, you can split a broadcast domain to synchronize the ONTAP configuration with the physical network topology.</p> <p>Typically, the list of unreachable ports defines the set of ports that should be split into another broadcast domain after you have verified that the physical and switch configuration is accurate.</p> <p>For more information, see <a href="#">Split broadcast domains</a>.</p>
misconfigured-reachability	<p>The port does not have layer 2 reachability to its assigned broadcast domain; however, the port does have layer 2 reachability to a different broadcast domain.</p> <p>You can repair the port reachability. When you run the following command, the system will assign the port to the broadcast domain to which it has reachability:</p> <pre>network port reachability repair -node -port</pre> <p>For more information, see <a href="#">Repair port reachability</a>.</p>
no-reachability	<p>The port does not have layer 2 reachability to any existing broadcast domain.</p> <p>You can repair the port reachability. When you run the following command, the system will assign the port to a new automatically created broadcast domain in the Default IPspace:</p> <pre>network port reachability repair -node -port</pre> <p>For more information, see <a href="#">Repair port reachability</a>.</p>

multi-domain-reachability	<p>The port has layer 2 reachability to its assigned broadcast domain; however, it also has layer 2 reachability to at least one other broadcast domain.</p> <p>Examine the physical connectivity and switch configuration to determine if it is incorrect or if the port's assigned broadcast domain needs to be merged with one or more broadcast domains.</p> <p>For more information, see <a href="#">Merge broadcast domains</a> or <a href="#">Repair port reachability</a>.</p>
unknown	<p>If the reachability-status is "unknown", then wait a few minutes and try the command again.</p>

After you repair a port, you need to check for and resolve displaced LIFs and VLANs. If the port was part of an interface group, you also need to understand what happened to that interface group. For more information, see [Repair port reachability](#).

### Convert 40GbE NIC ports into multiple 10GbE ports for 10GbE connectivity

You can convert the X1144A-R6 and the X91440A-R6 40GbE Network Interface Cards (NICs) to support four 10GbE ports.

If you are connecting a hardware platform that supports one of these NICs to a cluster that supports 10GbE cluster interconnect and customer data connections, the NIC must be converted to provide the necessary 10GbE connections.

#### Before you begin

You must be using a supported breakout cable.

#### About this task

For a complete list of platforms that support NICs, see the [Hardware Universe](#).



On the X1144A-R6 NIC, only port A can be converted to support the four 10GbE connections. Once port A is converted, port e is not available for use.

#### Steps

1. Enter maintenance mode.
2. Convert the NIC from 40GbE support to 10GbE support.

```
nicadmin convert -m [40G | 10G] [port-name]
```

3. After using the convert command, halt the node.
4. Install or change the cable.
5. Depending on the hardware model, use the SP (Service Processor) or BMC (Baseboard Management Controller) to power-cycle the node for the conversion to take effect.

#### Removing a NIC from the node on ONTAP 9.7 or earlier

This topic applies to ONTAP 9.7 or earlier. You might have to remove a faulty NIC from its

slot or move the NIC to another slot for maintenance purposes.

### Before you begin

- All LIFs hosted on the NIC ports must have been migrated or deleted.
- None of the NIC ports can be the home ports of any LIFs.
- You must have advanced privileges to delete the ports from a NIC.

### Steps

1. Delete the ports from the NIC:

```
network port delete
```

2. Verify that the ports have been deleted:

```
network port show
```

3. Repeat step 1, if the output of the network port show command still shows the deleted port.

### Removing a NIC from the node on ONTAP 9.8 or later

This topic applies to ONTAP 9.8 or later. You might have to remove a faulty NIC from its slot or move the NIC to another slot for maintenance purposes.

### Steps

1. Power down the node.
2. Physically remove the NIC from its slot.
3. Power on the node.
4. Verify that the port has been deleted:

```
network port show
```



ONTAP automatically removes the port from any interface groups. If the port was the only member of an interface group, the interface group is deleted.

5. If the port had any VLANs configured on it, they are displaced. You can view displaced VLANs using the following command:

```
cluster controller-replacement network displaced-vlans show
```



The `displaced-interface show`, `displaced-vlans show`, and `displaced-vlans restore` commands are unique and do not require the fully qualified command name, which starts with `cluster controller-replacement network`.

6. These VLANs are deleted, but can be restored using the following command:

```
displaced-vlans restore
```

7. If the port had any LIFs configured on it, ONTAP automatically chooses new home ports for those LIFs on another port in the same broadcast domain. If no suitable home port is found on the same filer, those LIFs are considered displaced. You can view displaced LIFs using the following command:

```
displaced-interface show
```

8. When a new port is added to the broadcast domain on the same node, the home ports for the LIFs are automatically restored. Alternatively, you can either set the home port using `network interface modify -home-port -home-node` or use the `displaced- interface restore` command.

## Configure IPspaces (cluster administrators only)

### Overview

IPspaces enable you to configure a single ONTAP cluster so that it can be accessed by clients from more than one administratively separate network domain, even if those clients are using the same IP address subnet range. This allows for separation of client traffic for privacy and security.

An IPspace defines a distinct IP address space in which storage virtual machines (SVMs) reside. Ports and IP addresses defined for an IPspace are applicable only within that IPspace. A distinct routing table is maintained for each SVM within an IPspace; therefore, no cross-SVM or cross- IPspace traffic routing occurs.



IPspaces support both IPv4 and IPv6 addresses on their routing domains.

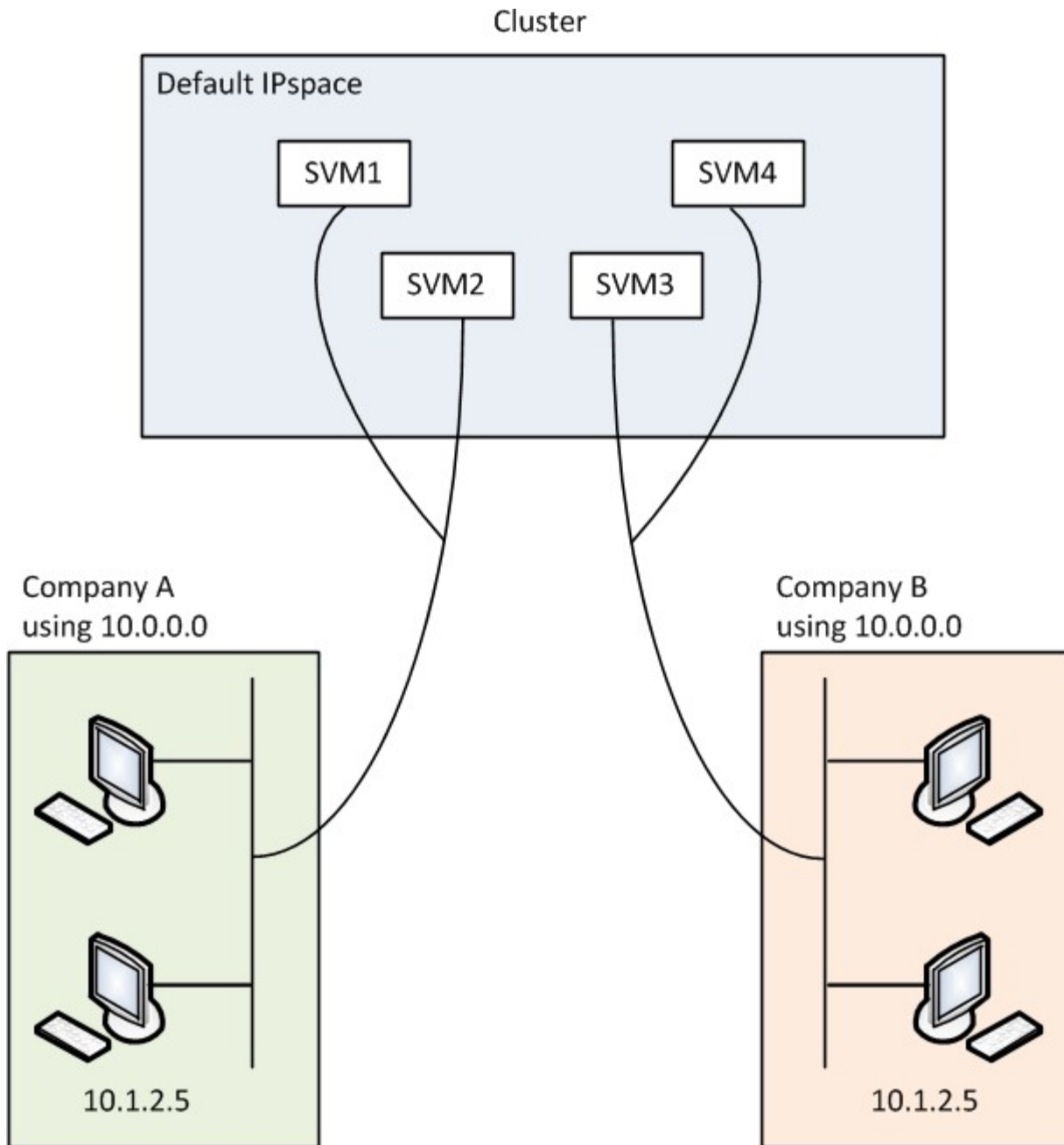
If you are managing storage for a single organization, then you do not need to configure IPspaces. If you are managing storage for multiple companies on a single ONTAP cluster, and you are certain that none of your customers have conflicting networking configurations, then you also do not need to use IPspaces. In many cases, the use of storage virtual machines (SVMs), with their own distinct IP routing tables, can be used to segregate unique networking configurations instead of using IPspaces.

### Example of using IPspaces

A common application for using IPspaces is when a Storage Service Provider (SSP) needs to connect customers of companies A and B to an ONTAP cluster on the SSP's premises and both companies are using the same private IP address ranges.

The SSP creates SVMs on the cluster for each customer and provides a dedicated network path from two SVMs to company A's network and from the other two SVMs to company B's network.

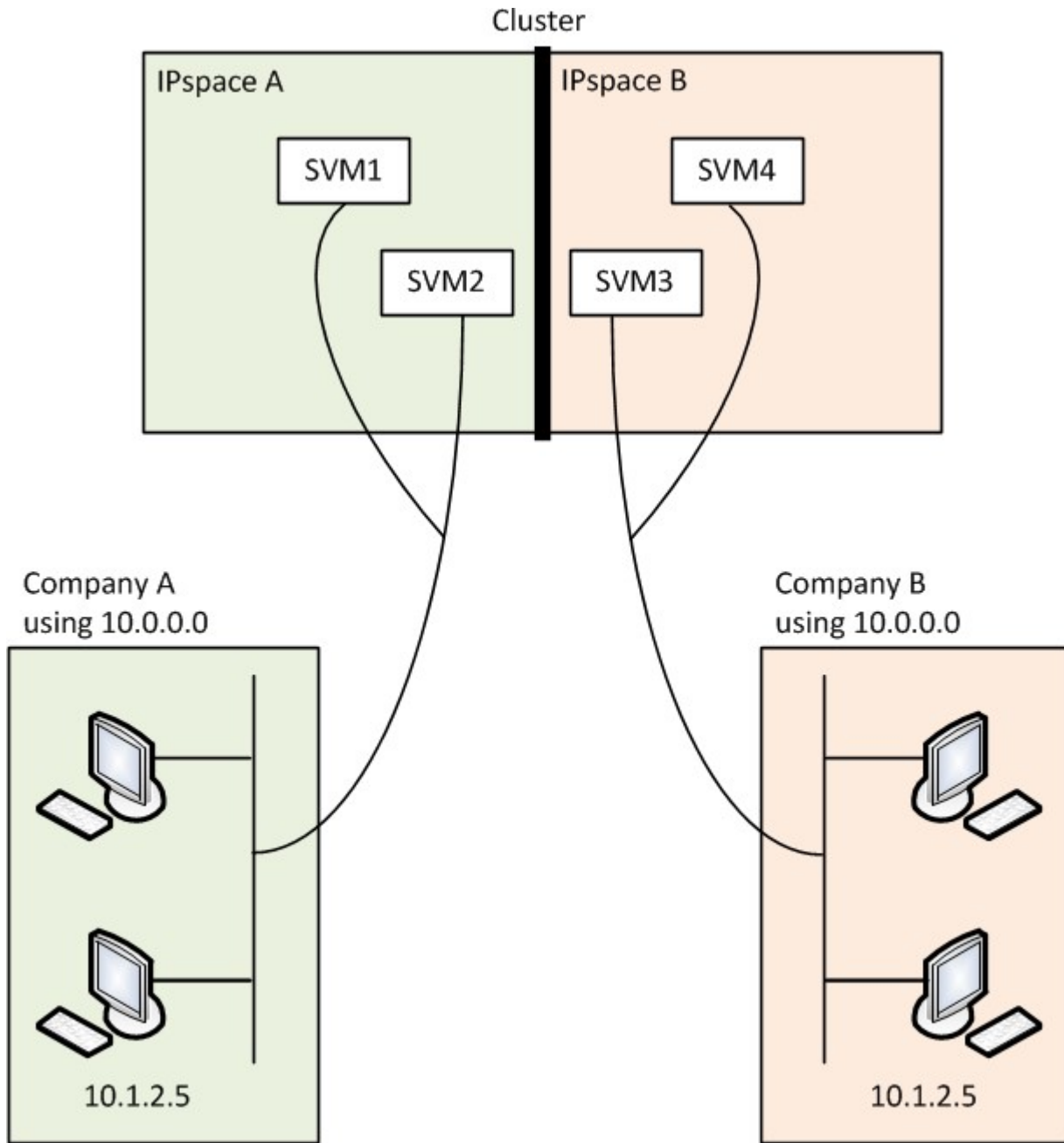
This type of deployment is shown in the following illustration, and it works if both companies use non-private IP address ranges. However, the illustration shows both companies using the same private IP address ranges, which causes problems.



Both companies use the private IP address subnet 10.0.0.0, causing the following problems:

- The SVMs in the cluster at the SSP location have conflicting IP addresses if both companies decide to use the same IP address for their respective SVMs.
- Even if the two companies agree on using different IP addresses for their SVMs, problems can arise.
- For example, if any client in A's network has the same IP address as a client in B's network, packets destined for a client in A's address space might get routed to a client in B's address space, and vice versa.
- If the two companies decide to use mutually exclusive address spaces (for example, A uses 10.0.0.0 with a network mask of 255.128.0.0 and B uses 10.128.0.0 with a network mask of 255.128.0.0), the SSP needs to configure static routes on the cluster to route traffic appropriately to A's and B's networks.
- This solution is neither scalable (because of static routes) nor secure (broadcast traffic is sent to all interfaces of the cluster). To overcome these problems, the SSP defines two IPspaces on the cluster—one for each company. Because no cross-IPspace traffic is routed, the data for each company is securely routed to its respective network even if all of the SVMs are configured in the 10.0.0.0 address space, as

shown in the following illustration:



Additionally, the IP addresses referred to by the various configuration files, such as the `/etc/hosts` file, the `/etc/hosts.equiv` file, and the `/etc/rc` file, are relative to that IPspace. Therefore, the IPspaces enable the SSP to configure the same IP address for the configuration and authentication data for multiple SVMs, without conflict.

### Standard properties of IPspaces

Special IPspaces are created by default when the cluster is first created. Additionally, special storage virtual machines (SVMs) are created for each IPspace.

Two IPspaces are created automatically when the cluster is initialized:

- "Default" IPspace

This IPspace is a container for ports, subnets, and SVMs that serve data. If your configuration does not need separate IPspaces for clients, all SVMs can be created in this IPspace. This IPspace also contains the cluster management and node management ports.

- "Cluster" IPspace

This IPspace contains all cluster ports from all nodes in the cluster. It is created automatically when the cluster is created. It provides connectivity to the internal private cluster network. As additional nodes join the cluster, cluster ports from those nodes are added to the "Cluster" IPspace.

A "system" SVM exists for each IPspace. When you create an IPspace, a default system SVM of the same name is created:

- The system SVM for the "Cluster" IPspace carries cluster traffic between nodes of a cluster on the internal private cluster network.

It is managed by the cluster administrator, and it has the name "Cluster".

- The system SVM for the "Default" IPspace carries management traffic for the cluster and nodes, including the intercluster traffic between clusters.

It is managed by the cluster administrator, and it uses the same name as the cluster.

- The system SVM for a custom IPspace that you create carries management traffic for that SVM.

It is managed by the cluster administrator, and it uses the same name as the IPspace.

One or more SVMs for clients can exist in an IPspace. Each client SVM has its own data volumes and configurations, and it is administered independently of other SVMs.

## Create IPspaces

IPspaces are distinct IP address spaces in which storage virtual machines (SVMs) reside. You can create IPspaces when you need your SVMs to have their own secure storage, administration, and routing.

### About this task

There is a cluster-wide limit of 512 IPspaces. The cluster-wide limit is reduced to 256 IPspaces for clusters that contain nodes with 6 GB of RAM or less for platforms such as FAS2220 or FAS2240. See the Hardware Universe to determine whether additional limits apply to your platform.

### [NetApp Hardware Universe](#)



An IPspace name cannot be "all" because "all" is a system-reserved name.

### Step

Create an IPspace:

```
network ipspace create -ipspace ipspace_name
```

`ipspace_name` is the name of the IPspace that you want to create. The following command creates the

IPspace ipspace1 on a cluster:

```
network ipspace create -ip-space ipspace1
```

### After you finish

If you create an IPspace in a cluster with a MetroCluster configuration, IPspace objects must be manually replicated to the partner clusters. Any SVMs that are created and assigned to an IPspace before the IPspace is replicated will not be replicated to the partner clusters.

Broadcast domains are created automatically in the "Default" IPspace and can be moved between IPspaces using the following command:

```
network port broadcast-domain move
```

For example, if you want to move a broadcast domain from "Default" to "ips1", using the following command:

```
network port broadcast-domain move -ip-space Default -broadcast-domain  
Default -to-ip-space ips1
```

### Display IPspaces

You can display the list of IPspaces that exist in a cluster, and you can view the storage virtual machines (SVMs), broadcast domains, and ports that are assigned to each IPspace.

#### Step

Display the IPspaces and SVMs in a cluster:

```
network ipspace show [-ip-space ipspace_name]
```

The following command displays all of the IPspaces, SVMs, and broadcast domains in the cluster:

```
network ipspace show
IPspace      Vserver List      Broadcast Domains
-----      -
Cluster
Default      Cluster           Cluster
            vs1, cluster-1    Default
ip-space1    vs3, vs4, ip-space1  bcast1
```

The following command displays the nodes and ports that are part of IPspace ipspace1:



```
network ipspace show -ipospace ipspace1
IPspace name: ipspace1
Ports: cluster-1-01:e0c, cluster-1-01:e0d, cluster-1-01:e0e, cluster-1-
02:e0c, cluster-1-02:e0d, cluster-1-02:e0e
Broadcast Domains: Default-1
Vservers: vs3, vs4, ipspace1
```

## Delete an IPspace

If you no longer need an IPspace, you can delete it.

### Before you begin

There must be no broadcast domains, network interfaces, or SVMs associated with the IPspace you want to delete.

The system-defined "Default" and "Cluster" IPspaces cannot be deleted.

### Step

Delete an IPspace:

```
network ipspace delete -ipospace ipspace_name
```

The following command deletes IPspace ipspace1 from the cluster:

```
network ipspace delete -ipospace ipspace1
```

## Configure broadcast domains (cluster administrators only)

### ONTAP 9.8 and later

#### About broadcast domains for ONTAP 9.8 and later

Broadcast domains are intended to group network ports that belong to the same layer 2 network. The ports in the group can then be used by a storage virtual machine (SVM) for data or management traffic.

A broadcast domain resides in an IPspace. During cluster initialization, the system creates two default broadcast domains:

- The "Default" broadcast domain contains ports that are in the "Default" IPspace.

These ports are used primarily to serve data. Cluster management and node management ports are also in this broadcast domain.

- The "Cluster" broadcast domain contains ports that are in the "Cluster" IPspace.

These ports are used for cluster communication and include all cluster ports from all nodes in the cluster.

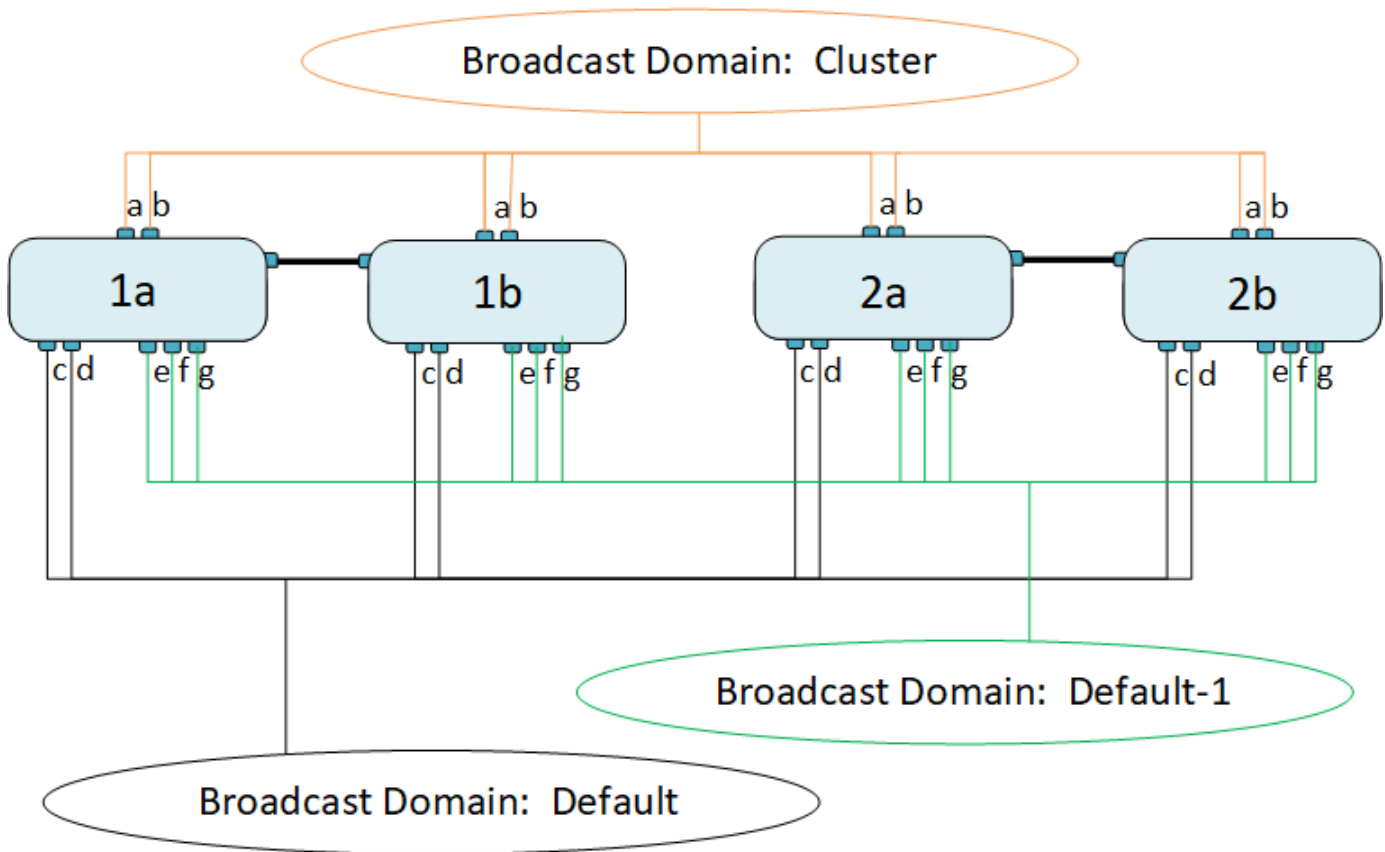
The system creates additional broadcast domains in the Default IPspace when necessary. The "Default" broadcast domain contains the home-port of the management LIF, plus any other ports that have layer 2 reachability to that port. Additional broadcast domains are named "Default-1", "Default-2", and so forth.

### Example of using broadcast domains

A broadcast domain is a set of network ports in the same IPspace that also has layer 2 reachability to one another, typically including ports from many nodes in the cluster.

The illustration shows the ports assigned to three broadcast domains in a four-node cluster:

- The "Cluster" broadcast domain is created automatically during cluster initialization, and it contains ports a and b from each node in the cluster.
- The "Default" broadcast domain is also created automatically during cluster initialization, and it contains ports c and d from each node in the cluster.
- The system automatically creates any additional broadcast domains during cluster initialization based on layer 2 network reachability. These additional broadcast domains are named Default-1, Default-2, and so forth.



A failover group of the same name and with the same network ports as each of the broadcast domains is created automatically. This failover group is automatically managed by the system, meaning that as ports are added or removed from the broadcast domain, they are automatically added or removed from this failover group.

### Add a broadcast domain

Broadcast domains group network ports in the cluster that belong to the same layer 2

network. The ports can then be used by SVMs.

Beginning with ONTAP 9.8, broadcast domains are automatically created during the cluster create or join operation. Beginning with ONTAP 9.12.0, in addition to the automatically created broadcast domains, you can manually add a broadcast domain in System Manager.

### **Before you begin**

The ports you plan to add to the broadcast domain must not belong to another broadcast domain. If the ports you want to use belong to another broadcast domain, but are unused, remove those ports from the original broadcast domain.

### **About this task**

- All broadcast domain names must be unique within an IPspace.
- The ports added to a broadcast domain can be physical network ports, VLANs, or link aggregation groups/interface groups (LAGs/ifgrps).
- The maximum transmission unit (MTU) of the ports added to a broadcast domain are updated to the MTU value set in the broadcast domain.
- The MTU value must match all the devices connected to that layer 2 network except for the e0M port handling management traffic.
- If you do not specify an IPspace name, the broadcast domain is created in the "Default" IPspace.

To make system configuration easier, a failover group of the same name is created automatically that contains the same ports.

## System Manager

### Steps

1. Select **Network > Overview > Broadcast domain**.
2. Click **+ Add**
3. Name the broadcast domain.
4. Set the MTU.
5. Select the IPspace.
6. Save the broadcast domain.

You can edit or delete a broadcast domain after it has been added.

### CLI

In ONTAP 9.7 or earlier, you can manually create a broadcast domain.

### Steps

1. View the ports that are not currently assigned to a broadcast domain:

```
network port show
```

If the display is large, use the `network port show -broadcast-domain` command to view only unassigned ports.

2. Create a broadcast domain:

```
network port broadcast-domain create -broadcast-domain  
broadcast_domain_name -mtu mtu_value [-ipspace ipspace_name] [-ports  
ports_list]
```

- a. `broadcast_domain_name` is the name of the broadcast domain you want to create.
- b. `mtu_value` is the MTU size for IP packets; 1500 and 9000 are typical values.

This value is applied to all ports that are added to this broadcast domain.

- c. `ipspace_name` is the name of the IPspace to which this broadcast domain will be added.

The "Default" IPspace is used unless you specify a value for this parameter.

- d. `ports_list` is the list of ports that will be added to the broadcast domain.

The ports are added in the format `node_name:port_number`, for example, `node1:e0c`.

3. Verify that the broadcast domain was created as desired:

```
network port show -instance -broadcast-domain new_domain
```

### Example

The following command creates broadcast domain `bcast1` in the Default IPspace, sets the MTU to 1500, and adds four ports:

```
network port broadcast-domain create -broadcast-domain bcast1 -mtu 1500 -ports
cluster1-01:e0e,cluster1-01:e0f,cluster1-02:e0e,cluster1-02:e0f
```

### After you finish

You can define the pool of IP addresses that will be available in the broadcast domain by creating a subnet, or you can assign SVMs and interfaces to the IPspace at this time. For more information, see [Cluster and SVM peering](#).

If you need to change the name of an existing broadcast domain, use the `network port broadcast-domain rename` command.

## Add or remove ports from a broadcast domain

Broadcast domains are automatically created during the cluster create or join operation. You do not need to manually remove ports from broadcast domains.

If network port reachability has changed, either through physical network connectivity or switch configuration, and a network port belongs in a different broadcast domain, see the following topic:

### [Repair port reachability](#)

## Split broadcast domains

If network port reachability has changed, either through physical network connectivity or switch configuration, and a group of network ports previously configured in a single broadcast domain has become partitioned into two different reachability sets, you can split a broadcast domain to synchronize the ONTAP configuration with the physical network topology.

To determine if a network port broadcast domain is partitioned into more than one reachability set, use the `network port reachability show -details` command and pay attention to which ports do not have connectivity to one another ("Unreachable ports"). Typically, the list of unreachable ports defines the set of ports that should be split into another broadcast domain, after you have verified that the physical and switch configuration is accurate.

## Step

Split a broadcast domain into two broadcast domains:

```
network port broadcast-domain split -ip-space <ip-space_name> -broadcast
-domain <broadcast_domain_name> -new-broadcast-domain
<broadcast_domain_name> -ports <node:port,node:port>
```

- `ip-space_name` is the name of the ipspace where the broadcast domain resides.
- `-broadcast-domain` is the name of the broadcast domain that will be split.
- `-new-broadcast-domain` is the name of the new broadcast domain that will be created.
- `-ports` is the node name and port to be added to the new broadcast domain.

## Merge broadcast domains

If network port reachability has changed, either through physical network connectivity or switch configuration, and two group of network ports previously configured in multiple broadcast domains now all share reachability, then merging two broadcast domains can be used to synchronize the ONTAP configuration with the physical network topology.

To determine if multiple broadcast domains belong to one reachability set, use the "network port reachability show -details" command and pay attention to which ports that are configured in another broadcast domain actually have connectivity to one another ("Unexpected ports"). Typically, the list of unexpected ports defines the set of ports that should be merged into the broadcast domain after you have verified that the physical and switch configuration is accurate.

### Step

Merge the ports from one broadcast domain into an existing broadcast domain:

```
network port broadcast-domain merge -ipSPACE <ipSPACE_name> -broadcast
-domain <broadcast_domain_name> -into-broadcast-domain
<broadcast_domain_name>
```

- `ipSPACE_name` is the name of the ipSPACE where the broadcast domains reside.
- `-broadcast-domain` is the name of the broadcast domain that will be merged.
- `-into-broadcast-domain` is the name of the broadcast domain that will receive additional ports.

## Change the MTU value for ports in a broadcast domain

You can modify the MTU value for a broadcast domain to change the MTU value for all ports in that broadcast domain. This can be done to support topology changes that have been made in the network.

### Before you begin

The MTU value must match all the devices connected to that layer 2 network except for the e0M port handling management traffic.

### About this task

Changing the MTU value causes a brief interruption in traffic over the affected ports. The system displays a prompt that you must answer with `y` to make the MTU change.

### Step

Change the MTU value for all ports in a broadcast domain:

```
network port broadcast-domain modify -broadcast-domain
<broadcast_domain_name> -mtu <mtu_value> [-ipSPACE <ipSPACE_name>]
```

- `broadcast_domain` is the name of the broadcast domain.
- `mtu` is the MTU size for IP packets; 1500 and 9000 are typical values.

- `ipospace` is the name of the IPspace in which this broadcast domain resides. The "Default" IPspace is used unless you specify a value for this option. The following command changes the MTU to 9000 for all ports in the broadcast domain `bcast1`:

```
network port broadcast-domain modify -broadcast-domain <Default-1> -mtu <
9000 >
```

Warning: Changing broadcast domain settings will cause a momentary data-serving interruption.

Do you want to continue? {y|n}: <y>

### Display broadcast domains

You can display the list of broadcast domains within each IPspace in a cluster. The output also shows the list of ports and the MTU value for each broadcast domain.

#### Step

Display the broadcast domains and associated ports in the cluster:

```
network port broadcast-domain show
```

The following command displays all the broadcast domains and associated ports in the cluster:

```
network port broadcast-domain show
IPspace Broadcast Update
Name Domain Name MTU Port List Status Details
-----
Cluster Cluster 9000
cluster-1-01:e0a complete
cluster-1-01:e0b complete
cluster-1-02:e0a complete
cluster-1-02:e0b complete
Default Default 1500
cluster-1-01:e0c complete
cluster-1-01:e0d complete
cluster-1-02:e0c complete
cluster-1-02:e0d complete
Default-1 1500
cluster-1-01:e0e complete
cluster-1-01:e0f complete
cluster-1-01:e0g complete
cluster-1-02:e0e complete
cluster-1-02:e0f complete
cluster-1-02:e0g complete
```

The following command displays the ports in the Default-1 broadcast domain that have an update status of error, which indicate that the port could not be updated properly:

```
network port broadcast-domain show -broadcast-domain Default-1 -port
-update-status error
```

IPspace	Broadcast			Update
Name	Domain Name	MTU	Port List	Status Details
-----	-----	-----	-----	-----
Default	Default-1	1500	cluster-1-02:e0g	error

For more information, see [ONTAP 9 commands](#).

### Delete a broadcast domain

If you no longer need a broadcast domain, you can delete it. This moves the ports associated with that broadcast domain to the "Default" IPspace.

### Before you begin

There must be no subnets, network interfaces, or SVMs associated with the broadcast domain you want to delete.

### About this task

- The system-created "Cluster" broadcast domain cannot be deleted.
- All failover groups related to the broadcast domain are removed when you delete the broadcast domain.

The procedure you follow depends on the interface that you use—System Manager or the CLI:




## System Manager

### Beginning with ONTAP 9.12.0, you can use System Manager to delete a broadcast domain

The delete option is not shown when the broadcast domain contains ports or is associated with a subnet.

#### Steps

1. Select **Network > Overview > Broadcast domain**.
2. Select  **> Delete** beside the broadcast domain you want to remove.

#### CLI

##### Use the CLI to delete a broadcast domain

#### Step

Delete a broadcast domain:

```
network port broadcast-domain delete -broadcast-domain broadcast_domain_name
[-ipspace ipspace_name]
```

The following command deletes broadcast domain Default-1 in IPspace ipspace1:

```
network port broadcast-domain delete -broadcast-domain Default-1 -ipspace
ipspace1
```

## ONTAP 9.7 and earlier

### Overview for ONTAP 9.7 and earlier

Broadcast domains are intended to group network ports that belong to the same layer 2 network. The ports in the group can then be used by a storage virtual machine (SVM) for data or management traffic.

A broadcast domain resides in an IPspace. During cluster initialization, the system creates two default broadcast domains:

- The Default broadcast domain contains ports that are in the Default IPspace. These ports are used primarily to serve data. Cluster management and node management ports are also in this broadcast domain.
- The Cluster broadcast domain contains ports that are in the Cluster IPspace. These ports are used for cluster communication and include all cluster ports from all nodes in the cluster.

If you have created unique IPspaces to separate client traffic, then you need to create a broadcast domain in each of those IPspaces.



Create a broadcast domain to group network ports in the cluster that belong to the same layer 2 network. The ports can then be used by SVMs.

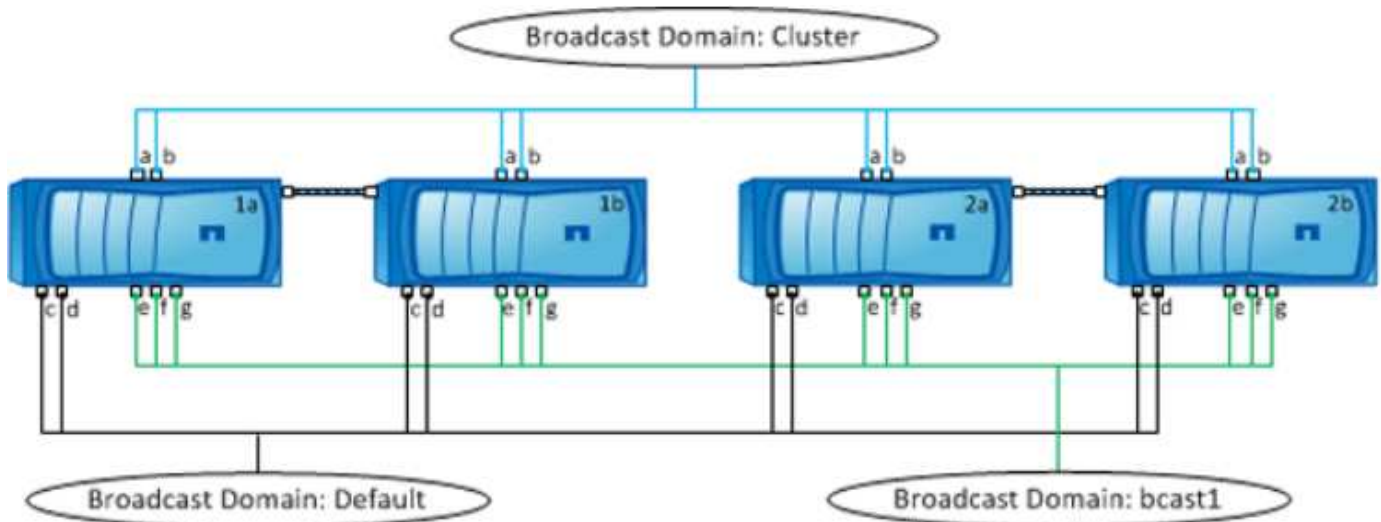
### Example of using broadcast domains

A broadcast domain is a set of network ports in the same IPspace that also has layer 2

reachability to one another, typically including ports from many nodes in the cluster.

The illustration shows the ports assigned to three broadcast domains in a four-node cluster:

- The Cluster broadcast domain is created automatically during cluster initialization, and it contains ports a and b from each node in the cluster.
- The Default broadcast domain is also created automatically during cluster initialization, and it contains ports c and d from each node in the cluster.
- The bcast1 broadcast domain has been created manually, and it contains ports e, f, and g from each node in the cluster.  
This broadcast domain was created by the system administrator specifically for a new client to access data through a new SVM.



A failover group of the same name and with the same network ports as each of the broadcast domains is created automatically. This failover group is automatically managed by the system, meaning that as ports are added or removed from the broadcast domain, they are automatically added or removed from this failover group.

#### Create a broadcast domain

In ONTAP 9.7 and earlier, you create a broadcast domain to group network ports in the cluster that belong to the same layer 2 network. The ports can then be used by SVMs.

#### Before you begin

Beginning with ONTAP 9.8, broadcast domains are automatically created during the cluster create or join operation. If you are running ONTAP 9.8 or later, these steps are not needed.

In ONTAP 9.7 and earlier, the ports you plan to add to the broadcast domain must not belong to another broadcast domain.

#### About this task

- All broadcast domain names must be unique within an IPspace.
- The ports added to a broadcast domain can be physical network ports, VLANs, or interface groups (ifgrps).
- If the ports you want to use belong to another broadcast domain, but are unused, you use the `network port broadcast-domain remove-ports` command to remove the ports from the existing broadcast

domain.

- The MTU of the ports added to a broadcast domain are updated to the MTU value set in the broadcast domain.
- The MTU value must match all of the devices connected to that layer 2 network except for the e0M port handling management traffic.
- If you do not specify an IPspace name, the broadcast domain is created in the "Default" IPspace.

To make system configuration easier, a failover group of the same name is created automatically that contains the same ports.

## Steps

1. View the ports that are not currently assigned to a broadcast domain:

```
network port show
```

If the display is large, use the `network port show -broadcast-domain` command to view only unassigned ports.

2. Create a broadcast domain:

```
network port broadcast-domain create -broadcast-domain broadcast_domain_name  
-mtu mtu_value [-ipspace ipspace_name] [-ports ports_list]
```

◦ *broadcast\_domain\_name* is the name of the broadcast domain you want to create.

◦ *mtu\_value* is the MTU size for IP packets; 1500 and 9000 are typical values.

This value is applied to all ports that are added to this broadcast domain.

◦ *ipspace\_name* is the name of the IPspace to which this broadcast domain will be added.

The "Default" IPspace is used unless you specify a value for this parameter.

◦ *ports\_list* is the list of ports that will be added to the broadcast domain.

The ports are added in the format *node\_name:port\_number*, for example, `node1:e0c`.

3. Verify that the broadcast domain was created as desired:

```
network port show -instance -broadcast-domain new_domain
```

## Example

The following command creates broadcast domain `bcast1` in the Default IPspace, sets the MTU to 1500, and adds four ports:

```
network port broadcast-domain create -broadcast-domain bcast1 -mtu 1500 -ports  
cluster1-01:e0e,cluster1-01:e0f,cluster1-02:e0e,cluster1-02:e0f
```

## After you finish

You can define the pool of IP addresses that will be available in the broadcast domain by creating a subnet, or you can assign SVMs and interfaces to the IPspace at this time. For more information, see [Cluster and SVM peering](#).

If you need to change the name of an existing broadcast domain, you use the `network port broadcast-domain rename` command.

### Add or remove ports from a broadcast domain

You can add network ports when initially creating a broadcast domain, or you can add ports to, or remove ports from, a broadcast domain that already exists. This allows you to efficiently use all the ports in the cluster.

### Before you begin

- Ports you plan to add to a broadcast domain must not belong to another broadcast domain.
- Ports that already belong to an interface group cannot be added individually to a broadcast domain.

### About this task

The following rules apply when adding and removing network ports:

When adding ports...	When removing ports...
The ports can be network ports, VLANs, or interface groups (ifgrps).	N/A
The ports are added to the system-defined failover group of the broadcast domain.	The ports are removed from all failover groups in the broadcast domain.
The MTU of the ports is updated to the MTU value set in the broadcast domain.	The MTU of the ports is unchanged.
The IPspace of the ports is updated to the IPspace value of the broadcast domain.	The ports are moved to the 'Default' IPspace with no broadcast domain attribute.



If you remove the last member port of an interface group using the `network port ifgrp remove-port` command, it causes the interface group port to be removed from the broadcast domain because an empty interface group port is not allowed in a broadcast domain.

### Steps

1. Display the ports that are currently assigned or unassigned to a broadcast domain by using the `network port show` command.
2. Add or remove network ports from the broadcast domain:

If you want to...	Use...
Add ports to a broadcast domain	<code>network port broadcast-domain add-ports</code>
Remove ports from a broadcast domain	<code>network port broadcast-domain remove-ports</code>

For more information about these commands, see [ONTAP 9 commands](#).

### Examples of adding and removing ports

The following command adds port e0g on node cluster-1-01 and port e0g on node cluster-1-02 to broadcast

domain bcast1 in the Default IPspace:

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain bcast1
-ports cluster-1-01:e0g,cluster1-02:e0g
```

The following command adds two cluster ports to broadcast domain Cluster in the Cluster IPspace:

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain Cluster
-ports cluster-2-03:e0f,cluster2-04:e0f -ip-space Cluster
```

The following command removes port e0e on node cluster1-01 from broadcast domain bcast1 in the Default IPspace:

```
cluster-1::> network port broadcast-domain remove-ports -broadcast-domain bcast1
-ports cluster-1-01:e0e
```

### Split broadcast domains

You can modify an existing broadcast domain by splitting it into two different broadcast domains, with each broadcast domain containing some of the original ports assigned to the original broadcast domain.

#### About this task

- If the ports are in a failover group, all of the ports in a failover group must be split.
- If the ports have LIFs associated with them, the LIFs cannot be part of a subnet's ranges.

#### Step

Split a broadcast domain into two broadcast domains:

```
network port broadcast-domain split -ip-space <ip-space_name> -broadcast
-domain <broadcast_domain_name> -new-broadcast-domain
<broadcast_domain_name> -ports <node:port,node:port>
```

- `ip-space_name` is the name of the IPspace where the broadcast domain resides.
- `-broadcast-domain` is the name of the broadcast domain that will be split.
- `-new-broadcast-domain` is the name of the new broadcast domain that will be created.
- `-ports` is the node name and port to be added to the new broadcast domain.

### Merge broadcast domains

You can move all of the ports from one broadcast domain into an existing broadcast domain using the merge command.

This operation reduces the steps required if you were to remove all ports from a broadcast domain and then add the ports to an existing broadcast domain.

#### Step

Merge the ports from one broadcast domain into an existing broadcast domain:

```
network port broadcast-domain merge -ipSPACE <ipSPACE_name> -broadcast-domain <broadcast_domain_name> -into-broadcast-domain <broadcast_domain_name>
```

- `ipSPACE_name` is the name of the IPspace where the broadcast domains reside.
- `-broadcast-domain` is the name of the broadcast domain that will be merged.
- `-into-broadcast-domain` is the name of the broadcast domain that will receive additional ports.

### Example

The following example merges broadcast domain `bd-data1` into broadcast domain `bd-data2`:

```
network port -ipSPACE Default broadcast-domain bd-data1 into-broadcast-domain bd-data2
```

### Change the MTU value for ports in a broadcast domain

You can modify the MTU value for a broadcast domain to change the MTU value for all ports in that broadcast domain. This can be done to support topology changes that have been made in the network.

### Before you begin

The MTU value must match all the devices connected to that layer 2 network except for the e0M port handling management traffic.

### About this task

Changing the MTU value causes a brief interruption in traffic over the affected ports. The system displays a prompt that you must answer with `y` to make the MTU change.

### Step

Change the MTU value for all ports in a broadcast domain:

```
network port broadcast-domain modify -broadcast-domain <broadcast_domain_name> -mtu <mtu_value> [-ipSPACE <ipSPACE_name>]
```

- `broadcast_domain` is the name of the broadcast domain.
- `mtu` is the MTU size for IP packets; 1500 and 9000 are typical values.
- `ipSPACE` is the name of the IPspace in which this broadcast domain resides. The "Default" IPspace is used unless you specify a value for this option. The following command changes the MTU to 9000 for all ports in the broadcast domain `bcast1`:

```
network port broadcast-domain modify -broadcast-domain <Default-1> -mtu <
9000 >
Warning: Changing broadcast domain settings will cause a momentary data-
serving interruption.
Do you want to continue? {y|n}: <y>
```

### Display broadcast domains

You can display the list of broadcast domains within each IPspace in a cluster. The output also shows the list of ports and the MTU value for each broadcast domain.

#### Step

Display the broadcast domains and associated ports in the cluster:

```
network port broadcast-domain show
```

The following command displays all the broadcast domains and associated ports in the cluster:

```
network port broadcast-domain show
IPspace Broadcast Update
Name Domain Name MTU Port List Status Details
-----
Cluster Cluster 9000
cluster-1-01:e0a complete
cluster-1-01:e0b complete
cluster-1-02:e0a complete
cluster-1-02:e0b complete
Default Default 1500
cluster-1-01:e0c complete
cluster-1-01:e0d complete
cluster-1-02:e0c complete
cluster-1-02:e0d complete
bcast1 1500
cluster-1-01:e0e complete
cluster-1-01:e0f complete
cluster-1-01:e0g complete
cluster-1-02:e0e complete
cluster-1-02:e0f complete
cluster-1-02:e0g complete
```

The following command displays the ports in the bcast1 broadcast domain that have an update status of error, which indicate that the port could not be updated properly:

```
network port broadcast-domain show -broadcast-domain bcast1 -port-update
-status error
```

IPspace	Broadcast			Update
Name	Domain Name	MTU	Port List	Status Details
Default	bcast1	1500	cluster-1-02:e0g	error

For more information, see [ONTAP 9 commands](#).

### Delete a broadcast domain

If you no longer need a broadcast domain, you can delete it. This moves the ports associated with that broadcast domain to the "Default" IPspace.

### Before you begin

There must be no subnets, network interfaces, or SVMs associated with the broadcast domain you want to delete.

### About this task

- The system-created "Cluster" broadcast domain cannot be deleted.
- All failover groups related to the broadcast domain are removed when you delete the broadcast domain.

### Step

Delete a broadcast domain:

```
network port broadcast-domain delete -broadcast-domain
<broadcast_domain_name> [-ipSPACE <ipSPACE_name>]
```

The following command deletes broadcast domain bcast1 in IPspace ipSPACE1:

```
network port broadcast-domain delete -broadcast-domain <bcast1> -ipSPACE
<ipSPACE1>
```

## Configure failover groups and policies for LIFs

### Overview

LIF failover refers to the automatic migration of a LIF to a different network port in response to a link failure on the LIF's current port. This is a key component to providing high availability for the connections to SVMs. Configuring LIF failover involves creating a failover group, modifying the LIF to use the failover group, and specifying a failover policy.

A failover group contains a set of network ports (physical ports, VLANs, and interface groups) from one or



more nodes in a cluster. The network ports that are present in the failover group define the failover targets available for the LIF. A failover group can have cluster management, node management, intercluster, and NAS data LIFs assigned to it.



When a LIF is configured without a valid failover target, an outage occurs when the LIF attempts to fail over. You can use the "network interface show -failover" command to verify the failover configuration.

When you create a broadcast domain, a failover group of the same name is created automatically that contains the same network ports. This failover group is automatically managed by the system, meaning that as ports are added or removed from the broadcast domain, they are automatically added or removed from this failover group. This is provided as an efficiency for administrators who do not want to manage their own failover groups.

## Create a failover group

You create a failover group of network ports so that a LIF can automatically migrate to a different port if a link failure occurs on the LIF's current port. This enables the system to reroute network traffic to other available ports in the cluster.

### About this task

You use the `network interface failover-groups create` command to create the group and to add ports to the group.

- The ports added to a failover group can be network ports, VLANs, or interface groups (ifgrps).
- All the ports added to the failover group must belong to the same broadcast domain.
- A single port can reside in multiple failover groups.
- If you have LIFs in different VLANs or broadcast domains, you must configure failover groups for each VLAN or broadcast domain.
- Failover groups do not apply in SAN iSCSI or FC environments.

### Step

Create a failover group:

```
network interface failover-groups create -vserver vserver_name -failover-group  
failover_group_name -targets ports_list
```

- *vserver\_name* is the name of the SVM that can use the failover group.
- *failover\_group\_name* is the name of the failover group you want to create.
- *ports\_list* is the list of ports that will be added to the failover group.  
Ports are added in the format *node\_name>:<port\_number>*, for example, `node1:e0c`.

The following command creates failover group fg3 for SVM vs3 and adds two ports:

```
network interface failover-groups create -vserver vs3 -failover-group fg3  
-targets cluster1-01:e0e,cluster1-02:e0e
```

### After you finish

- You should apply the failover group to a LIF now that the failover group has been created.
- Applying a failover group that does not provide a valid failover target for a LIF results in a warning message.

If a LIF that does not have a valid failover target attempts to fail over, an outage might occur.

## Configure failover settings on a LIF

You can configure a LIF to fail over to a specific group of network ports by applying a failover policy and a failover group to the LIF. You can also disable a LIF from failing over to another port.

### About this task

- When a LIF is created, LIF failover is enabled by default, and the list of available target ports is determined by the default failover group and failover policy based on the LIF type and service policy.

Beginning with 9.5, you can specify a service policy for the LIF that defines which network services can use the LIF. Some network services impose failover restrictions on a LIF.



If a LIF's service policy is changed in a way that further restricts failover, the LIF's failover policy is automatically updated by the system.

- You can modify the failover behavior of LIFs by specifying values for the `-failover-group` and `-failover-policy` parameters in the network interface modify command.
- Modification of a LIF that results in the LIF having no valid failover target results in a warning message.

If a LIF that does not have a valid failover target attempts to fail over, an outage might occur.

- Beginning with ONTAP 9.11.1, on All SAN Array (ASA) platforms, iSCSI LIF failover is automatically enabled on newly created iSCSI LIFs on newly created storage VMs.

Additionally, you can manually enable iSCSI LIF failover on pre-existing iSCSI LIFs, meaning LIFs that were created prior to upgrading to ONTAP 9.11.1 or later.

[iSCSI LIF failover for ASA platforms](#)

- The following list describes how the `-failover-policy` setting affects the target ports that are selected from the failover group:



For iSCSI LIF failover, only the failover policies `local-only`, `sfo-partner-only` and `disabled` are supported.

- `broadcast-domain-wide` applies to all ports on all nodes in the failover group.
- `system-defined` applies to only those ports on the LIF's home node and one other node in the cluster, typically a non- SFO partner, if it exists.
- `local-only` applies to only those ports on the LIF's home node.
- `sfo-partner-only` applies to only those ports on the LIF's home node and its SFO partner.
- `disabled` indicates the LIF is not configured for failover.

## Step

Configure failover settings for an existing interface:

```
network interface modify -vserver <vserver_name> -lif <lif_name> -failover
-policy <failover_policy> -failover-group <failover_group>
```

### Examples of configuring failover settings and disabling failover

The following command sets the failover policy to broadcast-domain-wide and uses the ports in failover group fg3 as failover targets for LIF data1 on SVM vs3:

```
network interface modify -vserver vs3 -lif data1 failover-policy
broadcast-domain-wide - failover-group fg3

network interface show -vserver vs3 -lif * -fields failover-
group,failover-policy

vserver lif          failover-policy          failover-group
-----
vs3      data1        broadcast-domain-wide  fg3
```

The following command disables failover for LIF data1 on SVM vs3:

```
network interface modify -vserver vs3 -lif data1 failover-policy disabled
```

### Commands for managing failover groups and policies

You can use the `network interface failover-groups` commands to manage failover groups. You use the `network interface modify` command to manage the failover groups and failover policies that are applied to a LIF.

If you want to...	Use this command...
Add network ports to a failover group	<code>network interface failover-groups add-targets</code>
Remove network ports from a failover group	<code>network interface failover-groups remove-targets</code>
Modify network ports in a failover group	<code>network interface failover-groups modify</code>
Display the current failover groups	<code>network interface failover-groups show</code>

Configure failover on a LIF	<code>network interface modify -failover -group -failover-policy</code>
Display the failover group and failover policy that is being used by each LIF	<code>network interface show -fields failover-group, failover-policy</code>
Rename a failover group	<code>network interface failover-groups rename</code>
Delete a failover group	<code>network interface failover-groups delete</code>



Modifying a failover group such that it does not provide a valid failover target for any LIF in the cluster can result in an outage when a LIF attempts to fail over.

For more information, see the man pages for the `network interface failover-groups` and `network interface modify` commands.

## Configure subnets (cluster administrators only)

### Overview

Subnets enable you to allocate specific blocks, or pools, of IP addresses for your ONTAP network configuration. This enables you to create LIFs more easily when using the `network interface create` command, by specifying a subnet name instead of having to specify IP address and network mask values.

A subnet is created within a broadcast domain, and it contains a pool of IP addresses that belong to the same layer 3 subnet. IP addresses in a subnet are allocated to ports in the broadcast domain when LIFs are created. When LIFs are removed, the IP addresses are returned to the subnet pool and are available for future LIFs.

It is recommended that you use subnets because they make the management of IP addresses much easier, and they make the creation of LIFs a simpler process. Additionally, if you specify a gateway when defining a subnet, a default route to that gateway is added automatically to the SVM when a LIF is created using that subnet.

### Create a subnet

You can create a subnet to allocate specific blocks of IPv4 or IPv6 addresses to be used later when you create LIFs for the SVM.

This enables you to create LIFs more easily by specifying a subnet name instead of having to specify IP address and network mask values for each LIF.

### Before you begin

You must be a cluster administrator to perform this task.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

## System Manager

Beginning with ONTAP 9.12.0, you can use System Manager to create a subnet

### Steps

1. Select **Network > Overview > Subnets**.
2. Click **+ Add** to create a subnet.
3. Name the subnet.
4. Specify the subnet IP address.
5. Set the subnet mask.
6. Define the range of IP addresses that comprise the subnet.
7. If useful, specify a gateway.
8. Select the broadcast domain to which the subnet belongs.
9. Save your changes.
  - a. If the IP address or range entered is already used by an interface, the following message is displayed:  
An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?
  - b. When you click **OK**, the existing LIF will be associated with the subnet.

## CLI

Use the CLI to create a subnet

### Steps

1. Create a subnet.

```
network subnet create -broadcast-domain ipspace1 -ip-space ipspace1 -subnet  
-name ipspace1 -subnets 10.0.0.0/24 -gateway 10.0.0.1 -ip-ranges  
"10.0.0.128-10.0.0.130,10.0.0.132"
```

The subnet name can be either a subnet IP value such as 192.0.2.0/24 or a string such as ipspace1 like the one used in this example.

2. Verify that the subnet configuration is correct.

The output from this example shows information about the subnet named ipspace1 in the ipspace1 IPspace. The subnet belongs to the broadcast domain name ipspace1. You can assign the IP addresses in this subnet to data LIFs for SVMs created in the ipspace1 IPspace.

```
network subnet show -ip-space ipspace1
```

## Add or remove IP addresses from a subnet

You can add IP addresses when initially creating a subnet, or you can add IP addresses to a subnet that already exists. You can also remove IP addresses from an existing subnet. This enables you to allocate only the required IP addresses for SVMs.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

## System Manager

Beginning with ONTAP 9.12.0, you can use System Manager to add or remove IP addresses to or from a subnet

### Steps

1. Select **Network > Overview > Subnets**.
2. Select **:** > **Edit** beside the subnet you want to change.
3. Add or remove IP addresses.
4. Save your changes.
  - a. If the IP address or range entered is already used by an interface, the following message is displayed:  
An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?
  - b. When you click **OK**, the existing LIF will be associated with the subnet.

### CLI

#### Use the CLI to add or remove IP addresses to or from a subnet

##### About this task

When adding IP addresses, you will receive an error if any service processor or network interfaces are using the IP addresses in the range being added. If you want to associate any manually addressed interfaces with the current subnet, you can set the `-force-update-lif-associations` option to `true`.

When removing IP addresses, you will receive an error if any service processor or network interfaces are using the IP addresses being removed. If you want the interfaces to continue to use the IP addresses after they are removed from the subnet, you can set the `-force-update-lif-associations` option to `true`.

### Step

Add or remove IP addresses from a subnet:

If you want to...	Use this command...
Add IP addresses to a subnet	<code>network subnet add-ranges</code>
Remove IP addresses from a subnet	<code>network subnet remove-ranges</code>

For more information about these commands, see the man pages.

The following command adds IP addresses 192.0.2.82 through 192.0.2.85 to subnet sub1:

```
network subnet add-ranges -subnet-name <sub1> -ip-ranges <192.0.2.82-192.0.2.85>
```

The following command removes IP address 198.51.100.9 from subnet sub3:

```
network subnet remove-ranges -subnet-name <sub3> -ip-ranges
<198.51.100.9>
```

If the current range includes 1 through 10 and 20 through 40, and you want to add 11 through 19 and 41 through 50 (basically allowing 1 through 50), you can overlap the existing range of addresses by using the following command. This command adds only the new addresses and does not affect the existing addresses:

```
network subnet add-ranges -subnet-name <sub3> -ip-ranges <198.51.10.1-
198.51.10.50>
```

### Change subnet properties

You can change the subnet address and mask value, gateway address, or range of IP addresses in an existing subnet.

#### About this task

- When modifying IP addresses, you must ensure there are no overlapping IP addresses in the network so that different subnets, or hosts, do not attempt to use the same IP address.
- If you add or change the gateway IP address, the modified gateway is applied to new SVMs when a LIF is created in them using the subnet. A default route to the gateway is created for the SVM if the route does not already exist. You may need to manually add a new route to the SVM when you change the gateway IP address.

The procedure you follow depends on the interface that you use—System Manager or the CLI:



## System Manager

Beginning with ONTAP 9.12.0, you can use System Manager to change subnet properties

### Steps

1. Select **Network > Overview > Subnets**.
2. Select **:** > **Edit** beside the subnet you want to change.
3. Make changes.
4. Save your changes.
  - a. If the IP address or range entered is already used by an interface, the following message is displayed:  
An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?
  - b. When you click **OK**, the existing LIF will be associated with the subnet.

### CLI

Use the CLI to change subnet properties

#### Step

Modify subnet properties:

```
network subnet modify -subnet-name <subnet_name> [-ipSPACE  
<ipSPACE_name>] [-subnet <subnet_address>] [-gateway <gateway_address>]  
[-ip-ranges <ip_address_list>] [-force-update-lif-associations <true>]
```

- `subnet_name` is the name of the subnet you want to modify.
- `ipSPACE` is the name of the IPspace where the subnet resides.
- `subnet` is the new address and mask of the subnet, if applicable; for example, 192.0.2.0/24.
- `gateway` is the new gateway of the subnet, if applicable; for example, 192.0.2.1. Entering "" removes the gateway entry.
- `ip_ranges` is the new list, or range, of IP addresses that will be allocated to the subnet, if applicable. The IP addresses can be individual addresses, a range or IP addresses, or a combination in a comma-separated list. The range specified here replaces the existing IP addresses.
- `force-update-lif-associations` is required when you change the IP address range. You can set the value to **true** for this option when modifying the range of IP addresses. This command fails if any service processor or network interfaces are using the IP addresses in the specified range. Setting this value to **true** associates any manually addressed interfaces with the current subnet and allows the command to succeed.

The following command modifies the gateway IP address of subnet sub3:

```
network subnet modify -subnet-name <sub3> -gateway <192.0.3.1>
```

## Display subnets

You can display the list of IP addresses that are allocated to each subnet within an IPspace. The output also shows the total number of IP addresses that are available in each subnet, and the number of addresses that are currently being used.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

### System Manager

Beginning with ONTAP 9.12.0, you can use System Manager to display subnets

#### Steps

1. Select **Network > Overview > Subnets**.
2. View the list of subnets.

### CLI

Use the CLI to display subnets

#### Step

Display the list of subnets and the associated IP address ranges that are used in those subnets:

```
network subnet show
```

The following command displays the subnets and the subnet properties:

```
network subnet show

IPspace: Default
Subnet
Name Subnet Broadcast Domain Gateway Avail/ Total Ranges
-----
-----
sub1 192.0.2.0/24 bcast1 192.0.2.1 5/9 192.0.2.92-
192.0.2.100
sub3 198.51.100.0/24 bcast3 198.51.100.1 3/3
198.51.100.7,198.51.100.9
```

## Delete a subnet

If you no longer need a subnet and want to deallocate the IP addresses that were assigned to the subnet, you can delete it.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

## System Manager

Beginning with ONTAP 9.12.0, you can use System Manager to delete a subnet

### Steps

1. Select **Network > Overview > Subnets**.
2. Select **⋮ > Delete** beside the subnet you want to remove.
3. Save your changes.

### CLI

Use the CLI to delete a subnet

#### About this task

You will receive an error if any service processor or network interfaces are currently using IP addresses in the specified ranges. If you want the interfaces to continue to use the IP addresses even after the subnet is deleted, you can set the `-force-update-lif-associations` option to true to remove the subnet's association with the LIFs.

#### Step

Delete a subnet:

```
network subnet delete -subnet-name subnet_name [-ipspace ipspace_name] [-force-update-lif-associations true]
```

The following command deletes subnet sub1 in IPspace ipspace1:

```
network subnet delete -subnet-name sub1 -ipspace ipspace1
```

## Configure LIFs (cluster administrators only)

### Overview

A LIF (logical interface) represents a network access point to a node in the cluster. You can configure LIFs on ports over which the cluster sends and receives communications over the network.

A cluster administrator can create, view, modify, migrate, revert, or delete LIFs. An SVM administrator can only view the LIFs associated with the SVM.

A LIF is an IP address or WWPN with associated characteristics, such as a service policy, a home port, a home node, a list of ports to fail over to, and a firewall policy. You can configure LIFs on ports over which the cluster sends and receives communications over the network.

LIFs can be hosted on the following ports:

- Physical ports that are not part of interface groups
- Interface groups
- VLANs
- Physical ports or interface groups that host VLANs

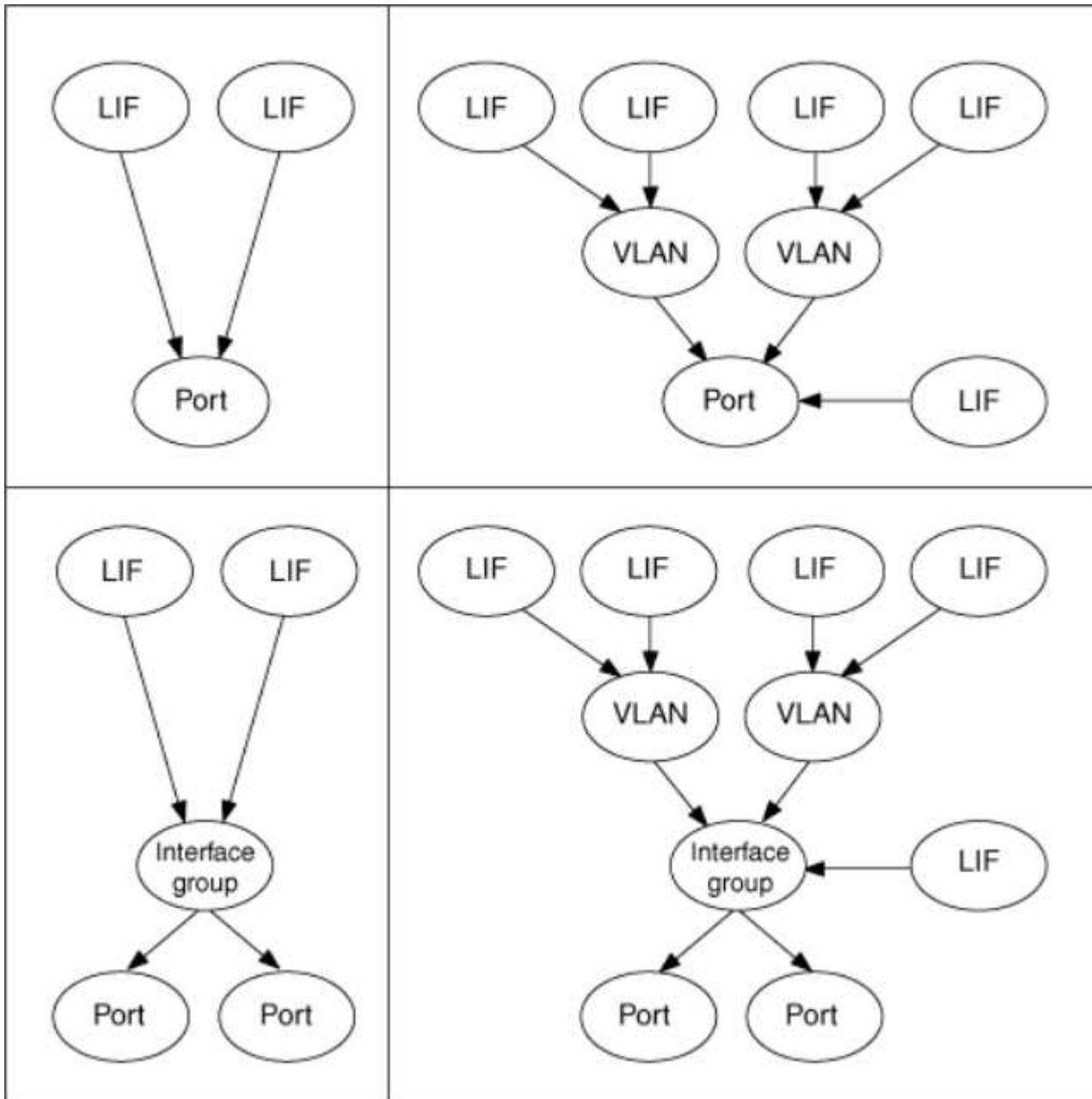
- Virtual IP (VIP) ports

Beginning with ONTAP 9.5, VIP LIFs are supported and are hosted on VIP ports.

While configuring SAN protocols such as FC on a LIF, it will be associated with a WWPN.

### SAN administration

The following figure illustrates the port hierarchy in an ONTAP system:



### LIF compatibility with port types

LIFs can have different characteristics to support different port types.



When intercluster and management LIFs are configured in the same subnet, the management traffic might be blocked by an external firewall and the AutoSupport and NTP connections might fail. You can recover the system by running the `network interface modify -vserver vserver name -lif intercluster LIF -status-admin up|down` command to toggle the intercluster LIF. However, you should set the intercluster LIF and management LIF in different subnets to avoid this issue.

LIF	Description
Data LIF	<p>A LIF that is associated with a storage virtual machine (SVM) and is used for communicating with clients.</p> <p>You can have multiple data LIFs on a port. These interfaces can migrate or fail over throughout the cluster. You can modify a data LIF to serve as an SVM management LIF by modifying its firewall policy to mgmt.</p> <p>Sessions established to NIS, LDAP, Active Directory, WINS, and DNS servers use data LIFs.</p>
Cluster LIF	<p>A LIF that is used to carry intracluster traffic between nodes in a cluster. Cluster LIFs must always be created on cluster ports.</p> <p>Cluster LIFs can fail over between cluster ports on the same node, but they cannot be migrated or failed over to a remote node. When a new node joins a cluster, IP addresses are generated automatically. However, if you want to assign IP addresses manually to the cluster LIFs, you must ensure that the new IP addresses are in the same subnet range as the existing cluster LIFs.</p>
Cluster management LIF	<p>LIF that provides a single management interface for the entire cluster.</p> <p>A cluster management LIF can fail over to any node in the cluster. It cannot fail over to cluster or intercluster ports</p>
Intercluster LIF	<p>A LIF that is used for cross-cluster communication, backup, and replication. You must create an intercluster LIF on each node in the cluster before a cluster peering relationship can be established.</p> <p>These LIFs can only fail over to ports in the same node. They cannot be migrated or failed over to another node in the cluster.</p>
Node management LIF	<p>A LIF that provides a dedicated IP address for managing a particular node in a cluster. Node management LIFs are created at the time of creating or joining the cluster. These LIFs are used for system maintenance, for example, when a node becomes inaccessible from the cluster.</p>
VIP LIF	<p>A VIP LIF is any data LIF created on a VIP port. To learn more, see <a href="#">Configure virtual IP (VIP) LIFs</a>.</p>

### LIF roles in ONTAP 9.5 and earlier

LIFs with different roles have different characteristics. A LIF role determines the kind of traffic that is supported over the interface, along with the failover rules that apply, the firewall restrictions that are in place, the security, the load balancing, and the routing behavior for each LIF. A LIF can have any one of the following roles: cluster, cluster management, data, intercluster, node management, and undef (undefined). The undef

role is used for BGP LIFs.

Beginning with ONTAP 9.6, LIF roles are deprecated. You should specify service policies for LIFs instead of a role. It is not necessary to specify a LIF role when creating a LIF with a service policy.

#### LIF security

	Data LIF	Cluster LIF	Node management LIF	Cluster management LIF	Intercluster LIF
Require private IP subnet?	No	Yes	No	No	No
Require secure network?	No	Yes	No	No	Yes
Default firewall policy	Very restrictive	Completely open	Medium	Medium	Very restrictive
Is firewall customizable?	Yes	No	Yes	Yes	Yes

#### LIF failover

	Data LIF	Cluster LIF	Node management LIF	Cluster management LIF	Intercluster LIF
Default behavior	Only those ports in the same failover group that are on the LIF's home node and on a non-SFO partner node	Only those ports in the same failover group that are on the LIF's home node	Only those ports in the same failover group that are on the LIF's home node	Any port in the same failover group	Only those ports in the same failover group that are on the LIF's home node
Is customizable?	Yes	No	Yes	Yes	Yes

#### LIF routing

	Data LIF	Cluster LIF	Node management LIF	Cluster management LIF	Intercluster LIF
When is a default route needed?	When clients or domain controller are on different IP subnet	Never	When any of the primary traffic types require access to a different IP subnet	When administrator is connecting from another IP subnet	When other intercluster LIFs are on a different IP subnet

When is a static route to a specific IP subnet needed?	Rare	Never	Rare	Rare	When nodes of another cluster have their intercluster LIFs in different IP subnets
When is a static host route to a specific server needed?	To have one of the traffic types listed under node management LIF, go through a data LIF rather than a node management LIF. This requires a corresponding firewall change.	Never	Rare	Rare	Rare

### LIF rebalancing

	Data LIF	Cluster LIF	Node management LIF	Cluster management LIF	Intercluster LIF
DNS: use as DNS server?	Yes	No	No	No	No
DNS: export as zone?	Yes	No	No	No	No

### LIF primary traffic types

	Data LIF	Cluster LIF	Node management LIF	Cluster management LIF	Intercluster LIF
Primary traffic types	NFS server, CIFS server, NIS client, Active Directory, LDAP, WINS, DNS client and server, iSCSI and FC server	Intracluster	SSH server, HTTPS server, NTP client, SNMP, AutoSupport client, DNS client, loading software updates	SSH server, HTTPS server	Cross-cluster replication

### LIFs and service policies in ONTAP 9.6 and later

You can assign service policies (instead of LIF roles) to LIFs that determine the kind of traffic that is supported for the LIFs. Service policies define a collection of network services supported by a LIF. ONTAP provides a set of built-in service policies that can be associated with a LIF.

You can display service policies and their details using the following command:

```
network interface service-policy show
```

### Service policies for system SVMs

The admin SVM and any system SVM contain service policies that can be used for LIFs in that SVM, including management and intercluster LIFs. These policies are automatically created by the system when an IPspace is created.

The following table lists the built-in policies for LIFs in system SVMs as of ONTAP 9.11.1. For other releases, display the service policies and their details using the following command:

```
network interface service-policy show
```

Policy	Included services	Equivalent role	Description
default-intercluster	intercluster-core, management-https	intercluster	Used by LIFs carrying intercluster traffic. Note: Service intercluster-core is available from ONTAP 9.5 with the name net-intercluster service policy.
default-route-announce	management-bgp	-	Used by LIFs carrying BGP peer connections Note: Available from ONTAP 9.5 with the name net-route-announce service policy.
default-management	management-core, management-https, management-http, management-ssh, management-autosupport, management-ems, management-dns-client, management-ad-client, management-ldap-client, management-nis-client, management-ntp-client	node-mgmt, or cluster-mgmt	Use this system scoped management policy to create node- and cluster-scoped management LIFs owned by a system SVM. These LIFs can be used for outbound connections to DNS, AD, LDAP, or NIS servers as well as some additional connections to support applications that run on behalf of the entire system.

The following table lists the services that LIFs can use on a system SVM as of ONTAP 9.11.1:

Service	Failover limitations	Description
intercluster-core	home-node-only	Core intercluster services
management-core	-	Core management services
management-ssh	-	Services for SSH management access



management-http	-	Services for HTTP management access
management-https	-	Services for HTTPS management access
management-autosupport	-	Services related to posting AutoSupport payloads
management-bgp	home-port-only	Services related to BGP peer interactions
backup-ndmp-control	-	Services for NDMP backup controls
management-ems	-	Services for management messaging access
management-ntp-client	-	Introduced in ONTAP 9.10.1. Services for NTP client access.
management-ntp-server	-	Introduced in ONTAP 9.11.1. Services for NTP server management access
management-portmap	-	Services for portmap management
management-rsh-server	-	Services for rsh server management
management-snmp-server	-	Services for SNMP server management
management-telnet-server	-	Services for telnet server management

### Service policies for data SVMs

All data SVMs contain service policies that can be used by LIFs in that SVM.

The following table lists the built-in policies for LIFs in data SVMs as of ONTAP 9.11.1. For other releases, display the service policies and their details using the following command:

```
network interface service-policy show
```

Policy	Included services	Equivalent data protocol	Description
--------	-------------------	--------------------------	-------------

default-management	management-https, management-http, management-ssh, management-dns-client, management-ad-client, management-ldap-client, management-nis-client	none	Use this SVM-scoped management policy to create SVM management LIFs owned by a data SVM. These LIFs can be used to provide SSH or HTTPS access to SVM administrators. When necessary, these LIFs can be used for outbound connections to an external DNS, AD, LDAP, or NIS servers.
default-data-blocks	data-core, data-iscsi	iscsi	Used by LIFs carrying block-oriented SAN data traffic. Starting in ONTAP 9.10.1, the "default-data-blocks" policy is deprecated. Use the "default-data-iscsi" service policy instead.
default-data-files	data-fpolicy-client, data-dns-server, data-flexcache, data-cifs, data-nfs, management-dns-client, management-ad-client, management-ldap-client, management-nis-client	nfs, cifs, fcache	Use the default-data-files policy to create NAS LIFs supporting file-based data protocols. Sometimes there is only one LIF present in the SVM, therefore this policy allows the LIF to be used for outbound connections to an external DNS, AD, LDAP, or NIS server. You can remove these services to from this policy if you prefer these connections utilize only management LIFs.
default-data-iscsi	data-core, data-iscsi	iscsi	Used by LIFs carrying iSCSI data traffic.
default-data-nvme-tcp	data-core, data-nvme-tcp	nvme-tcp	Used by LIFs carrying NVMe/TCP data traffic.

The following table lists the services that can be used on a data SVM along with any restrictions each service imposes on a LIF's failover policy as of ONTAP 9.11.1:

Service	Failover restrictions	Description
management-ssh	-	Services for SSH management access
management-http	-	Introduced in ONTAP 9.10.1 Services for HTTP management access
management-https	-	Services for HTTPS management access
management-portmap	-	Services for portmap management access
management-snmp-server	-	Introduced in ONTAP 9.10.1 Services for SNMP server management access

data-core	-	Core data services
data-nfs	-	NFS data service
data-cifs	-	CIFS data service
data-flexcache	-	FlexCache data service
data-iscsi	home-port-only	iSCSI data service
backup-ndmp-control	-	Introduced in ONTAP 9.10.1 Backup NDMP controls data service
data-dns-server	-	Introduced in ONTAP 9.10.1 DNS server data service
data-fpolicy-client	-	File-screening policy data service
data-nvme-tcp	home-port-only	Introduced in ONTAP 9.10.1 NVMe TCP data service
data-s3-server	-	Simple Storage Service (S3) server data service

You should be aware of how the service policies are assigned to the LIFs in data SVMs:

- If a data SVM is created with a list of data services, the built-in "default-data-files" and "default-data-blocks" service policies in that SVM are created using the specified services.
- If a data SVM is created without specifying a list of data services, the built-in "default-data-files" and "default-data-blocks" service policies in that SVM are created using a default list of data services.

The default data services list includes the iSCSI, NFS, NVMe, SMB, and FlexCache services.

- When a LIF is created with a list of data protocols, a service policy equivalent to the specified data protocols is assigned to the LIF.
- If an equivalent service policy does not exist, a custom service policy is created.
- When a LIF is created without a service policy or list of data protocols, the default-data-files service policy is assigned to the LIF by default.

#### **Data-core service**

The data-core service allows components that previously used LIFs with the data role to work as expected on clusters that have been upgraded to manage LIFs using service policies instead of LIF roles (which are deprecated in ONTAP 9.6).

Specifying data-core as a service does not open any ports in the firewall, but the service should be included in any service policy in a data SVM. For example, the default-data-files service policy contains the following services by default:

- data-core
- data-nfs
- data-cifs
- data-flexcache

The data-core service should be included in the policy to ensure all applications using the LIF work as expected, but the other three services can be removed, if desired.

#### Client-side LIF service

Beginning with ONTAP 9.10.1, ONTAP provides client-side LIF services for multiple applications. These services provide control over which LIFs are used for outbound connections on behalf of each application.

The following new services give administrators control over which LIFs are used as source addresses for certain applications.

Service	SVM restrictions	Description
management-ad-client	-	Beginning with ONTAP 9.11.1, ONTAP provides Active Directory client service for outbound connections to an external AD server.
management-dns-client	-	Beginning with ONTAP 9.11.1, ONTAP provides DNS client service for outbound connections to an external DNS server.
management-ldap-client	-	Beginning with ONTAP 9.11.1, ONTAP provides LDAP client service for outbound connections to an external LDAP server.
management-nis-client	-	Beginning with ONTAP 9.11.1, ONTAP provides NIS client service for outbound connections to an external NIS server.
management-ntp-client	system-only	Beginning with ONTAP 9.10.1, ONTAP provides NTP client service for outbound connections to an external NTP server.
data-fpolicy-client	data-only	Beginning with ONTAP 9.8, ONTAP provides client service for outbound FPolicy connections.

Each of the new services are automatically included in some of the built-in service policies, but administrators can remove them from the built-in policies or add them to custom policies to control which LIFs are used for outbound connections on behalf of each application.

#### Configure LIF service policies

You can configure LIF service policies to identify a single service or a list of services that will use a LIF.

## Create a service policy for LIFs

You can create a service policy for LIFs. You can assign a service policy to one or more LIFs; thereby allowing the LIF to carry traffic for a single service or a list of services.

You need advanced privileges to run the `network interface service-policy create` command.

### About this task

Built-in services and service policies are available for managing data and management traffic on both data and system SVMs. Most use cases are satisfied using a built-in service policy rather than creating a custom service policy.

You can modify these built-in service policies, if required.

### Steps

1. View the services that are available in the cluster:

```
network interface service show
```

Services represent the applications accessed by a LIF as well as the applications served by the cluster. Each service includes zero or more TCP and UDP ports on which the application is listening.

The following additional data and management services are available:

```
cluster1::> network interface service show

Service                Protocol:Ports
-----                -
cluster-core           -
data-cifs              -
data-core              -
data-flexcache         -
data-iscsi             -
data-nfs               -
intercluster-core      tcp:11104-11105
management-autosupport -
management-bgp         tcp:179
management-core        -
management-https       tcp:443
management-ssh         tcp:22
12 entries were displayed.
```

2. View the service policies that exist in the cluster:

```
cluster1::> network interface service-policy show
```

Vserver	Policy	Service: Allowed Addresses
-----		
-----		
cluster1		
	default-intercluster	intercluster-core: 0.0.0.0/0 management-https: 0.0.0.0/0
	default-management	management-core: 0.0.0.0/0 management-autosupport: 0.0.0.0/0 management-ssh: 0.0.0.0/0 management-https: 0.0.0.0/0
	default-route-announce	management-bgp: 0.0.0.0/0
Cluster		
	default-cluster	cluster-core: 0.0.0.0/0
vs0		
	default-data-blocks	data-core: 0.0.0.0/0 data-iscsi: 0.0.0.0/0
	default-data-files	data-core: 0.0.0.0/0 data-nfs: 0.0.0.0/0 data-cifs: 0.0.0.0/0 data-flexcache: 0.0.0.0/0
	default-management	data-core: 0.0.0.0/0 management-ssh: 0.0.0.0/0 management-https: 0.0.0.0/0

```
7 entries were displayed.
```

### 3. Create a service policy:

```
cluster1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them  
only when directed to do so by technical support.
```

```
Do you wish to continue? (y or n): y
```

```
cluster1::> network interface service-policy create -vserver <svm_name>  
-policy <service_policy_name> -services <service_name> -allowed  
-addresses <IP_address/mask,...>
```

- "service\_name" specifies a list of services that should be included in the policy.
- "IP\_address/mask" specifies the list of subnet masks for addresses that are allowed to access the services in the service policy. By default, all specified services are added with a default allowed address list of 0.0.0.0/0, which allows traffic from all subnets. When a non-default allowed address list is provided, LIFs using the policy are configured to block all requests with a source address that does not match any of the specified masks.

The following example shows how to create a data service policy, *svm1\_data\_policy*, for an SVM that includes *NFS* and *SMB* services:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver svm1
-policy svm1_data_policy -services data-nfs,data-cifs,data-core
```

The following example shows how to create an intercluster service policy:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver cluster1
-policy intercluster1 -services intercluster-core
```

#### 4. Verify that the service policy is created.

```
cluster1::> network interface service-policy show
```

The following output shows the service policies that are available:

```
cluster1::> network interface service-policy show
```

Vserver	Policy	Service: Allowed Addresses
-----		
-----		
cluster1		
	default-intercluster	intercluster-core: 0.0.0.0/0 management-https: 0.0.0.0/0
	intercluster1	intercluster-core: 0.0.0.0/0
	default-management	management-core: 0.0.0.0/0 management-autosupport: 0.0.0.0/0 management-ssh: 0.0.0.0/0 management-https: 0.0.0.0/0
	default-route-announce	management-bgp: 0.0.0.0/0
Cluster		
	default-cluster	cluster-core: 0.0.0.0/0
vs0		
	default-data-blocks	data-core: 0.0.0.0/0 data-iscsi: 0.0.0.0/0
	default-data-files	data-core: 0.0.0.0/0 data-nfs: 0.0.0.0/0 data-cifs: 0.0.0.0/0 data-flexcache: 0.0.0.0/0
	default-management	data-core: 0.0.0.0/0 management-ssh: 0.0.0.0/0 management-https: 0.0.0.0/0
	svm1_data_policy	data-core: 0.0.0.0/0 data-nfs: 0.0.0.0/0 data-cifs: 0.0.0.0/0

```
9 entries were displayed.
```

### After you finish

Assign the service policy to a LIF either at the time of creation or by modifying an existing LIF.



## Assign a service policy to a LIF

You can assign a service policy to a LIF either at the time of creating the LIF or by modifying the LIF. A service policy defines the list of services that can be used with the LIF.

### About this task

You can assign service policies for LIFs in the admin and data SVMs.

### Step

Depending on when you want to assign the service policy to a LIF, perform one of the following actions:

If you are...	Assign the service policy...
Creating a LIF	<code>network interface create -vserver svm_name -lif &lt;lif_name&gt; -home-node &lt;node_name&gt; -home-port &lt;port_name&gt; {(-address &lt;IP_address&gt; -netmask &lt;IP_address&gt;) -subnet-name &lt;subnet_name&gt;} -service-policy &lt;service_policy_name&gt;</code>
Modifying a LIF	<code>network interface modify -vserver &lt;svm_name&gt; -lif &lt;lif_name&gt; -service-policy &lt;service_policy_name&gt;</code>

When you specify a service policy for a LIF, you need not specify the data protocol and role for the LIF. Creating LIFs by specifying the role and data protocols is also supported.



A service policy can only be used by LIFs in the same SVM that you specified when creating the service policy.

### Examples

The following example shows how to modify the service policy of a LIF to use the default- management service policy:

```
cluster1::> network interface modify -vserver cluster1 -lif lif1 -service
-policy default-management
```

### Commands for managing LIF service policies

Use the `network interface service-policy` commands to manage LIF service policies.

If you want to...	Use this command...
Create a service policy (advanced privileges required)	<code>network interface service-policy create</code>
Add an additional service entry to an existing service policy (advanced privileges required)	<code>network interface service-policy add-service</code>
Clone an existing service policy (advanced privileges required)	<code>network interface service-policy clone</code>

Modify a service entry in an existing service policy (advanced privileges required)	<code>network interface service-policy modify-service</code>
Remove a service entry from an existing service policy (advanced privileges required)	<code>network interface service-policy remove-service</code>
Rename an existing service policy (advanced privileges required)	<code>network interface service-policy rename</code>
Delete an existing service policy (advanced privileges required)	<code>network interface service-policy delete</code>
Restore a built-in service-policy to its original state (advanced privileges required)	<code>network interface service-policy restore-defaults</code>
Display existing service policies	<code>network interface service-policy show</code>

### Create a LIF

A LIF is an IP address associated with a physical or logical port. If there is a component failure, a LIF can fail over to or be migrated to a different physical port, thereby continuing to communicate with the network.

#### Before you begin

- The underlying physical or logical network port must have been configured to the administrative up status.
- If you are planning to use a subnet name to allocate the IP address and network mask value for a LIF, the subnet must already exist.

Subnets contain a pool of IP addresses that belong to the same layer 3 subnet. They are created using System Manager or the `network subnet create` command.

- The mechanism for specifying the type of traffic handled by a LIF has changed. For ONTAP 9.5 and earlier, LIFs used roles to specify the type of traffic it would handle. Beginning with ONTAP 9.6, LIFs use service policies to specify the type of traffic it would handle.

#### About this task

- You cannot assign NAS and SAN protocols to the same LIF.

The supported protocols are SMB, NFS, FlexCache, iSCSI, and FC; iSCSI and FC cannot be combined with other protocols. However, NAS and Ethernet-based SAN protocols can be present on the same physical port.

- You can create both IPv4 and IPv6 LIFs on the same network port.
- All the name mapping and host-name resolution services used by an SVM, such as DNS, NIS, LDAP, and Active Directory, must be reachable from at least one LIF handling data traffic of the SVM.
- A LIF handling intracluster traffic between nodes should not be on the same subnet as a LIF handling management traffic or a LIF handling data traffic.

- Creating a LIF that does not have a valid failover target results in a warning message.
- If you have a large number of LIFs in your cluster, you can verify the LIF capacity supported on the cluster:
  - System Manager: Beginning with ONTAP 9.12.0, view the throughput on the Network Interface grid.
  - CLI: Use the `network interface capacity show` command and the LIF capacity supported on each node by using the `network interface capacity details show` command (at the advanced privilege level).
- Beginning with ONTAP 9.7, if other LIFs already exist for the SVM in the same subnet, you do not need to specify the home port of the LIF. ONTAP automatically chooses a random port on the specified home node in the same broadcast domain as the other LIFs already configured in the same subnet.

Beginning with ONTAP 9.4, FC-NVMe is supported. If you are creating an FC-NVMe LIF you should be aware of the following:

- The NVMe protocol must be supported by the FC adapter on which the LIF is created.
- FC-NVMe can be the only data protocol on data LIFs.
- One LIF handling management traffic must be configured for every storage virtual machine (SVM) supporting SAN.
- NVMe LIFs and namespaces must be hosted on the same node.
- Only one NVMe LIF handling data traffic can be configured per SVM.
- When you create a network interface with a subnet, ONTAP automatically selects an available IP address from the selected subnet and assigns it to the network interface. You can change the subnet if there is more than one subnet, but you cannot change the IP address.
- When you create (add) an SVM, for a network interface, you cannot specify an IP address that is in the range of an existing subnet. You will receive a subnet conflict error. This issue occurs in other workflows for a network interface, such as creating or modifying inter-cluster network interfaces in SVM settings or cluster settings.
- Beginning with ONTAP 9.11.1, the iSCSI LIF failover feature is available on All SAN Array (ASA) platforms.

iSCSI LIF failover is automatically enabled (the failover policy is set to `sfo-partner-only` and the `auto-revert` value is set to `true`) on newly created iSCSI LIFs if no iSCSI LIFs exist in the specified SVM or if all existing iSCSI LIFs in the specified SVM are already enabled with iSCSI LIF failover.

If after you upgrade to ONTAP 9.11.1 or later, you have existing iSCSI LIFs in an SVM that have not been enabled with the iSCSI LIF failover feature and you create new iSCSI LIFs in the same SVM, the new iSCSI LIFs assume the same failover policy (`disabled`) of the existing iSCSI LIFs in the SVM.

### [iSCSI LIF failover for ASA platforms](#)

Beginning with ONTAP 9.12.0, the procedure you follow depends on the interface that you use—System Manager or the CLI:

## System Manager

### Use System Manager to add a network interface

#### Steps

1. Select **Network > Overview > Network Interfaces**.
2. Select **+ Add**.
3. Select one of the following interface roles:
  - a. Data
  - b. Intercluster
  - c. SVM Management
4. Select the protocol:
  - a. SMB/CIFS and NFS
  - b. iSCSI
  - c. FC
  - d. NVMe/FC
  - e. NVMe/TCP
5. Name the LIF or accept the name generated from your previous selections.
6. Accept the home node or use the drop-down to select one.
7. If at least one subnet is configured in the IPspace of the selected SVM, the subnet drop-down is displayed.
  - a. If you select a subnet, choose it from the drop-down.
  - b. If you proceed without a subnet, the broadcast domain drop-down is displayed:
    - i. Specify the IP address. If the IP address is in use, a warning message will display.
    - ii. Specify a subnet mask.
8. Select the home port from the broadcast domain, either automatically (recommended) or by selecting one from the drop-down menu. The Home port control is displayed based on the broadcast domain or subnet selection.
9. Save the network interface.

#### CLI

### Use the CLI to create a LIF

#### Steps

1. Create a LIF:

```
network interface create -vserver vservice_name -lif lif_name
-service-policy service_policy_name -home-node node_name -home-port
port_name {-address IP_address - netmask Netmask_value | -subnet
-name subnet_name} -firewall- policy policy -auto-revert
{true|false}
```

- `-home-node` is the node to which the LIF returns when the `network interface revert` command is run on the LIF.

You can also specify whether the LIF should automatically revert to the home-node and home-port with the `-auto-revert` option.

- `-home-port` is the physical or logical port to which the LIF returns when the `network interface revert` command is run on the LIF.
- You can specify an IP address with the `-address` and `-netmask` options, or you enable allocation from a subnet with the `-subnet_name` option.
- When using a subnet to supply the IP address and network mask, if the subnet was defined with a gateway, a default route to that gateway is added automatically to the SVM when a LIF is created using that subnet.
- If you assign IP addresses manually (without using a subnet), you might need to configure a default route to a gateway if there are clients or domain controllers on a different IP subnet. The `network route create man` page contains information about creating a static route within an SVM.
- `-auto-revert` enables you to specify whether a data LIF is automatically reverted to its home node under circumstances such as startup, changes to the status of the management database, or when the network connection is made. The default setting is `false`, but you can set it to `true` depending on network management policies in your environment.
- `-service-policy` Beginning with ONTAP 9.5, you can assign a service policy for the LIF with the `-service-policy` option.  
When a service policy is specified for a LIF, the policy is used to construct a default role, failover policy, and data protocol list for the LIF. In ONTAP 9.5, service policies are supported only for intercluster and BGP peer services. In ONTAP 9.6, you can create service policies for several data and management services.
- `-data-protocol` enables you to create a LIF that supports the FCP or NVMe/FC protocols. This option is not required when creating an IP LIF.

2. **Optional:** Assign an IPv6 address in the `-address` option:

- Use the `network ndp prefix show` command to view the list of RA prefixes learned on various interfaces.

The `network ndp prefix show` command is available at the advanced privilege level.

- Use the format `prefix::id` to construct the IPv6 address manually.

`prefix` is the prefix learned on various interfaces.

For deriving the `id`, choose a random 64-bit hexadecimal number.

3. Verify that the LIF was created by using the `network interface show` command.

4. Verify that the configured IP address is reachable:

To verify an...	Use...
IPv4 address	<code>network ping</code>
IPv6 address	<code>network ping6</code>

## Examples

The following command creates a LIF and specifies the IP address and network mask values using the `-address` and `-netmask` parameters:

```
network interface create -vserver vs1.example.com -lif datalif1
-service-policy default-data-files -home-node node-4 -home-port e1c
-address 192.0.2.145 -netmask 255.255.255.0 -auto-revert true
```

The following command creates a LIF and assigns IP address and network mask values from the specified subnet (named `client1_sub`):

```
network interface create -vserver vs3.example.com -lif datalif3
-service-policy default-data-files -home-node node-3 -home-port e1c
-subnet-name client1_sub - auto-revert true
```

The following command creates an NVMe/FC LIF and specifies the `nvme-fc` data protocol:

```
network interface create -vserver vs1.example.com -lif datalif1 -data
-protocol nvme-fc -home-node node-4 -home-port 1c -address 192.0.2.145
-netmask 255.255.255.0 -auto-revert true
```

## Modify a LIF

You can modify a LIF by changing the attributes, such as home node or current node, administrative status, IP address, netmask, failover policy, firewall policy, and service policy. You can also change the address family of a LIF from IPv4 to IPv6.

### About this task

- When modifying a LIF's administrative status to down, any outstanding NFSv4 locks are held until the LIF's administrative status is returned to up.

To avoid lock conflicts that can occur when other LIFs attempt to access the locked files, you must move the NFSv4 clients to a different LIF before setting the administrative status to down.

- You cannot modify the data protocols used by an FC LIF. However, you can modify the services assigned to a service policy or change the service policy assigned to an IP LIF.

To modify the data protocols used by a FC LIF, you must delete and re-create the LIF. To make service policy changes to an IP LIF, there is a brief outage while the updates occur.

- You cannot modify either the home node or the current node of a node-scoped management LIF.
- When using a subnet to change the IP address and network mask value for a LIF, an IP address is allocated from the specified subnet; if the LIF's previous IP address is from a different subnet, the IP address is returned to that subnet.
- To modify the address family of a LIF from IPv4 to IPv6, you must use the colon notation for the IPv6

address and add a new value for the `-netmask-length` parameter.

- You cannot modify the auto-configured link-local IPv6 addresses.
- Modification of a LIF that results in the LIF having no valid failover target results in a warning message.

If a LIF that does not have a valid failover target attempts to fail over, an outage might occur.

- Beginning with ONTAP 9.5, you can modify the service policy associated with a LIF.

In ONTAP 9.5, service policies are supported only for intercluster and BGP peer services. In ONTAP 9.6, you can create service policies for several data and management services.

- Beginning with ONTAP 9.11.1, the iSCSI LIF failover feature is available on All SAN Array (ASA) platforms.

For pre-existing iSCSI LIFs, meaning LIFs created prior to upgrading to 9.11.1 or later, you can modify the failover policy to enable the iSCSI LIF failover feature.

### [iSCSI LIF failover for ASA platforms](#)

The procedure you follow depends on the interface that you use—System Manager or the CLI:

## System Manager

Beginning with ONTAP 9.12.0, you can use System Manager to edit a network interface

### Steps

1. Select **Network > Overview > Network Interfaces**.
2. Select **⋮ > Edit** beside the network interface you want to change.
3. Change one or more of the network interface settings. For details, see [Create a LIF](#).
4. Save your changes.

## CLI

### Use the CLI to modify a LIF

#### Steps

1. Modify a LIF's attributes by using the `network interface modify` command.

The following example shows how to modify the IP address and network mask of LIF `datalif2` using an IP address and the network mask value from subnet `client1_sub`:

```
network interface modify -vserver vs1 -lif datalif2 -subnet-name
client1_sub
```

The following example shows how to modify the service policy of a LIF.

```
network interface modify -vserver siteA -lif node1_inter1 -service
-policy example
```

2. Verify that the IP addresses are reachable.

If you are using...	Then use...
IPv4 addresses	<code>network ping</code>
IPv6 addresses	<code>network ping6</code>

## Migrate a LIF

You might have to migrate a LIF to a different port on the same node or a different node within the cluster, if the port is either faulty or requires maintenance. Migrating a LIF is similar to LIF failover, but LIF migration is a manual operation, while LIF failover is the automatic migration of a LIF in response to a link failure on the LIF's current network port.

### Before you begin

- A failover group must have been configured for the LIFs.



- The destination node and ports must be operational and must be able to access the same network as the source port.

### About this task

- BGP LIFs reside on the home-port and cannot be migrated to any other node or port.
- You must migrate LIFs hosted on the ports belonging to a NIC to other ports in the cluster, before removing the NIC from the node.
- You must execute the command for migrating a cluster LIF from the node where the cluster LIF is hosted.
- A node-scoped LIF, such as a node-scoped management LIF, cluster LIF, intercluster LIF, cannot be migrated to a remote node.
- When an NFSv4 LIF is migrated between nodes, a delay of up to 45 seconds results before the LIF is available on a new port.

To work around this problem, use NFSv4.1 where no delay is encountered.

- You can migrate iSCSI LIFs on All SAN Array (ASA) platforms running ONTAP 9.11.1 or later.

Migrating iSCSI LIFs is limited to ports on the home-node or the HA partner.

You can also use System Manager to migrate iSCSI LIFs.

[iSCSI LIF failover for ASA platforms](#)

- If your platform is not an All SAN Array (ASA) platform running ONTAP version 9.11.1 or later, you cannot migrate iSCSI LIFs from one node to another node.

To work around this restriction, you must create an iSCSI LIF on the destination node. For information about guidelines for creating an iSCSI LIF, see [SAN administration](#).

- VMware VAAI copy offload operations fail when you migrate the source or the destination LIF. For more information about VMware VAAI, see [NFS reference](#) or [SAN administration](#).

The procedure you follow depends on the interface that you use—System Manager or the CLI:

## System Manager

### Use System Manager to migrate a network interface

#### Steps

1. Select **Network > Overview > Network Interfaces**.
2. Select **⋮ > Migrate** beside the network interface you want to change.
3. Save your changes.

#### CLI

### Use the CLI to migrate a LIF

#### Step

Depending on whether you want to migrate a specific LIF or all the LIFs, perform the appropriate action:

If you want to migrate...	Enter the following command...
A specific LIF	<code>network interface migrate</code>
All the data and cluster-management LIFs on a node	<code>network interface migrate-all</code>
All of the LIFs off of a port	<code>network interface migrate-all -node &lt;node&gt; -port &lt;port&gt;</code>

The following example shows how to migrate a LIF named `datlif1` on the SVM `vs0` to the port `e0d` on `node0b`:

```
network interface migrate -vserver vs0 -lif datlif1 -dest-node node0b
-dest-port e0d
```

The following example shows how to migrate all the data and cluster-management LIFs from the current (local) node:

```
network interface migrate-all -node local
```

## Revert a LIF to its home port

You can revert a LIF to its home port after it fails over or is migrated to a different port either manually or automatically. If the home port of a particular LIF is unavailable, the LIF remains at its current port and is not reverted.

#### About this task

- If you administratively bring the home port of a LIF to the up state before setting the automatic revert option, the LIF is not returned to the home port.

- The LIF does not automatically revert unless the value of the "auto-revert" option is set to true.
- You must ensure that the "auto-revert" option is enabled for the LIFs to revert to their home ports.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

### System Manager

#### Use System Manager to revert a network interface to its home port

##### Steps

1. Select **Network > Overview > Network Interfaces**.
2. Select **> Revert** beside the network interface you want to change.
3. Save your changes.

### CLI

#### Use the CLI to revert a LIF to its home port

##### Step

Revert a LIF to its home port manually or automatically:

If you want to revert a LIF to its home port...	Then enter the following command...
Manually	<code>network interface revert -vserver vservice_name -lif lif_name</code>
Automatically	<code>network interface modify -vserver vservice_name -lif lif_name -auto-revert true</code>

### ONTAP 9.8 and later: Recover from an incorrectly configured cluster LIF

A cluster cannot be created when the cluster network is cabled to a switch but not all of the ports configured in the Cluster IPspace can reach the other ports configured in the Cluster IPspace.

#### About this task

In a switched cluster, if a cluster network interface (LIF) is configured on the wrong port, or if a cluster port is wired into the wrong network, the `cluster create` command can fail with the following error:

Not all local cluster ports have reachability to one another.  
Use the "network port reachability show -detail" command for more details.

The results of the `network port show` command might show that several ports are added to the Cluster IPspace because they are connected to a port that is configured with a cluster LIF. However, the results of the `network port reachability show -detail` command reveal which ports do not have connectivity to one another.

To recover from a cluster LIF configured on a port that is not reachable to the other ports configured with cluster LIFs, perform the following steps:

## Steps

1. Reset the home port of the cluster LIF to the correct port:

```
network port modify -home-port
```

2. Remove the ports that do not have cluster LIFs configured on them from the cluster broadcast domain:

```
network port broadcast-domain remove-ports
```

3. Create the cluster:

```
cluster create
```

## Result

When you complete the cluster creation, the system detects the correct configuration and places the ports into the correct broadcast domains.

## Delete a LIF

You can delete a network interface (LIF) that is no longer required.

### Before you begin

LIFs to be deleted must not be in use.

## Steps

1. Mark the LIFs you want to delete as administratively down using the following command:

```
network interface modify -vserver vs1 -lif lif_name -status -admin down
```

2. Use the `network interface delete` command to delete one or all LIFs:

If you want to delete...	Enter the command ...
A specific LIF	<pre>network interface delete -vserver vs1 -lif lif_name</pre>
All LIFs	<pre>network interface delete -vserver vs1 -lif *</pre>

The following command deletes the LIF `mgmtlif2`:

```
network interface delete -vserver vs1 -lif mgmtlif2
```

3. Use the `network interface show` command to confirm that the LIF is deleted.

## Configure virtual IP (VIP) LIFs

Some next-generation data centers use Network-Layer-3 mechanisms that require LIFs to be failed over across subnets. Beginning with ONTAP 9.5, VIP data LIFs and the associated routing protocol, border gateway protocol (BGP), are supported, which enable ONTAP to participate in these next-generation networks.

### About this task

A VIP data LIF is a LIF that is not part of any subnet and is reachable from all ports that host a BGP LIF in the same IPspace. A VIP data LIF eliminates the dependency of a host on individual network interfaces. Because multiple physical adapters carry the data traffic, the entire load is not concentrated on a single adapter and the associated subnet. The existence of a VIP data LIF is advertised to peer routers through the routing protocol, Border Gateway Protocol (BGP).

VIP data LIFs provide the following advantages:

- LIF portability beyond a broadcast domain or subnet: VIP data LIFs can fail over to any subnet in the network by announcing the current location of each VIP data LIF to routers through BGP.
- Aggregate throughput: VIP data LIFs can support aggregate throughput that exceeds the bandwidth of any individual port because the VIP LIFs can send or receive data from multiple subnets or ports simultaneously.

### Set up border gateway protocol (BGP)

Before creating VIP LIFs, you must set up BGP, which is the routing protocol used for announcing the existence of a VIP LIF to peer routers.

Beginning with ONTAP 9.9.1, VIP BGP provides default route automation using BGP peer grouping to simplify configuration.

ONTAP has a simple way to learn default routes using the BGP peers as next-hop routers when the BGP peer is on the same subnet. To use the feature, set the `-use-peer-as-next-hop` attribute to `true`. By default, this attribute is `false`.

If you have static routes configured, those are still preferred over these automated default routes.

### Before you begin

The peer router must be configured to accept a BGP connection from the BGP LIF for the configured autonomous system number (ASN).



ONTAP does not process any incoming route announcements from the router; therefore, you should configure the peer router to not send any route updates to the cluster.

### About this task

Setting up BGP involves optionally creating a BGP configuration, creating a BGP LIF, and creating a BGP peer group. ONTAP automatically creates a default BGP configuration with default values when the first BGP peer group is created on a given node. A BGP LIF is used to establish BGP TCP sessions with peer routers. For a peer router, a BGP LIF is the next hop to reach a VIP LIF. Failover is disabled for the BGP LIF. A BGP peer group advertises the VIP routes for all the SVMs in the peer group's IPspace.

Beginning with ONTAP 9.8, these fields have been added to the `network bgp peer-group` command:

- `-asn-prepend-type`
- `-asn-prepend-count`
- `-community`

These BGP attributes allows you to configure the AS Path and community attributes for the BGP peer group.

Beginning with ONTAP 9.9.1, these fields have been added:

- `-asn` or `-peer-asn` (4-byte value)  
The attribute itself is not new, but it now uses a 4-byte integer.
- `-med`
- `-use-peer-as-next-hop`

You can make advanced route selections with Multi-Exit Discriminator (MED) support for path prioritization. MED is an optional attribute in the BGP update message that tells routers to select the best route for the traffic. The MED is an unsigned 32-bit integer (0 - 4294967295); lower values are preferred.



While ONTAP supports the above BGP attributes, routers need not honor them. NetApp highly recommends you confirm which attributes are supported by your router and configure BGP peer-groups accordingly. For details, refer to the BGP documentation provided by your router.

## Steps

1. Log in to the advanced privilege level:

```
set -privilege advanced
```

2. Optional: Create a BGP configuration or modify the default BGP configuration of the cluster by performing one of the following actions:

- a. Create a BGP configuration:

```
network bgp config create -node {node_name | local} -asn asn_integer  
-holdtime  
hold_time -routerid local_router_IP_address
```

Sample with a 2-byte ASN:

```
network bgp config create -node node1 -asn 65502 -holdtime 180  
-routerid 1.1.1.1
```

Sample with a 4-byte ASN:

```
network bgp config create -node node1 -asn 85502 -holdtime 180  
-routerid 1.1.1.1
```

b. Modify the default BGP configuration:

```
network bgp defaults modify -asn asn_integer -holdtime hold_time
network bgp defaults modify -asn 65502
```

- `asn_integer` specifies the ASN. Beginning with ONTAP 9.8, ASN for BGP supports a 2-byte non-negative integer. This is a 16-bit number (1 - 65534 available values). Beginning with ONTAP 9.9.1, ASN for BGP supports a 4-byte non-negative integer (1 - 4294967295). The default ASN is 65501. ASN 23456 is reserved for ONTAP session establishment with peers that do not announce 4-byte ASN capability.
- `hold_time` specifies the hold time in seconds. The default value is 180s.

3. Create a BGP LIF for the system SVM:

```
network interface create -vserver system_svm -lif lif_name -service
-policy default-route-announce -home-node home_node -home-port home_port
-address ip_address -netmask netmask
```

You can use the `default-route-announce` service policy for the BGP LIF or any custom service policy which contains the "management-bgp" service.

```
network interface create -vserver cluster1 -lif bgp1 -service-policy
default-route-announce -home-node cluster1-01 -home-port e0c -address
10.10.10.100 -netmask 255.255.255.0
```

4. Create a BGP peer group that is used to establish BGP sessions with the remote peer routers and configure the VIP route information that is advertised to the peer routers:

Sample 1: Create a peer group without an auto default route

In this case, the admin has to create a static route to the BGP peer.

```
network bgp peer-group create -peer-group group_name -ip-space
ip-space_name -bgp-lif bgp_lif -peer-address peer-router_ip_address -peer
-asn 65502 -route-preference integer
-asn-prepend-type <ASN_prepend_type> -asn-prepend-count integer -med
integer -community BGP community list <0-65535>:<0-65535>
```

```
network bgp peer-group create -peer-group group1 -ip-space Default -bgp
-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65502 -route-preference 100
-asn-prepend-type local-asn -asn-prepend-count 2 -med 100 -community
9000:900,8000:800
```

## Sample 2: Create a peer group with an auto default route

```
network bgp peer-group create -peer-group group_name -ipSPACE
ipSPACE_name -bgp-lif bgp_lif -peer-address peer-router_ip_address -peer
-asn 65502 -use-peer-as-next-hop true -route-preference integer -asn
-prepend-type <ASN_prepend_type> -asn-prepend-count integer -med integer
-community BGP community list <0-65535>:<0-65535>
```

```
network bgp peer-group create -peer-group group1 -ipSPACE Default -bgp
-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65502 -use-peer-as-next-hop
true -route-preference 100 -asn-prepend-type local-asn -asn-prepend
-count 2 -med 100 -community 9000:900,8000:800
```

### Create a virtual IP (VIP) data LIF

The existence of a VIP data LIF is advertised to peer routers through the routing protocol, Border Gateway Protocol (BGP).

#### Before you begin

- The BGP peer group must be set up and the BGP session for the SVM on which the LIF is to be created must be active.
- A static route to the BGP router or any other router in the BGP LIF's subnet must be created for any outgoing VIP traffic for the SVM.
- You should turn on multipath routing so that the outgoing VIP traffic can utilize all the available routes.

If multipath routing is not enabled, all the outgoing VIP traffic goes from a single interface.

#### Steps

1. Create a VIP data LIF:

```
network interface create -vserver svm_name -lif lif_name -role data
-data-protocol
{nfs|cifs|iscsi|fcache|none|fc-nvme} -home-node home_node -address
ip_address -is-vip true
```

A VIP port is automatically selected if you do not specify the home port with the `network interface create` command.

By default, the VIP data LIF belongs to the system-created broadcast domain named 'Vip', for each IPspace. You cannot modify the VIP broadcast domain.

A VIP data LIF is reachable simultaneously on all ports hosting a BGP LIF of an IPspace. If there is no active BGP session for the VIP's SVM on the local node, the VIP data LIF fails over to the next VIP port on the node that has a BGP session established for that SVM.



2. Verify that the BGP session is in the up status for the SVM of the VIP data LIF:

```
network bgp vserver-status show

Node          Vserver  bgp status
-----
node1         vs1      up
```

If the BGP status is `down` for the SVM on a node, the VIP data LIF fails over to a different node where the BGP status is `up` for the SVM. If BGP status is `down` on all the nodes, the VIP data LIF cannot be hosted anywhere, and has LIF status as `down`.

### Commands for managing the BGP

Beginning with ONTAP 9.5, you use the `network bgp` commands to manage the BGP sessions in ONTAP.

### Manage BGP configuration

If you want to...	Use this command...
Create a BGP configuration	<code>network bgp config create</code>
Modify BGP configuration	<code>network bgp config modify</code>
Delete BGP configuration	<code>network bgp config delete</code>
Display BGP configuration	<code>network bgp config show</code>
Displays the BGP status for the SVM of the VIP LIF	<code>network bgp vserver-status show</code>

### Manage BGP default values

If you want to...	Use this command...
Modify BGP default values	<code>network bgp defaults modify</code>
Display BGP default values	<code>network bgp defaults show</code>

### Manage BGP peer groups

If you want to...	Use this command...
Create a BGP peer group	<code>network bgp peer-group create</code>
Modify a BGP peer group	<code>network bgp peer-group modify</code>
Delete a BGP peer group	<code>network bgp peer-group delete</code>
Display BGP peer groups information	<code>network bgp peer-group show</code>
Rename a BGP peer group	<code>network bgp peer-group rename</code>

### Related information

[ONTAP 9 commands](#)

## Configure host-name resolution

### Overview

ONTAP must be able to translate host names to numerical IP addresses in order to provide access to clients and to access services. You must configure storage virtual machines (SVMs) to use local or external name services to resolve host information. ONTAP supports configuring an external DNS server or configuring the local hosts file for host name resolution.

When using an external DNS server, you can configure Dynamic DNS (DDNS), which automatically sends new or changed DNS information from your storage system to the DNS server. Without dynamic DNS updates, you must manually add DNS information (DNS name and IP address) to the identified DNS servers when a new system is brought online or when existing DNS information changes. This process is slow and error-prone. During disaster recovery, manual configuration can result in a long downtime.

### Configure DNS for host-name resolution

You use DNS to access either local or remote sources for host information. You must configure DNS to access one or both of these sources.

ONTAP must be able to look up host information to provide proper access to clients. You must configure name services to enable ONTAP to access local or external DNS services to obtain the host information.

ONTAP stores name service configuration information in a table that is the equivalent of the `/etc/nsswitch.conf` file on UNIX systems.

### Configure an SVM and data LIFs for host-name resolution using an external DNS server

You can use the `vserver services name-service dns` command to enable DNS on an SVM, and configure it to use DNS for host-name resolution. Host names are resolved using external DNS servers.

### Before you begin

A site-wide DNS server must be available for host name lookups.

You should configure more than one DNS server to avoid a single-point-of-failure. The `vserver services name-service dns create` command issues a warning if you enter only one DNS server name.

### About this task

See [Configure dynamic DNS services](#) for more information about configuring dynamic DNS on the SVM.

### Steps

1. Enable DNS on the SVM:

```
vserver services name-service dns create -vserver vserver_name -domains domain_name - name-servers ip_addresses -state enabled
```

The following command enables external DNS server servers on the SVM vs1:

```
vserver services name-service dns create -vserver <vs1.example.com>
-domains <example.com> -name-servers <192.0.2.201,192.0.2.202> -state
<enabled>
```



The `vserver services name-service dns create` command performs an automatic configuration validation and reports an error message if ONTAP cannot contact the name server.

## 2. Enable DNS on LIFs owned by the SVM:

If you are	Use this command:
Modifying an existing LIF zone-name	<code>network interface modify -lif lifname -dns-zone</code>
Creating a new LIF zone-name	<code>network interface create -lif lifname -dns-zone</code>

```
vserver services name-service dns create -vserver <vs1> -domains
<example.com> -name-servers <192.0.2.201, 192.0.2.202> -state <enabled>
network interface modify -lif <datalif1> -dns-zone
<zonename.whatever.com>
```

## 3. Validate the status of the name servers by using the `vserver services name-service dns check` command.

```
vserver services name-service dns check -vserver vs1.example.com
VserverName      Server      Status      Status Details
-----
vs1.example.com  10.0.0.50  up          Response time (msec): 2
vs1.example.com  10.0.0.51  up          Response time (msec): 2
```

### Configure the Name Service Switch Table for Host-Name Resolution

You must configure the name service switch table correctly to enable ONTAP to consult local or external name service to retrieve host information.

#### Before you begin

You must have decided which name service to use for host mapping in your environment.

#### Steps

1. Add the necessary entries to the name service switch table:

```
vserver services name-service <ns-switch> create -vserver <vserver_name>
-database <database_name> -source <source_names>
```

2. Verify that the name service switch table contains the expected entries in the desired order:

```
vserver services name-service <ns-switch> show -vserver <vserver_name>
```

### Example

The following example creates an entry in the name service switch table for SVM vs1 to first use the local hosts file and then an external DNS server to resolve host names:

```
vserver services name-service ns-switch create -vserver vs1 -database
hosts -sources files dns
```

### Manage the hosts table (cluster administrators only)

A cluster administrator can add, modify, delete, and view the host name entries in the hosts table of the admin storage virtual machine (SVM). An SVM administrator can configure the host name entries only for the assigned SVM.

#### Commands for managing local host-name entries

You can use the `vserver services name-service dns hosts` command to create, modify, or delete DNS host table entries.

When you are creating or modifying the DNS host-name entries, you can specify multiple alias addresses separated by commas.

If you want to...	Use this command...
Create a DNS host-name entry	<code>vserver services name-service dns hosts create</code>
Modify a DNS host-name entry	<code>vserver services name-service dns hosts modify</code>
Delete a DNS host-name entry	<code>vserver services name-service dns hosts delete</code>

For more information, see the [ONTAP 9 commands](#) for the `vserver services name-service dns hosts` commands.

### Balance network loads to optimize user traffic (cluster administrators only)

#### Overview

You can configure your cluster to serve client requests from appropriately loaded LIFs.

This results in a more balanced utilization of LIFs and ports, which in turn allows for better performance of the cluster.

DNS load balancing helps in selecting an appropriately loaded data LIF and balancing user network traffic across all available ports (physical, interface groups, and VLANs).

With DNS load balancing, LIFs are associated with the load balancing zone of an SVM. A site-wide DNS server is configured to forward all DNS requests and return the least-loaded LIF based on the network traffic and the availability of the port resources (CPU usage, throughput, open connections, and so on). DNS load balancing provides the following benefits:

- New client connections balanced across available resources.
- No manual intervention required for deciding which LIFs to use when mounting a particular SVM.
- DNS load balancing supports NFSv3, NFSv4, NFSv4.1, SMB 2.0, SMB 2.1, and SMB 3.0.

### **How DNS load balancing works**

Clients mount an SVM by specifying an IP address (associated with a LIF) or a host name (associated with multiple IP addresses). By default, LIFs are selected by the site-wide DNS server in a round-robin manner, which balances the workload across all LIFs.

Round-robin load balancing can result in overloading some LIFs, so you have the option of using a DNS load balancing zone that handles the host-name resolution in an SVM. Using a DNS load balancing zone, ensures better balance of the new client connections across available resources, leading to improved performance of the cluster.

A DNS load balancing zone is a DNS server inside the cluster that dynamically evaluates the load on all LIFs and returns an appropriately loaded LIF. In a load balancing zone, DNS assigns a weight (metric), based on the load, to each LIF.

Every LIF is assigned a weight based on its port load and CPU utilization of its home node. LIFs that are on less-loaded ports have a higher probability of being returned in a DNS query. Weights can also be manually assigned.

### **Create a DNS load balancing zone**

You can create a DNS load balancing zone to facilitate the dynamic selection of a LIF based on the load, that is, the number of clients mounted on a LIF. You can create a load balancing zone while creating a data LIF.

#### **Before you begin**

The DNS forwarder on the site-wide DNS server must be configured to forward all requests for the load balancing zone to the configured LIFs.

The Knowledgebase article [How to set up DNS load balancing in Cluster-Mode](#) on the NetApp Support Site contains more information about configuring DNS load balancing using conditional forwarding.

#### **About this task**

- Any data LIF can respond to DNS queries for a DNS load balancing zone name.
- A DNS load balancing zone must have a unique name in the cluster, and the zone name must meet the following requirements:

- It should not exceed 256 characters.
- It should include at least one period.
- The first and the last character should not be a period or any other special character.
- It cannot include any spaces between characters.
- Each label in the DNS name should not exceed 63 characters.

A label is the text appearing before or after the period. For example, the DNS zone named `storage.company.com` has three labels.

### Step

Use the `network interface create` command with the `dns-zone` option to create a DNS load balancing zone.

If the load balancing zone already exists, the LIF is added to it. For more information about the command, see [ONTAP 9 commands](#).

The following example demonstrates how to create a DNS load balancing zone named `storage.company.com` while creating the LIF `lif1`:

```
network interface create -vserver vs0 -lif lif1 -home-node node1
-home-port e0c -address 192.0.2.129 -netmask 255.255.255.128 -dns-zone
```

### Add or remove a LIF from a load balancing zone

You can add or remove a LIF from the DNS load balancing zone of a virtual machine (SVM). You can also remove all the LIFs simultaneously from a load balancing zone.

#### Before you begin

- All the LIFs in a load balancing zone should belong to the same SVM.
- A LIF can be a part of only one DNS load balancing zone.
- Failover groups for each subnet must have been set up, if the LIFs belong to different subnets.

#### About this task

A LIF that is in the administrative down status is temporarily removed from the DNS load balancing zone. When the LIF returns to the administrative up status, the LIF is automatically added to the DNS load balancing zone.

### Step

Add a LIF to or remove a LIF from a load balancing zone:

If you want to...	Enter...
Add a LIF	<pre>network interface modify -vserver vs1 -lif lif1 -dns-zone zone_name</pre> <p>Example:</p> <pre>network interface modify -vserver vs1 -lif data1 -dns-zone cifs.company.com</pre>

Remove a single LIF	<pre>network interface modify -vserver vserver_name -lif lif_name -dns-zone none</pre> <p>Example:</p> <pre>network interface modify -vserver vs1 -lif data1 -dns -zone none</pre>
Remove all LIFs	<pre>network interface modify -vserver vserver_name -lif * -dns-zone none</pre> <p>Example:</p> <pre>network interface modify -vserver vs0 -lif * -dns-zone none</pre> <p>You can remove an SVM from a load balancing zone by removing all the LIFs in the SVM from that zone.</p>

## Secure your network

### Configure network security using federal information processing standards (FIPS)

ONTAP is compliant in the Federal Information Processing Standards (FIPS) 140-2 for all SSL connections. You can turn on and off SSL FIPS mode, set SSL protocols globally, and turn off any weak ciphers such as RC4 within ONTAP.

By default, SSL on ONTAP is set with FIPS compliance disabled and SSL protocol enabled with the following:

- TLSv1.3 (beginning in ONTAP 9.11.1)
- TLSv1.2
- TLSv1.1
- TLSv1

When SSL FIPS mode is enabled, SSL communication from ONTAP to external client or server components outside of ONTAP will use FIPS compliant crypto for SSL.

If you want administrator accounts to access SVMs with an SSH public key, you must ensure that the host key algorithm is supported before enabling SSL FIPS mode.

**Note:** Host key algorithm support has changed in ONTAP 9.11.1 and later releases.

ONTAP release	Supported key types	Unsupported key types
9.11.1 and later	ecdsa-sha2-nistp256	rsa-sha2-512 rsa-sha2-256 ssh-ed25519 ssh-dss ssh-rsa
9.10.1 and earlier	ecdsa-sha2-nistp256 ssh-ed25519	ssh-dss ssh-rsa

Existing SSH public key accounts without the supported key algorithms must be reconfigured with a supported

key type before enabling FIPS, or the administrator authentication will fail.

For more information, see [Enable SSH public key accounts](#).

For more information about SSL FIPS mode configuration, see the `security config modify man` page.

### Enable FIPS

It is recommended that all secure users adjust their security configuration immediately after system installation or upgrade. When SSL FIPS mode is enabled, SSL communication from ONTAP to external client or server components outside of ONTAP will use FIPS compliant crypto for SSL.



When FIPS is enabled, you cannot install or create a certificate with an RSA key length of 4096.

### Steps

1. Change to advanced privilege level:

```
set -privilege advanced
```

2. Enable FIPS:

```
security config modify -interface SSL -is-fips-enabled true
```

3. When prompted to continue, enter `y`

4. If you are running ONTAP 9.8 or earlier manually reboot each node in the cluster one by one. Beginning in ONTAP 9.9.1, rebooting is not required.

### Example

If you are running ONTAP 9.9.1 or later, you will not see the warning message.

```
security config modify -interface SSL -is-fips-enabled true
```

```
Warning: This command will enable FIPS compliance and can potentially  
cause some non-compliant components to fail. MetroCluster and Vserver DR  
require FIPS to be enabled on both sites in order to be compatible.
```

```
Do you want to continue? {y|n}: y
```

```
Warning: When this command completes, reboot all nodes in the cluster.  
This is necessary to prevent components from failing due to an  
inconsistent security configuration state in the cluster. To avoid a  
service outage, reboot one node at a time and wait for it to completely  
initialize before rebooting the next node. Run "security config status  
show" command to monitor the reboot status.
```

```
Do you want to continue? {y|n}: y
```

### Disable FIPS

If you are still running an older system configuration and want to configure ONTAP with backward compatibility, you can turn on SSLv3 only when FIPS is disabled.



## Steps

1. Change to advanced privilege level:

```
set -privilege advanced
```

2. Disable FIPS by typing:

```
security config modify -interface SSL -is-fips-enabled false
```

3. When prompted to continue, enter *y*.

4. If you are running ONTAP 9.8 or earlier, manually reboot each node in the cluster. Beginning in ONTAP 9.9.1, rebooting is not required.

## Example

If you are running ONTAP 9.9.1 or later, you will not see the warning message.

```
security config modify -interface SSL -supported-protocols SSLv3
```

```
Warning: Enabling the SSLv3 protocol may reduce the security of the  
interface, and is not recommended.
```

```
Do you want to continue? {y|n}: y
```

```
Warning: When this command completes, reboot all nodes in the cluster.  
This is necessary to prevent components from failing due to an  
inconsistent security configuration state in the cluster. To avoid a  
service outage, reboot one node at a time and wait for it to completely  
initialize before rebooting the next node. Run "security config status  
show" command to monitor the reboot status.
```

```
Do you want to continue? {y|n}: y
```

## View FIPS compliance status

You can see whether the entire cluster is running the current security configuration settings.

## Steps

1. One by one, reboot each node in the cluster.

Do not reboot all cluster nodes simultaneously. A reboot is required to make sure that all applications in the cluster are running the new security configuration, and for all changes to FIPS on/off mode, protocols, and ciphers.

2. View the current compliance status:

```
security config show
```

## Example

```
security config show

                Cluster                               Cluster
Security
Interface FIPS Mode  Supported Protocols      Supported Ciphers Config
Ready
-----
-----
SSL          false    TLSv1_2, TLSv1_1, TLSv1  ALL:!LOW:!aNULL:  yes
                                   !EXP:!eNULL
```

## Configure IP security (IPsec) over wire encryption

Beginning with ONTAP 9.8, ONTAP uses the IPsec protocol in transport mode to ensure data is continuously secure and encrypted, even while in transit. IPsec offers data encryption for all IP traffic including the NFS, iSCSI, and SMB protocols. IPsec provides the only encryption in flight option for iSCSI traffic.

Beginning with ONTAP 9.9.1, the encryption algorithms used by IPsec are FIPS 140-2 validated. The algorithms are generated by the NetApp Cryptographic Module in ONTAP which carries the FIPS 140-2 validation.

Beginning with ONTAP 9.10.1, you can use either pre-shared keys (PSKs) or certificates for authentication with IPsec. Previously, only PSKs were supported with IPsec.

After IPsec is configured, network traffic between the client and ONTAP is protected with preventive measures to combat replay and man-in-the-middle (MITM) attacks.

For NetApp SnapMirror and cluster peering traffic encryption, cluster peering encryption (CPE), transport layer security (TLS) is still recommended over IPsec for secure in-transit over the wire. This is because TLS has better performance than IPsec.

While IPsec capability is enabled on the cluster, the network requires a Security Policy Database (SPD) entry to match the to-be-protected traffic and to specify protection details (such as cipher suite and authentication method) before traffic can flow. A corresponding SPD entry is also needed on each client. The SPD requirement is needed for both PSK and certification authentication methods.

### Enable IPsec on the cluster

You can enable IPsec on the cluster to ensure data is continuously secure and encrypted, even while in transit.

### Steps

1. Discover if IPsec is enabled already:

```
security ipsec config show
```

If the result includes `IPsec Enabled: false`, proceed to the next step.

2. Enable IPsec:

```
security ipsec config modify -is-enabled true
```

3. Run the discovery command again:

```
security ipsec config show
```

The result now includes `IPsec Enabled: true`.

### Preparing for IPsec policy creation with certificate authentication

You can skip this step if you are only using pre-shared keys PSKs for authentication and will not use certificate authentication.

Before creating an IPsec policy that uses certificates for authentication you must ensure that the following prerequisites are met:

- Both ONTAP and the client must have the other party's CA certificate installed so that the end entity (either ONTAP or the client) certificates are verifiable by both sides
- A certificate is installed for the ONTAP LIF that participates in the policy



ONTAP LIFs can share certificates. A one-to-one mapping between certificates and LIFs is not required.

### Steps

1. You must install all CA certificates used during the mutual authentication, including both ONTAP-side and client-side CAs, to ONTAP certificate management unless it is already installed (as is the case of an ONTAP self-signed root-CA).

#### Sample command

```
cluster::> security certificate install -vserver svm_name -type server-ca  
-cert-name my_ca_cert
```

2. To ensure that the CA installed is within the IPsec CA searching path during authentication, add the ONTAP certificate management CAs to the IPsec module using the “security ipsec ca-certificate add” command.

#### Sample command

```
cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs  
my_ca_cert
```

3. Create and install a certificate for use by the ONTAP LIF. The issuer CA of this certificate must already be installed to ONTAP and added to IPsec.

#### Sample command

```
cluster::> security certificate install -vserver svm_name -type server -cert  
-name my_nfs_server_cert
```

For more information about certificates in ONTAP, see the security certificate commands in the ONTAP 9 documentation.

### Define the security policy database (SPD)

IPsec requires an SPD entry before allowing traffic to flow on the network. This is true whether you are using a PSK or a certificate for authentication.

### Step

1. Use the `security ipsec policy create` command to:
  - a. Select the ONTAP IP address or subnet of IP addresses to participate in the IPsec transport.
  - b. Select the client IP addresses that will connect to the ONTAP IP addresses.



The client must support Internet Key Exchange version 2 (IKEv2) with a pre-shared key (PSK).

- c. Optional. Select the upper layer protocols (UDP, TCP, ICMP, etc. ), the local port numbers, and the remote port numbers to protect. The corresponding parameters are `protocols`, `local-ports` and `remote-ports` respectively.

Skip this step to protect all traffic between the ONTAP IP address and client IP address. Protecting all traffic is the default.

- d. Either enter PSK or PKI for the `auth-method` parameter for the desired authentication method.
  - i. If you enter a PSK, after finishing all other optional parameters, hit <enter> for the prompt to enter and verify the pre-shared key.
  - ii. If you enter a PKI, you need to also enter the `cert-name`, `local-identity`, `remote-identity` parameters. If the remote side certificate's identity is unknown or if multiple client identities are expected, enter the special word `ANYTHING`.

#### Sample command for PSK authentications

```
security ipsec policy create -vserver <vs1> -name <test34> -local-ip
-subnets <192.168.134.34/32> -remote-ip-subnets <192.168.134.44/32>
Enter the preshared key for IPsec Policy _test34_ on Vserver _vs1_:
```

#### Sample command for certificate authentications

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32 -local-ports 2049
-protocols tcp -auth-method PKI -cert-name my_nfs_server_cert -local
-identity CN=netapp.ipsec.lif1.vs0 -remote-identity ANYTHING
```

IP traffic cannot flow between the client and server until both ONTAP and the client have setup the matching IPsec policies, and authentication credentials (either PSK or certificate) are in place on both sides. For details, see the client side's IPsec configuration.

#### Use IPsec identities

For the pre-shared key authentication method, identities are optional unless required by an IPsec client (such as Libreswan). For the PKI/certificate authentication method, both local and remote identities are mandatory. The identities specify what identity is certified within each side's certificate and are used in the verification process. If the remote-identity is unknown or if it could be many different identities, use the special identity `ANYTHING`.

#### About this task

Within ONTAP, identities are specified by modifying the SPD entry or during SPD policy creation. The SPD can

be an IP address or string format identity name.

### Step

To modify an existing SPD's identity settings, use the following command:

```
security ipsec policy modify
```

### Sample command

```
security ipsec policy modify -vserver vs1 -name test34 -local-identity  
192.168.134.34 -remote-identity client.fooboo.com
```

### IPsec multiple client configuration

When a small number of clients need to leverage IPsec, using a single SPD entry for each client is sufficient. However, when hundreds or even thousands of clients need to leverage IPsec, NetApp recommends using an IPsec multiple client configuration.

### About this task

ONTAP supports connecting multiple clients across many networks to a single SVM IP address with IPsec enabled. You can accomplish this using one of the following methods:

- **Subnet configuration**

To allow all clients on a particular subnet (192.168.134.0/24 for example) to connect to a single SVM IP address using a single SPD policy entry, you must specify the `remote-ip-subnets` in subnet form. Additionally, you must specify the `remote-identity` field with the correct client side identity.



When using a single policy entry in a subnet configuration, IPsec clients in that subnet share the IPsec identity and pre-shared key (PSK). However, this is not true with certificate authentication. When using certificates each client can use either their own unique certificate or a shared certificate to authenticate. ONTAP IPsec checks the validity of the certificate based on the CAs installed on its local trust store. ONTAP also supports certificate revocation list (CRL) checking.

- **Allow all clients configuration**

To allow any client, regardless of their source IP address, to connect to the SVM IPsec-enabled IP address, use the `0.0.0.0/0` wild card when specifying the `remote-ip-subnets` field.

Additionally, you must specify the `remote-identity` field with the correct client side identity. For certificate authentication, you can enter `ANYTHING`.

Also, when the `0.0.0.0/0` wild card is used, you must configure a specific local or remote port number to use. For example, `NFS port 2049`.

### Step

1. Use one of the following commands to configure IPsec for multiple clients:
  - a. If you are using a **subnet configuration** to support multiple IPsec clients:

```
security ipsec policy create -vserver vserver_name -name policy_name  
-local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets  
IP_address/subnet -local-identity local_id -remote-identity remote_id
```

### Sample command

```
security ipsec policy create -vserver vs1 -name subnet134 -local-ip
-subnets 192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 -local
-identity ontap_side_identity -remote-identity client_side_identity
```

- b. If you are using an **allow all clients configuration** to support multiple IPsec clients:

```
security ipsec policy create -vserver vserver_name -name policy_name
-local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local
-ports port_number -local-identity local_id -remote-identity remote_id
```

### Sample command

```
security ipsec policy create -vserver vs1 -name test35 -local-ip-subnets
IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local-ports 2049 -local
-identity ontap_side_identity -remote-identity client_side_identity
```

### IPsec statistics

Through negotiation, a security channel called an IKE Security Association (SA) can be established between the ONTAP SVM IP address and the client IP address. IPsec SAs are installed on both endpoints to do the actual data encryption and decryption work.

You can use statistics commands to check the status of both IPsec SAs and IKE SAs.

### Sample commands

IKE SA sample command:

```
security ipsec show-ikesasa -node hosting_node_name_for_svm_ip
```

IPsec SA sample command and output:

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip
```

```
cluster1::> security ipsec show-ikesa -node cluster1-node1
      Policy Local          Remote
Vserver  Name  Address          Address          Initiator-SPI      State
-----  -
vs1      test34
          192.168.134.34  192.168.134.44  c764f9ee020cec69
ESTABLISHED
```

IPsec SA sample command and output:

```

security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip

cluster1::> security ipsec show-ipsecsa -node cluster1-node1
      Policy  Local              Remote              Inbound  Outbound
Vserver  Name    Address              Address              SPI      SPI
State
-----
-----
vs1      test34
              192.168.134.34  192.168.134.44  c4c5b3d6  c2515559
INSTALLED

```

## Configure firewall policies for LIFs

Setting up a firewall enhances the security of the cluster and helps prevent unauthorized access to the storage system. By default, the onboard firewall is configured to allow remote access to a specific set of IP services for data, management, and intercluster LIFs.

Beginning with ONTAP 9.10.1:

- Firewall service policies are deprecated and are replaced by LIF service policies. Previously, the onboard firewall was managed using firewall policies. This functionality is now accomplished using a LIF service policy.
- All firewall policies are empty and do not open any ports in the underlying firewall. Instead, all ports must be opened using a LIF service policy.
- No action is required after an upgrade to 9.10.1 or later to transition from firewall service policies to LIF service policies. The system automatically constructs LIF service policies consistent with the firewall service policies in use in the previous ONTAP release. If you use scripts or other tools that create and manage custom firewall policies, you might need to upgrade those scripts to create custom service policies instead.

To learn more, see [LIFs and service policies in ONTAP 9.6 and later](#).

Firewall policies can be used to control access to management service protocols such as SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPs, RSH, DNS, or SNMP. Firewall policies cannot be set for data protocols such as NFS or SMB.

You can manage firewall service and policies in the following ways:

- Enabling or disabling firewall service
- Displaying the current firewall service configuration
- Creating a new firewall policy with the specified policy name and network services
- Applying a firewall policy to a logical interface
- Creating a new firewall policy that is an exact copy of an existing policy

You can use this to make a policy with similar characteristics within the same SVM, or to copy the policy to

a different SVM.

- Displaying information about firewall policies
- Modifying the IP addresses and netmasks that are used by a firewall policy
- Deleting a firewall policy that is not being used by a LIF

### Firewall policies and LIFs

LIF firewall policies are used to restrict access to the cluster over each LIF. You need to understand how the default firewall policy affects system access over each type of LIF, and how you can customize a firewall policy to increase or decrease security over a LIF.

When configuring a LIF using the `network interface create` or `network interface modify` command, the value specified for the `-firewall-policy` parameter determines the service protocols and IP addresses that are allowed access to the LIF.

In many cases you can accept the default firewall policy value. In other cases, you might need to restrict access to certain IP addresses and certain management service protocols. The available management service protocols include SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPs, RSH, DNS, and SNMP.

The firewall policy for all cluster LIFs defaults to "" and cannot be modified.

The following table describes the default firewall policies that are assigned to each LIF, depending on their role (ONTAP 9.5 and earlier) or service policy (ONTAP 9.6 and later), when you create the LIF:

Firewall policy	Default service protocols	Default access	LIFs applied to
mgmt	dns, http, https, ndmp, ndmps, ntp, snmp, ssh	Any address (0.0.0.0/0)	Cluster management, SVM management, and node management LIFs
mgmt-nfs	dns, http, https, ndmp, ndmps, ntp, portmap, snmp, ssh	Any address (0.0.0.0/0)	Data LIFs that also support SVM management access
intercluster	https, ndmp, ndmps	Any address (0.0.0.0/0)	All intercluster LIFs
data	dns, ndmp, ndmps, portmap	Any address (0.0.0.0/0)	All data LIFs

### Portmap service configuration

The portmap service maps RPC services to the ports on which they listen.

The portmap service was always accessible in ONTAP 9.3 and earlier, became configurable in ONTAP 9.4 through ONTAP 9.6, and is managed automatically beginning with ONTAP 9.7.

- In ONTAP 9.3 and earlier, the portmap service (`rpcbind`) was always accessible on port 111 in network configurations that relied on the built-in ONTAP firewall rather than a third-party firewall.
- From ONTAP 9.4 through ONTAP 9.6, you can modify firewall policies to control whether the portmap



service is accessible on particular LIFs.

- Beginning with ONTAP 9.7, the portmap firewall service is eliminated. Instead, the portmap port is opened automatically for all LIFs that support the NFS service.

### **Portmap service is configurable in the firewall in ONTAP 9.4 through ONTAP 9.6.**

The remainder of this topic discusses how to configure the portmap firewall service for ONTAP 9.4 through ONTAP 9.6 releases.

Depending on your configuration, you may be able to disallow access to the service on specific types of LIFs, typically management and intercluster LIFs. In some circumstances, you might even be able to disallow access on data LIFs.

#### **What behavior you can expect**

The ONTAP 9.4 through ONTAP 9.6 behavior is designed to provide a seamless transition on upgrade. If the portmap service is already being accessed over specific types of LIFs, it will continue to be accessible over those types of LIFs. As in previous ONTAP versions, you can specify the services accessible within the firewall in the firewall policy for the LIF type.

All nodes in the cluster must be running ONTAP 9.4 through ONTAP 9.6 for the behavior to take effect. Only inbound traffic is affected.

The new rules are as follows:

- On upgrade to release 9.4 through 9.6, ONTAP adds the portmap service to all existing firewall policies, default or custom.
- When you create a new cluster or new IPspace, ONTAP adds the portmap service only to the default data policy, not to the default management or intercluster policies.
- You can add the portmap service to default or custom policies as needed, and remove the service as needed.

#### **How to add or remove the portmap service**

To add the portmap service to an SVM or cluster firewall policy (make it accessible within the firewall), enter:

```
system services firewall policy create -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

To remove the portmap service from an SVM or cluster firewall policy (make it inaccessible within the firewall), enter:

```
system services firewall policy delete -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

You can use the network interface modify command to apply the firewall policy to an existing LIF. For complete command syntax, see [ONTAP 9 commands](#).

#### **Create a firewall policy and assigning it to a LIF**

Default firewall policies are assigned to each LIF when you create the LIF. In many cases, the default firewall settings work well and you do not need to change them. If you want to change the network services or IP addresses that can access a LIF, you can create a custom firewall policy and assign it to the LIF.

#### **About this task**

- You cannot create a firewall policy with the `policy` name `data`, `intercluster`, `cluster`, or `mgmt`.

These values are reserved for the system-defined firewall policies.

- You cannot set or modify a firewall policy for cluster LIFs.

The firewall policy for cluster LIFs is set to `0.0.0.0/0` for all services types.

- If you need to remove a service from a policy, you must delete the existing firewall policy and create a new policy.
- If IPv6 is enabled on the cluster, you can create firewall policies with IPv6 addresses.

After IPv6 is enabled, `data`, `intercluster`, and `mgmt` firewall policies include `::/0`, the IPv6 wildcard, in their list of accepted addresses.

- When using System Manager to configure data protection functionality across clusters, you must ensure that the intercluster LIF IP addresses are included in the allowed list, and that HTTPS service is allowed on both the intercluster LIFs and on your company-owned firewalls.

By default, the `intercluster` firewall policy allows access from all IP addresses (`0.0.0.0/0`, or `::/0` for IPv6) and enables HTTPS, NDMP, and NDMPS services. If you modify this default policy, or if you create your own firewall policy for intercluster LIFs, you must add each intercluster LIF IP address to the allowed list and enable HTTPS service.

- Beginning with ONTAP 9.6, the HTTPS and SSH firewall services are not supported.

In ONTAP 9.6, the `management-https` and `management-ssh` LIF services are available for HTTPS and SSH management access.

## Steps

1. Create a firewall policy that will be available to the LIFs on a specific SVM:

```
system services firewall policy create -vserver vserver_name -policy
policy_name -service network_service -allow-list ip_address/mask
```

You can use this command multiple times to add more than one network service and list of allowed IP addresses for each service in the firewall policy.

2. Verify that the policy was added correctly by using the `system services firewall policy show` command.
3. Apply the firewall policy to a LIF:

```
network interface modify -vserver vserver_name -lif lif_name -firewall-policy
policy_name
```

4. Verify that the policy was added correctly to the LIF by using the `network interface show -fields firewall-policy` command.

## Example of creating a firewall policy and applying it to a LIF

The following command creates a firewall policy named `data_http` that enables HTTP and HTTPS protocol access from IP addresses on the 10.10 subnet, applies that policy to the LIF named `data1` on SVM `vs1`, and then shows all of the firewall policies on the cluster:

```
system services firewall policy create -vserver vs1 -policy data_http  
-service http - allow-list 10.10.0.0/16
```

```
system services firewall policy show
```

Vserver	Policy	Service	Allowed
-----			
cluster-1	data		
		dns	0.0.0.0/0
		ndmp	0.0.0.0/0
		ndmps	0.0.0.0/0
cluster-1	intercluster		
		https	0.0.0.0/0
		ndmp	0.0.0.0/0
		ndmps	0.0.0.0/0
cluster-1	mgmt		
		dns	0.0.0.0/0
		http	0.0.0.0/0
		https	0.0.0.0/0
		ndmp	0.0.0.0/0
		ndmps	0.0.0.0/0
		ntp	0.0.0.0/0
		snmp	0.0.0.0/0
		ssh	0.0.0.0/0
vs1	data_http		
		http	10.10.0.0/16
		https	10.10.0.0/16

```
network interface modify -vserver vs1 -lif data1 -firewall-policy data_http
```

```
network interface show -fields firewall-policy
```

vserver	lif	firewall-policy
-----		
Cluster	node1_clus_1	
Cluster	node1_clus_2	
Cluster	node2_clus_1	
Cluster	node2_clus_2	
cluster-1	cluster_mgmt	mgmt
cluster-1	node1_mgmt1	mgmt
cluster-1	node2_mgmt1	mgmt
vs1	data1	data_http
vs3	data2	data

## Commands for managing firewall service and policies

You can use the `system services firewall` commands to manage firewall service, the `system services firewall policy` commands to manage firewall policies, and the `network interface modify` command to manage firewall settings for LIFs.

If you want to...	Use this command...
Enable or disable firewall service	<code>system services firewall modify</code>
Display the current configuration for firewall service	<code>system services firewall show</code>
Create a firewall policy or add a service to an existing firewall policy	<code>system services firewall policy create</code>
Apply a firewall policy to a LIF	<code>network interface modify -lif lifname -firewall-policy</code>
Modify the IP addresses and netmasks associated with a firewall policy	<code>system services firewall policy modify</code>
Display information about firewall policies	<code>system services firewall policy show</code>
Create a new firewall policy that is an exact copy of an existing policy	<code>system services firewall policy clone</code>
Delete a firewall policy that is not used by a LIF	<code>system services firewall policy delete</code>

For more information, see the man pages for the `system services firewall`, `system services firewall policy`, and `network interface modify` commands in [ONTAP 9 commands](#).

## Configure QoS marking (cluster administrators only)

### Overview

Network Quality of Service (QoS) marking helps you to prioritize different traffic types based on the network conditions to effectively utilize the network resources. You can set the differentiated services code point (DSCP) value of the outgoing IP packets for the supported traffic types per IPspace.

### DSCP marking for UC compliance

You can enable differentiated services code point (DSCP) marking on outgoing (egress) IP packet traffic for a given protocol with a default or user-provided DSCP code. DSCP marking is a mechanism for classifying and managing network traffic and is a component of Unified Capability (UC) compliance.

DSCP marking (also known as *QoS marking* or *quality of service marking*) is enabled by providing an IPspace, protocol, and DSCP value. The protocols on which DSCP marking can be applied are NFS, SMB, iSCSI, SnapMirror, NDMP, FTP, HTTP/HTTPS, SSH, Telnet, and SNMP.

If you do not provide a DSCP value when enabling DSCP marking for a given protocol, a default is used:

- The default value for data protocols/traffic is 0x0A (10).
- The default value for control protocols/traffic is 0x30 (48).

## Modify QoS marking values

You can modify the Quality of Service (QoS) marking values for different protocols, for each IPspace.

### Before you begin

All nodes in the cluster must be running the same version of ONTAP.

### Step

Modify QoS marking values by using the `network qos-marking modify` command.

- The `-ipspace` parameter specifies the IPspace for which the QoS marking entry is to be modified.
- The `-protocol` parameter specifies the protocol for which the QoS marking entry is to be modified. The `network qos-marking modify man page` describes the possible values of the protocol.
- The `-dscp` parameter specifies the Differentiated Services Code Point (DSCP) value. The possible values ranges from 0 through 63.
- The `-is-enabled` parameter is used to enable or disable the QoS marking for the specified protocol in the IPspace provided by the `-ipspace` parameter.

The following command enables the QoS marking for the NFS protocol in default IPspace:

```
network qos-marking modify -ipspace Default -protocol NFS -is-enabled true
```

The following command sets the DSCP value to 20 for the NFS protocol in the default IPspace:

```
network qos-marking modify -ipspace Default -protocol NFS -dscp 20
```

## Display QoS marking values

You can display the QoS marking values for different protocols, for each IPspace.

### Step

Display QoS marking values by using the `network qos-marking show` command.

The following command displays the QoS marking for all protocols in the default IPspace:

```

network qos-marking show -ipSPACE Default
IPspace                Protocol                DSCP  Enabled?
-----                -
Default
                        CIFS                    10    false
                        FTP                    48    false
                        HTTP-admin            48    false
                        HTTP-filesrv         10    false
                        NDMP                    10    false
                        NFS                    10    true
                        SNMP                    48    false
                        SSH                    48    false
                        SnapMirror          10    false
                        Telnet                48    false
                        iSCSI                10    false

11 entries were displayed.

```

## Manage SNMP on the cluster (cluster administrators only)

### Overview

You can configure SNMP to monitor SVMs in your cluster to avoid issues before they occur, and to respond to issues if they do occur. Managing SNMP involves configuring SNMP users and configuring SNMP trap host destinations (management workstations) for all SNMP events. SNMP is disabled by default on data LIFs.

You can create and manage read-only SNMP users in the data SVM. Data LIFs must be configured to receive SNMP requests on the SVM.

SNMP network management workstations, or managers, can query the SVM SNMP agent for information. The SNMP agent gathers information and forwards it to the SNMP managers. The SNMP agent also generates trap notifications whenever specific events occur. The SNMP agent on the SVM has read-only privileges; it cannot be used for any set operations or for taking a corrective action in response to a trap. ONTAP provides an SNMP agent compatible with SNMP versions v1, v2c, and v3. SNMPv3 offers advanced security by using passphrases and encryption.

For more information about SNMP support in ONTAP systems, see [TR-4220: SNMP Support in Data ONTAP](#).

### What MIBs are

A MIB (Management Information Base) is a text file that describes SNMP objects and traps.

MIBs describe the structure of the management data of the storage system and they use a hierarchical namespace containing object identifiers (OIDs). Each OID identifies a variable that can be read by using SNMP.

Because MIBs are not configuration files and ONTAP does not read these files, SNMP functionality is not

affected by MIBs. ONTAP provides the following MIB file:

- A NetApp custom MIB (`netapp.mib`)

ONTAP supports IPv6 (RFC 2465), TCP (RFC 4022), UDP (RFC 4113), and ICMP (RFC 2466) MIBs, which show both IPv4 and IPv6 data, are supported.

ONTAP also provides a short cross-reference between object identifiers (OIDs) and object short names in the `traps.dat` file.



The latest versions of the ONTAP MIBs and `traps.dat` files are available on the NetApp Support Site. However, the versions of these files on the support site do not necessarily correspond to the SNMP capabilities of your ONTAP version. These files are provided to help you evaluate SNMP features in the latest ONTAP version.

## SNMP traps

SNMP traps capture system monitoring information that is sent as an asynchronous notification from the SNMP agent to the SNMP manager.

There are three types of SNMP traps: standard, built-in, and user-defined. User-defined traps are not supported in ONTAP.

A trap can be used to check periodically for operational thresholds or failures that are defined in the MIB. If a threshold is reached or a failure is detected, the SNMP agent sends a message (trap) to the traphosts alerting them of the event.



ONTAP supports SNMPv1 traps and, starting in ONTAP 9.1, SNMPv3 traps. ONTAP does not support SNMPv2c traps and INFORMs.

## Standard SNMP traps

These traps are defined in RFC 1215. There are five standard SNMP traps that are supported by ONTAP: `coldStart`, `warmStart`, `linkDown`, `linkUp`, and `authenticationFailure`.



The `authenticationFailure` trap is disabled by default. You must use the `system snmp authtrap` command to enable the trap. For more information, see the man pages: [ONTAP 9 commands](#)

## Built-in SNMP traps

Built-in traps are predefined in ONTAP and are automatically sent to the network management stations on the traphost list if an event occurs. These traps, such as `diskFailedShutdown`, `cpuTooBusy`, and `volumeNearlyFull`, are defined in the custom MIB.

Each built-in trap is identified by a unique trap code.

## Create an SNMP community and assigning it to a LIF

You can create an SNMP community that acts as an authentication mechanism between the management station and the storage virtual machine (SVM) when using SNMPv1 and SNMPv2c.



By creating SNMP communities in a data SVM, you can execute commands such as `snmpwalk` and `snmpget` on the data LIFs.

### About this task

- In new installations of ONTAP, SNMPv1 and SNMPv2c are disabled by default.

SNMPv1 and SNMPv2c are enabled after you create an SNMP community.

- ONTAP supports read-only communities.
- By default, the "data" firewall policy that is assigned to data LIFs has SNMP service set to `deny`.

You must create a new firewall policy with SNMP service set to `allow` when creating an SNMP user for a data SVM.

- You can create SNMP communities for SNMPv1 and SNMPv2c users for both the admin SVM and the data SVM.
- Because an SVM is not part of the SNMP standard, queries on data LIFs must include the NetApp root OID (1.3.6.1.4.1.789)—for example, `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

### Steps

1. Create an SNMP community by using the `system snmp community add` command. The following command shows how to create an SNMP community in the admin SVM `cluster-1`:

```
system snmp community add -type ro -community-name comty1 -vserver
cluster-1
```

The following command shows how to create an SNMP community in the data SVM `vs1`:

```
system snmp community add -type ro -community-name comty2 -vserver vs1
```

2. Verify that the communities have been created by using the `system snmp community show` command.

The following command shows the two communities created for SNMPv1 and SNMPv2c:

```
system snmp community show
cluster-1
rocomty1
vs1
rocomty2
```

3. Check whether SNMP is allowed as a service in the "data" firewall policy by using the `system services firewall policy show` command.

The following command shows that the `snmp` service is not allowed in the default "data" firewall policy (the `snmp` service is allowed in the "mgmt" firewall policy only):

```

system services firewall policy show
Vserver Policy          Service    Allowed
-----
cluster-1
  data
    dns          0.0.0.0/0
    ndmp         0.0.0.0/0
    ndmps        0.0.0.0/0
cluster-1
  intercluster
    https        0.0.0.0/0
    ndmp         0.0.0.0/0
    ndmps        0.0.0.0/0
cluster-1
  mgmt
    dns          0.0.0.0/0
    http         0.0.0.0/0
    https        0.0.0.0/0
    ndmp         0.0.0.0/0
    ndmps        0.0.0.0/0
    ntp          0.0.0.0/0
    snmp         0.0.0.0/0
    ssh          0.0.0.0/0

```

4. Create a new firewall policy that allows access using the `snmp` service by using the `system services firewall policy create` command.

The following commands create a new data firewall policy named "data1" that allows the `snmp`

```

system services firewall policy create -policy data1 -service snmp
-vserver vs1 -allow-list 0.0.0.0/0

cluster-1::> system services firewall policy show -service snmp
Vserver Policy          Service    Allowed
-----
cluster-1
  mgmt
    snmp          0.0.0.0/0
vs1
  data1
    snmp          0.0.0.0/0

```

5. Apply the firewall policy to a data LIF by using the `network interface modify` command with the `-firewall -policy` parameter.

The following command assigns the new "data1" firewall policy to LIF "datalif1":

```
network interface modify -vserver vs1 -lif datalif1 -firewall-policy data1
```

### Configure SNMPv3 users in a cluster

SNMPv3 is a secure protocol when compared to SNMPv1 and SNMPv2c. To use SNMPv3, you must configure an SNMPv3 user to run the SNMP utilities from the SNMP manager.

#### Step

Use the "security login create command" to create an SNMPv3 user.

You are prompted to provide the following information:

- Engine ID: Default and recommended value is local Engine ID
- Authentication protocol
- Authentication password
- Privacy protocol
- Privacy protocol password

#### Result

The SNMPv3 user can log in from the SNMP manager by using the user name and password and run the SNMP utility commands.

#### SNMPv3 security parameters

SNMPv3 includes an authentication feature that, when selected, requires users to enter their names, an authentication protocol, an authentication key, and their desired security level when invoking a command.

The following table lists the SNMPv3 security parameters :

Parameter	Command-line option	Description
engineID	-e EngineID	Engine ID of the SNMP agent. Default value is local EngineID (recommended).
securityName	-u Name	User name must not exceed 32 characters.
authProtocol	-a {none   MD5   SHA   SHA-256}	Authentication type can be none, MD5, SHA, or SHA-256.
authKey	-A PASSPHRASE	Passphrase with a minimum of eight characters.

securityLevel	-l {authNoPriv   AuthPriv   noAuthNoPriv}	Security level can be Authentication, No Privacy; Authentication, Privacy; or no Authentication, no Privacy.
privProtocol	-x { none   des   aes128}	Privacy protocol can be none, des, or aes128
privPassword	-X password	Password with a minimum of eight characters.

### Examples for different security levels

This example shows how an SNMPv3 user created with different security levels can use the SNMP client-side commands, such as `snmpwalk`, to query the cluster objects.

For better performance, you should retrieve all objects in a table rather than a single object or a few objects from the table.



You must use `snmpwalk` 5.3.1 or later when the authentication protocol is SHA.

### Security level: authPriv

The following output shows the creation of an SNMPv3 user with the `authPriv` security level.

```
security login create -username snmpv3user -application snmp -authmethod
usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]:sha
```

### FIPS mode

```
Which authentication protocol do you want to choose (sha, sha2-256) [sha]

Enter authentication protocol password (minimum 8 characters long):
Enter authentication protocol password again:
Which privacy protocol do you want to choose (none, des) [none]: des
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

### snmpwalk Test

The following output shows the SNMPv3 user running the `snmpwalk` command:

For better performance, you should retrieve all objects in a table rather than a single object or a few objects from the table.

```
$ snmpwalk -v 3 -u snmpv3user -a SHA -A password1! -x DES -X password1! -l
authPriv 192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

### Security level: authNoPriv

The following output shows the creation of an SNMPv3 user with the authNoPriv security level.

```
security login create -username snmpv3user1 -application snmp -authmethod
usm -role admin
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: md5
```

### FIPS Mode

```
Which privacy protocol do you want to choose (aes128) [aes128]

Enter authentication protocol password (minimum 8 characters long):
Enter authentication protocol password again:
Which privacy protocol do you want to choose (none, des) [none]: none
```

### snmpwalk Test

The following output shows the SNMPv3 user running the snmpwalk command:

For better performance, you should retrieve all objects in a table rather than a single object or a few objects from the table.

```
$ snmpwalk -v 3 -u snmpv3user1 -a MD5 -A password1! -l authNoPriv
192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

## Security level: noAuthNoPriv

The following output shows the creation of an SNMPv3 user with the noAuthNoPriv security level.

```
security login create -username snmpv3user2 -application snmp -authmethod
usm -role admin
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: none
```

## FIPS Mode

FIPS will not allow you to choose none

## snmpwalk Test

The following output shows the SNMPv3 user running the snmpwalk command:

For better performance, you should retrieve all objects in a table rather than a single object or a few objects from the table.

```
$ snmpwalk -v 3 -u snmpv3user2 -l noAuthNoPriv 192.0.2.62
.1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

## Configure traphosts to receive SNMP notifications

You can configure the traphost (SNMP manager) to receive notifications (SNMP trap PDUs) when SNMP traps are generated in the cluster. You can specify either the host name or the IP address (IPv4 or IPv6) of the SNMP traphost.

### Before you begin

- SNMP and SNMP traps must be enabled on the cluster.



SNMP and SNMP traps are enabled by default.

- DNS must be configured on the cluster for resolving the traphost names.
- IPv6 must be enabled on the cluster to configure SNMP traphosts by using IPv6 addresses.
- For ONTAP 9.1 and later versions, you must have specified the authentication of a predefined User-based Security Model (USM) and privacy credentials when creating traphosts.

### Step

Add an SNMP traphost:

```
system snmp traphost add
```



Traps can be sent only when at least one SNMP management station is specified as a traphost.

The following command adds a new SNMPv3 traphost named `yyy.example.com` with a known USM user:

```
system snmp traphost add -peer-address yyy.example.com -usm-username  
MyUsmUser
```

The following command adds a traphost using the IPv6 address of the host:

```
system snmp traphost add -peer-address 2001:0db8:1:1:209:6bff:feae:6d67
```

### Commands for managing SNMP

You can use the `system snmp` commands to manage SNMP, traps, and traphosts. You can use the `security` commands to manage SNMP users per SVM. You can use the `event` commands to manage events related to SNMP traps.

#### Commands for configuring SNMP

If you want to...	Use this command...
Enable SNMP on the cluster	<pre>options -option-name snmp.enable -option-value on</pre> <p>The SNMP service must be allowed under the management (mgmt) firewall policy. You can verify whether SNMP is allowed by using the <code>system services firewall policy show</code> command.</p>
Disable SNMP on the cluster	<pre>options -option-name snmp.enable -option-value off</pre>

#### Commands for managing SNMP v1, v2c, and v3 users

If you want to...	Use this command...
Configure SNMP users	<pre>security login create</pre>
Display SNMP users	<pre>security snmpusers and security login show -application snmp</pre>

Delete SNMP users	<code>security login delete</code>
Modify the access-control role name of a login method for SNMP users	<code>security login modify</code>

#### Commands for providing contact and location information

If you want to...	Use this command...
Display or modify the contact details of the cluster	<code>system snmp contact</code>
Display or modify the location details of the cluster	<code>system snmp location</code>

#### Commands for managing SNMP communities

If you want to...	Use this command...
Add a read-only (ro) community for an SVM or for all SVMs in the cluster	<code>system snmp community add</code>
Delete a community or all communities	<code>system snmp community delete</code>
Display the list of all communities	<code>system snmp community show</code>

Because SVMs are not part of the SNMP standard, queries on data LIFs must include the NetApp root OID (1.3.6.1.4.1.789), for example, `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

#### Command for displaying SNMP option values

If you want to...	Use this command...
Display the current values of all SNMP options, including cluster contact, contact location, whether the cluster is configured to send traps, the list of traphosts, and list of communities and access control type	<code>system snmp show</code>

#### Commands for managing SNMP traps and traphosts

If you want to...	Use this command...
Enable SNMP traps sent from the cluster	<code>system snmp init -init 1</code>
Disable SNMP traps sent from the cluster	<code>system snmp init -init 0</code>



Add a traphost that receives SNMP notifications for specific events in the cluster	<code>system snmp traphost add</code>
Delete a traphost	<code>system snmp traphost delete</code>
Display the list of traphosts	<code>system snmp traphost show</code>

### Commands for managing events related to SNMP traps

If you want to...	Use this command...
Display the events for which SNMP traps (built-in) are generated	<code>event route show</code>  Use the <code>-snmp-support true</code> parameter to view only SNMP-related events.  Use the <code>instance -messagename &lt;message&gt;</code> parameter to view a detailed description why an event might have occurred, and any corrective action.  Routing of individual SNMP trap events to specific traphost destinations is not supported. All SNMP trap events are sent to all traphost destinations.
Display a list of SNMP trap history records, which are event notifications that have been sent to SNMP traps	<code>event snmhistory show</code>
Delete an SNMP trap history record	<code>event snmhistory delete</code>

For more information about the `system snmp`, `security`, and `event` commands, see the man pages: [ONTAP 9 commands](#)

## Manage routing in an SVM

### Overview

The routing table for an SVM determines the network path the SVM uses to communicate with a destination. It's important to understand how routing tables work so that you can prevent network problems before they occur.

Routing rules are as follows:

- ONTAP routes traffic over the most specific available route.
- ONTAP routes traffic over a default gateway route (having 0 bits of netmask) as a last resort, when more specific routes are not available.

In the case of routes with the same destination, netmask, and metric, there is no guarantee that the system will use the same route after a reboot or after an upgrade. This is especially an issue if you have configured multiple default routes.

It is a best practice to configure one default route only for an SVM. To avoid disruption, you should ensure that the default route is able to reach any network address that is not reachable by a more specific route. For more information, see the Knowledgebase article [SU134: Network access might be disrupted by incorrect routing configuration in clustered ONTAP](#)

## Create a static route

You can create static routes within a storage virtual machine (SVM) to control how LIFs use the network for outbound traffic.

When you create a route entry associated with an SVM, the route will be used by all LIFs that are owned by the specified SVM and that are on the same subnet as the gateway.

### Step

Use the `network route create` command to create a route.

```
network route create -vserver vs0 -destination 0.0.0.0/0 -gateway
10.61.208.1
```

## Enable multipath routing

If multiple routes have the same metric for a destination, only one of the routes is picked for outgoing traffic. This leads to other routes being unutilized for sending outgoing traffic. You can enable multipath routing to load balance and utilize all the available routes.

### Steps

1. Log in to the advanced privilege level:

```
set -privilege advanced
```

2. Enable multipath routing:

```
network options multipath-routing modify -is-enabled true
```

Multipath routing is enabled for all nodes in the cluster.

```
network options multipath-routing modify -is-enabled true
```

## Delete a static route

You can delete an unneeded static route from a storage virtual machine (SVM).

### Step

Use the `network route delete` command to delete a static route.

For more information about this command, see the `network route` man page: [ONTAP 9 commands](#).

The following example deletes a static route associated with SVM vs0 with a gateway of 10.63.0.1 and a

destination IP address of 0.0.0.0/0:

```
network route delete -vserver vs0 -gateway 10.63.0.1 -destination
0.0.0.0/0
```

## Display routing information

You can display information about the routing configuration for each SVM on your cluster. This can help you diagnose routing problems involving connectivity issues between client applications or services and a LIF on a node in the cluster.

### Steps

1. Use the `network route show` command to display routes within one or more SVMs. The following example shows a route configured in the vs0 SVM:

```
network route show
(network route show)
Vserver          Destination      Gateway          Metric
-----
vs0
                0.0.0.0/0       172.17.178.1    20
```

2. Use the `network route show-lifs` command to display the association of routes and LIFs within one or more SVMs.

The following example shows LIFs with routes owned by the vs0 SVM:

```
network route show-lifs
(network route show-lifs)

Vserver: vs0
Destination      Gateway          Logical Interfaces
-----
0.0.0.0/0       172.17.178.1    cluster_mgmt,
                LIF-b-01_mgmt1,
                LIF-b-02_mgmt1
```

3. Use the `network route active-entry show` command to display installed routes on one or more nodes, SVMs, subnets, or routes with specified destinations.

The following example shows all installed routes on a specific SVM:

```
network route active-entry show -vserver Data0
```

Vserver: Data0

Node: node-1

Subnet Group: 0.0.0.0/0

Destination	Gateway	Interface	Metric	Flags
127.0.0.1	127.0.0.1	lo	10	UHS
127.0.10.1	127.0.20.1	losk	10	UHS
127.0.20.1	127.0.20.1	losk	10	UHS

Vserver: Data0

Node: node-1

Subnet Group: fd20:8b1e:b255:814e::/64

Destination	Gateway	Interface	Metric	Flags
default	fd20:8b1e:b255:814e::1	e0d	20	UGS
fd20:8b1e:b255:814e::/64	link#4	e0d	0	UC

Vserver: Data0

Node: node-2

Subnet Group: 0.0.0.0/0

Destination	Gateway	Interface	Metric	Flags
127.0.0.1	127.0.0.1	lo	10	UHS

Vserver: Data0

Node: node-2

Subnet Group: 0.0.0.0/0

Destination	Gateway	Interface	Metric	Flags
127.0.10.1	127.0.20.1	losk	10	UHS
127.0.20.1	127.0.20.1	losk	10	UHS

Vserver: Data0

Node: node-2

Subnet Group: fd20:8b1e:b255:814e::/64

Destination	Gateway	Interface	Metric	Flags
default	fd20:8b1e:b255:814e::1	e0d	20	UGS
fd20:8b1e:b255:814e::/64	link#4	e0d	0	UC
fd20:8b1e:b255:814e::1	link#4	e0d	0	UHL

11 entries were displayed.

## Remove dynamic routes from routing tables

When ICMP redirects are received for IPv4 and IPv6, dynamic routes are added to the routing table. By default, the dynamic routes are removed after 300 seconds. If you want to maintain dynamic routes for a different amount of time, you can change the time out value.

### About this task

You can set the timeout value from 0 to 65,535 seconds. If you set the value to 0, the routes never expire. Removing dynamic routes prevents loss of connectivity caused by the persistence of invalid routes.

### Steps

1. Display the current timeout value.

- For IPv4:

```
network tuning icmp show
```

- For IPv6:

```
network tuning icmp6 show
```

2. Modify the timeout value.

- For IPv4:

```
network tuning icmp modify -node node_name -redirect-timeout  
timeout_value
```

- For IPv6:

```
network tuning icmp6 modify -node node_name -redirect-v6-timeout  
timeout_value
```

3. Verify that the timeout value was modified correctly.

- For IPv4:

```
network tuning icmp show
```

- For IPv6:

```
network tuning icmp6 show
```

## ONTAP port usage on a storage system

### Overview

A number of well-known ports are reserved for ONTAP communications with specific services. Port conflicts will occur if a port value in your storage network environment is the same as on ONTAP port.

The following table lists the TCP ports and UDP ports that are used by ONTAP.

Service	Port/Protocol	Description
ssh	22/TCP	Secure shell login
telnet	23/TCP	Remote login
DNS	53/TCP	Load Balanced DNS
http	80/TCP	Hyper Text Transfer Protocol
rpcbind	111/TCP	Remote procedure call
rpcbind	111/UDP	Remote procedure call
ntp	123/UDP	Network Time Protocol
msrpc	135/UDP	MSRPC
netbios-ssn	139/TCP	NetBIOS service session
snmp	161/UDP	Simple network management protocol
https	443/TCP	HTTP over TLS
microsoft-ds	445/TCP	Microsoft-ds
mount	635/TCP	NFS mount
mount	635/UDP	NFS Mount
named	953/UDP	Name daemon
nfs	2049/UDP	NFS Server daemon
nfs	2049/TCP	NFS Server daemon
nrv	2050/TCP	NetApp Remote Volume protocol
iscsi	3260/TCP	iSCSI target port
lockd	4045/TCP	NFS lock daemon
lockd	4045/UDP	NFS lock daemon
NFS	4046/TCP	Network Status Monitor
NSM	4046/UDP	Network Status Monitor
rquotad	4049/UDP	NFS rquotad protocol
krb524	4444/UDP	Kerberos 524
mdns	5353/UDP	Multicast DNS

HTTPS	5986/UDP	HTTPS Port - Listening binary protocol
https	8443/TCP	7MTT GUI Tool through https
ndmp	10000/TCP	Network Data Management Protocol
Cluster peering	11104/TCP	Cluster peering
Cluster peering	11105/TCP	Cluster peering
NDMP	18600 - 18699/TCP	NDMP
cifs witness port	40001/TCP	cifs witness port
tls	50000/TCP	Transport layer security
iscsi	65200/TCP	ISCSI port

### ONTAP internal ports

The following table lists the TCP ports and UDP ports that are used internally by ONTAP. These ports are used to establish intracluster LIF communication:

Port/Protocol	Description
514	Syslog
900	NetApp Cluster RPC
902	NetApp Cluster RPC
904	NetApp Cluster RPC
905	NetApp Cluster RPC
910	NetApp Cluster RPC
911	NetApp Cluster RPC
913	NetApp Cluster RPC
914	NetApp Cluster RPC
915	NetApp Cluster RPC
918	NetApp Cluster RPC
920	NetApp Cluster RPC
921	NetApp Cluster RPC
924	NetApp Cluster RPC
925	NetApp Cluster RPC
927	NetApp Cluster RPC
928	NetApp Cluster RPC
929	NetApp Cluster RPC
931	NetApp Cluster RPC
932	NetApp Cluster RPC

933	NetApp Cluster RPC
934	NetApp Cluster RPC
935	NetApp Cluster RPC
936	NetApp Cluster RPC
937	NetApp Cluster RPC
939	NetApp Cluster RPC
940	NetApp Cluster RPC
951	NetApp Cluster RPC
954	NetApp Cluster RPC
955	NetApp Cluster RPC
956	NetApp Cluster RPC
958	NetApp Cluster RPC
961	NetApp Cluster RPC
963	NetApp Cluster RPC
964	NetApp Cluster RPC
966	NetApp Cluster RPC
967	NetApp Cluster RPC
5125	Alternate Control Port for disk
5133	Alternate Control Port for disk
5144	Alternate Control Port for disk
65502	Node scope SSH
65503	LIF Sharing
7810	NetApp Cluster RPC
7811	NetApp Cluster RPC
7812	NetApp Cluster RPC
7813	NetApp Cluster RPC
7814	NetApp Cluster RPC
7815	NetApp Cluster RPC
7816	NetApp Cluster RPC
7817	NetApp Cluster RPC
7818	NetApp Cluster RPC
7819	NetApp Cluster RPC
7820	NetApp Cluster RPC
7821	NetApp Cluster RPC



7822	NetApp Cluster RPC
7823	NetApp Cluster RPC
7824	NetApp Cluster RPC
8023	Node Scope TELNET
8514	Node Scope RSH
9877	KMIP Client Port (Internal Local Host Only)

## View network information

### Overview

You can view information related to ports, LIFs, routes, failover rules, failover groups, firewall rules, DNS, NIS, and connections.

This information can be useful in situations such as reconfiguring networking settings, or when troubleshooting the cluster.

If you are a cluster administrator, you can view all the available networking information. If you are an SVM administrator, you can view only the information related to your assigned SVMs.

### Display network port information

You can display information about a specific port, or about all ports on all nodes in the cluster.

### About this task

The following information is displayed:

- Node name
- Port name
- IPspace name
- Broadcast domain name
- Link status (up or down)
- MTU setting
- Port speed setting and operational status (1 gigabit or 10 gigabits per second)
- Auto-negotiation setting (true or false)
- Duplex mode and operational status (half or full)
- The port's interface group, if applicable
- The port's VLAN tag information, if applicable
- The port's health status (health or degraded)
- Reasons for a port being marked as degraded

If data for a field is not available (for example, the operational duplex and speed for an inactive port would not be available), the field value is listed as – .

## Step

Display network port information by using the `network port show` command.

You can display detailed information for each port by specifying the `-instance` parameter, or get specific information by specifying field names using the `-fields` parameter.

```
network port show
Node: node1

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e0a      Cluster      Cluster      up    9000  auto/1000  healthy
false
e0b      Cluster      Cluster      up    9000  auto/1000  healthy
false
e0c      Default      Default      up    1500  auto/1000  degraded
false
e0d      Default      Default      up    1500  auto/1000  degraded
true
Node: node2

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e0a      Cluster      Cluster      up    9000  auto/1000  healthy
false
e0b      Cluster      Cluster      up    9000  auto/1000  healthy
false
e0c      Default      Default      up    1500  auto/1000  healthy
false
e0d      Default      Default      up    1500  auto/1000  healthy
false
8 entries were displayed.
```

## Display information about a VLAN (cluster administrators only)

You can display information about a specific VLAN or about all VLANs in the cluster.

### About this task

You can display detailed information for each VLAN by specifying the `-instance` parameter. You can display specific information by specifying field names using the `-fields` parameter.

### Step

Display information about VLANs by using the `network port vlan show` command. The following command displays information about all VLANs in the cluster:

```
network port vlan show
                Network Network
Node   VLAN Name Port   VLAN ID  MAC Address
-----
cluster-1-01
    a0a-10  a0a    10      02:a0:98:06:10:b2
    a0a-20  a0a    20      02:a0:98:06:10:b2
    a0a-30  a0a    30      02:a0:98:06:10:b2
    a0a-40  a0a    40      02:a0:98:06:10:b2
    a0a-50  a0a    50      02:a0:98:06:10:b2
cluster-1-02
    a0a-10  a0a    10      02:a0:98:06:10:ca
    a0a-20  a0a    20      02:a0:98:06:10:ca
    a0a-30  a0a    30      02:a0:98:06:10:ca
    a0a-40  a0a    40      02:a0:98:06:10:ca
    a0a-50  a0a    50      02:a0:98:06:10:ca
```

## Display interface group information (cluster administrators only)

You can display information about an interface group to determine its configuration.

### About this task

The following information is displayed:

- Node on which the interface group is located
- List of network ports that are included in the interface group
- Interface group's name
- Distribution function (MAC, IP, port, or sequential)
- Interface group's Media Access Control (MAC) address
- Port activity status; that is, whether all aggregated ports are active (full participation), whether some are active (partial participation), or whether none are active

### Step

Display information about interface groups by using the `network port ifgrp show` command.

You can display detailed information for each node by specifying the `-instance` parameter. You can display specific information by specifying field names using the `-fields` parameter.

The following command displays information about all interface groups in the cluster:

```
network port ifgrp show
      Port      Distribution      Active
Node    IfGrp    Function    MAC Address    Ports    Ports
-----
cluster-1-01
      a0a      ip          02:a0:98:06:10:b2    full    e7a, e7b
cluster-1-02
      a0a      sequential  02:a0:98:06:10:ca    full    e7a, e7b
cluster-1-03
      a0a      port        02:a0:98:08:5b:66    full    e7a, e7b
cluster-1-04
      a0a      mac         02:a0:98:08:61:4e    full    e7a, e7b
```

The following command displays detailed interface group information for a single node:

```
network port ifgrp show -instance -node cluster-1-01

      Node: cluster-1-01
Interface Group Name: a0a
Distribution Function: ip
      Create Policy: multimode
      MAC Address: 02:a0:98:06:10:b2
Port Participation: full
      Network Ports: e7a, e7b
      Up Ports: e7a, e7b
      Down Ports: -
```

## Display LIF information

You can view detailed information about a LIF to determine its configuration.

You might also want to view this information to diagnose basic LIF problems, such as checking for duplicate IP addresses or verifying whether the network port belongs to the correct subnet. storage virtual machine (SVM) administrators can view only the information about the LIFs associated with the SVM.

### About this task

The following information is displayed:

- IP address associated with the LIF
- Administrative status of the LIF

- Operational status of the LIF

The operational status of data LIFs is determined by the status of the SVM with which the data LIFs are associated. When the SVM is stopped, the operational status of the LIF changes to down. When the SVM is started again, the operational status changes to up

- Node and the port on which the LIF resides

If data for a field is not available (for example, if there is no extended status information), the field value is listed as –.

### **Step**

Display LIF information by using the network interface show command.

You can view detailed information for each LIF by specifying the -instance parameter, or get specific information by specifying field names using the -fields parameter.

The following command displays general information about all LIFs in a cluster:

network interface show

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Is Port
Home					
example	lif1	up/up	192.0.2.129/22	node-01	e0d
false node	cluster_mgmt	up/up	192.0.2.3/20	node-02	e0c
false node-01	clus1	up/up	192.0.2.65/18	node-01	e0a
true	clus2	up/up	192.0.2.66/18	node-01	e0b
true	mgmt1	up/up	192.0.2.1/20	node-01	e0c
true node-02	clus1	up/up	192.0.2.67/18	node-02	e0a
true	clus2	up/up	192.0.2.68/18	node-02	e0b
true	mgmt2	up/up	192.0.2.2/20	node-02	e0d
true vs1	d1	up/up	192.0.2.130/21	node-01	e0d
false	d2	up/up	192.0.2.131/21	node-01	e0d
true	data3	up/up	192.0.2.132/20	node-02	e0c
true					

The following command shows detailed information about a single LIF:

```
network interface show -lif data1 -instance

      Vserver Name: vs1
Logical Interface Name: data1
      Role: data
      Data Protocol: nfs,cifs
      Home Node: node-01
      Home Port: e0c
      Current Node: node-03
      Current Port: e0c
Operational Status: up
Extended Status: -
      Is Home: false
      Network Address: 192.0.2.128
      Netmask: 255.255.192.0
Bits in the Netmask: 18
      IPv4 Link Local: -
      Subnet Name: -
Administrative Status: up
      Failover Policy: local-only
      Firewall Policy: data
      Auto Revert: false
Fully Qualified DNS Zone Name: xxx.example.com
DNS Query Listen Enable: false
      Failover Group Name: Default
      FCP WWPN: -
      Address family: ipv4
      Comment: -
      IPspace of LIF: Default
```

## Display routing information

You can display information about routes within an SVM.

### Step

Depending on the type of routing information that you want to view, enter the applicable command:

To view information about...	Enter...
Static routes, per SVM	<code>network route show</code>
LIFs on each route, per SVM	<code>network route show-lifs</code>

You can display detailed information for each route by specifying the `-instance` parameter. The following

command displays the static routes within the SVMs in cluster- 1:

```
network route show
Vserver          Destination      Gateway          Metric
-----
Cluster
cluster-1        0.0.0.0/0       10.63.0.1        10
vs1               0.0.0.0/0       198.51.9.1       10
vs3               0.0.0.0/0       192.0.2.1        20
vs3               0.0.0.0/0       192.0.2.1        20
```

The following command displays the association of static routes and logical interfaces (LIFs) within all SVMs in cluster-1:

```
network route show-lifs
Vserver: Cluster
Destination      Gateway          Logical Interfaces
-----
0.0.0.0/0        10.63.0.1        -

Vserver: cluster-1
Destination      Gateway          Logical Interfaces
-----
0.0.0.0/0        198.51.9.1       cluster_mgmt,
cluster-1_mgmt1,

Vserver: vs1
Destination      Gateway          Logical Interfaces
-----
0.0.0.0/0        192.0.2.1        data1_1, data1_2

Vserver: vs3
Destination      Gateway          Logical Interfaces
-----
0.0.0.0/0        192.0.2.1        data2_1, data2_2
```

### Display DNS host table entries (cluster administrators only)

The DNS host table entries map host names to IP addresses. You can display the host names and alias names and the IP address that they map to for all SVMs in a cluster.

#### Step



Display the host name entries for all SVMs by using the `vserver services name-service dns hosts show` command.

The following example displays the host table entries:

```
vserver services name-service dns hosts show
Vserver      Address          Hostname         Aliases
-----
cluster-1
            10.72.219.36    lnx219-36       -
vs1
            10.72.219.37    lnx219-37       lnx219-37.example.com
```

You can use the `vserver services name-service dns` command to enable DNS on an SVM, and configure it to use DNS for host-name resolution. Host names are resolved using external DNS servers.

### Display DNS domain configurations

You can display the DNS domain configuration of one or more storage virtual machines (SVMs) in your cluster to verify that it is configured properly.

#### Step

Viewing the DNS domain configurations by using the `vserver services name-service dns show` command.

The following command displays the DNS configurations for all SVMs in the cluster:

```
vserver services name-service dns show
Vserver      State    Domains          Name Servers
-----
cluster-1    enabled  xyz.company.com  192.56.0.129,
192.56.0.130
vs1          enabled  xyz.company.com  192.56.0.129,
192.56.0.130
vs2          enabled  xyz.company.com  192.56.0.129,
192.56.0.130
vs3          enabled  xyz.company.com  192.56.0.129,
192.56.0.130
```

The following command displays detailed DNS configuration information for SVM vs1:

```
vserver services name-service dns show -vserver vs1
      Vserver: vs1
      Domains: xyz.company.com
      Name Servers: 192.56.0.129, 192.56.0.130
      Enable/Disable DNS: enabled
      Timeout (secs): 2
      Maximum Attempts: 1
```

## Display information about failover groups

You can view information about failover groups, including the list of nodes and ports in each failover group, whether failover is enabled or disabled, and the type of failover policy that is being applied to each LIF.

### Steps

1. Display the target ports for each failover group by using the `network interface failover-groups show` command.

The following command displays information about all failover groups on a two-node cluster:

```
network interface failover-groups show
      Vserver      Group      Failover
      -----      -
      Cluster
      vs1          Cluster
                  cluster1-01:e0a, cluster1-01:e0b,
                  cluster1-02:e0a, cluster1-02:e0b
      vs1          Default
                  cluster1-01:e0c, cluster1-01:e0d,
                  cluster1-01:e0e, cluster1-02:e0c,
                  cluster1-02:e0d, cluster1-02:e0e
```

2. Display the target ports and broadcast domain for a specific failover group by using the `network interface failover-groups show` command.

The following command displays detailed information about failover group data12 for SVM vs4:

```
network interface failover-groups show -vserver vs4 -failover-group data12
```

```
Vserver Name: vs4
Failover Group Name: data12
Failover Targets: cluster1-01:e0f, cluster1-01:e0g, cluster1-02:e0f,
                  cluster1-02:e0g
Broadcast Domain: Default
```

3. Display the failover settings used by all LIFs by using the `network interface show` command.

The following command displays the failover policy and failover group that is being used by each LIF:

```
network interface show -vserver * -lif * -fields failover-
group,failover-policy
vserver    lif                failover-policy    failover-group
-----
Cluster    cluster1-01_clus_1 local-only          Cluster
Cluster    cluster1-01_clus_2 local-only          Cluster
Cluster    cluster1-02_clus_1 local-only          Cluster
Cluster    cluster1-02_clus_2 local-only          Cluster
cluster1   cluster_mgmt       broadcast-domain-wide Default
cluster1   cluster1-01_mgmt1 local-only          Default
cluster1   cluster1-02_mgmt1 local-only          Default
vs1        data1              disabled           Default
vs3        data2              system-defined     group2
```

### Display LIF failover targets

You might have to check whether the failover policies and the failover groups of a LIF are configured correctly. To prevent misconfiguration of the failover rules, you can display the failover targets for a single LIF or for all LIFs.

#### About this task

Displaying LIF failover targets enables you to check for the following:

- Whether the LIFs are configured with the correct failover group and failover policy
- Whether the resulting list of failover target ports is appropriate for each LIF
- Whether the failover target of a data LIF is not a management port (e0M)

#### Step

Display the failover targets of a LIF by using the `failover` option of the `network interface show` command.

The following command displays information about the failover targets for all LIFs in a two-node cluster. The

Failover Targets row shows the (prioritized) list of node-port combinations for a given LIF.

```

network interface show -failover
      Logical      Home           Failover      Failover
Vserver Interface   Node:Port     Policy        Group
-----
Cluster
      node1_clus1  node1:e0a    local-only    Cluster
      Failover Targets: node1:e0a,
                        node1:e0b
      node1_clus2  node1:e0b    local-only    Cluster
      Failover Targets: node1:e0b,
                        node1:e0a
      node2_clus1  node2:e0a    local-only    Cluster
      Failover Targets: node2:e0a,
                        node2:e0b
      node2_clus2  node2:e0b    local-only    Cluster
      Failover Targets: node2:e0b,
                        node2:e0a
cluster1
      cluster_mgmt node1:e0c    broadcast-domain-wide
                        Failover Targets: node1:e0c,
                        node1:e0d,
                        node2:e0c,
                        node2:e0d
                        node1_mgmt1  node1:e0c    local-only    Default
                        Failover Targets: node1:e0c,
                        node1:e0d
                        node2_mgmt1  node2:e0c    local-only    Default
                        Failover Targets: node2:e0c,
                        node2:e0d
vs1
      data1        node1:e0e    system-defined bcast1
      Failover Targets: node1:e0e,
                        node1:e0f,
                        node2:e0e,
                        node2:e0f

```

### Display LIFs in a load balancing zone

You can verify whether a load balancing zone is configured correctly by displaying all of the LIFs that belong to it. You can also view the load balancing zone of a particular LIF, or the load balancing zones for all LIFs.

#### Step

Display the LIFs and load balancing details that you want by using one of the following commands

To display...	Enter...
LIFs in a particular load balancing zone	<pre>network interface show -dns-zone zone_name</pre> <p>zone_name specifies the name of the load balancing zone.</p>
The load balancing zone of a particular LIF	<pre>network interface show -lif lif_name -fields dns-zone</pre>
The load balancing zones of all LIFs	<pre>network interface show -fields dns-zone</pre>

### Examples of displaying load balancing zones for LIFs

The following command displays the details of all LIFs in the load balancing zone storage.company.com for SVM vs0:

```
net int show -vserver vs0 -dns-zone storage.company.com
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
vs0	lif3	up/up	10.98.226.225/20	ndeux-11	e0c	true
	lif4	up/up	10.98.224.23/20	ndeux-21	e0c	true
	lif5	up/up	10.98.239.65/20	ndeux-11	e0c	true
	lif6	up/up	10.98.239.66/20	ndeux-11	e0c	true
	lif7	up/up	10.98.239.63/20	ndeux-21	e0c	true
	lif8	up/up	10.98.239.64/20	ndeux-21	e0c	true

The following command displays the DNS zone details of the LIF data3:

```
network interface show -lif data3 -fields dns-zone
```

Vserver	lif	dns-zone
vs0	data3	storage.company.com

The following command displays the list of all LIFs in the cluster and their corresponding DNS zones:

```

network interface show -fields dns-zone
Vserver      lif          dns-zone
-----      -
cluster      cluster_mgmt none
ndeux-21     clus1       none
ndeux-21     clus2       none
ndeux-21     mgmt1       none
vs0          data1       storage.company.com
vs0          data2       storage.company.com

```

## Display cluster connections

You can display all the active connections in the cluster or a count of active connections on the node by client, logical interface, protocol, or service. You can also display all the listening connections in the cluster.

### Display active connections by client (cluster administrators only)

You can view the active connections by client to verify the node that a specific client is using and to view possible imbalances between client counts per node.

### About this task

The count of active connections by client is useful in the following scenarios:

- Finding a busy or overloaded node.
- Determining why a particular client's access to a volume is slow.

You can view details about the node that the client is accessing and then compare it with the node on which the volume resides. If accessing the volume requires traversing the cluster network, clients might experience decreased performance because of the remote access to the volume on an oversubscribed remote node.

- Verifying that all nodes are being used equally for data access.
- Finding clients that have an unexpectedly high number of connections.
- Verifying whether certain clients have connections to a node.

### Step

Display a count of the active connections by client on a node by using the `network connections active show-clients` command.

For more information about this command, see the man page: [ONTAP 9 commands](#)

```

network connections active show-clients
Node      Vserver Name      Client IP Address      Count
-----
node0     vs0                192.0.2.253            1
          vs0                192.0.2.252            2
          Cluster          192.10.2.124           5
node1     vs0                192.0.2.250            1
          vs0                192.0.2.252            3
          Cluster          192.10.2.123           4
node2     vs1                customer.example.com    1
          vs1                192.0.2.245            3
          Cluster          192.10.2.122           4
node3     vs1                customer.example.org    1
          vs1                customer.example.net    3
          Cluster          192.10.2.121           4

```

### Display active connections by protocol (cluster administrators only)

You can display a count of the active connections by protocol (TCP or UDP) on a node to compare the usage of protocols within the cluster.

#### About this task

The count of active connections by protocol is useful in the following scenarios:

- Finding the UDP clients that are losing their connection.  
If a node is near its connection limit, UDP clients are the first to be dropped.
- Verifying that no other protocols are being used.

#### Step

Display a count of the active connections by protocol on a node by using the `network connections active show-protocols` command.

For more information about this command, see the man page.

```

network connections active show-protocols
Node      Vserver Name  Protocol  Count
-----
node0
          vs0         UDP        19
          Cluster    TCP        11
node1
          vs0         UDP        17
          Cluster    TCP         8
node2
          vs1         UDP        14
          Cluster    TCP        10
node3
          vs1         UDP        18
          Cluster    TCP         4

```

### Display active connections by service (cluster administrators only)

You can display a count of the active connections by service type (for example, by NFS, SMB, mount, and so on) for each node in a cluster. This is useful to compare the usage of services within the cluster, which helps to determine the primary workload of a node.

#### About this task

The count of active connections by service is useful in the following scenarios:

- Verifying that all nodes are being used for the appropriate services and that the load balancing for that service is working.
- Verifying that no other services are being used. Display a count of the active connections by service on a node by using the `network connections active show-services` command.

For more information about this command, see the man page: [ONTAP 9 commands](#)



```

network connections active show-services
Node      Vserver Name      Service      Count
-----
node0
    vs0          mount           3
    vs0          nfs             14
    vs0          nlm_v4         4
    vs0          cifs_srv       3
    vs0          port_map       18
    vs0          rclopcp        27
    Cluster     ctlopcp        60
node1
    vs0          cifs_srv       3
    vs0          rclopcp        16
    Cluster     ctlopcp        60
node2
    vs1          rclopcp        13
    Cluster     ctlopcp        60
node3
    vs1          cifs_srv       1
    vs1          rclopcp        17
    Cluster     ctlopcp        60

```

### Display active connections by LIF on a node and SVM

You can display a count of active connections for each LIF, by node and storage virtual machine (SVM), to view connection imbalances between LIFs within the cluster.

#### About this task

The count of active connections by LIF is useful in the following scenarios:

- Finding an overloaded LIF by comparing the number of connections on each LIF.
- Verifying that DNS load balancing is working for all data LIFs.
- Comparing the number of connections to the various SVMs to find the SVMs that are used the most.

#### Step

Display a count of active connections for each LIF by SVM and node by using the `network connections active show-lifs` command.

For more information about this command, see the man page: [ONTAP 9 commands](#)

```

network connections active show-lifs
Node      Vserver Name  Interface Name  Count
-----
node0
    vs0        datalif1       3
    Cluster    node0_clus_1   6
    Cluster    node0_clus_2   5
node1
    vs0        datalif2       3
    Cluster    node1_clus_1   3
    Cluster    node1_clus_2   5
node2
    vs1        datalif2       1
    Cluster    node2_clus_1   5
    Cluster    node2_clus_2   3
node3
    vs1        datalif1       1
    Cluster    node3_clus_1   2
    Cluster    node3_clus_2   2

```

### Display active connections in a cluster

You can display information about the active connections in a cluster to view the LIF, port, remote host, service, storage virtual machines (SVMs), and protocol used by individual connections.

#### About this task

Viewing the active connections in a cluster is useful in the following scenarios:

- Verifying that individual clients are using the correct protocol and service on the correct node.
- If a client is having trouble accessing data using a certain combination of node, protocol, and service, you can use this command to find a similar client for configuration or packet trace comparison.

#### Step

Display the active connections in a cluster by using the `network connections active show` command.

For more information about this command, see the man page: [ONTAP 9 commands](#)

The following command shows the active connections on the node node1:

```

network connections active show -node node1
Vserver  Interface          Remote
Name     Name:Local Port      Host:Port           Protocol/Service
-----  -
Node: node1
Cluster  node1_clus_1:50297  192.0.2.253:7700   TCP/ctlopcp
Cluster  node1_clus_1:13387  192.0.2.253:7700   TCP/ctlopcp
Cluster  node1_clus_1:8340   192.0.2.252:7700   TCP/ctlopcp
Cluster  node1_clus_1:42766  192.0.2.252:7700   TCP/ctlopcp
Cluster  node1_clus_1:36119  192.0.2.250:7700   TCP/ctlopcp
vs1     data1:111           host1.aa.com:10741  UDP/port-map
vs3     data2:111           host1.aa.com:10741  UDP/port-map
vs1     data1:111           host1.aa.com:12017  UDP/port-map
vs3     data2:111           host1.aa.com:12017  UDP/port-map

```

The following command shows the active connections on SVM vs1:

```

network connections active show -vserver vs1
Vserver  Interface          Remote
Name     Name:Local Port      Host:Port           Protocol/Service
-----  -
Node: node1
vs1     data1:111           host1.aa.com:10741  UDP/port-map
vs1     data1:111           host1.aa.com:12017  UDP/port-map

```

### Display listening connections in a cluster

You can display information about the listening connections in a cluster to view the LIFs and ports that are accepting connections for a given protocol and service.

#### About this task

Viewing the listening connections in a cluster is useful in the following scenarios:

- Verifying that the desired protocol or service is listening on a LIF if client connections to that LIF fail consistently.
- Verifying that a UDP/rclopcp listener is opened at each cluster LIF if remote data access to a volume on one node through a LIF on another node fails.
- Verifying that a UDP/rclopcp listener is opened at each cluster LIF if SnapMirror transfers between two nodes in the same cluster fail.
- Verifying that a TCP/ctlopcp listener is opened at each intercluster LIF if SnapMirror transfers between two nodes in different clusters fail.

#### Step

Display the listening connections per node by using the `network connections listening show` command.

```

network connections listening show
Vserver Name      Interface Name:Local Port      Protocol/Service
-----
Node: node0
Cluster           node0_clus_1:7700             TCP/ctlopcp
vs1               data1:4049                    UDP/unknown
vs1               data1:111                      TCP/port-map
vs1               data1:111                      UDP/port-map
vs1               data1:4046                     TCP/sm
vs1               data1:4046                     UDP/sm
vs1               data1:4045                     TCP/nlm-v4
vs1               data1:4045                     UDP/nlm-v4
vs1               data1:2049                     TCP/nfs
vs1               data1:2049                     UDP/nfs
vs1               data1:635                      TCP/mount
vs1               data1:635                      UDP/mount
Cluster           node0_clus_2:7700             TCP/ctlopcp

```

### Commands for diagnosing network problems

You can diagnose problems on your network by using commands such as `ping`, `tracert`, `ndp`, and `tcpdump`. You can also use commands such as `ping6` and `tracert6` to diagnose IPv6 problems.

If you want to...	Enter this command...
Test whether the node can reach other hosts on your network	<code>network ping</code>
Test whether the node can reach other hosts on your IPv6 network	<code>network ping6</code>
Trace the route that the IPv4 packets take to a network node	<code>network tracert</code>
Trace the route that the IPv6 packets take to a network node	<code>network tracert6</code>
Manage the Neighbor Discovery Protocol (NDP)	<code>network ndp</code>
Display statistics about packets that are received and sent on a specified network interface or on all network interfaces	<code>run -node <i>node_name</i> ifstat</code> <b>Note:</b> This command is available from the nodeshell.
Display information about neighboring devices that are discovered from each node and port in the cluster, including the remote device type and device platform	<code>network device-discovery show</code>
View the CDP neighbors of the node (ONTAP supports only CDPv1 advertisements)	<code>run -node <i>node_name</i> cdpd show-neighbors</code> <b>Note:</b> This command is available from the nodeshell.

Trace the packets that are sent and received in the network	<pre>network tcpdump start -node <i>node-name</i>                         -port <i>port_name</i></pre> <p><b>Note:</b> This command is available from the nodeshell.</p>
Measure latency and throughput between intercluster or intracluster nodes	<pre>network test -path -source-node               <i>source_nodename local</i> -destination               -cluster <i>destination_clustername</i>               -destination-node <i>destination_nodename</i>               -session-type <i>Default, AsyncMirrorLocal,</i>               <i>AsyncMirrorRemote, SyncMirrorRemote,</i>               <i>RemoteDataTransfer</i></pre> <p>For more information, see the <a href="#">Performance management</a>.</p>

For more information about these commands, see the appropriate man pages: [ONTAP 9 commands](#)

### Display network connectivity with neighbor discovery protocols

In a data center, you can use neighbor discovery protocols to view network connectivity between a pair of physical or virtual systems and their network interfaces. ONTAP supports two neighbor discovery protocols: Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP).

#### About this task

Neighbor discovery protocols enable you to automatically discover and view information about directly connected protocol-enabled devices in a network. Each device advertises identification, capabilities, and connectivity information. This information is transmitted in Ethernet frames to a multicast MAC address and is received by all neighboring protocol-enabled devices.

For two devices to become neighbors, each must have a protocol enabled and correctly configured. Discovery protocol functionality is limited to directly connected networks. Neighbors can include protocol-enabled devices such as switches, routers, bridges, and so on. ONTAP supports two neighbor discovery protocols, which can be used individually or together.

#### Cisco Discovery Protocol (CDP)

CDP is a proprietary link layer protocol developed by Cisco Systems. It is enabled by default in ONTAP for cluster ports, but must be enabled explicitly for data ports.

#### Link Layer Discovery Protocol (LLDP)

LLDP is a vendor-neutral protocol specified in the standards document IEEE 802.1AB. It must be enabled explicitly for all ports.

#### Use CDP to detect network connectivity

Using CDP to detect network connectivity consists of reviewing deployment considerations, enabling it on data ports, viewing neighbor devices, and adjusting CDP configuration values as needed. CDP is enabled by default on cluster ports.

CDP must also be enabled on any switches and routers before information about neighbor devices can be

displayed.

ONTAP release	Description
9.10.1 and earlier	CDP is also used by the cluster switch health monitor to automatically discover your cluster and management network switches.
9.11.1 and later	CDP is also used by the cluster switch health monitor to automatically discover your cluster, storage, and management network switches.

## Related information

[System administration](#)

## Considerations for using CDP

By default, CDP-compliant devices send CDPv2 advertisements. CDP-compliant devices send CDPv1 advertisements only when they receive CDPv1 advertisements. ONTAP supports only CDPv1. Therefore, when an ONTAP node sends CDPv1 advertisements, CDP-compliant neighboring devices send back CDPv1 advertisements.

You should consider the following information before enabling CDP on a node:

- CDP is supported for all ports.
- CDP advertisements are sent and received by ports that are in the up state.
- CDP must be enabled on both the transmitting and receiving devices for sending and receiving CDP advertisements.
- CDP advertisements are sent at regular intervals, and you can configure the time interval.
- When IP addresses are changed for a LIF, the node sends the updated information in the next CDP advertisement.
- ONTAP 9.10.1 and earlier:
  - CDP is always enabled on cluster ports.
  - CDP is disabled, by default, on all non-cluster ports.
- ONTAP 9.11.1 and later:
  - CDP is always enabled on cluster and storage ports.
  - CDP is disabled, by default, on all non-cluster and non-storage ports.



Sometimes when LIFs are changed on the node, the CDP information is not updated at the receiving device side (for example, a switch). If you encounter such a problem, you should configure the network interface of the node to the down status and then to the up status.

- Only IPv4 addresses are advertised in CDP advertisements.
- For physical network ports with VLANs, all of the LIFs configured on the VLANs on that port are advertised.
- For physical ports that are part of an interface group, all of the IP addresses configured on that interface group are advertised on each physical port.
- For an interface group that hosts VLANs, all of the LIFs configured on the interface group and the VLANs are advertised on each of the network ports.

- Due to CDP packets being restricted to no more than 1500 bytes, on ports configured with a large number of LIFs only a subset of these IP addresses may be reported on the adjacent switch.

## Enable or disable CDP

To discover and send advertisements to CDP-compliant neighboring devices, CDP must be enabled on each node of the cluster.

By default in ONTAP 9.10.1 and earlier, CDP is enabled on all cluster ports of a node and disabled on all non-cluster ports of a node.

By default in ONTAP 9.11.1 and later, CDP is enabled on all cluster and storage ports of a node and disabled on all non-cluster and non-storage ports of a node.

### About this task

The `cdpd.enable` option controls whether CDP is enabled or disabled on the ports of a node:

- For ONTAP 9.10.1 and earlier, on enables CDP on non-cluster ports.
- For ONTAP 9.11.1 and later, on enables CDP on non-cluster and non-storage ports.
- For ONTAP 9.10.1 and earlier, off disables CDP on non-cluster ports; you cannot disable CDP on cluster ports.
- For ONTAP 9.11.1 and later, off disables CDP on non-cluster and non-storage ports; you cannot disable CDP on cluster ports.

When CDP is disabled on a port that is connected to a CDP-compliant device, network traffic might not be optimized.

### Steps

1. Display the current CDP setting for a node, or for all nodes in a cluster:

To view the CDP setting of...	Enter...
A node	<code>run - node &lt;node_name&gt; options cdpd.enable</code>
All nodes in a cluster	<code>options cdpd.enable</code>

2. Enable or disable CDP on all ports of a node, or on all ports of all nodes in a cluster:

To enable or disable CDP on...	Enter...
A node	<code>run -node node_name options cdpd.enable {on or off}</code>
All nodes in a cluster	<code>options cdpd.enable {on or off}</code>

## View CDP neighbor information

You can view information about the neighboring devices that are connected to each port of the nodes of your cluster, provided that the port is connected to a CDP-compliant device. You can use the `network device-discovery show -protocol cdp` command to view neighbor information.

### About this task

In ONTAP 9.10.1 and earlier, because CDP is always enabled for cluster ports, CDP neighbor information is always displayed for those ports. CDP must be enabled on non-cluster ports for neighbor information to appear for those ports.

In ONTAP 9.11.1 and later, because CDP is always enabled for cluster and storage ports, CDP neighbor information is always displayed for those ports. CDP must be enabled on non-cluster and non-storage ports for neighbor information to appear for those ports.

### Step

Display information about all CDP-compliant devices that are connected to the ports on a node in the cluster:

```
network device-discovery show -node node -protocol cdp
```

The following command shows the neighbors that are connected to the ports on node `sti2650-212`:

```
network device-discovery show -node sti2650-212 -protocol cdp
Node/          Local   Discovered
Protocol       Port    Device (LLDP: ChassisID)  Interface      Platform
-----
sti2650-212/cdp
                e0M    RTP-LF810-510K37.gdl.eng.netapp.com (SAL1942R8JS)
                                Ethernet1/14    N9K-
C93120TX
                e0a    CS:RTP-CS01-510K35          0/8            CN1610
                e0b    CS:RTP-CS01-510K36          0/8            CN1610
                e0c    RTP-LF350-510K34.gdl.eng.netapp.com (FDO21521S76)
                                Ethernet1/21    N9K-
C93180YC-FX
                e0d    RTP-LF349-510K33.gdl.eng.netapp.com (FDO21521S4T)
                                Ethernet1/22    N9K-
C93180YC-FX
                e0e    RTP-LF349-510K33.gdl.eng.netapp.com (FDO21521S4T)
                                Ethernet1/23    N9K-
C93180YC-FX
                e0f    RTP-LF349-510K33.gdl.eng.netapp.com (FDO21521S4T)
                                Ethernet1/24    N9K-
C93180YC-FX
```

The output lists the Cisco devices that are connected to each port of the specified node.



## Configure the hold time for CDP messages

Hold time is the period of time for which CDP advertisements are stored in cache in neighboring CDP-compliant devices. Hold time is advertised in each CDPv1 packet and is updated whenever a CDPv1 packet is received by a node.

- The value of the `cdpd.holdtime` option should be set to the same value on both nodes of an HA pair.
- The default hold time value is 180 seconds, but you can enter values ranging from 10 seconds to 255 seconds.
- If an IP address is removed before the hold time expires, the CDP information is cached until the hold time expires.

### Steps

1. Display the current CDP hold time for a node, or for all nodes in a cluster:

To view the hold time of...	Enter...
A node	<code>run -node node_name options cdpd.holdtime</code>
All nodes in a cluster	<code>options cdpd.holdtime</code>

2. Configure the CDP hold time on all ports of a node, or on all ports of all nodes in a cluster:

To set the hold time on...	Enter...
A node	<code>run -node node_name options cdpd.holdtime holdtime</code>
All nodes in a cluster	<code>options cdpd.holdtime holdtime</code>

## Set the interval for sending CDP advertisements

CDP advertisements are sent to CDP neighbors at periodic intervals. You can increase or decrease the interval for sending CDP advertisements depending on network traffic and changes in the network topology.

- The value of the `cdpd.interval` option should be set to the same value on both nodes of an HA pair.
- The default interval is 60 seconds, but you can enter a value from 5 seconds to 900 seconds.

### Steps

1. Display the current CDP advertisement time interval for a node, or for all nodes in a cluster:

To view the interval for...	Enter...
A node	<code>run -node node_name options cdpd.interval</code>
All nodes in a cluster	<code>options cdpd.interval</code>

2. Configure the interval for sending CDP advertisements for all ports of a node, or for all ports of all nodes in a cluster:

To set the interval for...	Enter...
A node	<code>run -node node_name options cdpd.interval interval</code>
All nodes in a cluster	<code>options cdpd.interval interval</code>

## View or clear CDP statistics

You can view the CDP statistics for the cluster and non-cluster ports on each node to detect potential network connectivity issues. CDP statistics are cumulative from the time they were last cleared.

### About this task

In ONTAP 9.10.1 and earlier, because CDP is always enabled for ports, CDP statistics are always displayed for traffic on those ports. CDP must be enabled on ports for statistics to appear for those ports.

In ONTAP 9.11.1 and later, because CDP is always enabled for cluster and storage ports, CDP statistics are always displayed for traffic on those ports. CDP must be enabled on non-cluster or non-storage ports for statistics to appear for those ports.

### Step

Display or clear the current CDP statistics for all ports on a node:

If you want to...	Enter...
View the CDP statistics	<code>run -node node_name cdpd show-stats</code>
Clear the CDP statistics	<code>run -node node_name cdpd zero-stats</code>

## Example of showing and clearing statistics

The following command shows the CDP statistics before they are cleared. The output displays the total number of packets that have been sent and received since the last time the statistics were cleared.

```
run -node node1 cdpd show-stats

RECEIVE
Packets:          9116 | Csum Errors:      0 | Unsupported Vers: 4561
Invalid length:   0   | Malformed:        0 | Mem alloc fails:   0
Missing TLVs:     0   | Cache overflow:   0 | Other errors:      0

TRANSMIT
Packets:          4557 | Xmit fails:       0 | No hostname:       0
Packet truncated: 0   | Mem alloc fails:  0 | Other errors:      0

OTHER
Init failures:    0
```

The following command clears the CDP statistics:

```
run -node node1 cdpd zero-stats
```

```
run -node node1 cdpd show-stats
```

#### RECEIVE

Packets:	0		Csum Errors:	0		Unsupported Vers:	0
Invalid length:	0		Malformed:	0		Mem alloc fails:	0
Missing TLVs:	0		Cache overflow:	0		Other errors:	0

#### TRANSMIT

Packets:	0		Xmit fails:	0		No hostname:	0
Packet truncated:	0		Mem alloc fails:	0		Other errors:	0

#### OTHER

Init failures:	0
----------------	---

After the statistics are cleared, they begin to accumulate after the next CDP advertisement is sent or received.

### Use LLDP to detect network connectivity

Using LLDP to detect network connectivity consists of reviewing deployment considerations, enabling it on all ports, viewing neighbor devices, and adjusting LLDP configuration values as needed.

LLDP must also be enabled on any switches and routers before information about neighbor devices can be displayed.

ONTAP currently reports the following type-length-value structures (TLVs):

- Chassis ID
- Port ID
- Time-To-Live (TTL)
- System name

The system name TLV is not sent on CNA devices.

Certain converged network adapters (CNAs), such as the X1143 adapter and the UTA2 onboard ports, contain offload support for LLDP:

- LLDP offload is used for Data Center Bridging (DCB).
- Displayed information might differ between the cluster and the switch.

The Chassis ID and Port ID data displayed by the switch might be different for CNA and non-CNA ports.

For example:

- For non-CNA ports:
  - Chassis ID is a fixed MAC address of one of the ports on the node
  - Port ID is the port name of the respective port on the node
- For CNA ports:
  - Chassis ID and Port ID are the MAC addresses of the respective ports on the node.

However, the data displayed by the cluster is consistent for these port types.



The LLDP specification defines access to the collected information through an SNMP MIB. However, ONTAP does not currently support the LLDP MIB.

## Enable or disable LLDP

To discover and send advertisements to LLDP-compliant neighboring devices, LLDP must be enabled on each node of the cluster. Beginning with ONTAP 9.7, LLDP is enabled on all ports of a node by default.

### About this task

For ONTAP 9.10.1 and earlier, the `lldp.enable` option controls whether LLDP is enabled or disabled on the ports of a node:

- `on` enables LLDP on all ports.
- `off` disables LLDP on all ports.

For ONTAP 9.11.1 and later, the `lldp.enable` option controls whether LLDP is enabled or disabled on the non-cluster and non-storage ports of a node:

- `on` enables LLDP on all non-cluster and non-storage ports.
- `off` disables LLDP on all non-cluster and non-storage ports.

### Steps

1. Display the current LLDP setting for a node, or for all nodes in a cluster:
  - Single node: `run -node node_name options lldp.enable`
  - All nodes: `options lldp.enable`
2. Enable or disable LLDP on all ports of a node, or on all ports of all nodes in a cluster:

To enable or disable LLDP on...	Enter...
A node	<code>run -node node_name options lldp.enable {on off}</code>
All nodes in a cluster	<code>options lldp.enable {on off}</code>

- Single node:

```
run -node node_name options lldp.enable {on|off}
```

- All nodes:

```
options lldp.enable {on|off}
```

## View LLDP neighbor information

You can view information about the neighboring devices that are connected to each port of the nodes of your cluster, provided that the port is connected to an LLDP-compliant device. You use the network device-discovery show command to view neighbor information.

### Step

1. Display information about all LLDP-compliant devices that are connected to the ports on a node in the cluster:

```
network device-discovery show -node node -protocol lldp
```

The following command shows the neighbors that are connected to the ports on node cluster-1\_01. The output lists the LLDP-enabled devices that are connected to each port of the specified node. If the `-protocol` option is omitted, the output also lists CDP-enabled devices.

```
network device-discovery show -node cluster-1_01 -protocol lldp
Node/          Local   Discovered
Protocol       Port   Device                Interface           Platform
-----
cluster-1_01/lldp
                e2a    0013.c31e.5c60        GigabitEthernet1/36
                e2b    0013.c31e.5c60        GigabitEthernet1/35
                e2c    0013.c31e.5c60        GigabitEthernet1/34
                e2d    0013.c31e.5c60        GigabitEthernet1/33
```

## Adjust the interval for transmitting LLDP advertisements

LLDP advertisements are sent to LLDP neighbors at periodic intervals. You can increase or decrease the interval for sending LLDP advertisements depending on network traffic and changes in the network topology.

### About this task

The default interval recommended by IEEE is 30 seconds, but you can enter a value from 5 seconds to 300 seconds.

### Steps

1. Display the current LLDP advertisement time interval for a node, or for all nodes in a cluster:
  - Single node:

```
run -node <node_name> options lldp.xmit.interval
```

- All nodes:

```
options lldp.xmit.interval
```

2. Adjust the interval for sending LLDP advertisements for all ports of a node, or for all ports of all nodes in a cluster:

- Single node:

```
run -node <node_name> options lldp.xmit.interval <interval>
```

- All nodes:

```
options lldp.xmit.interval <interval>
```

## Adjust the time-to-live value for LLDP advertisements

Time-To-Live (TTL) is the period of time for which LLDP advertisements are stored in cache in neighboring LLDP-compliant devices. TTL is advertised in each LLDP packet and is updated whenever an LLDP packet is received by a node. TTL can be modified in outgoing LLDP frames.

### About this task

- TTL is a calculated value, the product of the transmit interval (`lldp.xmit.interval`) and the hold multiplier (`lldp.xmit.hold`) plus one.
- The default hold multiplier value is 4, but you can enter values ranging from 1 to 100.
- The default TTL is therefore 121 seconds, as recommended by IEEE, but by adjusting the transmit interval and hold multiplier values, you can specify a value for outgoing frames from 6 seconds to 30001 seconds.
- If an IP address is removed before the TTL expires, the LLDP information is cached until the TTL expires.

### Steps

1. Display the current hold multiplier value for a node, or for all nodes in a cluster:

- Single node:

```
run -node <node_name> options lldp.xmit.hold
```

- All nodes:

```
options lldp.xmit.hold
```

2. Adjust the hold multiplier value on all ports of a node, or on all ports of all nodes in a cluster:

- Single node:

```
run -node <node_name> options lldp.xmit.hold <hold_value>
```

- All nodes:

```
options lldp.xmit.hold <hold_value>
```

### View or clear LLDP statistics

You can view the LLDP statistics for the cluster and non-cluster ports on each node to detect potential network connectivity issues. LLDP statistics are cumulative from the time they were last cleared.

#### About this task

For ONTAP 9.10.1 and earlier, because LLDP is always enabled for cluster ports, LLDP statistics are always displayed for traffic on those ports. LLDP must be enabled on non-cluster ports for statistics to appear for those ports.

For ONTAP 9.11.1 and later, because LLDP is always enabled for cluster and storage ports, LLDP statistics are always displayed for traffic on those ports. LLDP must be enabled on non-cluster and non-storage ports for statistics to appear for those ports.

#### Step

Display or clear the current LLDP statistics for all ports on a node:

If you want to...	Enter...
View the LLDP statistics	<code>run -node node_name lldp stats</code>
Clear the LLDP statistics	<code>run -node node_name lldp stats -z</code>

### Show and clear statistics example

The following command shows the LLDP statistics before they are cleared. The output displays the total number of packets that have been sent and received since the last time the statistics were cleared.

```
cluster-1::> run -node vsim1 lldp stats
```

```
RECEIVE
```

```
  Total frames:      190k | Accepted frames:   190k | Total drops:
0
```

```
TRANSMIT
```

```
  Total frames:      5195 | Total failures:      0
```

```
OTHER
```

```
  Stored entries:      64
```

The following command clears the LLDP statistics.

```
cluster-1::> The following command clears the LLDP statistics:
```

```
run -node vsim1 lldp stats -z
```

```
run -node node1 lldp stats
```

```
RECEIVE
```

```
  Total frames:      0 | Accepted frames:      0 | Total drops:
0
```

```
TRANSMIT
```

```
  Total frames:      0 | Total failures:      0
```

```
OTHER
```

```
  Stored entries:      64
```

After the statistics are cleared, they begin to accumulate after the next LLDP advertisement is sent or received.



# NAS storage management

## Manage NAS protocols with System Manager

### NAS management overview with System Manager

The topics in this section show you how to configure and manage NAS environments with System Manager in ONTAP 9.7 and later releases.

If you are using the classic System Manager (available only in ONTAP 9.7 and earlier), see these topics:

- [NFS configuration overview](#)
- [SMB configuration overview](#)

System Manager supports workflows for:

- Initial configuration of clusters that you intend to use for NAS file services.
- Additional volume provisioning for changing storage needs.
- Configuration and maintenance for industry-standard authentication and security facilities.

Using System Manager, you can manage NAS services at the component level:

- Protocols – NFS, SMB, or both (NAS multiprotocol)
- Name services – DNS, LDAP, and NIS
- Name service switch
- Kerberos security
- Exports and shares
- Qtrees
- Name mapping of users and groups

### Provision NFS storage for VMware datastores

Before using Virtual Storage Console for VMware vSphere (VSC) to provision NFS volumes on an ONTAP based storage system for ESXi hosts, enable NFS using System Manager for ONTAP 9.7 or later.

After creating an [NFS-enabled storage VM](#) in System Manager, you then provision NFS volumes and manage datastores using VSC.

Beginning with VSC 7.0, VSC is part of the [ONTAP Tools for VMware vSphere virtual appliance](#), which includes VSC, vStorage APIs for Storage Awareness (VASA) Provider, and Storage Replication Adapter (SRA) for VMware vSphere capabilities.

Be sure to check the [NetApp Interoperability Matrix](#) to confirm compatibility between your current ONTAP and VSC releases.

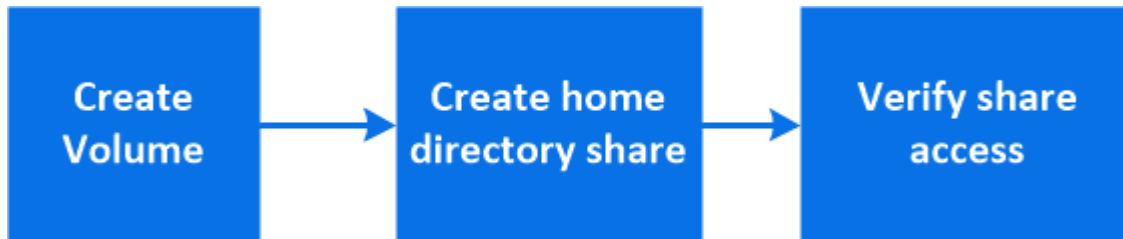
To set up NFS access for ESXi hosts to datastores using System Manager Classic (for ONTAP 9.7 and earlier releases), see [NFS configuration for ESXi using VSC overview](#)

For more information, see [TR-4597: VMware vSphere for ONTAP](#) and the documentation for your VSC release.

## Provision NAS storage for home directories

Create volumes to provide storage for home directories using the SMB protocol.

This procedure creates new volumes for home directories on an [existing SMB-enabled storage VM](#). You can accept systems defaults when configuring volumes or specify custom configurations.



You can create FlexVol volumes, or for large file systems with high performance requirements, you can create FlexGroup volumes. See also [Provision NAS storage for large file systems using FlexGroup volumes](#).

You can also save the specifications of this volume to an Ansible Playbook. For more details, go to [Use Ansible Playbooks to add or edit volumes or LUNs](#).

### Steps

1. Add a new volume in an SMB-enabled storage VM.
  - a. Click **Storage > Volumes** and then click **Add**.
  - b. Enter a name, select the storage VM, and enter a size.

Only storage VMs configured with the SMB protocol are listed. If only one storage VM configured with the SMB protocol is available, the **Storage VM** field is not shown.

- If you click **Save** at this point, System Manager uses system defaults to create and add a FlexVol volume.
- You can click **More options** to customize the configuration of the volume to enable services such as authorization, quality of service, and data protection. Refer to [Customize the volume configuration](#), then return here to complete the following steps.

2. Click **Storage > Shares**, click **Add**, and select **Home Directory**.
3. On a Windows client, do the following to verify that the share is accessible.

- a. In Windows Explorer, map a drive to the share in the following format:

```
\\_SMB_Server_Name__Share_Name_
```

If the share name was created with variables (%w, %d, or %u), be sure to test access with a resolved name.

- b. On the newly created drive, create a test file, and then delete the file.

### Customize the volume configuration

You can customize the volume configuration when you add volumes instead of accepting the system defaults.

## Procedure

After clicking **More options**, select the functionality you need and enter the required values.

- Cache for remote volume.
- Performance service level (quality of service, QoS).

Beginning with ONTAP 9.8, you can specify a Custom QoS policy or disable QoS, in addition to the default Value selection.

- To disable QoS, select **Custom, Existing**, then **none**.
- If you select **Custom** and specify an existing service level, a local tier is automatically chosen.
- Beginning with ONTAP 9.9.1, if you choose to create a custom performance service level, you can use System Manager to manually select the local tier (**Manual placement**) on which you want to place the volume you are creating.

This option is not available if you select the remote cache or FlexGroup volume options.

- FlexGroup volumes (select **Distribute volume data across the cluster**).

This option is not available if you previously selected **Manual placement** under **Performance Service Level**. Otherwise, the volume you are adding becomes a FlexVol volume by default.

- Access permissions for the protocols for which the volume is configured.
- Data protection with SnapMirror (local or remote), then specify the protection policy and settings for the destination cluster from the pull-down lists.
- Click **Save** to create the volume and add it to the cluster and storage VM.



After you save the volume, return to [Step 2 in the workflow](#) to complete provisioning for home directories.

## Provision NAS storage for Linux servers using NFS

Create volumes to provide storage for Linux servers using the NFS protocol with ONTAP System Manager (9.7 and later).

This procedure creates new volumes on an [existing NFS-enabled storage VM](#). You can accept system defaults when configuring volumes or specify custom configurations.

You can create FlexVol volumes, or for large file systems with high performance requirements, you can create FlexGroup volumes. See also [Provision NAS storage for large file systems using FlexGroup volumes](#).

You can also save the specifications of this volume to an Ansible Playbook. For more details, go to [Use Ansible Playbooks to add or edit volumes or LUNs](#).

If you want details about the range of ONTAP NFS protocol capabilities, consult the [NFS reference overview](#).

### Steps

1. Add a new volume in an NFS-enabled storage VM.
  - a. Click **Storage > Volumes** and then click **Add**.
  - b. Enter a name, select the storage VM, and enter a size.

Only storage VMs configured with the NFS protocol are listed. If only one storage VM configured with the SMB protocol is available, the **Storage VM** field is not shown.

- If you click **Save** at this point, System Manager uses system defaults to create and add a FlexVol volume.



The default export policy grants full access to all users.

- You can click **More options** to customize the configuration of the volume to enable services such as authorization, quality of service, and data protection. Refer to [Customize the volume configuration](#), then return here to complete the following steps.

2. On a Linux client, do the following to verify access.

- a. Create and mount the volume using the network interface of the storage VM.
- b. On the newly mounted volume, create a test file, write text to it, and then delete the file.

After verifying access, you can [restrict client access with the volume's export policy](#) and set any desired UNIX ownership and permissions on the mounted volume.

## Customize the volume configuration

You can customize the volume configuration when you add volumes instead of accepting the system defaults.

### Procedure

After clicking **More options**, select the functionality you need and enter the required values.

- Cache for remote volume.
- Performance service level (quality of service, QoS).

Beginning with ONTAP 9.8, you can specify a Custom QoS policy or disable QoS, in addition to the default Value selection.

- To disable QoS, select **Custom, Existing**, then **none**.
- If you select **Custom** and specify an existing service level, a local tier is automatically chosen.
- Beginning with ONTAP 9.9.1, if you choose to create a custom performance service level, you can use System Manager to manually select the local tier (**Manual placement**) on which you want to place the volume you are creating.

This option is not available if you select the remote cache or FlexGroup volume options.

- FlexGroup volumes (select **Distribute volume data across the cluster**).

This option is not available if you previously selected **Manual placement** under **Performance Service Level**. Otherwise, the volume you are adding becomes a FlexVol volume by default.

- Access permissions for the protocols for which the volume is configured.
- Data protection with SnapMirror (local or remote), then specify the protection policy and settings for the destination cluster from the pull-down lists.
- Click **Save** to create the volume and add it to the cluster and storage VM.



After you save the volume, return to [Step 2 in the workflow](#) to complete provisioning for Linux servers using NFS.

### Other ways to do this in ONTAP

To perform this task with...	Refer to...
System Manager Classic (ONTAP 9.7 and earlier)	<a href="#">NFS configuration overview</a>
The ONTAP command line interface (CLI)	<a href="#">NFS configuration overview with the CLI</a>

## Manage access using export policies

Enable Linux client access to NFS servers by using export policies.

This procedure creates or modifies export policies for an [existing NFS-enabled storage VM](#).

### Steps

1. In System Manager, Click **Storage > Volumes**.
2. Click an NFS-enabled volume and click **More**.
3. Click **Edit Export Policy** and then click **Select an existing policy** or **Add a new policy**.

## Provision NAS storage for Windows servers using SMB

Create volumes to provide storage for Windows servers using the SMB protocol using System Manager, which is available with ONTAP 9.7 and later.

This procedure creates new volumes on an [existing SMB-enabled storage VM](#) and creates a share for the volume root (/) directory. You can accept systems defaults when configuring volumes or specify custom configurations. After initial SMB configuration, you can also create additional shares and modify their properties.

You can create FlexVol volumes, or for large file systems with high performance requirements, you can create FlexGroup volumes. See also [Provision NAS storage for large file systems using FlexGroup volumes](#).

You can also save the specifications of this volume to an Ansible Playbook. For more details, go to [Use Ansible Playbooks to add or edit volumes or LUNs](#).

If you want details about the range of ONTAP SMB protocol capabilities, consult the [SMB reference overview](#).

### Steps

1. Add a new volume in an SMB-enabled storage VM.
  - a. Click **Storage > Volumes** and then click **Add**.
  - b. Enter a name, select the storage VM, and enter a size.

Only storage VMs configured with the SMB protocol are listed. If only one storage VM configured with the SMB protocol is available, the **Storage VM** field is not shown.

- If you click **Save** at this point, System Manager uses system defaults to create and add a FlexVol volume.

- You can click **More options** to customize the configuration of the volume to enable services such as authorization, quality of service, and data protection. Refer to [Customize the volume configuration](#), then return here to complete the following steps.
2. Switch to a Windows client to verify that the share is accessible.
    - a. In Windows Explorer, map a drive to the share in the following format:  
`\\_SMB_Server_Name__Share_Name_`
    - b. On the newly created drive, create a test file, write text to it, and then delete the file.

After verifying access, you can restrict client access with the share ACL and set any desired security properties on the mapped drive. See [Create an SMB share](#) for more information.

## Add or modify shares

You can add additional shares after initial SMB configuration. Shares are created with default values and properties you select. These can be modified later.

You can set the following share properties when configuring a share:

- Access permissions
- Share properties
  - Enable continuous availability to shares that contain Hyper-V and SQL Server over SMB data (beginning with ONTAP 9.10.1). See also:
    - [Continuously available share requirements for Hyper-V over SMB](#)
    - [Continuously available share requirements for SQL Server over SMB](#)
  - Encrypt data with SMB 3.0 while accessing this share.

After initial configuration, you can also modify these properties:

- Symbolic links
  - Enable or disable symlinks and widelinks
- Share properties
  - Allow clients to access Snapshot copies directory.
  - Enable oplocks, allowing clients to lock files and cache content locally (default).
  - Enable access-based enumeration (ABE) to display shared resources based on the access permissions of the user.

## Procedures

To add a new share in an SMB-enabled volume, click **Storage > Shares**, click **Add**, and select **Share**.

To modify an existing share, click **Storage > Shares**, then click the  and select **Edit**.

## Customize the volume configuration

You can customize the volume configuration when you add volumes instead of accepting the system defaults.

### Procedure

After clicking **More options**, select the functionality you need and enter the required values.

- Cache for remote volume.
- Performance service level (quality of service, QoS).

Beginning with ONTAP 9.8 you can specify a Custom QoS policy or disable QoS, in addition to the default value selection.

- To disable QoS, select **Custom, Existing**, then **none**.
- If you select **Custom** and specify an existing service level, a local tier is automatically chosen.
- Beginning with ONTAP 9.9.1, if you choose to create a custom performance service level, you can use System Manager to manually select the local tier (**Manual placement**) on which you want to place the volume you are creating.

This option is not available if you select the remote cache or FlexGroup volume options.

- FlexGroup volumes (select **Distribute volume data across the cluster**).

This option is not available if you previously selected **Manual placement** under **Performance Service Level**. Otherwise, the volume you are adding becomes a FlexVol volume by default.

**This option is not available if you previously selected \*Manual placement** under **Performance Service Level**. Otherwise, the volume you are adding becomes a FlexVol volume by default.

**Access permission for the protocols for which the volume is configured.**

**\*Data protection with SnapMirror (local or remote), then specify the protection policy and settings for the destination cluster from the pull-down lists.**

**\*Click \*Save** to create the volume and add it to the cluster and storage VM.

You can customize the volume configuration when you add volumes instead of accepting the system defaults.

### Procedure

After clicking **More options**, select the functionality you need and enter the required values.

- Cache for remote volume.
- Performance service level (quality of service, QoS).

Beginning with ONTAP 9.8, you can specify a Custom QoS policy or disable QoS, in addition to the default Value selection.

- To disable QoS, select **Custom, Existing**, then **none**.
- If you select **Custom** and specify an existing service level, a local tier is automatically chosen.
- Beginning with ONTAP 9.9.1, if you choose to create a custom performance service level, you can use System Manager to manually select the local tier (**Manual placement**) on which you want to place the volume you are creating.

This option is not available if you select the remote cache or FlexGroup volume options.

- FlexGroup volumes (select **Distribute volume data across the cluster**).

This option is not available if you previously selected **Manual placement** under **Performance Service Level**. Otherwise, the volume you are adding becomes a FlexVol volume by default.

- Access permissions for the protocols for which the volume is configured.

- Data protection with SnapMirror (local or remote), then specify the protection policy and settings for the destination cluster from the pull-down lists.
- Click **Save** to create the volume and add it to the cluster and storage VM.



After you save the volume, return to [Step 2 in the workflow](#) to complete provisioning for Windows servers using SMB.

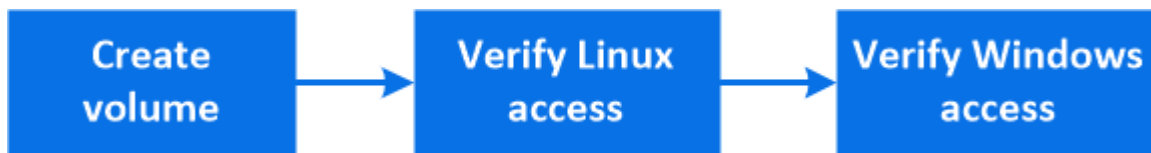
### Other ways to do this in ONTAP

To perform this task with...	Refer to...
System Manager Classic (ONTAP 9.7 and earlier)	<a href="#">SMB configuration overview</a>
The ONTAP command line interface	<a href="#">SMB configuration overview with the CLI</a>

## Provision NAS storage for both Windows and Linux using both NFS and SMB

Create volumes to provide storage for clients using either the NFS or SMB protocol.

This procedure creates new volumes on an [existing storage VM enabled for both NFS and SMB protocols](#).



You can create FlexVol volumes, or for large file systems with high performance requirements, you can create FlexGroup volumes. See also [Provision NAS storage for large file systems using FlexGroup volumes](#).

You can also save the specifications of this volume to an Ansible Playbook. For more details, go to [Use Ansible Playbooks to add or edit volumes or LUNs](#).

### Steps

1. Add a new volume in a storage VM enabled for both NFS and SMB.
  - a. Click **Storage > Volumes** and then click **Add**.
  - b. Enter a name, select the storage VM, and enter a size. Only storage VMs configured with both the NFS and SMB protocols are listed. If only one storage VM configured with the NFS and SMB protocols is available, the **Storage VM** field is not shown.
  - c. Click **More Options** and select **Share via NFS**.

The default setting grants full access to all users. You can add more restrictive rules to the export policy later.

- d. Select **Share via SMB**.

The share is created with a default Access Control List (ACL) set to "Full Control" for the **Everyone** group. You can add restrictions to the ACL later.

- e. If you click **Save** at this point, System Manager uses system defaults to create and add a FlexVol volume.

Alternatively, you can continue to enable any additional required services such as authorization, quality of



service, and data protection. Refer to [Customize the volume configuration](#), then return here to complete the following steps.

2. On a Linux client, verify that the export is accessible.
  - a. Create and mount the volume using the network interface of the storage VM.
  - b. On the newly mounted volume, create a test file, write text to it, and then delete the file.
3. On a Windows client, do the following to verify that the share is accessible.
  - a. In Windows Explorer, map a drive to the share in the following format:  
`\\_SMB_Server_Name__Share_Name_`
  - b. On the newly created drive, create a test file, write text to it, and then delete the file.

After verifying access, you can [restrict client access with the volume's export policy](#), [restrict client access with the share ACL](#), and set any desired ownership and permissions on the exported and shared volume.

## Customize the volume configuration

You can customize the volume configuration when you add volumes instead of accepting the system defaults.

### Procedure

After clicking **More options**, select the functionality you need and enter the required values.

- Cache for remote volume.
- Performance service level (quality of service, QoS).

Beginning with ONTAP 9.8, you can specify a Custom QoS policy or disable QoS, in addition to the default Value selection.

- To disable QoS, select **Custom, Existing**, then **none**.
- If you select **Custom** and specify an existing service level, a local tier is automatically chosen.
- Beginning with ONTAP 9.9.1, if you choose to create a custom performance service level, you can use System Manager to manually select the local tier (**Manual placement**) on which you want to place the volume you are creating.

This option is not available if you select the remote cache or FlexGroup volume options.

- FlexGroup volumes (select **Distribute volume data across the cluster**).

This option is not available if you previously selected **Manual placement** under **Performance Service Level**. Otherwise, the volume you are adding becomes a FlexVol volume by default.

- Access permissions for the protocols for which the volume is configured.
- Data protection with SnapMirror (local or remote), then specify the protection policy and settings for the destination cluster from the pull-down lists.
- Click **Save** to create the volume and add it to the cluster and storage VM.

After you save the volume, return to [Step 2 in the workflow](#) to complete multiprotocol provisioning for Windows and Linux servers.

## Other ways to do this in ONTAP

To perform these tasks with...	See this content...
System Manager Classic (ONTAP 9.7 and earlier)	<a href="#">SMB and NFS multiprotocol configuration overview</a>
The ONTAP command line interface	<a href="#">SMB configuration overview with the CLI</a> <a href="#">NFS configuration overview with the CLI</a> <a href="#">What the security styles and their effects are</a> <a href="#">Case-sensitivity of file and directory names in a multiprotocol environment</a>

## Secure client access with Kerberos

Enable Kerberos to secure storage access for NAS clients.

This procedure configures Kerberos on an existing storage VM enabled for [NFS](#) or [SMB](#).

Before beginning you should have configured DNS, NTP, and [LDAP](#) on the storage system.



### Steps

1. At the ONTAP command line, set UNIX permissions for the storage VM root volume.
  - a. Display the relevant permissions on the storage VM root volume: `volume show -volume root_vol_name-fields user,group,unix-permissions`

The root volume of the storage VM must have the following configuration:

Name...	Setting...
UID	root or ID 0
GID	root or ID 0
UNIX permissions	755

- b. If these values are not shown, use the `volume modify` command to update them.
2. Set user permissions for the storage VM root volume.
    - a. Display the local UNIX users: `vserver services name-service unix-user show -vserver vserver_name`

The storage VM should have the following UNIX users configured:

User name	User ID	Primary group ID
nfs	500	0
root	0	0

**Note:** The NFS user is not required if a Kerberos-UNIX name mapping exists for the SPN of the NFS

client user; see step 5.

b. If these values are not shown, use the `vserver services name-service unix-user modify` command to update them.

3. Set group permissions for the storage VM root volume.

a. Display the local UNIX groups: `vserver services name-service unix-group show -vserver vserver_name`

The storage VM should have the following UNIX groups configured:


Group name	Group ID
daemon	1
root	0

b. If these values are not shown, use the `vserver services name-service unix-group modify` command to update them.

4. Switch to System Manager to configure Kerberos

5. In System Manager, click **Storage > Storage VMs** and select the storage VM.

6. Click **Settings**.

7. Click  under Kerberos.

8. Click **Add** under Kerberos Realm, and complete the following sections:

- Add Kerberos Realm

Enter configuration details depending on KDC vendor.

- Add Network Interface to Realm

Click **Add** and select a network interface.

9. If desired, add mappings from Kerberos principal names to local user names.

a. Click **Storage > Storage VMs** and select the storage VM.

b. Click **Settings**, and then click  under **Name Mapping**.

c. Under **Kerberos to UNIX**, add patterns and replacements using regular expressions.

## Provide client access with name services



Enable ONTAP to look up host, user, group, or netgroup information using LDAP or NIS to authenticate NAS clients.

This procedure creates or modifies LDAP or NIS configurations on an existing storage VM enabled for [NFS](#) or [SMB](#).

For LDAP configurations, you should have the LDAP configuration details required in your environment and you should be using a default ONTAP LDAP schema.

### Steps

1. Configure the required service: click **Storage > Storage VMs**.

2. Select the storage VM, click **Settings**, and then click  for LDAP or NIS.
3. Include any changes in the name services switch: click  under Name Services Switch.

## Manage directories and files

Expand the System Manager volume display to view and delete directories and files.

Beginning with ONTAP 9.9.1, directories are deleted with low-latency fast directory delete functionality.

For more information about viewing file systems in ONTAP 9.9.1 and later, see [File System Analytics overview](#).

### Step

1. Click **Storage > Volumes**. Then expand a volume to view its contents.

## Manage host-specific users and groups with System Manager

Beginning with ONTAP 9.10.1, you can use System Manager to manage users and groups that are specific to a UNIX or Windows host.

You can perform the following procedures:

Windows	UNIX
<ul style="list-style-type: none"> <li>• <a href="#">View Windows users and groups</a></li> <li>• <a href="#">Add, edit, or delete a Windows group</a></li> <li>• <a href="#">Manage Windows Users</a></li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">View UNIX users and groups</a></li> <li>• <a href="#">Add, edit, or delete a UNIX group</a></li> <li>• <a href="#">Manage UNIX Users</a></li> </ul>



### View Windows users and groups

In System Manager, you can view a list of Windows users and groups.

#### Steps

1. In System Manager, click **Storage > Storage VMs**.
2. Select the storage VM, then select the **Settings** tab.
3. Scroll to the **Host Users and Groups** area.

The **Windows** section displays a summary of the number of users in each group associated with the selected storage VM.

4. Click  in the **Windows** section.
5. Click the **Groups** tab, then click  next to a group name to view details about that group.
6. To view the users in a group, select the group, then click the **Users** tab.

### Add, edit, or delete a Windows group

In System Manager, you can manage Windows groups by adding, editing, or deleting them.

#### Steps

1. In System Manager, view the list of Windows groups. Refer to [View Windows users and groups](#).
2. On the **Groups** tab, you can manage groups with the following tasks:

To perform this action...	Perform these steps...
Add a group	<ol style="list-style-type: none"> <li>1. Click <b>+ Add</b>.</li> <li>2. Enter the group information.</li> <li>3. Specify privileges.</li> <li>4. Specify group members (add local users, domain users, or domain groups).</li> </ol>
Edit a group	<ol style="list-style-type: none"> <li>1. Next to the group name, click <b>:</b>, then click <b>Edit</b>.</li> <li>2. Modify the group information.</li> </ol>
Delete a group	<ol style="list-style-type: none"> <li>1. Check the box next to the group or groups you want to delete.</li> <li>2. Click <b>Delete</b>.</li> </ol> <p><b>Note:</b> You can also delete a single group by clicking <b>:</b> next to the group name, then clicking <b>Delete</b>.</p>






## Manage Windows Users

In System Manager, you can manage Windows users by adding, editing, deleting, enabling, or disabling them. You can also change the password of a Windows user.

### Steps

1. In System Manager, view the list of users for the group. Refer to [View Windows users and groups](#).
2. On the **Users** tab, you can manage users with the following tasks:

To perform this action...	Perform these steps...
Add a user	<ol style="list-style-type: none"> <li>1. Click <b>+ Add</b>.</li> <li>2. Enter the user information.</li> </ol>
Edit a user	<ol style="list-style-type: none"> <li>1. Next to the user name, click <b>:</b>, then click <b>Edit</b>.</li> <li>2. Modify the user information.</li> </ol>

Delete a user	<ol style="list-style-type: none"> <li>1. Check the box next to the user or users you want to delete.</li> <li>2. Click  <b>Delete</b> .</li> </ol> <p><b>Note:</b> You can also delete a single user by clicking  next to the user name, then clicking <b>Delete</b>.</p>
Change user password	<ol style="list-style-type: none"> <li>1. Next to the user name, click , then click <b>Change Password</b>.</li> <li>2. Enter the new password and confirm it.</li> </ol>
Enable a user	<ol style="list-style-type: none"> <li>1. Check the box next to each disabled user you want to enable.</li> <li>2. Click  <b>Enable</b> .</li> </ol>
Disable a users	<ol style="list-style-type: none"> <li>1. Check the box next to each enabled user you want to disable.</li> <li>2. Click  <b>Disable</b> .</li> </ol>


## View UNIX users and groups

In System Manager, you can view a list of UNIX users and groups.

### Steps

1. In System Manager, click **Storage > Storage VMs**.
2. Select the storage VM, then select the **Settings** tab.
3. Scroll to the **Host Users and Groups** area.

The **UNIX** section displays a summary of the number of users in each group associated with the selected storage VM.

4. Click  in the **UNIX** section.
5. Click the **Groups** tab to view details about that group.
6. To view the users in a group, select the group, then click the **Users** tab.




## Add, edit, or delete a UNIX group

In System Manager, you can manage UNIX groups by adding, editing, or deleting them.

### Steps

1. In System Manager, view the list of UNIX groups. Refer to [View UNIX users and groups](#).
2. On the **Groups** tab, you can manage groups with the following tasks:

To perform this action...	Perform these steps...
---------------------------	------------------------




Add a group	<ol style="list-style-type: none"> <li>1. Click  <b>Add</b> .</li> <li>2. Enter the group information.</li> <li>3. (Optional) Specify associated users.</li> </ol>
Edit a group	<ol style="list-style-type: none"> <li>1. Select the group.</li> <li>2. Click  <b>Edit</b> .</li> <li>3. Modify the group information.</li> <li>4. (Optional) Add or remove users.</li> </ol>
Delete a group	<ol style="list-style-type: none"> <li>1. Select the group or groups you want to delete.</li> <li>2. Click  <b>Delete</b> .</li> </ol>

## Manage UNIX Users

In System Manager, you can manage Windows users by adding, editing, or deleting them.

### Steps

1. In System Manager, view the list of users for the group. Refer to [View UNIX users and groups](#).
2. On the **Users** tab, you can manage users with the following tasks:

To perform this action...	Perform these steps...
Add a user	<ol style="list-style-type: none"> <li>1. Click  <b>Add</b> .</li> <li>2. Enter the user information.</li> </ol>
Edit a user	<ol style="list-style-type: none"> <li>1. Select the user you want to edit.</li> <li>2. Click  <b>Edit</b> .</li> <li>3. Modify the user information.</li> </ol>
Delete a user	<ol style="list-style-type: none"> <li>1. Select the user or users you want to delete.</li> <li>2. Click  <b>Delete</b> .</li> </ol>

## Monitor NFS active clients

Beginning with ONTAP 9.8, System Manager shows which NFS client connections are active when NFS is licensed on a cluster.

This allows you to quickly verify which NFS clients are actively connect to a storage VM, which are connected but idle, and which are disconnected.

For each NFS client IP address, the **NFS Clients** display shows:

- \* Time of last access
- \* Network interface IP address
- \* NFS connection version

\* Storage VM name

In addition, a list of NFS clients active in the last 48 hours is also shown in the **Storage>Volumes** display and a count of NFS clients is included in the **Dashboard** display.

## Step

1. Display NFS client activity: Click **Hosts > NFS Clients**.

## Enable NAS storage





### Enable NAS storage for Linux servers using NFS

Create or modify storage VMs to enable NFS servers for serving data to Linux clients.


This procedure enables a new or existing storage VM for the NFS protocol. It is assumed that configuration details are available for any networking, authentication, or security services required in your environment.



## Steps

1. Enable NFS on a storage VM.
  - a. For new storage VMs: click **Storage > Storage VMs**, click **Add**, enter a storage VM name, and in the **SMB/CIFS, NFS, S3** tab, select **Enable NFS**.
    - Confirm the default language.
    - Add network interfaces.
    - Update storage VM administrator account information (optional).
  - b. For existing storage VMs: click **Storage > Storage VMs**, select a storage VM, click **Settings**, and then click  under **NFS**.
2. Open the export policy of the storage VM root volume:
  - a. Click **Storage > Volumes**, select the root volume of the storage VM (which by default is *volume-name\_root*), and then click on the policy that is displayed under **Export Policy**.
  - b. Click **Add** to add a rule.
    - Client specification = 0.0.0.0/0
    - Access protocols = NFS
    - Access details = UNIX Read-Only
3. Configure DNS for host-name resolution: click **Storage > Storage VMs**, select the storage VM, click **Settings**, and then click  under **DNS**.
4. Configure name services as required.
  - a. Click **Storage > Storage VMs**, select the storage VM, click **Settings**, and then click for  LDAP or NIS.
  - b. Include any changes in the name services switch file: click  in the Name Services Switch tile.

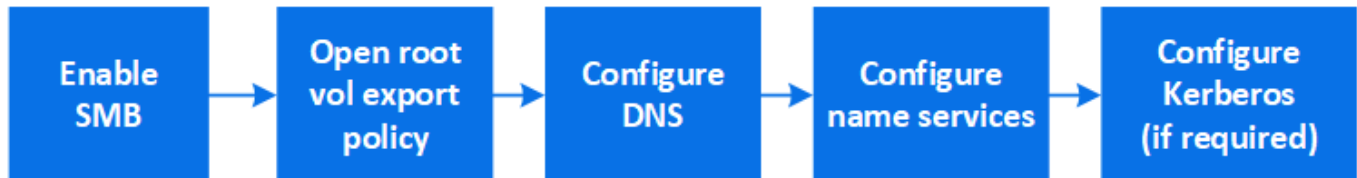


5. Configure Kerberos if required:
  - a. Click **Storage > Storage VMs**, select the storage VM, and then click **Settings**.
  - b. Click  in the Kerberos tile and then click **Add**.



### Enable NAS storage for Windows servers using SMB

Create or modify storage VMs to enable SMB servers for serving data to Windows clients.

This procedure enables a new or existing storage VM for the SMB protocol. It is assumed that configuration details are available for any networking, authentication, or security services required in your environment.





### Steps


1. Enable SMB on a storage VM.
  - a. For new storage VMs: click **Storage > Storage VMs**, click **Add**, enter a storage VM name, and in the **SMB/CIFS, NFS, S3** tab, select **Enable SMB/CIFS**.
    - Enter the following information:
      - Administrator name and password
      - Server name
      - Active directory domain
    - Confirm the Organizational Unit.
    - Confirm the DNS values.
    - Confirm the default language.
    - Add network interfaces.
    - Update storage VM administrator account information (optional).
  - b. For existing storage VMs: click **Storage > Storage VMs**, select a storage VM, click **Settings**, and then click  under **SMB**.
2. Open the export policy of the storage VM root volume:
  - a. Click **Storage > Volumes**, select the root volume of the storage VM (which by default is *volume-name\_root*), and then click on the policy that is displayed under **Export Policy**.
  - b. Click **Add** to add a rule.
    - Client specification = 0.0.0.0/0
    - Access protocols = SMB
    - Access details = NTFS Read-Only
3. Configure DNS for host-name resolution:
  - a. Click **Storage > Storage VMs**, select the storage VM, click **Settings**, and then click  under **DNS**.
  - b. Switch to the DNS server and map the SMB server.

- Create forward (A - Address record) and reverse (PTR - Pointer record) lookup entries to map the SMB server name to the IP address of the data network interface.
- If you use NetBIOS aliases, create an alias canonical name (CNAME resource record) lookup entry to map each alias to the IP address of the SMB server's data network interface.

4. Configure name services as required

- Click **Storage > Storage VMs**, select the storage VM, click **Settings**, and then click  under **LDAP** or **NIS**.
- Include any changes in the name services switch file: click  under **Name Services Switch**.

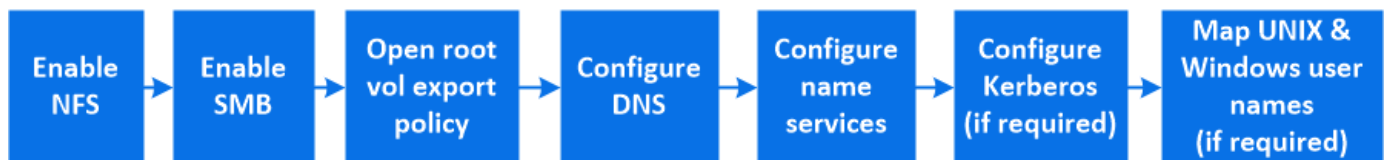
5. Configure Kerberos if required:

- Click **Storage > Storage VMs**, select the storage VM, and then click **Settings**.
- Click  under **Kerberos** and then click **Add**.



### Enable NAS storage for both Windows and Linux using both NFS and SMB






Create or modify storage VMs to enable NFS and SMB servers to serve data to Linux and Windows clients.

This procedure enables a new or existing storage VM to serve both NFS and SMB protocols. It is assumed that configuration details are available for any networking, authentication, or security services required in your environment.



#### Steps

- Enable NFS and SMB on a storage VM.
  - For new storage VMs: click **Storage > Storage VMs**, click **Add**, enter a storage VM name, and in the **SMB/CIFS, NFS, S3** tab, select **Enable SMB/CIFS** and **Enable NFS**.
    - Enter the following information:
      - Administrator name and password
      - Server name
      - Active directory domain
    - Confirm the Organizational Unit.
    - Confirm the DNS values.
    - Confirm the default language.
    - Add network interfaces.
    - Update storage VM administrator account information (optional).
  - For existing storage VMs: click **Storage > Storage VMs**, select a storage VM, and then click **Settings**. Complete the following sub-steps if NFS or SMB is not already enabled.
    - Click  under **NFS**.
    - Click  under **SMB**.

2. Open the export policy of the storage VM root volume:
  - a. Click **Storage > Volumes**, select the root volume of the storage VM (which by default is *volume-name\_root*), and then click on the policy that is displayed under **Export Policy**.
  - b. Click **Add** to add a rule.
    - Client specification = 0.0.0.0/0
    - Access protocols = NFS
    - Access details = NFS Read-Only
3. Configure DNS for host-name resolution:
  - a. Click **Storage > Storage VMs**, select the storage VM, click **Settings**, and then click  under **DNS**.
  - b. When DNS configuration is complete, switch to the DNS server and map the SMB server.
    - Create forward (A - Address record) and reverse (PTR - Pointer record) lookup entries to map the SMB server name to the IP address of the data network interface.
    - If you use NetBIOS aliases, create an alias canonical name (CNAME resource record) lookup entry to map each alias to the IP address of the SMB server's data network interface.
4. Configure name services as required:
  - a. Click **Storage > Storage VMs**, select the storage VM, click **Settings**, and then click  for LDAP or NIS.
  - b. Include any changes in the name services switch file: click  under **Name Services Switch**.
5. Configure Kerberos if required: click  in the Kerberos tile and then click **Add**.
6. Map UNIX and Windows user names if required: click  under **Name Mapping** and then click **Add**.

You should use this procedure only if your site has Windows and UNIX user accounts that do not map implicitly, which is when the lowercase version of each Windows user name matches the UNIX user name. This procedure can be done using LDAP, NIS, or local users. If you have two sets of users that do not match, you should configure name mapping.

## Configure NFS with the CLI

### NFS configuration overview with the CLI

You can use ONTAP 9 CLI commands to configure NFS client access to files contained in a new volume or qtree in a new or existing storage virtual machine (SVM).

Use these procedures if you want to configure access to a volume or qtree in the following way:

- You want to use any version of NFS currently supported by ONTAP: NFSv3, NFSv4, NFSv4.1, NFSv4.2, or NFSv4.1 with pNFS.
- You want to use the command-line interface (CLI), not System Manager or an automated scripting tool.

To use System Manager to configure NAS multiprotocol access, see [Provision NAS storage for both Windows and Linux using both NFS and SMB](#).

- You want to use best practices, not explore every available option.

Details about command syntax are available from CLI help and ONTAP man pages.

- UNIX file permissions will be used to secure the new volume.
- You have cluster administrator privileges, not SVM administrator privileges.

If you want details about the range of ONTAP NFS protocol capabilities, consult the [NFS reference overview](#).

### Other ways to do this in ONTAP

To perform these tasks with...	Refer to...
The redesigned System Manager (available with ONTAP 9.7 and later)	<a href="#">Provision NAS storage for Linux servers using NFS</a>
System Manager Classic (available with ONTAP 9.7 and earlier)	<a href="#">NFS configuration overview</a>

## NFS configuration workflow

Configuring NFS involves assessing physical storage and networking requirements, and then choosing a workflow that is specific to your goal—configuring NFS access to a new or existing SVM, or adding a volume or qtree to an existing SVM that is already fully configured for NFS access.

## Preparation

### Assess physical storage requirements

Before provisioning NFS storage for clients, you must ensure that there is sufficient space in an existing aggregate for the new volume. If there is not, you can add disks to an existing aggregate or create a new aggregate of the desired type.

### Steps

1. Display available space in existing aggregates:

```
storage aggregate show
```

If there is an aggregate with sufficient space, record its name in the worksheet.

```

cluster::> storage aggregate show
Aggregate      Size Available Used% State  #Vols  Nodes  RAID Status
-----
aggr_0        239.0GB   11.13GB   95% online    1 node1  raid_dp,
normal
aggr_1        239.0GB   11.13GB   95% online    1 node1  raid_dp,
normal
aggr_2        239.0GB   11.13GB   95% online    1 node2  raid_dp,
normal
aggr_3        239.0GB   11.13GB   95% online    1 node2  raid_dp,
normal
aggr_4        239.0GB   238.9GB   95% online    5 node3  raid_dp,
normal
aggr_5        239.0GB   239.0GB   95% online    4 node4  raid_dp,
normal

6 entries were displayed.

```

2. If there are no aggregates with sufficient space, add disks to an existing aggregate by using the `storage aggregate add-disks` command, or create a new aggregate by using the `storage aggregate create` command.

## Related information

[ONTAP concepts](#)

## Assess networking requirements

Before providing NFS storage to clients, you must verify that networking is correctly configured to meet the NFS provisioning requirements.

### What you'll need

The following cluster networking objects must be configured:

- Physical and logical ports
- Broadcast domains
- Subnets (if required)
- IPspaces (as required, in addition to the default IPspace)
- Failover groups (as required, in addition to the default failover group for each broadcast domain)
- External firewalls

### Steps

1. Display the available physical and virtual ports:

```
network port show
```

- When possible, you should use the port with the highest speed for the data network.
- All components in the data network must have the same MTU setting for best performance.

2. If you are planning to use a subnet name to allocate the IP address and network mask value for a LIF, verify that the subnet exists and has sufficient addresses available: +

```
network subnet show
```

Subnets contain a pool of IP addresses that belong to the same layer 3 subnet. Subnets are created by using the `network subnet create` command.

3. Display available IPspaces:

```
network ipspace show
```

You can use the default IPspace or a custom IPspace.

4. If you want to use IPv6 addresses, verify that IPv6 is enabled on the cluster:

```
network options ipv6 show
```

If required, you can enable IPv6 by using the `network options ipv6 modify` command.

## Decide where to provision new NFS storage capacity

Before you create a new NFS volume or qtree, you must decide whether to place it in a new or existing SVM, and how much configuration the SVM requires. This decision determines your workflow.

### Choices

- If you want to provision a volume or qtree on a new SVM, or on an existing SVM that has NFS enabled but not configured, complete the steps in both "Configuring NFS access to an SVM" and "Adding NFS storage to an NFS-enabled SVM".

[Configure NFS access to an SVM](#)

[Add NFS storage to an NFS-enabled SVM](#)

You might choose to create a new SVM if one of the following is true:

- You are enabling NFS on a cluster for the first time.
- You have existing SVMs in a cluster in which you do not want to enable NFS support.
- You have one or more NFS-enabled SVMs in a cluster, and you want another NFS server in an isolated namespace (multi-tenancy scenario).  
You should also choose this option to provision storage on an existing SVM that has NFS enabled but not configured. This might be the case if you created the SVM for SAN access or if no protocols were enabled when the SVM was created.

After enabling NFS on the SVM, proceed to provision a volume or qtree.

- If you want to provision a volume or qtree on an existing SVM that is fully configured for NFS access, complete the steps in "Adding NFS storage to an NFS-enabled SVM".

[Adding NFS storage to an NFS-enabled SVM](#)

## Worksheet for gathering NFS configuration information

The NFS configuration worksheet enables you to collect the required information to set up NFS access for clients.

You should complete one or both sections of the worksheet depending on the decision you made about where to provision storage:

- If you are configuring NFS access to an SVM, you should complete both sections.

[Configuring NFS access to an SVM](#)

[Adding storage capacity to an NFS-enabled SVM](#)

- If you are adding storage capacity to an NFS-enabled SVM, you should complete only the second section.

[Adding storage capacity to an NFS-enabled SVM](#)

See the command man pages for details about the parameters.

### Configure NFS access to an SVM

#### Parameters for creating an SVM


You supply these values with the `vserver create` command if you are creating a new SVM.

Field	Description	Your value
<code>-vserver</code>	A name you supply for the new SVM that is either a fully qualified domain name (FQDN) or follows another convention that enforces unique SVM names across a cluster.	
<code>-aggregate</code>	The name of an aggregate in the cluster with sufficient space for new NFS storage capacity.	
<code>-rootvolume</code>	A unique name you supply for the SVM root volume.	
<code>-rootvolume-security-style</code>	Use the UNIX security style for the SVM.	unix
<code>-language</code>	Use the default language setting in this workflow.	C.UTF-8
<code>ipspace</code>	IPspaces are distinct IP address spaces in which (storage virtual machines (SVMs)) reside.	

## Parameters for creating an NFS server

You supply these values with the `vserver nfs create` command when you create a new NFS server and specify supported NFS versions.

If you are enabling NFSv4 or later, you should use LDAP for improved security.

Field	Description	Your value
<code>-v3, -v4.0, -v4.1, -v4.1-pnfs</code>	Enable NFS versions as needed.   v4.2 is also supported in ONTAP 9.8 and later when v4.1 is enabled.	
<code>-v4-id-domain</code>	ID mapping domain name.	
<code>-v4-numeric-ids</code>	Support for numeric owner IDs (enabled or disabled).	

## Parameters for creating a LIF

You supply these values with the `network interface create` command when you are creating LIFs.

If you are using Kerberos, you should enable Kerberos on multiple LIFs.

Field	Description	Your value
<code>-lif</code>	A name you supply for the new LIF.	
<code>-role</code>	Use the data LIF role in this workflow.	<code>data</code>
<code>-data-protocol</code>	Use only the NFS protocol in this workflow.	<code>nfs</code>
<code>-home-node</code>	The node to which the LIF returns when the <code>network interface revert</code> command is run on the LIF.	
<code>-home-port</code>	The port or interface group to which the LIF returns when the <code>network interface revert</code> command is run on the LIF.	



-address	The IPv4 or IPv6 address on the cluster that will be used for data access by the new LIF.	
-netmask	The network mask and gateway for the LIF.	
-subnet	A pool of IP addresses. Used instead of -address and -netmask to assign addresses and netmasks automatically.	
-firewall-policy	Use the default data firewall policy in this workflow.	data

### Parameters for DNS host name resolution

You supply these values with the `vserver services name-service dns create` command when you are configuring DNS.

Field	Description	Your value
-domains	Up to five DNS domain names.	
-name-servers	Up to three IP addresses for each DNS name server.	

### Name service information

#### Parameters for creating local users

You supply these values if you are creating local users by using the `vserver services name-service unix-user create` command. If you are configuring local users by loading a file containing UNIX users from a uniform resource identifier (URI), you do not need to specify these values manually.

	User name (-user)	User ID (-id)	Group ID (-primary-gid)	Full name (-full-name)
Example	johnm	123	100	John Miller
1				
2				
3				
...				

n				
---	--	--	--	--

### Parameters for creating local groups

You supply these values if you are creating local groups by using the `vserver services name-service unix-group create` command. If you are configuring local groups by loading a file containing UNIX groups from a URI, you do not need to specify these values manually.

	Group name (-name)	Group ID (-id)
Example	Engineering	100
1		
2		
3		
...		
n		

### Parameters for NIS

You supply these values with the `vserver services name-service nis-domain create` command.



Beginning with ONTAP 9.2, the field `-nis-servers` replaces the field `-servers`. This new field can take either a hostname or an IP address for the NIS server.

Field	Description	Your value
<code>-domain</code>	The NIS domain that the SVM will use for name lookups.	
<code>-active</code>	The active NIS domain server.	true or false
<code>-servers</code>	ONTAP 9.0, 9.1: One or more IP addresses of NIS servers used by the NIS domain configuration.	
<code>-nis-servers</code>	ONTAP 9.2: A comma-separated list of IP addresses and hostnames for the NIS servers used by the domain configuration.	

### Parameters for LDAP

You supply these values with the `vserver services name-service ldap client create` command.

You will also need a self-signed root CA certificate `.pem` file.



Beginning with ONTAP 9.2, the field `-ldap-servers` replaces the field `-servers`. This new field can take either a hostname or an IP address for the LDAP server.

Field	Description	Your value
<code>-vserver</code>	The name of the SVM for which you want to create an LDAP client configuration.	
<code>-client-config</code>	The name you assign for the new LDAP client configuration.	
<code>-servers</code>	ONTAP 9.0, 9.1: One or more LDAP servers by IP address in a comma-separated list.	
<code>-ldap-servers</code>	ONTAP 9.2: A comma-separated list of IP addresses and hostnames for the LDAP servers.	
<code>-query-timeout</code>	Use the default 3 seconds for this workflow.	3
<code>-min-bind-level</code>	The minimum bind authentication level. The default is <code>anonymous</code> . Must be set to <code>sasl</code> if signing and sealing is configured.	
<code>-preferred-ad-servers</code>	One or more preferred Active Directory servers by IP address in a comma-delimited list.	
<code>-ad-domain</code>	The Active Directory domain.	
<code>-schema</code>	The schema template to use. You can use a default or custom schema.	
<code>-port</code>	Use the default LDAP server port 389 for this workflow.	389
<code>-bind-dn</code>	The Bind user distinguished name.	

Field	Description	Your value
<code>-base-dn</code>	The base distinguished name. The default is "" (root).	
<code>-base-scope</code>	Use the default base search scope <code>subnet</code> for this workflow.	<code>subnet</code>
<code>-session-security</code>	Enables LDAP signing or signing and sealing. The default is <code>none</code> .	
<code>-use-start-tls</code>	Enables LDAP over TLS. The default is <code>false</code> .	

### Parameters for Kerberos authentication

You supply these values with the `vserver nfs kerberos realm create` command. Some of the values will differ depending on whether you use Microsoft Active Directory as a Key Distribution Center (KDC) server, or MIT or other UNIX KDC server.

Field	Description	Your value
<code>-vserver</code>	The SVM that will communicate with the KDC.	
<code>-realm</code>	The Kerberos realm.	
<code>-clock-skew</code>	Permitted clock skew between clients and servers.	
<code>-kdc-ip</code>	KDC IP address.	
<code>-kdc-port</code>	KDC port number.	
<code>-adserver-name</code>	Microsoft KDC only: AD server name.	
<code>-adserver-ip</code>	Microsoft KDC only: AD server IP address.	
<code>-adminserver-ip</code>	UNIX KDC only: Admin server IP address.	
<code>-adminserver-port</code>	UNIX KDC only: Admin server port number.	

<code>-passwordserver-ip</code>	UNIX KDC only: Password server IP address.	
<code>-passwordserver-port</code>	UNIX KDC only: Password server port.	
<code>-kdc-vendor</code>	KDC vendor.	{ Microsoft   Other }
<code>-comment</code>	Any desired comments.	

You supply these values with the `vserver nfs kerberos interface enable` command.

Field	Description	Your value
<code>-vserver</code>	The name of the SVM for which you want to create a Kerberos configuration.	
<code>-lif</code>	The data LIF on which you will enable Kerberos. You can enable Kerberos on multiple LIFs.	
<code>-spn</code>	The Service Principle Name (SPN)	
<code>-permitted-enc-types</code>	The permitted encryption types for Kerberos over NFS; <code>aes-256</code> is recommended, depending on client capabilities.	
<code>-admin-username</code>	The KDC administrator credentials to retrieve the SPN secret key directly from the KDC. A password is required	
<code>-keytab-uri</code>	The keytab file from the KDC containing the SPN key if you do not have KDC administrator credentials.	
<code>-ou</code>	The organizational unit (OU) under which the Microsoft Active Directory server account will be created when you enable Kerberos using a realm for Microsoft KDC.	

## Adding storage capacity to an NFS-enabled SVM

### Parameters for creating export policies and rules

You supply these values with the `vserver export-policy create` command.

Field	Description	Your value
<code>-vserver</code>	The name of the SVM that will host the new volume.	
<code>-policyname</code>	A name you supply for a new export policy.	

You supply these values for each rule with the `vserver export-policy rule create` command.

Field	Description	Your value
<code>-clientmatch</code>	Client match specification.	
<code>-ruleindex</code>	Position of export rule in the list of rules.	
<code>-protocol</code>	Use NFS in this workflow.	<code>nfs</code>
<code>-rorule</code>	Authentication method for read-only access.	
<code>-rwrule</code>	Authentication method for read-write access.	
<code>-superuser</code>	Authentication method for superuser access.	
<code>-anon</code>	User ID to which anonymous users are mapped.	

You must create one or more rules for each export policy.

<code>-ruleindex</code>	<code>-clientmatch</code>	<code>-rorule</code>	<code>-rwrule</code>	<code>-superuser</code>	<code>-anon</code>
Examples	<code>0.0.0.0/0,@rootaccess_netgroup</code>	<code>any</code>	<code>krb5</code>	<code>sys</code>	<code>65534</code>
1					
2					
3					
...					

n					
---	--	--	--	--	--

### Parameters for creating a volume

You supply these values with the `volume create` command if you are creating a volume instead of a qtree.

Field	Description	Your value
<code>-vserver</code>	The name of a new or existing SVM that will host the new volume.	
<code>-volume</code>	A unique descriptive name you supply for the new volume.	
<code>-aggregate</code>	The name of an aggregate in the cluster with sufficient space for the new NFS volume.	
<code>-size</code>	An integer you supply for the size of the new volume.	
<code>-user</code>	Name or ID of the user that is set as the owner of the volume's root.	
<code>-group</code>	Name or ID of the group that is set as the owner of the volume's root.	
<code>--security-style</code>	Use the UNIX security style for this workflow.	<code>unix</code>
<code>-junction-path</code>	Location under root ( <code>/</code> ) where the new volume is to be mounted.	
<code>-export-policy</code>	If you are planning to use an existing export policy, you can enter its name when you create the volume.	

### Parameters for creating a qtree

You supply these values with the `volume qtree create` command if you are creating a qtree instead of a volume.

Field	Description	Your value
<code>-vserver</code>	The name of the SVM on which the volume containing the qtree resides.	

<code>-volume</code>	The name of the volume that will contain the new qtree.	
<code>-qtree</code>	A unique descriptive name you supply for the new qtree, 64 characters or less.	
<code>-qtree-path</code>	The qtree path argument in the format <code>/vol/volume_name/qtree_name\&gt;</code> can be specified instead of specifying volume and qtree as separate arguments.	
<code>-unix-permissions</code>	Optional: The UNIX permissions for the qtree.	
<code>-export-policy</code>	If you are planning to use an existing export policy, you can enter its name when you create the qtree.	

## Configure NFS access to an SVM

### Create an SVM

If you do not already have at least one SVM in a cluster to provide data access to NFS clients, you must create one.

#### Steps

1. Create an SVM:

```
vserver create -vserver vserver_name -rootvolume root_volume_name -aggregate
aggregate_name -rootvolume-security-style unix -language C.UTF-8 -ipspace
ipspace_name
```

- Use the UNIX setting for the `-rootvolume-security-style` option.
- Use the default `C.UTF-8` `-language` option.
- The `ipspace` setting is optional.

2. Verify the configuration and status of the newly created SVM:

```
vserver show -vserver vserver_name
```

The `Allowed Protocols` field must include NFS. You can edit this list later.

The `Vserver Operational State` field must display the `running` state. If it displays the `initializing` state, it means that some intermediate operation such as root volume creation failed, and you must delete the SVM and re-create it.



## Examples

The following command creates an SVM for data access in the IPspace ipspaceA:

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style unix -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

The following command shows that an SVM was created with a root volume of 1 GB, and it was started automatically and is in `running` state. The root volume has a default export policy that does not include any rules, so the root volume is not exported upon creation.

```
cluster1::> vserver show -vserver vs1.example.com
                                Vserver: vs1.example.com
                                Vserver Type: data
                                Vserver Subtype: default
                                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                Aggregate: aggr1
                                NIS Domain: -
                                Root Volume Security Style: unix
                                LDAP Client: -
                                Default Volume Language Code: C.UTF-8
                                Snapshot Policy: default
                                Comment:
                                Quota Policy: default
                                List of Aggregates Assigned: -
                                Limit on Maximum Number of Volumes allowed: unlimited
                                Vserver Admin State: running
                                Vserver Operational State: running
                                Vserver Operational State Stopped Reason: -
                                Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                                Disallowed Protocols: -
                                QoS Policy Group: -
                                Config Lock: false
                                IPspace Name: ipspaceA
```

### Verify that the NFS protocol is enabled on the SVM

Before you can configure and use NFS on SVMs, you must verify that the protocol is enabled.

## About this task

This is typically done during SVM setup, but if you did not enable the protocol during setup, you can enable it later by using the `vserver add-protocols` command.



You cannot add or remove a protocol from a LIF once it is created.

You can also disable protocols on SVMs using the `vserver remove-protocols` command.

## Steps

1. Check which protocols are currently enabled and disabled for the SVM:

```
vserver show -vserver vserver_name -protocols
```

You can also use the `vserver show-protocols` command to view the currently enabled protocols on all SVMs in the cluster.

2. If necessary, enable or disable a protocol:

- To enable the NFS protocol:

```
vserver add-protocols -vserver vserver_name -protocols nfs
```

- To disable a protocol:

```
vserver remove-protocols -vserver vserver_name -protocols protocol_name  
[,protocol_name,...]
```

3. Confirm that the enabled and disabled protocols were updated correctly:

```
vserver show -vserver vserver_name -protocols
```

## Example

The following command displays which protocols are currently enabled and disabled (allowed and disallowed) on the SVM named `vs1`:

```
vs1::> vserver show -vserver vs1.example.com -protocols  
Vserver          Allowed Protocols          Disallowed Protocols  
-----          -  
vs1.example.com  nfs                          cifs, fcp, iscsi, ndmp
```

The following command allows access over NFS by adding `nfs` to the list of enabled protocols on the SVM named `vs1`:

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols nfs
```

## Open the export policy of the SVM root volume

The default export policy of the SVM root volume must include a rule to allow all clients open access through NFS. Without such a rule, all NFS clients are denied access to the

## SVM and its volumes.

### About this task

When a new SVM is created, a default export policy (called default) is created automatically for the root volume of the SVM. You must create one or more rules for the default export policy before clients can access data on the SVM.

You should verify that access is open to all NFS clients in the default export policy, and later restrict access to individual volumes by creating custom export policies for individual volumes or qtrees.

### Steps

1. If you are using an existing SVM, check the default root volume export policy:

```
vserver export-policy rule show
```

The command output should be similar to the following:

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

                                Vserver: vs1.example.com
                                Policy Name: default
                                Rule Index: 1
                                Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                                RO Access Rule: any
                                RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                                Superuser Security Types: any
                                Honor SetUID Bits in SETATTR: true
                                Allow Creation of Devices: true
```

If such a rule exists that allows open access, this task is complete. If not, proceed to the next step.

2. Create an export rule for the SVM root volume:

```
vserver export-policy rule create -vserver vserver_name -policyname default
-ruleindex 1 -protocol nfs -clientmatch 0.0.0.0/0 -rorule any -rwrule any
-superuser any
```

If the SVM will only contain volumes secured by Kerberos, you can set the export rule options `-rorule`, `-rwrule`, and `-superuser` for the root volume to `krb5` or `krb5i`. For example:

```
-rorule krb5i -rwrule krb5i -superuser krb5i
```

3. Verify rule creation by using the `vserver export-policy rule show` command.

### Result

Any NFS client can now access any volume or qtree created on the SVM.

## Create an NFS server

After verifying that NFS is licensed on your cluster, you can use the `vserver nfs create` command to create an NFS server on the SVM and specify the NFS versions it supports.

### What you'll need

The SVM must have been configured to allow the NFS protocol.

### About this task

The SVM can be configured to support one or more versions of NFS. If you are supporting NFSv4 or later:

- The NFSv4 user ID mapping domain name must be the same on the NFSv4 server and target clients.  
It does not necessarily need to be the same as an LDAP or NIS domain name as long as the NFSv4 server and clients are using the same name.
- Target clients must support the NFSv4 numeric ID setting.
- For security reasons, you should use LDAP for name services in NFSv4 deployments.

### Steps

1. Verify that NFS is licensed on your cluster:

```
system license show -package nfs
```

If it is not, contact your sales representative.

2. Create an NFS server:

```
vserver nfs create -vserver vserver_name -v3 {enabled|disabled} -v4.0  
{enabled|disabled} -v4-id-domain nfsv4_id_domain -v4-numeric-ids  
{enabled|disabled} -v4.1 {enabled|disabled} -v4.1-pnfs {enabled|disabled}
```

You can choose to enable any combination of NFS versions. If you want to support pNFS, you must enable both `-v4.1` and `-v4.1-pnfs` options.

If you enable v4 or later, you should also be sure that the following options are set correctly:

- `-v4-id-domain`

This optional parameter specifies the domain portion of the string form of user and group names as defined by the NFSv4 protocol. By default, ONTAP uses the NIS domain if one is set; if not, the DNS domain is used. You must supply a value that matches the domain name used by target clients.

- `-v4-numeric-ids`

This optional parameter specifies whether the support for numeric string identifiers in NFSv4 owner attributes is enabled. The default setting is enabled but you should verify that the target clients support it.

You can enable additional NFS features later by using the `vserver nfs modify` command.

3. Verify that NFS is running:

```
vserver nfs status -vserver vserver_name
```

4. Verify that NFS is configured as desired:

```
vserver nfs show -vserver vserver_name
```

### Examples

The following command creates an NFS server on the SVM named vs1 with NFSv3 and NFSv4.0 enabled:

```
vs1::> vserver nfs create -vserver vs1 -v3 enabled -v4.0 enabled -v4-id  
-domain my_domain.com
```

The following commands verify the status and configuration values of the new NFS server named vs1:

```
vs1::> vserver nfs status -vserver vs1  
The NFS server is running on Vserver "vs1".  
  
vs1::> vserver nfs show -vserver vs1  
  
                Vserver: vs1  
    General NFS Access: true  
                NFS v3: enabled  
                NFS v4.0: enabled  
    UDP Protocol: enabled  
    TCP Protocol: enabled  
    Default Windows User: -  
    NFSv4.0 ACL Support: disabled  
    NFSv4.0 Read Delegation Support: disabled  
    NFSv4.0 Write Delegation Support: disabled  
    NFSv4 ID Mapping Domain: my_domain.com  
    ...
```

### Create a LIF

A LIF is an IP address associated with a physical or logical port. If there is a component failure, a LIF can fail over to or be migrated to a different physical port, thereby continuing to communicate with the network.

#### What you'll need

- The underlying physical or logical network port must have been configured to the administrative up status.
- If you are planning to use a subnet name to allocate the IP address and network mask value for a LIF, the subnet must already exist.

Subnets contain a pool of IP addresses that belong to the same layer 3 subnet. They are created using the `network subnet create` command.

- The mechanism for specifying the type of traffic handled by a LIF has changed. For ONTAP 9.5 and earlier, LIFs used roles to specify the type of traffic it would handle. Beginning with ONTAP 9.6, LIFs use service policies to specify the type of traffic it would handle.

### About this task

- You can create both IPv4 and IPv6 LIFs on the same network port.
- If you are using Kerberos authentication, enable Kerberos on multiple LIFs.
- If you have a large number of LIFs in your cluster, you can verify the LIF capacity supported on the cluster by using the `network interface capacity show` command and the LIF capacity supported on each node by using the `network interface capacity details show` command (at the advanced privilege level).
- Beginning with ONTAP 9.7, if other LIFs already exist for the SVM in the same subnet, you do not need to specify the home port of the LIF. ONTAP automatically chooses a random port on the specified home node in the same broadcast domain as the other LIFs already configured in the same subnet.

Beginning with ONTAP 9.4, FC-NVMe is supported. If you are creating an FC-NVMe LIF you should be aware of the following:

- The NVMe protocol must be supported by the FC adapter on which the LIF is created.
- FC-NVMe can be the only data protocol on data LIFs.
- One LIF handling management traffic must be configured for every storage virtual machine (SVM) supporting SAN.
- NVMe LIFs and namespaces must be hosted on the same node.
- Only one NVMe LIF handling data traffic can be configured per SVM

### Steps

1. Create a LIF:

```
network interface create -vserver vservice_name -lif lif_name -role data -data
-protocol nfs -home-node node_name -home-port port_name {-address IP_address
-netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto
-revert {true|false}
```

Option	Description
<b>ONTAP 9.5 and earlier</b>	<pre>network interface create -vserver vservice_name -lif lif_name -role data -data-protocol nfs -home-node node_name -home-port port_name {- address IP_address -netmask IP_address   -subnet-name subnet_name} -firewall -policy data -auto-revert {true false}</pre>

**ONTAP 9.6 and later**

```
network interface create -vserver
vserver_name -lif lif_name -role data
-data-protocol nfs -home-node
node_name -home-port port_name {-
address IP_address -netmask IP_address
| -subnet-name subnet_name} -firewall
-policy data -auto-revert {true|false}
```

- The `-role` parameter is not required when creating a LIF using a service policy (beginning with ONTAP 9.6).
- The `-data-protocol` parameter must be specified when the LIF is created, and cannot be modified later without destroying and re-creating the data LIF.

The `-data-protocol` parameter is not required when creating a LIF using a service policy (beginning with ONTAP 9.6).

- `-home-node` is the node to which the LIF returns when the `network interface revert` command is run on the LIF.

You can also specify whether the LIF should automatically revert to the home-node and home-port with the `-auto-revert` option.

- `-home-port` is the physical or logical port to which the LIF returns when the `network interface revert` command is run on the LIF.
- You can specify an IP address with the `-address` and `-netmask` options, or you enable allocation from a subnet with the `-subnet_name` option.
- When using a subnet to supply the IP address and network mask, if the subnet was defined with a gateway, a default route to that gateway is added automatically to the SVM when a LIF is created using that subnet.
- If you assign IP addresses manually (without using a subnet), you might need to configure a default route to a gateway if there are clients or domain controllers on a different IP subnet. The `network route create man` page contains information about creating a static route within an SVM.
- For the `-firewall-policy` option, use the same default data as the LIF role.

You can create and add a custom firewall policy later if desired.

- `-auto-revert` allows you to specify whether a data LIF is automatically reverted to its home node under circumstances such as startup, changes to the status of the management database, or when the network connection is made. The default setting is `false`, but you can set it to `false` depending on network management policies in your environment.

2. Verify that the LIF was created successfully by using the `network interface show` command.
3. Verify that the configured IP address is reachable:

To verify an...	Use...
IPv4 address	<code>network ping</code>

IPv6 address	network ping6
--------------	---------------

4. If you are using Kerberos, repeat Steps 1 through 3 to create additional LIFs.

Kerberos must be enabled separately on each of these LIFs.

### Examples

The following command creates a LIF and specifies the IP address and network mask values using the `-address` and `-netmask` parameters:

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol nfs -home-node node-4 -home-port elc -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

The following command creates a LIF and assigns IP address and network mask values from the specified subnet (named `client1_sub`):

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol nfs -home-node node-3 -home-port elc -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

The following command shows all the LIFs in cluster-1. Data LIFs `datalif1` and `datalif3` are configured with IPv4 addresses, and `datalif4` is configured with an IPv6 address:



```
network interface show
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is
Home						
-----						
cluster-1						
true	cluster_mgmt	up/up	192.0.2.3/24	node-1	e1a	
node-1						
true	clus1	up/up	192.0.2.12/24	node-1	e0a	
true	clus2	up/up	192.0.2.13/24	node-1	e0b	
node-2						
true	mgmt1	up/up	192.0.2.68/24	node-1	e1a	
true	clus1	up/up	192.0.2.14/24	node-2	e0a	
true	clus2	up/up	192.0.2.15/24	node-2	e0b	
true	mgmt1	up/up	192.0.2.69/24	node-2	e1a	
vs1.example.com						
true	datalif1	up/down	192.0.2.145/30	node-1	e1c	
vs3.example.com						
true	datalif3	up/up	192.0.2.146/30	node-2	e0c	
true	datalif4	up/up	2001::2/64	node-2	e0c	

5 entries were displayed.

The following command shows how to create a NAS data LIF that is assigned with the default-data-files service policy:

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport e0d -service-policy default-data-files -subnet-name ipspace1
```

### Enable DNS for host-name resolution

You can use the `vserver services name-service dns` command to enable DNS on an SVM, and configure it to use DNS for host-name resolution. Host names are

resolved using external DNS servers.

### What you'll need

A site-wide DNS server must be available for host name lookups.

You should configure more than one DNS server to avoid a single-point-of-failure. The `vserver services name-service dns create` command issues a warning if you enter only one DNS server name.

### About this task

The *Network Management Guide* contains information about configuring dynamic DNS on the SVM.

### Steps

1. Enable DNS on the SVM:

```
vserver services name-service dns create -vserver vserver_name -domains domain_name -name-servers ip_addresses -state enabled
```

The following command enables external DNS server servers on the SVM vs1:

```
vserver services name-service dns create -vserver vs1.example.com -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state enabled
```



Beginning with ONTAP 9.2, the `vserver services name-service dns create` command performs an automatic configuration validation and reports an error message if ONTAP cannot contact the name server.

2. Display the DNS domain configurations by using the `vserver services name-service dns show` command.

The following command displays the DNS configurations for all SVMs in the cluster:

```
vserver services name-service dns show
```

Vserver	State	Domains	Name Servers
cluster1	enabled	example.com	192.0.2.201, 192.0.2.202
vs1.example.com	enabled	example.com	192.0.2.201, 192.0.2.202

The following command displays detailed DNS configuration information for SVM vs1:

```
vserver services name-service dns show -vserver vs1.example.com
      Vserver: vs1.example.com
      Domains: example.com
      Name Servers: 192.0.2.201, 192.0.2.202
      Enable/Disable DNS: enabled
      Timeout (secs): 2
      Maximum Attempts: 1
```

3. Validate the status of the name servers by using the `vserver services name-service dns check` command.

The `vserver services name-service dns check` command is available beginning with ONTAP 9.2.

```
vserver services name-service dns check -vserver vs1.example.com
```

Vserver	Name Server	Status	Status Details
vs1.example.com	10.0.0.50	up	Response time (msec): 2
vs1.example.com	10.0.0.51	up	Response time (msec): 2

## Configure name services

### Configure name services overview

Depending on the configuration of your storage system, ONTAP needs to be able to look up host, user, group, or netgroup information to provide proper access to clients. You must configure name services to enable ONTAP to access local or external name services to obtain this information.

You should use a name service such as NIS or LDAP to facilitate name lookups during client authentication. It is best to use LDAP whenever possible for greater security, especially when deploying NFSv4 or later. You should also configure local users and groups in case external name servers are not available.

Name service information must be kept synchronized on all sources.

### Configure the name service switch table

You must configure the name service switch table correctly to enable ONTAP to consult local or external name services to retrieve host, user, group, netgroup, or name mapping information.

### What you'll need

You must have decided which name services you want to use for host, user, group, netgroup, or name mapping as applicable to your environment.

If you plan to use netgroups, all IPv6 addresses specified in netgroups must be shortened and compressed as specified in RFC 5952.

### About this task

Do not include information sources that are not being used. For example, if NIS is not being used in your environment, do not specify the `-sources nis` option.

### Steps

1. Add the necessary entries to the name service switch table:

```
vserver services name-service ns-switch create -vserver vserver_name -database database_name -sources source_names
```

2. Verify that the name service switch table contains the expected entries in the desired order:

```
vserver services name-service ns-switch show -vserver vserver_name
```

If you want to make any corrections, you must use the `vserver services name-service ns-switch modify` or `vserver services name-service ns-switch delete` commands.

### Example

The following example creates a new entry in the name service switch table for the SVM `vs1` to use the local netgroup file and an external NIS server to look up netgroup information in that order:

```
cluster::> vserver services name-service ns-switch create -vserver vs1 -database netgroup -sources files,nis
```

### After you finish

- You must configure the name services you have specified for the SVM to provide data access.
- If you delete any name service for the SVM, you must remove it from the name service switch table as well.

The client access to the storage system might not work as expected, if you fail to delete the name service from the name service switch table.

## Configure local UNIX users and groups

### Configure local UNIX users and groups overview

You can use local UNIX users and groups on the SVM for authentication and name mappings. You can create UNIX users and groups manually, or you can load a file containing UNIX users or groups from a uniform resource identifier (URI).

There is a default maximum limit of 32,768 local UNIX user groups and group members combined in the cluster. The cluster administrator can modify this limit.

### Create a local UNIX user

You can use the `vserver services name-service unix-user create` command to create local UNIX users. A local UNIX user is a UNIX user you create on the

SVM as a UNIX name services option to be used in the processing of name mappings.

### Step

1. Create a local UNIX user:

```
vserver services name-service unix-user create -vserver vserver_name -user  
user_name -id integer -primary-gid integer -full-name full_name
```

`-user user_name` specifies the user name. The length of the user name must be 64 characters or fewer.

`-id integer` specifies the user ID that you assign.

`-primary-gid integer` specifies the primary group ID. This adds the user to the primary group. After creating the user, you can manually add the user to any desired additional group.

### Example

The following command creates a local UNIX user named johnm (full name "John Miller") on the SVM named vs1. The user has the ID 123 and the primary group ID 100.

```
node::> vserver services name-service unix-user create -vserver vs1 -user  
johnm -id 123  
-primary-gid 100 -full-name "John Miller"
```

### Load local UNIX users from a URI

As an alternative to manually creating individual local UNIX users in SVMs, you can simplify the task by loading a list of local UNIX users into SVMs from a uniform resource identifier (URI) (`vserver services name-service unix-user load-from-uri`).

### Steps

1. Create a file containing the list of local UNIX users you want to load.

The file must contain user information in the UNIX `/etc/passwd` format:

```
user_name: password: user_ID: group_ID: full_name
```

The command discards the value of the `password` field and the values of the fields after the `full_name` field (`home_directory` and `shell`).

The maximum supported file size is 2.5 MB.

2. Verify that the list does not contain any duplicate information.

If the list contains duplicate entries, loading the list fails with an error message.

3. Copy the file to a server.

The server must be reachable by the storage system over HTTP, HTTPS, FTP, or FTPS.

4. Determine what the URI for the file is.

The URI is the address you provide to the storage system to indicate where the file is located.

5. Load the file containing the list of local UNIX users into SVMs from the URI:

```
vserver services name-service unix-user load-from-uri -vserver vserver_name
-uri {ftp|http|ftps|https}://uri -overwrite {true|false}
```

`-overwrite {true|false}` specifies whether to overwrite entries. The default is `false`.

### Example

The following command loads a list of local UNIX users from the URI `ftp://ftp.example.com/passwd` into the SVM named `vs1`. Existing users on the SVM are not overwritten by information from the URI.

```
node::> vserver services name-service unix-user load-from-uri -vserver vs1
-uri ftp://ftp.example.com/passwd -overwrite false
```

### Create a local UNIX group

You can use the `vserver services name-service unix-group create` command to create UNIX groups that are local to the SVM. Local UNIX groups are used with local UNIX users.

#### Step

1. Create a local UNIX group:

```
vserver services name-service unix-group create -vserver vserver_name -name
group_name -id integer
```

`-name group_name` specifies the group name. The length of the group name must be 64 characters or fewer.

`-id integer` specifies the group ID that you assign.

### Example

The following command creates a local group named `eng` on the SVM named `vs1`. The group has the ID 101.

```
vs1::> vserver services name-service unix-group create -vserver vs1 -name
eng -id 101
```

### Add a user to a local UNIX group

You can use the `vserver services name-service unix-group adduser` command to add a user to a supplemental UNIX group that is local to the SVM.

#### Step

1. Add a user to a local UNIX group:

```
vserver services name-service unix-group adduser -vserver vserver_name -name
group_name -username user_name
```

`-name group_name` specifies the name of the UNIX group to add the user to in addition to the user's primary group.

### Example

The following command adds a user named max to a local UNIX group named eng on the SVM named vs1:

```
vs1::> vserver services name-service unix-group adduser -vserver vs1 -name
eng
-username max
```

### Load local UNIX groups from a URI

As an alternative to manually creating individual local UNIX groups, you can load a list of local UNIX groups into SVMs from a uniform resource identifier (URI) by using the `vserver services name-service unix-group load-from-uri` command.

#### Steps

1. Create a file containing the list of local UNIX groups you want to load.

The file must contain group information in the UNIX `/etc/group` format:

```
group_name: password: group_ID: comma_separated_list_of_users
```

The command discards the value of the `password` field.

The maximum supported file size is 1 MB.

The maximum length of each line in the group file is 32,768 characters.

2. Verify that the list does not contain any duplicate information.

The list must not contain duplicate entries, or else loading the list fails. If there are entries already present in the SVM, you must either set the `-overwrite` parameter to `true` to overwrite all existing entries with the new file, or ensure that the new file does not contain any entries that duplicate existing entries.

3. Copy the file to a server.

The server must be reachable by the storage system over HTTP, HTTPS, FTP, or FTPS.

4. Determine what the URI for the file is.

The URI is the address you provide to the storage system to indicate where the file is located.

5. Load the file containing the list of local UNIX groups into the SVM from the URI:

```
vserver services name-service unix-group load-from-uri -vserver vserver_name
-uri {ftp|http|ftps|https}://uri -overwrite {true|false}
```

`-overwrite {true|false}` specifies whether to overwrite entries. The default is `false`. If you specify this parameter as `true`, ONTAP replaces the entire existing local UNIX group database of the specified SVM with the entries from the file you are loading.

### Example

The following command loads a list of local UNIX groups from the URI `ftp://ftp.example.com/group` into the SVM named `vs1`. Existing groups on the SVM are not overwritten by information from the URI.

```
vs1::> vserver services name-service unix-group load-from-uri -vserver vs1
-uri ftp://ftp.example.com/group -overwrite false
```

### Work with netgroups

#### Working with netgroups overview

You can use netgroups for user authentication and to match clients in export policy rules. You can provide access to netgroups from external name servers (LDAP or NIS), or you can load netgroups from a uniform resource identifier (URI) into SVMs using the `vserver services name-service netgroup load` command.

#### What you'll need

Before working with netgroups, you must ensure the following conditions are met:

- All hosts in netgroups, regardless of source (NIS, LDAP, or local files), must have both forward (A) and reverse (PTR) DNS records to provide consistent forward and reverse DNS lookups.

In addition, if an IP address of a client has multiple PTR records, all of those host names must be members of the netgroup and have corresponding A records.

- The names of all hosts in netgroups, regardless of their source (NIS, LDAP, or local files), must be correctly spelled and use the correct case. Case inconsistencies in host names used in netgroups can lead to unexpected behavior, such as failed export checks.
- All IPv6 addresses specified in netgroups must be shortened and compressed as specified in RFC 5952.

For example, `2011:hu9:0:0:0:0:3:1` must be shortened to `2011:hu9::3:1`.

#### About this task

When you work with netgroups, you can perform the following operations:

- You can use the `vserver export-policy netgroup check-membership` command to help determine whether a client IP is a member of a certain netgroup.
- You can use the `vserver services name-service getxxbyyy netgrp` command to check whether a client is part of a netgroup.

The underlying service for doing the lookup is selected based on the configured name service switch order.



## Load netgroups into SVMs

One of the methods you can use to match clients in export policy rules is by using hosts listed in netgroups. You can load netgroups from a uniform resource identifier (URI) into SVMs as an alternative to using netgroups stored in external name servers (`vserver services name-service netgroup load`).

### What you'll need

Netgroup files must meet the following requirements before being loaded into an SVM:

- The file must use the same proper netgroup text file format that is used to populate NIS.

ONTAP checks the netgroup text file format before loading it. If the file contains errors, it will not be loaded and a message is displayed indicating the corrections you have to perform in the file. After correcting the errors, you can reload the netgroup file into the specified SVM.

- Any alphabetic characters in host names in the netgroup file should be lowercase.
- The maximum supported file size is 5 MB.
- The maximum supported level for nesting netgroups is 1000.
- Only primary DNS host names can be used when defining host names in the netgroup file.

To avoid export access issues, host names should not be defined using DNS CNAME or round robin records.

- The user and domain portions of triples in the netgroup file should be kept empty because ONTAP does not support them.

Only the host/IP part is supported.

### About this task

ONTAP supports netgroup-by-host searches for the local netgroup file. After you load the netgroup file, ONTAP automatically creates a `netgroup.byhost` map to enable netgroup-by-host searches. This can significantly speed up local netgroup searches when processing export policy rules to evaluate client access.

### Step

1. Load netgroups into SVMs from a URI:

```
vserver services name-service netgroup load -vserver vserver_name -source {ftp|http|https|https}://uri
```

Loading the netgroup file and building the `netgroup.byhost` map can take several minutes.

If you want to update the netgroups, you can edit the file and load the updated netgroup file into the SVM.

### Example

The following command loads netgroup definitions into the SVM named `vs1` from the HTTP URL `http://intranet/downloads/corp-netgroup`:

```
vs1::> vserver services name-service netgroup load -vserver vs1
-source http://intranet/downloads/corp-netgroup
```

### Verify the status of netgroup definitions

After loading netgroups into the SVM, you can use the `vserver services name-service netgroup status` command to verify the status of netgroup definitions. This enables you to determine whether netgroup definitions are consistent on all of the nodes that back the SVM.

#### Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Verify the status of netgroup definitions:

```
vserver services name-service netgroup status
```

You can display additional information in a more detailed view.

3. Return to the admin privilege level:

```
set -privilege admin
```

#### Example

After the privilege level is set, the following command displays netgroup status for all SVMs:

```
vs1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when

directed to do so by technical support.

```
Do you wish to continue? (y or n): y
```

```
vs1::*> vserver services name-service netgroup status
```

Virtual

```
Server      Node          Load Time          Hash Value
```

```
-----  
-----
```

```
vs1
```

```
node1      9/20/2006 16:04:53
```

```
e6cb38ec1396a280c0d2b77e3a84eda2
```

```
node2      9/20/2006 16:06:26
```

```
e6cb38ec1396a280c0d2b77e3a84eda2
```

```
node3      9/20/2006 16:08:08
```

```
e6cb38ec1396a280c0d2b77e3a84eda2
```

```
node4      9/20/2006 16:11:33
```

```
e6cb38ec1396a280c0d2b77e3a84eda2
```

### Create an NIS domain configuration

If a Network Information Service (NIS) is used in your environment for name services, you must create an NIS domain configuration for the SVM by using the `vserver services name-service nis-domain create` command.

### What you'll need

All configured NIS servers must be available and reachable before you configure the NIS domain on the SVM.

If you plan to use NIS for directory searches, the maps in your NIS servers cannot have more than 1,024 characters for each entry. Do not specify the NIS server that does not comply with this limit. Otherwise, client access dependent on NIS entries might fail.

### About this task

You can create multiple NIS domains. However, you can only use one that is set to `active`.

If your NIS database contains a `netgroup.byhost` map, ONTAP can use it for quicker searches. The `netgroup.byhost` and `netgroup` maps in the directory must be kept in sync at all times to avoid client access issues. Beginning with ONTAP 9.7, NIS `netgroup.byhost` entries can be cached using the `vserver services name-service nis-domain netgroup-database` commands.

Using NIS for host name resolution is not supported.

### Steps

1. Create an NIS domain configuration:

```
vserver services name-service nis-domain create -vserver vs1 -domain
domain_name -active true -servers IP_addresses
```

You can specify up to 10 NIS servers.



Beginning with ONTAP 9.2, the field `-nis-servers` replaces the field `-servers`. This new field can take either a hostname or an IP address for the NIS server.

2. Verify that the domain is created:

```
vserver services name-service nis-domain show
```

### Example

The following command creates and makes an active NIS domain configuration for an NIS domain called `nisdomain` on the SVM named `vs1` with an NIS server at IP address `192.0.2.180`:

```
vs1::> vserver services name-service nis-domain create -vserver vs1
-domain nisdomain -active true -nis-servers 192.0.2.180
```

## Use LDAP

### Overview of using LDAP

If LDAP is used in your environment for name services, you need to work with your LDAP administrator to determine requirements and appropriate storage system configurations, then enable the SVM as an LDAP client.

Beginning with ONTAP 9.10.1, LDAP channel binding is supported by default for both Active Directory and name services LDAP connections. ONTAP will try channel binding with LDAP connections only if Start-TLS or LDAPS is enabled along with session security set to either `sign` or `seal`. To disable or reenabling LDAP channel binding with name servers, use the `-try-channel-binding` parameter with the `ldap client modify` command.

For more information, see

[2020 LDAP channel binding and LDAP signing requirements for Windows](#).

- Before configuring LDAP for ONTAP, you should verify that your site deployment meets best practices for LDAP server and client configuration. In particular, the following conditions must be met:
  - The domain name of the LDAP server must match the entry on the LDAP client.
  - The LDAP user password hash types supported by the LDAP server must include those supported by ONTAP:
    - CRYPT (all types) and SHA-1 (SHA, SSHA).
    - Beginning with ONTAP 9.8, SHA-2 hashes (SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384, and SSHA-512) are also supported.
  - If the LDAP server requires session security measures, you must configure them in the LDAP client.

The following session security options are available:

- LDAP signing (provides data integrity checking) and LDAP signing and sealing (provides data integrity checking and encryption)
- START TLS
- LDAPS (LDAP over TLS or SSL)
- To enable signed and sealed LDAP queries, the following services must be configured:
  - LDAP servers must support the GSSAPI (Kerberos) SASL mechanism.
  - LDAP servers must have DNS A/AAAA records as well as PTR records set up on the DNS server.
  - Kerberos servers must have SRV records present on the DNS server.
- To enable START TLS or LDAPS, the following points should be considered.
  - It is a NetApp best practice to use Start TLS rather than LDAPS.
  - If LDAPS is used, the LDAP server must be enabled for TLS or for SSL in ONTAP 9.5 and later. SSL is not supported in ONTAP 9.0-9.4.
  - A certificate server must already be configured in the domain.
- To enable LDAP referral chasing (in ONTAP 9.5 and later), the following conditions must be satisfied:
  - Both domains should be configured with one of the following trust relationships:
    - Two-way
    - One-way, where the primary trusts the referral domain
    - Parent-child
  - DNS must be configured to resolve all referred server names.
  - Domain passwords should be same to authenticate when `--bind-as-cifs-server` set to true.

The following configurations are not supported with LDAP referral chasing.



- For all ONTAP versions:
  - LDAP clients on an admin SVM
- For ONTAP 9.8 and earlier (they are supported in 9.9.1 and later):
  - LDAP signing and sealing (the `-session-security` option)
  - Encrypted TLS connections (the `-use-start-tls` option)
  - Communications over LDAPS port 636 (the `-use-ldaps-for-ad-ldap` option)

- You must enter an LDAP schema when configuring the LDAP client on the SVM.

In most cases, one of the default ONTAP schemas will be appropriate. However, if the LDAP schema in your environment differs from these, you must create a new LDAP client schema for ONTAP before creating the LDAP client. Consult with your LDAP administrator about requirements for your environment.

- Using LDAP for host name resolution is not supported.

For additional information, see [NetApp Technical Report 4835: How to Configure LDAP in ONTAP](#).

### Create a new LDAP client schema

If the LDAP schema in your environment differs from the ONTAP defaults, you must

create a new LDAP client schema for ONTAP before creating the LDAP client configuration.

### About this task

Most LDAP servers can use the default schemas provided by ONTAP:

- MS-AD-BIS (the preferred schema for most Windows 2012 and later AD servers)
- AD-IDMU (Windows 2008, Windows 2012 and later AD servers)
- AD-SFU (Windows 2003 and earlier AD servers)
- RFC-2307 (UNIX LDAP servers)

If you need to use a non-default LDAP schema, you must create it before creating the LDAP client configuration. Consult with your LDAP administrator before creating a new schema.

The default LDAP schemas provided by ONTAP cannot be modified. To create a new schema, you create a copy and then modify the copy accordingly.

### Steps

1. Display the existing LDAP client schema templates to identify the one you want to copy:

```
vserver services name-service ldap client schema show
```

2. Set the privilege level to advanced:

```
set -privilege advanced
```

3. Make a copy of an existing LDAP client schema:

```
vserver services name-service ldap client schema copy -vserver vserver_name  
-schema existing_schema_name -new-schema-name new_schema_name
```

4. Modify the new schema and customize it for your environment:

```
vserver services name-service ldap client schema modify
```

5. Return to the admin privilege level:

```
set -privilege admin
```

### Install the self-signed root CA certificate on the SVM

If LDAP authentication with TLS is required when binding to LDAP servers, you must first install the self-signed root CA certificate on the SVM.

### About this task

When LDAP over TLS is enabled, the ONTAP LDAP client on the SVM does not support revoked certificates in ONTAP 9.0 and 9.1.

Beginning with ONTAP 9.2, all applications within ONTAP that use TLS communications can check digital certificate status using Online Certificate Status Protocol (OCSP). If OCSP is enabled for LDAP over TLS, revoked certificates are rejected and the connection fails.

## Steps

1. Install the self-signed root CA certificate:

- a. Begin the certificate installation:

```
security certificate install -vserver vserver_name -type server-ca
```

The console output displays the following message:

```
Please enter Certificate: Press <Enter> when done
```

- b. Open the certificate `.pem` file with a text editor, copy the certificate, including the lines beginning with `-----BEGIN CERTIFICATE-----` and ending with `-----END CERTIFICATE-----`, and then paste the certificate after the command prompt.
- c. Verify that the certificate is displayed correctly.
- d. Complete the installation by pressing Enter.

2. Verify that the certificate is installed:

```
security certificate show -vserver vserver_name
```

## Create an LDAP client configuration

If you want ONTAP to access the external LDAP servers in your environment, you must first set up an LDAP client on the storage system.

### What you'll need

One of the first three servers in the AD-domain resolved list must be up and serving data. Otherwise, this task fails.



There are multiple servers, out of which more than two servers are down at any point of time.

## Steps

1. Consult with your LDAP administrator to determine the appropriate configuration values for the `vserver services name-service ldap client create` command:

- a. Specify a domain-based or an address-based connection to LDAP servers.

The `-ad-domain` and `-servers` options are mutually exclusive.

- Use the `-ad-domain` option to enable LDAP server discovery in the Active Directory domain.

You can use the `-preferred-ad-servers` option to specify one or more preferred Active Directory servers by IP address in a comma-delimited list. After the client is created, you can modify this list by using the `vserver services name-service ldap client modify` command.

- Use the `-servers` option to specify one or more LDAP servers (AD or UNIX) by IP address in a comma-delimited list.



The `-servers` option is deprecated in ONTAP 9.2. Beginning with ONTAP 9.2, the `-ldap-servers` field replaces the `-servers` field. This new field can take either a host name or an IP address for the LDAP server.

b. Specify a default or custom LDAP schema.

Most LDAP servers can use the default read-only schemas that are provided by ONTAP. It is best to use those default schemas unless there is a requirement to do otherwise. If so, you can create your own schema by copying a default schema (they are read-only), and then modifying the copy.

Default schemas:

- MS-AD-BIS

Based on RFC-2307bis, this is the preferred LDAP schema for most standard Windows 2012 and later LDAP deployments.

- AD-IDMU

Based on Active Directory Identity Management for UNIX, this schema is appropriate for most Windows 2008, Windows 2012, and later AD servers.

- AD-SFU

Based on Active Directory Services for UNIX, this schema is appropriate for most Windows 2003 and earlier AD servers.

- RFC-2307

Based on RFC-2307 (*An Approach for Using LDAP as a Network Information Service*), this schema is appropriate for most UNIX AD servers.

c. Select bind values.

- `-min-bind-level {anonymous|simple|sasl}` specifies the minimum bind authentication level.

The default value is **anonymous**.

- `-bind-dn LDAP_DN` specifies the bind user.

For Active Directory servers, you must specify the user in the account (DOMAIN\user) or principal (user@domain.com) form. Otherwise, you must specify the user in distinguished name (CN=user,DC=domain,DC=com) form.

- `-bind-password password` specifies the bind password.

d. Select session security options, if required.

You can enable either LDAP signing and sealing or LDAP over TLS if required by the LDAP server.

- `--session-security {none|sign|seal}`

You can enable signing (sign, data integrity), signing and sealing (seal, data integrity and encryption), or neither (none, no signing or sealing). The default value is none.



You should also set `-min-bind-level {sasl}` unless you want the bind authentication to fall back to **anonymous** or **simple** if the signing and sealing bind fails.

- `-use-start-tls {true|false}`

If set to **true** and the LDAP server supports it, the LDAP client uses an encrypted TLS connection to the server. The default value is **false**. You must install a self-signed root CA certificate of the LDAP server to use this option.



If the SVM has a SMB server added to a domain and the LDAP server is one of the domain controllers of the home-domain of the SMB server, then you can modify the `-session-security-for-ad-ldap` option by using the `vserver cifs security modify` command.

e. Select port, query, and base values.

The default values are recommended, but you must verify with your LDAP administrator that they are appropriate for your environment.

- `-port port` specifies the LDAP server port.

The default value is 389.

If you plan to use Start TLS to secure the LDAP connection, you must use the default port 389. Start TLS begins as a plaintext connection over the LDAP default port 389, and that connection is then upgraded to TLS. If you change the port, Start TLS fails.

- `-query-timeout integer` specifies the query timeout in seconds.

The allowed range is from 1 through 10 seconds. The default value is 3 seconds.

- `-base-dn LDAP_DN` specifies the base DN.

Multiple values can be entered if needed (for example, if LDAP referral chasing is enabled). The default value is "" (root).

- `-base-scope {base|onelevel|subtree}` specifies the base search scope.

The default value is `subtree`.

- `-referral-enabled {true|false}` specifies whether LDAP referral chasing is enabled.

Beginning with ONTAP 9.5, this allows the ONTAP LDAP client to refer look-up requests to other LDAP servers if an LDAP referral response is returned by the primary LDAP server indicating that the desired records are present on referred LDAP servers. The default value is **false**.

To search for records present in the referred LDAP servers, the base-dn of the referred records must be added to the base-dn as part of LDAP client configuration.

2. Create an LDAP client configuration on the SVM:

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain
```

```
-preferred-ad-servers preferred_ad_server_list -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```



You must provide the SVM name when creating an LDAP client configuration.

3. Verify that the LDAP client configuration is created successfully:

```
vserver services name-service ldap client show -client-config
client_config_name
```

### Examples

The following command creates a new LDAP client configuration named `ldap1` for the SVM `vs1` to work with an Active Directory server for LDAP:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100
```

The following command creates a new LDAP client configuration named `ldap1` for the SVM `vs1` to work with an Active Directory server for LDAP on which signing and sealing is required:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

The following command creates a new LDAP client configuration named `ldap1` for the SVM `vs1` to work with an Active Directory server for LDAP where LDAP referral chasing is required:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

The following command modifies the LDAP client configuration named `ldap1` for the SVM `vs1` by specifying the base DN:

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

The following command modifies the LDAP client configuration named `ldap1` for the SVM `vs1` by enabling referral chasing:

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com" -referral-enabled true
```

## Associate the LDAP client configuration with SVMs

To enable LDAP on an SVM, you must use the `vserver services name-service ldap create` command to associate an LDAP client configuration with the SVM.

### What you'll need

- An LDAP domain must already exist within the network and must be accessible to the cluster that the SVM is located on.
- An LDAP client configuration must exist on the SVM.

### Steps

1. Enable LDAP on the SVM:

```
vserver services name-service ldap create -vserver vserver_name -client-config
client_config_name
```



Beginning with ONTAP 9.2, the `vserver services name-service ldap create` command performs an automatic configuration validation and reports an error message if ONTAP is unable to contact the name server.

The following command enables LDAP on the "vs1" SVM and configures it to use the "ldap1" LDAP client configuration:

```
cluster1::> vserver services name-service ldap create -vserver vs1
-client-config ldap1 -client-enabled true
```

2. Validate the status of the name servers by using the `vserver services name-service ldap check` command.

The following command validates LDAP servers on the SVM `vs1`.

```
cluster1::> vserver services name-service ldap check -vserver vs1

| Vserver: vs1 |
| Client Configuration Name: c1 |
| LDAP Status: up |
| LDAP Status Details: Successfully connected to LDAP server |
| "10.11.12.13". |
```

The name service check command is available beginning with ONTAP 9.2.

### Verify LDAP sources in the name service switch table

You must verify that LDAP sources for name services are listed correctly in the name service switch table for the SVM.

#### Steps

1. Display the current name service switch table contents:

```
vserver services name-service ns-switch show -vserver svm_name
```

The following command shows the results for the SVM My\_SVM:

```
ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM

Vserver      Database      Source
-----      -
My_SVM      hosts        files,
              dns
My_SVM      group        files,ldap
My_SVM      passwd       files,ldap
My_SVM      netgroup     files
My_SVM      namemap      files
5 entries were displayed.
```

namemap specifies the sources to search for name mapping information and in what order. In a UNIX-only environment, this entry is not necessary. Name mapping is only required in a mixed environment using both UNIX and Windows.

2. Update the ns-switch entry as appropriate:

If you want to update the ns-switch entry for...	Enter the command...
User information	<pre>vserver services name-service ns-switch modify -vserver vserver_name -database passwd -sources ldap,files</pre>

If you want to update the ns-switch entry for...	Enter the command...
Group information	<pre>vserver services name-service ns- switch modify -vserver vserver_name -database group -sources ldap,files</pre>
Netgroup information	<pre>vserver services name-service ns- switch modify -vserver vserver_name -database netgroup -sources ldap,files</pre>

## Use Kerberos with NFS for strong security

### Overview of using Kerberos with NFS for strong security

If Kerberos is used in your environment for strong authentication, you need to work with your Kerberos administrator to determine requirements and appropriate storage system configurations, and then enable the SVM as a Kerberos client.

Your environment should meet the following guidelines:

- Your site deployment should follow best practices for Kerberos server and client configuration before you configure Kerberos for ONTAP.
- If possible, use NFSv4 or later if Kerberos authentication is required.

NFSv3 can be used with Kerberos. However, the full security benefits of Kerberos are only realized in ONTAP deployments of NFSv4 or later.

- To promote redundant server access, Kerberos should be enabled on several data LIFs on multiple nodes in the cluster using the same SPN.
- When Kerberos is enabled on the SVM, one of the following security methods must be specified in export rules for volumes or qtrees depending on your NFS client configuration.
  - `krb5` (Kerberos v5 protocol)
  - `krb5i` (Kerberos v5 protocol with integrity checking using checksums)
  - `krb5p` (Kerberos v5 protocol with privacy service)

In addition to the Kerberos server and clients, the following external services must be configured for ONTAP to support Kerberos:

- Directory service

You should use a secure directory service in your environment, such as Active Directory or OpenLDAP, that is configured to use LDAP over SSL/TLS. Do not use NIS, whose requests are sent in clear text and are hence not secure.

- NTP

You must have a working time server running NTP. This is necessary to prevent Kerberos authentication failure due to time skew.

- Domain name resolution (DNS)

Each UNIX client and each SVM LIF must have a proper service record (SRV) registered with the KDC under forward and reverse lookup zones. All participants must be properly resolvable via DNS.

### Verify permissions for Kerberos configuration

Kerberos requires that certain UNIX permissions be set for the SVM root volume and for local users and groups.

### Steps

1. Display the relevant permissions on the SVM root volume:

```
volume show -volume root_vol_name-fields user,group,unix-permissions
```

The root volume of the SVM must have the following configuration:

Name...	Setting...
UID	root or ID 0
GID	root or ID 0
UNIX permissions	755

If these values are not shown, use the `volume modify` command to update them.

2. Display the local UNIX users:

```
vserver services name-service unix-user show -vserver vserver_name
```

The SVM must have the following UNIX users configured:

User name	User ID	Primary group ID	Comment
nfs	500	0	<p>Required for GSS INIT phase.</p> <p>The first component of the NFS client user SPN is used as the user.</p> <p>The nfs user is not required if a Kerberos-UNIX name mapping exists for the SPN of the NFS client user.</p>
root	0	0	Required for mounting.

If these values are not shown, you can use the `vserver services name-service unix-user modify` command to update them.

### 3. Display the local UNIX groups:

```
vserver services name-service unix-group show -vserver vserver _name
```

The SVM must have the following UNIX groups configured:

Group name	Group ID
daemon	1
root	0

If these values are not shown, you can use the `vserver services name-service unix-group modify` command to update them.

## Create an NFS Kerberos realm configuration

If you want ONTAP to access external Kerberos servers in your environment, you must first configure the SVM to use an existing Kerberos realm. To do so, you need to gather configuration values for the Kerberos KDC server, and then use the `vserver nfs kerberos realm create` command to create the Kerberos realm configuration on an SVM.

### What you'll need

The cluster administrator should have configured NTP on the storage system, client, and KDC server to avoid authentication issues. Time differences between a client and server (clock skew) are a common cause of authentication failures.

### Steps

1. Consult with your Kerberos administrator to determine the appropriate configuration values to supply with the `vserver nfs kerberos realm create` command.
2. Create a Kerberos realm configuration on the SVM:

```
vserver nfs kerberos realm create -vserver vserver_name -realm realm_name  
{AD_KDC_server_values |AD_KDC_server_values} -comment "text"
```

3. Verify that the Kerberos realm configuration was created successfully:

```
vserver nfs kerberos realm show
```

### Examples

The following command creates an NFS Kerberos realm configuration for the SVM vs1 that uses a Microsoft Active Directory server as the KDC server. The Kerberos realm is AUTH.EXAMPLE.COM. The Active Directory server is named ad-1 and its IP address is 10.10.8.14. The permitted clock skew is 300 seconds (the default). The IP address of the KDC server is 10.10.8.14, and its port number is 88 (the default). "Microsoft Kerberos config" is the comment.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
AUTH.EXAMPLE.COM -adserver-name ad-1
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88
-kdc-vendor Microsoft
-comment "Microsoft Kerberos config"
```

The following command creates an NFS Kerberos realm configuration for the SVM vs1 that uses an MIT KDC. The Kerberos realm is SECURITY.EXAMPLE.COM. The permitted clock skew is 300 seconds. The IP address of the KDC server is 10.10.9.1, and its port number is 88. The KDC vendor is Other to indicate a UNIX vendor. The IP address of the administrative server is 10.10.9.1, and its port number is 749 (the default). The IP address of the password server is 10.10.9.1, and its port number is 464 (the default). "UNIX Kerberos config" is the comment.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
SECURITY.EXAMPLE.COM. -clock-skew 300
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1
-adminserver-port 749
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX
Kerberos config"
```

### Configure NFS Kerberos permitted encryption types

By default, ONTAP supports the following encryption types for NFS Kerberos: DES, 3DES, AES-128, and AES-256. You can configure the permitted encryption types for each SVM to suit the security requirements for your particular environment by using the `vserver nfs modify` command with the `-permitted-enc-types` parameter.

#### About this task

For greatest client compatibility, ONTAP supports both weak DES and strong AES encryption by default. This means, for example, that if you want to increase security and your environment supports it, you can use this procedure to disable DES and 3DES and require clients to use only AES encryption.

You should use the strongest encryption available. For ONTAP, that is AES-256. You should confirm with your KDC administrator that this encryption level is supported in your environment.

- Enabling or disabling AES entirely (both AES-128 and AES-256) on SVMs is disruptive because it destroys the original DES principal/keytab file, thereby requiring that the Kerberos configuration be disabled on all LIFs for the SVM.

Before making this change, you should verify that NFS clients do not rely on AES encryption on the SVM.

- Enabling or disabling DES or 3DES does not require any changes to the Kerberos configuration on LIFs.

#### Step

1. Enable or disable the permitted encryption type you want:



If you want to enable or disable...	Follow these steps...
DES or 3DES	<p>a. Configure the NFS Kerberos permitted encryption types of the SVM:</p> <pre data-bbox="889 268 1442 365">vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types</pre> <p>Separate multiple encryption types with a comma.</p> <p>b. Verify that the change was successful:</p> <pre data-bbox="889 583 1474 680">vserver nfs show -vserver vserver_name -fields permitted-enc- types</pre>

If you want to enable or disable...	Follow these steps...
AES-128 or AES-256	<p>a. Identify on which SVM and LIF Kerberos is enabled:</p> <pre>vserver nfs kerberos interface show</pre> <p>b. Disable Kerberos on all LIFs on the SVM whose NFS Kerberos permitted encryption type you want to modify:</p> <pre>vserver nfs kerberos interface disable -lif lif_name</pre> <p>c. Configure the NFS Kerberos permitted encryption types of the SVM:</p> <pre>vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types</pre> <p>Separate multiple encryption types with a comma.</p> <p>d. Verify that the change was successful:</p> <pre>vserver nfs show -vserver vserver_name -fields permitted-enc- types</pre> <p>e. Reenable Kerberos on all LIFs on the SVM:</p> <pre>vserver nfs kerberos interface enable -lif lif_name -spn service_principal_name</pre> <p>f. Verify that Kerberos is enabled on all LIFs:</p> <pre>vserver nfs kerberos interface show</pre>

### Enable Kerberos on a data LIF

You can use the `vserver nfs kerberos interface enable` command to enable Kerberos on a data LIF. This enables the SVM to use Kerberos security services for NFS.

#### About this task

If you are using an Active Directory KDC, the first 15 characters of any SPNs used must be unique across SVMs within a realm or domain.

#### Steps

1. Create the NFS Kerberos configuration:

```
vserver nfs kerberos interface enable -vserver vserver_name -lif
```

```
logical_interface -spn service_principal_name
```

ONTAP requires the secret key for the SPN from the KDC to enable the Kerberos interface.

For Microsoft KDCs, the KDC is contacted and a user name and password prompt are issued at the CLI to obtain the secret key. If you need to create the SPN in a different OU of the Kerberos realm, you can specify the optional `-ou` parameter.

For non-Microsoft KDCs, the secret key can be obtained using one of two methods:

If you...	You must also include the following parameter with the command...
Have the KDC administrator credentials to retrieve the key directly from the KDC	<code>-admin-username kdc_admin_username</code>
Do not have the KDC administrator credentials but have a keytab file from the KDC containing the key	<code>-keytab-uri {ftp http}://uri</code>

2. Verify that Kerberos was enabled on the LIF:

```
vserver nfs kerberos-config show
```

3. Repeat steps 1 and 2 to enable Kerberos on multiple LIFs.

### Example

The following command creates and verifies an NFS Kerberos configuration for the SVM named `vs1` on the logical interface `ves03-d1`, with the SPN `nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM` in the OU `lab2ou`:

```
vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vserver nfs kerberos-config show
      Logical
Vserver Interface Address      Kerberos  SPN
-----
vs0      ves01-a1
          10.10.10.30  disabled  -
vs2      ves01-d1
          10.10.10.40  enabled   nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```

## Add storage capacity to an NFS-enabled SVM

## Add storage capacity to an NFS-enabled SVM overview

To add storage capacity to an NFS-enabled SVM, you must create a volume or qtree to provide a storage container, and create or modify an export policy for that container. You can then verify NFS client access from the cluster and test access from client systems.

### What you'll need

- NFS must be completely set up on the SVM.
- The default export policy of the SVM root volume must contain a rule that permits access to all clients.
- Any updates to your name services configuration must be complete.
- Any additions or modifications to a Kerberos configuration must be complete.

### Create an export policy

Before creating export rules, you must create an export policy to hold them. You can use the `vserver export-policy create` command to create an export policy.

#### Steps

1. Create an export policy:

```
vserver export-policy create -vserver vserver_name -policyname policy_name
```

The policy name can be up to 256 characters long.

2. Verify that the export policy was created:

```
vserver export-policy show -policyname policy_name
```

#### Example

The following commands create and verify the creation of an export policy named `exp1` on the SVM named `vs1`:

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1

vs1::> vserver export-policy show -policyname exp1
Vserver          Policy Name
-----
vs1              exp1
```

### Add a rule to an export policy

Without rules, the export policy cannot provide client access to data. To create a new export rule, you must identify clients and select a client match format, select the access and security types, specify an anonymous user ID mapping, select a rule index number, and select the access protocol. You can then use the `vserver export-policy rule create` command to add the new rule to an export policy.

## What you'll need

- The export policy you want to add the export rules to must already exist.
- DNS must be correctly configured on the data SVM and DNS servers must have correct entries for NFS clients.

This is because ONTAP performs DNS lookups using the DNS configuration of the data SVM for certain client match formats, and failures in export policy rule matching can prevent client data access.

- If you are authenticating with Kerberos, you must have determined which of the following security methods is used on your NFS clients:
  - `krb5` (Kerberos V5 protocol)
  - `krb5i` (Kerberos V5 protocol with integrity checking using checksums)
  - `krb5p` (Kerberos V5 protocol with privacy service)

## About this task

It is not necessary to create a new rule if an existing rule in an export policy covers your client match and access requirements.

If you are authenticating with Kerberos and if all volumes of the SVM are accessed over Kerberos, you can set the export rule options `-rorule`, `-rwrule`, and `-superuser` for the root volume to `krb5`, `krb5i`, or `krb5p`.

## Steps

1. Identify the clients and the client match format for the new rule.

The `-clientmatch` option specifies the clients to which the rule applies. Single or multiple client match values can be specified; specifications of multiple values must be separated by commas. You can specify the match in any of the following formats:

Client match format	Example
Domain name preceded by the "." character	<code>.example.com</code> or <code>.example.com, .example.net, ...</code>
Host name	<code>host1</code> or <code>host1, host2, ...</code>
IPv4 address	<code>10.1.12.24</code> or <code>10.1.12.24, 10.1.12.25, ...</code>
IPv4 address with a subnet mask expressed as a number of bits	<code>10.1.12.10/4</code> or <code>10.1.12.10/4, 10.1.12.11/4, ...</code>
IPv4 address with a network mask	<code>10.1.16.0/255.255.255.0</code> or <code>10.1.16.0/255.255.255.0, 10.1.17.0/255.255.255.0, ...</code>
IPv6 address in dotted format	<code>::1.2.3.4</code> or <code>::1.2.3.4, ::1.2.3.5, ...</code>

Client match format	Example
IPv6 address with a subnet mask expressed as a number of bits	ff::00/32 or ff::00/32, ff::01/32, ...
A single netgroup with the netgroup name preceded by the @ character	@netgroup1 or @netgroup1, @netgroup2, ...

You can also combine types of client definitions; for example, `.example.com, @netgroup1`.

When specifying IP addresses, note the following:

- Entering an IP address range, such as `10.1.12.10-10.1.12.70`, is not allowed.

Entries in this format are interpreted as a text string and treated as a host name.

- When specifying individual IP addresses in export rules for granular management of client access, do not specify IP addresses that are dynamically (for example, DHCP) or temporarily (for example, IPv6) assigned.

Otherwise, the client loses access when its IP address changes.

- Entering an IPv6 address with a network mask, such as `ff::12/ff::00`, is not allowed.

## 2. Select the access and security types for client matches.

You can specify one or more of the following access modes to clients that authenticate with the specified security types:

- `-rorule` (read-only access)
- `-rwrule` (read-write access)
- `-superuser` (root access)



A client can only get read-write access for a specific security type if the export rule allows read-only access for that security type as well. If the read-only parameter is more restrictive for a security type than the read-write parameter, the client might not get read-write access. The same is true for superuser access.

You can specify a comma-separated list of multiple security types for a rule. If you specify the security type as `any` or `never`, do not specify any other security types. Choose from the following valid security types:

When security type is set to...	A matching client can access the exported data...
<code>any</code>	Always, regardless of incoming security type.

When security type is set to...	A matching client can access the exported data...
none	If listed alone, clients with any security type are granted access as anonymous. If listed with other security types, clients with a specified security type are granted access and clients with any other security type are granted access as anonymous.
never	Never, regardless of incoming security type.
krb5	If it is authenticated by Kerberos 5. Authentication only: The header of each request and response is signed.
krb5i	If it is authenticated by Kerberos 5i. Authentication and integrity: The header and body of each request and response is signed.
krb5p	If it is authenticated by Kerberos 5p. Authentication, integrity, and privacy: The header and body of each request and response is signed, and the NFS data payload is encrypted.
ntlm	If it is authenticated by CIFS NTLM.
sys	If it is authenticated by NFS AUTH_SYS.

The recommended security type is `sys`, or if Kerberos is used, `krb5`, `krb5i`, or `krb5p`.

If you are using Kerberos with NFSv3, the export policy rule must allow `-rorule` and `-rwrule` access to `sys` in addition to `krb5`. This is because of the need to allow Network Lock Manager (NLM) access to the export.

### 3. Specify an anonymous user ID mapping.

The `-anon` option specifies a UNIX user ID or user name that is mapped to client requests that arrive with a user ID of 0 (zero), which is typically associated with the user name `root`. The default value is `65534`. NFS clients typically associate user ID `65534` with the user name `nobody` (also known as *root squashing*). In ONTAP, this user ID is associated with the user `pcuser`. To disable access by any client with a user ID of 0, specify a value of `65535`.

### 4. Select the rule index order.

The `-ruleindex` option specifies the index number for the rule. Rules are evaluated according to their order in the list of index numbers; rules with lower index numbers are evaluated first. For example, the rule with index number 1 is evaluated before the rule with index number 2.

If you are adding...	Then...
The first rule to an export policy	Enter 1.
Additional rules to an export policy	<p>a. Display existing rules in the policy:</p> <pre>vserver export-policy rule show -instance -policyname <i>your_policy</i></pre> <p>b. Select an index number for the new rule depending on the order it should be evaluated.</p>

5. Select the applicable NFS access value: {nfs|nfs3|nfs4}.

`nfs` matches any version, `nfs3` and `nfs4` match only those specific versions.

6. Create the export rule and add it to an existing export policy:

```
vserver export-policy rule create -vserver vserver_name -policyname
policy_name -ruleindex integer -protocol {nfs|nfs3|nfs4} -clientmatch { text |
"text,text,..." } -rorule security_type -rwrule security_type -superuser
security_type -anon user_ID
```

7. Display the rules for the export policy to verify that the new rule is present:

```
vserver export-policy rule show -policyname policy_name
```

The command displays a summary for that export policy, including a list of rules applied to that policy. ONTAP assigns each rule a rule index number. After you know the rule index number, you can use it to display detailed information about the specified export rule.

8. Verify that the rules applied to the export policy are configured correctly:

```
vserver export-policy rule show -policyname policy_name -vserver vserver_name
-ruleindex integer
```

## Examples

The following commands create and verify the creation of an export rule on the SVM named `vs1` in an export policy named `rs1`. The rule has the index number 1. The rule matches any client in the domain `eng.company.com` and the netgroup `@netgroup1`. The rule enables all NFS access. It enables read-only and read-write access to users that authenticated with `AUTH_SYS`. Clients with the UNIX user ID 0 (zero) are anonymized unless authenticated with Kerberos.



```
vs1::> vserver export-policy rule create -vserver vs1 -policyname expl
-ruleindex 1 -protocol nfs
-clientmatch eng.company.com,@netgroup1 -rorule sys -rwrule sys -anon 65534
-superuser krb5
```

```
vs1::> vserver export-policy rule show -policyname nfs_policy
```

Virtual Server	Policy Name	Rule Index	Access Protocol	Client Match	RO Rule
vs1	expl	1	nfs	eng.company.com, @netgroup1	sys

```
vs1::> vserver export-policy rule show -policyname expl -vserver vs1
-ruleindex 1
```

```
                Vserver: vs1
                Policy Name: expl
                Rule Index: 1
                Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
eng.company.com,@netgroup1
                RO Access Rule: sys
                RW Access Rule: sys
User ID To Which Anonymous Users Are Mapped: 65534
                Superuser Security Types: krb5
                Honor SetUID Bits in SETATTR: true
                Allow Creation of Devices: true
```

The following commands create and verify the creation of an export rule on the SVM named vs2 in an export policy named expol2. The rule has the index number 21. The rule matches clients to members of the netgroup dev\_netgroup\_main. The rule enables all NFS access. It enables read-only access for users that authenticated with AUTH\_SYS and requires Kerberos authentication for read-write and root access. Clients with the UNIX user ID 0 (zero) are denied root access unless authenticated with Kerberos.

```
vs2::> vsserver export-policy rule create -vserver vs2 -policyname expol2
-ruleindex 21 -protocol nfs
-clientmatch @dev_netgroup_main -rorule sys -rwrule krb5 -anon 65535
-superuser krb5
```

```
vs2::> vsserver export-policy rule show -policyname nfs_policy
Virtual Policy      Rule      Access      Client      RO
Server  Name        Index    Protocol    Match      Rule
-----
vs2     expol2        21       nfs         @dev_netgroup_main  sys
```

```
vs2::> vsserver export-policy rule show -policyname expol2 -vserver vs1
-ruleindex 21
```

```

                                Vserver: vs2
                                Policy Name: expol2
                                Rule Index: 21
                                Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
                                @dev_netgroup_main
                                RO Access Rule: sys
                                RW Access Rule: krb5
User ID To Which Anonymous Users Are Mapped: 65535
                                Superuser Security Types: krb5
                                Honor SetUID Bits in SETATTR: true
                                Allow Creation of Devices: true
```

## Create a volume or qtree storage container

### Create a volume

You can create a volume and specify its junction point and other properties by using the `volume create` command.

### What you'll need

The SVM security style must be UNIX, and NFS should be set up and running.

### About this task

A volume must include a *junction path* for its data to be made available to clients. You can specify the junction path when you create a new volume. If you create a volume without specifying a junction path, you must *mount* the volume in the SVM namespace using the `volume mount` command.

### Steps

1. Create the volume with a junction point:

```
volume create -vserver vserver_name -volume volume_name -aggregate
aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style unix -user
```

```
user_name_or_number -group group_name_or_number -junction-path junction_path
[-policy export_policy_name]
```

The choices for `-junction-path` are the following:

- Directly under root, for example, `/new_vol`

You can create a new volume and specify that it be mounted directly to the SVM root volume.

- Under an existing directory, for example, `/existing_dir/new_vol`

You can create a new volume and specify that it be mounted to an existing volume (in an existing hierarchy), expressed as a directory.

If you want to create a volume in a new directory (in a new hierarchy under a new volume), for example, `/new_dir/new_vol`, then you must first create a new parent volume that is junctioned to the SVM root volume. You would then create the new child volume in the junction path of the new parent volume (new directory).

+

If you plan to use an existing export policy, you can specify it when you create the volume. You can also add an export policy later with the `volume modify` command.

2. Verify that the volume was created with the desired junction point:

```
volume show -vserver vserver_name -volume volume_name -junction
```

## Examples

The following command creates a new volume named `users1` on the SVM `vs1.example.com` and the aggregate `aggr1`. The new volume is made available at `/users`. The volume is 750 GB in size, and its volume guarantee is of type `volume` (by default).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction

          Junction
Vserver   Volume  Active  Junction Path  Junction
-----  -
vs1.example.com  users1  true    /users         RW_volume
```

The following command creates a new volume named "home4" on the SVM "vs1.example.com" and the aggregate "aggr1". The directory `/eng/` already exists in the namespace for the `vs1` SVM, and the new volume is made available at `/eng/home`, which becomes the home directory for the `/eng/` namespace. The volume is 750 GB in size, and its volume guarantee is of type `volume` (by default).

```

cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction

```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1.example.com	home4	true	/eng/home	RW_volume

### Create a qtree

You can create a qtree to contain your data and specify its properties by using the `volume qtree create` command.

### What you'll need

- The SVM and the volume that will contain the new qtree must already exist.
- The SVM security style must be UNIX, and NFS should be set up and running.

### Steps

1. Create the qtree:

```

volume qtree create -vserver vserver_name { -volume volume_name -qtree
qtree_name | -qtree-path qtree_path } -security-style unix [-policy
export_policy_name]

```

You can specify the volume and qtree as separate arguments or specify the qtree path argument in the format `/vol/volume_name/_qtree_name`.

By default, qtrees inherit the export policies of their parent volume, but they can be configured to use their own. If you plan to use an existing export policy, you can specify it when you create the qtree. You can also add an export policy later with the `volume qtree modify` command.

2. Verify that the qtree was created with the desired junction path:

```

volume qtree show -vserver vserver_name { -volume volume_name -qtree
qtree_name | -qtree-path qtree_path }

```

### Example

The following example creates a qtree named `qt01` located on SVM `vs1.example.com` that has a junction path `/vol/data1`:

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style unix
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01
```

```
          Vserver Name: vs1.example.com
          Volume Name: data1
          Qtree Name: qt01
Actual (Non-Junction) Qtree Path: /vol/data1/qt01
          Security Style: unix
          Oplock Mode: enable
          Unix Permissions: ---rwxr-xr-x
          Qtree Id: 2
          Qtree Status: normal
          Export Policy: default
Is Export Policy Inherited: true
```

## Secure NFS access using export policies

### Secure NFS access using export policies

You can use export policies to restrict NFS access to volumes or qtrees to clients that match specific parameters. When provisioning new storage, you can use an existing policy and rules, add rules to an existing policy, or create a new policy and rules. You can also check the configuration of export policies



Beginning with ONTAP 9.3, you can enable export policy configuration checking as a background job that records any rules violations in an error rule list. The `vserver export-policy config-checker` commands invoke the checker and display results, which you can use to verify your configuration and delete erroneous rules from the policy. The commands only validate export configuration for host names, netgroups, and anonymous users.

### Manage the processing order of export rules

You can use the `vserver export-policy rule setindex` command to manually set an existing export rule's index number. This enables you to specify the precedence by which ONTAP applies export rules to client requests.

#### About this task

If the new index number is already in use, the command inserts the rule at the specified spot and reorders the list accordingly.

#### Step

1. Modify the index number of a specified export rule:

```
vserver export-policy rule setindex -vserver virtual_server_name -policyname
policy_name -ruleindex integer -newruleindex integer
```

### Example

The following command changes the index number of an export rule at index number 3 to index number 2 in an export policy named rs1 on the SVM named vs1:

```
vs1::> vserver export-policy rule setindex -vserver vs1
-policyname rs1 -ruleindex 3 -newruleindex 2
```

### Assign an export policy to a volume

Each volume contained in the SVM must be associated with an export policy that contains export rules for clients to access data in the volume.

#### About this task

You can associate an export policy to a volume when you create the volume or at any time after you create the volume. You can associate one export policy to the volume, although one policy can be associated to many volumes.

#### Steps

1. If an export policy was not specified when the volume was created, assign an export policy to the volume:

```
volume modify -vserver vserver_name -volume volume_name -policy
export_policy_name
```

2. Verify that the policy was assigned to the volume:

```
volume show -volume volume_name -fields policy
```

### Example

The following commands assign the export policy `nfs_policy` to the volume `vol1` on the SVM `vs1` and verify the assignment:

```
cluster::> volume modify -vserver vs1 -volume vol1 -policy nfs_policy

cluster::>volume show -volume vol -fields policy
vserver volume      policy
-----
vs1      vol1      nfs_policy
```

### Assign an export policy to a qtree

Instead of exporting an entire volume, you can also export a specific qtree on a volume to make it directly accessible to clients. You can export a qtree by assigning an export policy to it. You can assign the export policy either when you create a new qtree or by modifying an existing qtree.

## What you'll need

The export policy must exist.

## About this task

By default, qtrees inherit the parent export policy of the containing volume if not otherwise specified at the time of creation.

You can associate an export policy to a qtree when you create the qtree or at any time after you create the qtree. You can associate one export policy to the qtree, although one policy can be associated with many qtrees.

## Steps

1. If an export policy was not specified when the qtree was created, assign an export policy to the qtree:

```
volume qtree modify -vserver vs1 -qtree-path /vol/volume_name/qtree_name -export-policy export_policy_name
```

2. Verify that the policy was assigned to the qtree:

```
volume qtree show -qtree qtree_name -fields export-policy
```

## Example

The following commands assign the export policy `nfs_policy` to the qtree `qt1` on the SVM `vs1` and verify the assignment:

```
cluster::> volume modify -vserver vs1 -qtree-path /vol/vol1/qt1 -policy
nfs_policy

cluster::>volume qtree show -volume vol1 -fields export-policy
vserver volume qtree export-policy
-----
vs1      data1  qt01  nfs_policy
```

## Verify NFS client access from the cluster

You can give select clients access to the share by setting UNIX file permissions on a UNIX administration host. You can check client access by using the `vserver export-policy check-access` command, adjusting the export rules as necessary.

## Steps

1. On the cluster, check client access to exports by using the `vserver export-policy check-access` command.

The following command checks read/write access for an NFSv3 client with the IP address `1.2.3.4` to the volume `home2`. The command output shows that the volume uses the export policy `exp-home-dir` and that access is denied.

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
1.2.3.4 -volume home2 -authentication-method sys -protocol nfs3 -access
-type read-write
```

Path	Policy	Policy Owner	Policy Owner Type	Rule Index	Access
/	default	vs1_root	volume	1	read
/eng	default	vs1_root	volume	1	read
/eng/home2	exp-home-dir	home2	volume	1	denied

3 entries were displayed.

2. Examine the output to determine whether the export policy works as intended and the client access behaves as expected.

Specifically, you should verify which export policy is used by the volume or qtree and the type of access the client has as a result.

3. If necessary, reconfigure the export policy rules.

### Test NFS access from client systems

After you verify NFS access to the new storage object, you should test the configuration by logging in to an NFS administration host and reading data from and writing data to the SVM. You should then repeat the process as a non-root user on a client system.

#### What you'll need

- The client system must have an IP address that is allowed by the export rule you specified earlier.
- You must have the login information for the root user.

#### Steps

1. On the cluster, verify the IP address of the LIF that is hosting the new volume:

```
network interface show -vserver svm_name
```

2. Log in as the root user to the administration host client system.
3. Change the directory to the mount folder:

```
cd /mnt/
```

4. Create and mount a new folder using the IP address of the SVM:
  - a. Create a new folder:

```
mkdir /mnt/folder
```

- b. Mount the new volume at this new directory:



```
mount -t nfs -o hard IPAddress:/volume_name /mnt/folder
```

- c. Change the directory to the new folder:

```
cd folder
```

The following commands create a folder named test1, mount the vol1 volume at the 192.0.2.130 IP address on the test1 mount folder, and change to the new test1 directory:

```
host# mkdir /mnt/test1
host# mount -t nfs -o hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

5. Create a new file, verify that it exists, and write text to it:

- a. Create a test file:

```
touch filename
```

- b. Verify that the file exists.:

```
ls -l filename
```

- c. Enter:

```
cat > filename
```

Type some text, and then press Ctrl+D to write text to the test file.

- d. Display the content of the test file.

```
cat filename
```

- e. Remove the test file:

```
rm filename
```

- f. Return to the parent directory:

```
cd ..
```

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

6. As root, set any desired UNIX ownership and permissions on the mounted volume.
7. On a UNIX client system identified in your export rules, log in as one of the authorized users who now has access to the new volume, and repeat the procedures in steps 3 to 5 to verify that you can mount the volume and create a file.

## Where to find additional information

After you have successfully tested NFS client access, you can perform additional NFS configuration or add SAN access. When protocol access is complete, you should protect the root volume of storage virtual machine (SVM).

### NFS configuration

You can further configure NFS access using the following information and technical reports:

- [NFS management](#)

Describes how to configure and manage file access using NFS.

- [NetApp Technical Report 4067: NFS Best Practice and Implementation Guide](#)

Serves as an NFSv3 and NFSv4 operational guide, and provides an overview of the ONTAP operating system with a focus on NFSv4.

- [NetApp Technical Report 4073: Secure Unified Authentication](#)

Explains how to configure ONTAP for use with UNIX-based Kerberos version 5 (krb5) servers for NFS storage authentication and Windows Server Active Directory (AD) as the KDC and Lightweight Directory Access Protocol (LDAP) identity provider.

- [NetApp Technical Report 3580: NFSv4 Enhancements and Best Practices Guide Data ONTAP Implementation](#)

Describes the best practices that should be followed while implementing NFSv4 components on AIX, Linux, or Solaris clients attached to systems running ONTAP.

### Networking configuration

You can further configure networking features and name services using the following information and technical reports:

- [NFS management](#)

Describes how to configure and manage ONTAP networking.

- [NetApp Technical Report 4182: Ethernet Storage Design Considerations and Best Practices for Clustered Data ONTAP Configurations](#)

Describes the implementation of ONTAP network configurations, and provides common network deployment scenarios and best practice recommendations.

- [NetApp Technical Report 4668: Name Services Best Practices Guide](#)

Explains how to configure LDAP, NIS, DNS, and local file configuration for authentication purposes.

## SAN protocol configuration

If you want to provide or modify SAN access to the new SVM, you can use the FC or iSCSI configuration information, which is available for multiple host operating systems.

## Root volume protection

After configuring protocols on the SVM, you should ensure that its root volume is protected:

- [Data protection](#)

Describes how to create a load-sharing mirror to protect the SVM root volume, which is a NetApp best practice for NAS-enabled SVMs. Also describes how to quickly recover from volume failures or losses by promoting the SVM root volume from a load-sharing mirror.

## How ONTAP exports differ from 7-Mode exports

### How ONTAP exports differ from 7-Mode exports

If you are unfamiliar with how ONTAP implements NFS exports, you can compare 7-Mode and ONTAP export configuration tools, as well as sample 7-Mode `/etc/exports` files with clustered policies and rules.

In ONTAP there is no `/etc/exports` file and no `exportfs` command. Instead, you must define an export policy. Export policies enable you to control client access in much the same way as you did in 7-Mode, but give you additional functionality such as the ability to reuse the same export policy for multiple volumes.

### Related information


[NFS management](#)

[NetApp Technical Report 4067: NFS Best Practice and Implementation Guide](#)

### Comparison of exports in 7-Mode and ONTAP

Exports in ONTAP are defined and used differently than they are in 7-Mode environments.

Areas of difference	7-Mode	ONTAP
How exports are defined	Exports are defined in the <code>/etc/exports</code> file.	Exports are defined by creating an export policy within an SVM. An SVM can include more than one export policy.

Scope of export	<ul style="list-style-type: none"> <li>Exports apply to a specified file path or qtree.</li> <li>You must create a separate entry in <code>/etc/exports</code> for each file path or qtree.</li> <li>Exports are persistent only if they are defined in the <code>/etc/exports</code> file.</li> </ul>	<ul style="list-style-type: none"> <li>Export policies apply to an entire volume, including all of the file paths and qtrees contained in the volume.</li> <li>Export policies can be applied to more than one volume if you want.</li> <li>All export policies are persistent across system restarts.</li> </ul>
Fencing (specifying different access for specific clients to the same resources)	To provide specific clients different access to a single exported resource, you have to list each client and its permitted access in the <code>/etc/exports</code> file.	Export policies are composed of a number of individual export rules. Each export rule defines specific access permissions for a resource and lists the clients that have those permissions. To specify different access for specific clients, you have to create an export rule for each specific set of access permissions, list the clients that have those permissions, and then add the rules to the export policy.
Name aliasing	When you define an export, you can choose to make the name of the export different from the name of the file path. You should use the <code>-actual</code> parameter when defining such an export in the <code>/etc/exports</code> file.	<p>You can choose to make the name of the exported volume different from the actual volume name. To do this, you must mount the volume with a custom junction path name within the SVM namespace.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>By default, volumes are mounted with their volume name. To customize a volume's junction path name you need to unmount it, rename it, and then remount it.</p> </div>

### Examples of ONTAP export policies

You can review example export policies to better understand how export policies work in ONTAP.

#### Sample ONTAP implementation of a 7-Mode export

The following example shows a 7-Mode export as it appears in the `/etc/export` file:

```
/vol/vol1 -sec=sys,ro=@readonly_netgroup,rw=@readwrite_netgroup1:
@readwrite_netgroup2:@rootaccess_netgroup,root=@rootaccess_netgroup
```

To reproduce this export as a clustered export policy, you have to create an export policy with three export rules, and then assign the export policy to the volume vol1.

Rule	Element	Value
Rule 1	-clientmatch (client specification)	@readonly_netgroup
	-ruleindex(position of export rule in the list of rules)	1
	-protocol	nfs
	-rorule(allow read-only access)	sys (client authenticated with AUTH_SYS)
	-rwrule(allow read-write access)	never
	-superuser(allow superuser access)	none( <i>root squashed to anon</i> )
Rule 2	-clientmatch	@rootaccess_netgroup
	-ruleindex	2
	-protocol	nfs
	-rorule	sys
	-rwrule	sys
	-superuser	sys

Rule	Element	Value
Rule 3	-clientmatch	@readwrite_netgroup1,@readwrite_netgroup2
	-ruleindex	3
	-protocol	nfs
	-rorule	sys
	-rwrule	sys
	-superuser	none

1. Create an export policy called exp\_vol1:

```
vserver export-policy create -vserver NewSVM -policyname exp_vol1
```

2. Create three rules with the following parameters to the base command:

◦ Base command:

```
vserver export-policy rule create -vserver NewSVM -policyname exp_vol1
```

◦ Rule parameters:

```
-clientmatch @readonly_netgroup -ruleindex 1 -protocol nfs -rorule sys
-rwrule never -superuser none
```

```
-clientmatch @rootaccess_netgroup -ruleindex 2 -protocol nfs -rorule sys
-rwrule sys -superuser sys
```

```
-clientmatch @readwrite_netgroup1,@readwrite_netgroup2 -ruleindex 3
-protocol nfs -rorule sys -rwrule sys -superuser none
```

3. Assign the policy to the volume vol1:

```
volume modify -vserver NewSVM -volume vol1 -policy exp_vol1
```

### Sample consolidation of 7-Mode exports

The following example shows a 7-Mode `/etc/export` file that includes one line for each of 10 qtrees:

```
/vol/vol1/q_1472 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1471 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1473 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1570 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1571 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_2237 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2238 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2239 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2240 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2241 -sec=sys,rw=host2057s,root=host2057s
```

In ONTAP, one of two policies is needed for each qtree: one with a rule including `-clientmatch host1519s`, or one with a rule including `-clientmatch host2057s`.

1. Create two export policies called `exp_vol1q1` and `exp_vol1q2`:

- `vserver export-policy create -vserver NewSVM -policyname exp_vol1q1`
- `vserver export-policy create -vserver NewSVM -policyname exp_vol1q2`

2. Create a rule for each policy:

- `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q1 -clientmatch host1519s -rwrule sys -superuser sys`
- `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q2 -clientmatch host1519s -rwrule sys -superuser sys`

3. Apply the policies to the qtrees:

- `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_1472 -export -policy exp_vol1q1`
- [next 4 qtrees...]
- `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_2237 -export -policy exp_vol1q2`
- [next 4 qtrees...]

If you need to add additional qtrees for those hosts later, you would use the same export policies.

## Manage NFS with the CLI

### NFS reference overview

ONTAP includes file access features available for the NFS protocol. You can enable an NFS server and export volumes or qtrees.

You perform these procedure under the following circumstances:

- You want to understand the range of ONTAP NFS protocol capabilities.
- You want to perform less common configuration and maintenance tasks, not basic NFS configuration.

- You want to use the command-line interface (CLI), not System Manager or an automated scripting tool.

## Understand NAS file access

### Namespaces and junction points

#### Namespaces and junction points overview

A NAS *namespace* is a logical grouping of volumes joined together at *junction points* to create a single file system hierarchy. A client with sufficient permissions can access files in the namespace without specifying the location of the files in storage. Junctioned volumes can reside anywhere in the cluster.

Rather than mounting every volume containing a file of interest, NAS clients mount an NFS *export* or access an SMB *share*. The export or share represents the entire namespace or an intermediate location within the namespace. The client accesses only the volumes mounted below its access point.

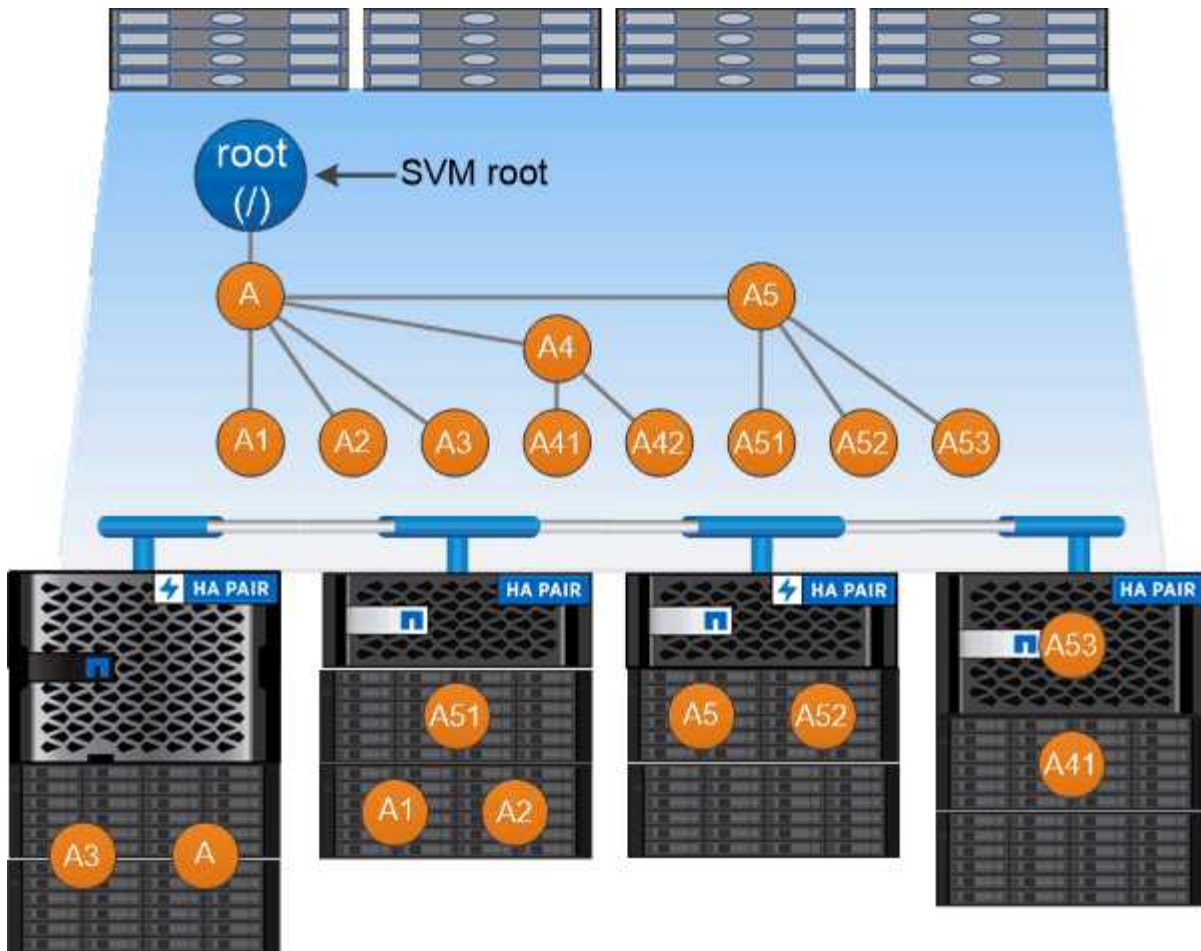
You can add volumes to the namespace as needed. You can create junction points directly below a parent volume junction or on a directory within a volume. A path to a volume junction for a volume named “vol3” might be /vol1/vol2/vol3, or /vol1/dir2/vol3, or even /dir1/dir2/vol3. The path is called the *junction path*.

Every SVM has a unique namespace. The SVM root volume is the entry point to the namespace hierarchy.



To ensure that data remains available in the event of a node outage or failover, you should create a *load-sharing mirror* copy for the SVM root volume.





*A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.*

### Example

The following example creates a volume named “home4” located on SVM vs1 that has a junction path /eng/home:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

### What the typical NAS namespace architectures are

There are several typical NAS namespace architectures that you can use as you create your SVM name space. You can choose the namespace architecture that matches your business and workflow needs.

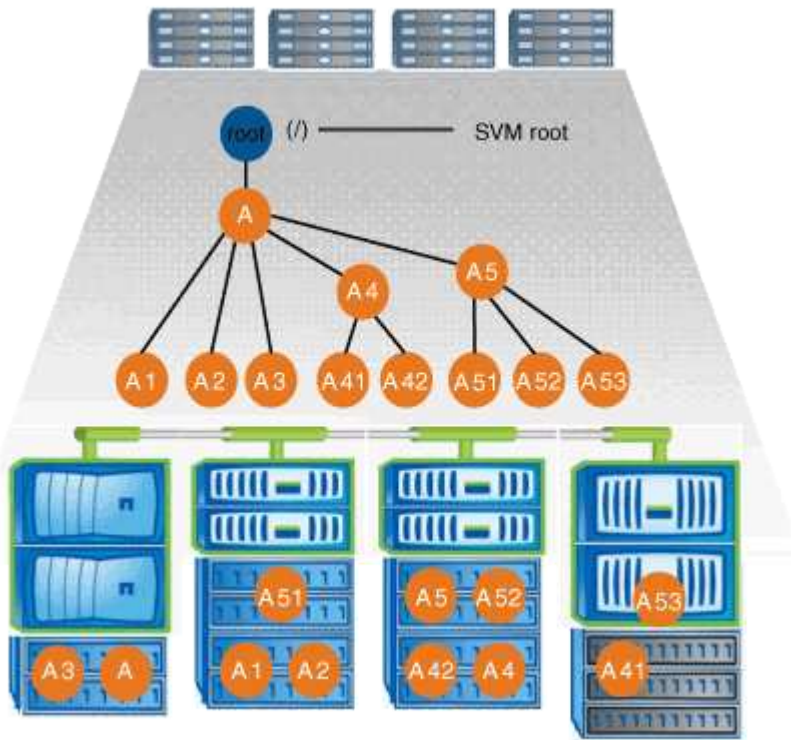
The top of the namespace is always the root volume, which is represented by a slash (/). The namespace architecture under the root falls into three basic categories:

- A single branched tree, with only a single junction to the root of the namespace

- Multiple branched trees, with multiple junction points to the root of the namespace
- Multiple stand-alone volumes, each with a separate junction point to the root of the name space

### Namespace with single branched tree

An architecture with a single branched tree has a single insertion point to the root of the SVM namespace. The single insertion point can be either a junctioned volume or a directory beneath the root. All other volumes are mounted at junction points beneath the single insertion point (which can be a volume or a directory).

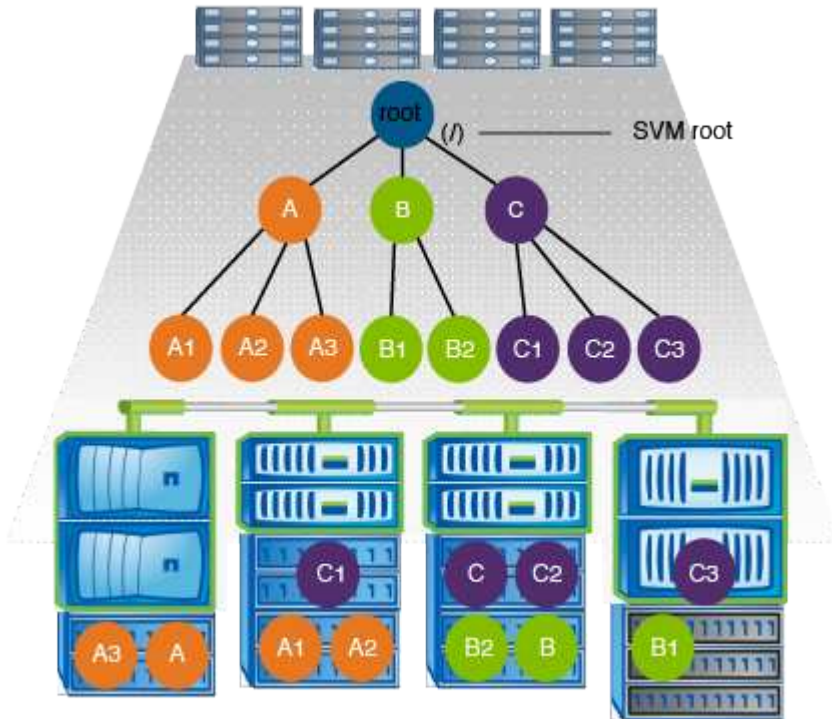


For example, a typical volume junction configuration with the above namespace architecture might look like the following configuration, where all volumes are junctioned below the single insertion point, which is a directory named "data":

Vserver	Volume	Junction Active	Junction Path	Junction Path Source
vs1	corp1	true	/data/dir1/corp1	RW_volume
vs1	corp2	true	/data/dir1/corp2	RW_volume
vs1	data1	true	/data/data1	RW_volume
vs1	eng1	true	/data/data1/eng1	RW_volume
vs1	eng2	true	/data/data1/eng2	RW_volume
vs1	sales	true	/data/data1/sales	RW_volume
vs1	vol1	true	/data/vol1	RW_volume
vs1	vol2	true	/data/vol2	RW_volume
vs1	vol3	true	/data/vol3	RW_volume
vs1	vs1_root	-	/	-

## Namespace with multiple branched trees

An architecture with multiple branched trees has multiple insertion points to the root of the SVM namespace. The insertion points can be either junctioned volumes or directories beneath the root. All other volumes are mounted at junction points beneath the insertion points (which can be volumes or directories).



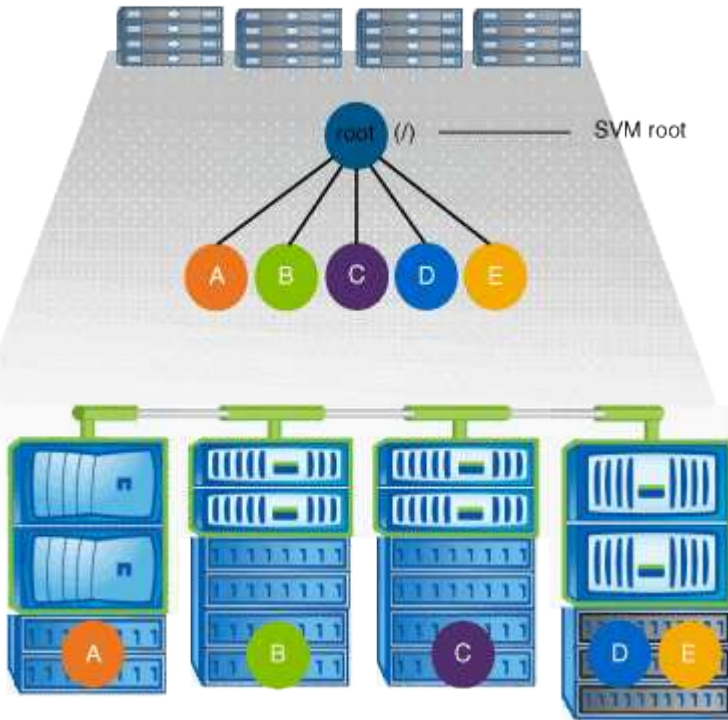
For example, a typical volume junction configuration with the above namespace architecture might look like the following configuration, where there are three insertion points to the root volume of the SVM. Two insertion points are directories named “data” and “projects”. One insertion point is a junctioned volume named “audit”:

Vserver	Volume	Junction Active	Junction Path	Junction Path Source
vs1	audit	true	/audit	RW_volume
vs1	audit_logs1	true	/audit/logs1	RW_volume
vs1	audit_logs2	true	/audit/logs2	RW_volume
vs1	audit_logs3	true	/audit/logs3	RW_volume
vs1	eng	true	/data/eng	RW_volume
vs1	mktg1	true	/data/mktg1	RW_volume
vs1	mktg2	true	/data/mktg2	RW_volume
vs1	project1	true	/projects/project1	RW_volume
vs1	project2	true	/projects/project2	RW_volume
vs1	vs1_root	-	/	-

## Namespace with multiple stand-alone volumes

In an architecture with stand-alone volumes, every volume has an insertion point to the root of the SVM namespace; however, the volume is not junctioned below another volume. Each volume has a unique path,

and is either junctioned directly below the root or is junctioned under a directory below the root.



For example, a typical volume junction configuration with the above namespace architecture might look like the following configuration, where there are five insertion points to the root volume of the SVM, with each insertion point representing a path to one volume.

Vserver	Volume	Junction Active	Junction Path	Junction Path Source
vs1	eng	true	/eng	RW_volume
vs1	mktg	true	/vol/mktg	RW_volume
vs1	project1	true	/project1	RW_volume
vs1	project2	true	/project2	RW_volume
vs1	sales	true	/sales	RW_volume
vs1	vs1_root	-	/	-

## How ONTAP controls access to files

### How ONTAP controls access to files overview

ONTAP controls access to files according to the authentication-based and file-based restrictions that you specify.

When a client connects to the storage system to access files, ONTAP has to perform two tasks:

- Authentication

ONTAP has to authenticate the client by verifying the identity with a trusted source. In addition, the

authentication type of the client is one method that can be used to determine whether a client can access data when configuring export policies (optional for CIFS).

- Authorization

ONTAP has to authorize the user by comparing the user's credentials with the permissions configured on the file or directory and determining what type of access, if any, to provide.

To properly manage file access control, ONTAP must communicate with external services such as NIS, LDAP, and Active Directory servers. Configuring a storage system for file access using CIFS or NFS requires setting up the appropriate services depending on your environment in ONTAP.

#### Authentication-based restrictions

With authentication-based restrictions, you can specify which client machines and which users can connect to the storage virtual machine (SVM).

ONTAP supports Kerberos authentication from both UNIX and Windows servers.

#### File-based restrictions

ONTAP evaluates three levels of security to determine whether an entity is authorized to perform a requested action on files and directories residing on an SVM. Access is determined by the effective permissions after evaluation of the three security levels.

Any storage object can contain up to three types of security layers:

- Export (NFS) and share (SMB) security

Export and share security applies to client access to a given NFS export or SMB share. Users with administrative privileges can manage export and share-level security from SMB and NFS clients.

- Storage-Level Access Guard file and directory security

Storage-Level Access Guard security applies to SMB and NFS client access to SVM volumes. Only NTFS access permissions are supported. For ONTAP to perform security checks on UNIX users for access to data on volumes for which Storage-Level Access Guard has been applied, the UNIX user must map to a Windows user on the SVM that owns the volume.



If you view the security settings on a file or directory from an NFS or SMB client, you will not see Storage-Level Access Guard security. Storage-Level Access Guard security cannot be revoked from a client, even by a system (Windows or UNIX) administrator.

- NTFS, UNIX, and NFSv4 native file-level security

Native file-level security exists on the file or directory that represents the storage object. You can set file-level security from a client. File permissions are effective regardless of whether SMB or NFS is used to access the data.

#### How ONTAP handles NFS client authentication

## How ONTAP handles NFS client authentication overview

NFS clients must be properly authenticated before they can access data on the SVM. ONTAP authenticates the clients by checking their UNIX credentials against the name services that you configure.

When an NFS client connects to the SVM, ONTAP obtains the UNIX credentials for the user by checking different name services, depending on the name services configuration of the SVM. ONTAP can check credentials for local UNIX accounts, NIS domains, and LDAP domains. At least one of them must be configured so that ONTAP can successfully authenticate the user. You can specify multiple name services and the order in which ONTAP searches them.

In a pure NFS environment with UNIX volume security styles, this configuration is sufficient to authenticate and provide the proper file access for a user connecting from an NFS client.

If you are using mixed, NTFS, or unified volume security styles, ONTAP must obtain a SMB user name for the UNIX user for authentication with a Windows domain controller. This can happen either by mapping individual users using local UNIX accounts or LDAP domains, or by using a default SMB user instead. You can specify which name services ONTAP searches in which order, or specify a default SMB user.

### How ONTAP uses name services

ONTAP uses name services to obtain information about users and clients. ONTAP uses this information to authenticate users accessing data on or administering the storage system, and to map user credentials in a mixed environment.

When you configure the storage system, you must specify what name services you want ONTAP to use for obtaining user credentials for authentication. ONTAP supports the following name services:

- Local users (file)
- External NIS domains (NIS)
- External LDAP domains (LDAP)

You use the `vserver services name-service ns-switch` command family to configure SVMs with the sources to search for network information and the order in which to search them. These commands provide the equivalent functionality of the `/etc/nsswitch.conf` file on UNIX systems.

When an NFS client connects to the SVM, ONTAP checks the specified name services to obtain the UNIX credentials for the user. If name services are configured correctly and ONTAP can obtain the UNIX credentials, ONTAP successfully authenticates the user.

In an environment with mixed security styles, ONTAP might have to map user credentials. You must configure name services appropriately for your environment to allow ONTAP to properly map user credentials.

ONTAP also uses name services for authenticating SVM administrator accounts. You must keep this in mind when configuring or modifying the name service switch to avoid accidentally disabling authentication for SVM administrator accounts. For more information about SVM administration users, see [xref:./nfs-admin/./authentication/index.html](#)[Administrator authentication and RBAC].

### How ONTAP grants SMB file access from NFS clients

ONTAP uses Windows NT File System (NTFS) security semantics to determine whether a UNIX user, on an NFS client, has access to a file with NTFS permissions.

ONTAP does this by converting the user's UNIX User ID (UID) into a SMB credential, and then using the SMB credential to verify that the user has access rights to the file. A SMB credential consists of a primary Security Identifier (SID), usually the user's Windows user name, and one or more group SIDs that correspond to Windows groups of which the user is a member.

The time ONTAP takes converting the UNIX UID into a SMB credential can be from tens of milliseconds to hundreds of milliseconds because the process involves contacting a domain controller. ONTAP maps the UID to the SMB credential and enters the mapping in a credential cache to reduce the verification time caused by the conversion.

### **How the NFS credential cache works**

When an NFS user requests access to NFS exports on the storage system, ONTAP must retrieve the user credentials either from external name servers or from local files to authenticate the user. ONTAP then stores these credentials in an internal credential cache for later reference. Understanding how the NFS credential caches works enables you to handle potential performance and access issues.

Without the credential cache, ONTAP would have to query name services every time an NFS user requested access. On a busy storage system that is accessed by many users, this can quickly lead to serious performance problems, causing unwanted delays or even denials to NFS client access.

With the credential cache, ONTAP retrieves the user credentials and then stores them for a predetermined amount of time for quick and easy access should the NFS client send another request. This method offers the following advantages:

- It eases the load on the storage system by handling fewer requests to external name servers (such as NIS or LDAP).
- It eases the load on external name servers by sending fewer requests to them.
- It speeds up user access by eliminating the wait time for obtaining credentials from external sources before the user can be authenticated.

ONTAP stores both positive and negative credentials in the credential cache. Positive credentials means that the user was authenticated and granted access. Negative credentials means that the user was not authenticated and was denied access.

By default, ONTAP stores positive credentials for 24 hours; that is, after initially authenticating a user, ONTAP uses the cached credentials for any access requests by that user for 24 hours. If the user requests access after 24 hours, the cycle starts over: ONTAP discards the cached credentials and obtains the credentials again from the appropriate name service source. If the credentials changed on the name server during the previous 24 hours, ONTAP caches the updated credentials for use for the next 24 hours.

By default, ONTAP stores negative credentials for two hours; that is, after initially denying access to a user, ONTAP continues to deny any access requests by that user for two hours. If the user requests access after 2 hours, the cycle starts over: ONTAP obtains the credentials again from the appropriate name service source. If the credentials changed on the name server during the previous two hours, ONTAP caches the updated credentials for use for the next two hours.

## **Create and manage data volumes in NAS namespaces**

## Create data volumes with specified junction points

You can specify the junction point when you create a data volume. The resultant volume is automatically mounted at the junction point and is immediately available to configure for NAS access.

### What you'll need

The aggregate in which you want to create the volume must already exist.



The following characters cannot be used in the junction path: \* # " > < | ? \

In addition, the junction path length cannot be more than 255 characters.

### Steps

1. Create the volume with a junction point:

```
volume create -vserver vserver_name -volume volume_name -aggregate  
aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style  
{ntfs|unix|mixed} -junction-path junction_path
```

The junction path must start with the root (/) and can contain both directories and junctioned volumes. The junction path does not need to contain the name of the volume. Junction paths are independent of the volume name.

Specifying a volume security style is optional. If you do not specify a security style, ONTAP creates the volume with the same security style that is applied to the root volume of the storage virtual machine (SVM). However, the root volume's security style might not be the security style you want applied to the data volume you create. The recommendation is to specify the security style when you create the volume to minimize difficult-to-troubleshoot file-access issues.

The junction path is case insensitive; /ENG is the same as /eng. If you create a CIFS share, Windows treats the junction path as if it is case sensitive. For example, if the junction is /ENG, the path of a SMB share must start with /ENG, not /eng.

There are many optional parameters that you can use to customize a data volume. To learn more about them, see the man pages for the `volume create` command.

2. Verify that the volume was created with the desired junction point:

```
volume show -vserver vserver_name -volume volume_name -junction
```

### Example

The following example creates a volume named "home4" located on SVM vs1 that has a junction path /eng/home:



```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1 -volume home4 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1	home4	true	/eng/home	RW_volume

## Create data volumes without specifying junction points

You can create a data volume without specifying a junction point. The resultant volume is not automatically mounted, and is not available to configure for NAS access. You must mount the volume before you can configure SMB shares or NFS exports for that volume.

### What you'll need

The aggregate in which you want to create the volume must already exist.

### Steps

1. Create the volume without a junction point by using the following command:

```
volume create -vserver vserver_name -volume volume_name -aggregate
aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
{ntfs|unix|mixed}
```

Specifying a volume security style is optional. If you do not specify a security style, ONTAP creates the volume with the same security style that is applied to the root volume of the storage virtual machine (SVM). However, the root volume's security style might not be the security style you want applied to the data volume. The recommendation is to specify the security style when you create the volume to minimize difficult-to-troubleshoot file-access issues.

There are many optional parameters that you can use to customize a data volume. To learn more about them, see the man pages for the `volume create` command.

2. Verify that the volume was created without a junction point:

```
volume show -vserver vserver_name -volume volume_name -junction
```

### Example

The following example creates a volume named "sales" located on SVM vs1 that is not mounted at a junction point:

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1	data	true	/data	RW_volume
vs1	home4	true	/eng/home	RW_volume
vs1	vs1_root	-	/	-
vs1	sales	-	-	-

## Mount or unmount existing volumes in the NAS namespace

A volume must be mounted on the NAS namespace before you can configure NAS client access to data contained in the storage virtual machine (SVM) volumes. You can mount a volume to a junction point if it is not currently mounted. You can also unmount volumes.

### About this task

If you unmount and offline a volume, all data within the junction point, including data in volumes with junction points contained within the unmounted volume's namespace, are inaccessible to NAS clients.



To discontinue NAS client access to a volume, it is not sufficient to simply unmount the volume. You must offline the volume, or take other steps to ensure that client-side file handle caches are invalidated. For more information, see the following Knowledge Base article:

[NFSv3 clients still have access to a volume after being removed from the namespace in ONTAP](#)

When you unmount and offline a volume, data within the volume is not lost. Additionally, existing volume export policies and SMB shares created on the volume or on directories and junction points within the unmounted volume are retained. If you remount the unmounted volume, NAS clients can access the data contained within the volume using existing export policies and SMB shares.

### Steps

1. Perform the desired action:

If you want to...	Enter the commands...
Mount a volume	<pre>volume mount -vserver svm_name -volume volume_name -junction-path junction_path</pre>
Unmount a volume	<pre>volume unmount -vserver svm_name -volume volume_name volume offline -vserver svm_name -volume volume_name</pre>

2. Verify that the volume is in the desired mount state:

```
volume show -vserver vs1 -volume volume_name -fields state,junction-  
path,junction-active
```

**Examples**

The following example mounts a volume named “sales” located on SVM vs1 to the junction point /sales:

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales  
  
cluster1::> volume show -vserver vs1 state,junction-path,junction-active
```

vserver	volume	state	junction-path	junction-active
vs1	data	online	/data	true
vs1	home4	online	/eng/home	true
vs1	sales	online	/sales	true

The following example unmounts and offlines a volume named “data” located on SVM vs1:

```
cluster1::> volume unmount -vserver vs1 -volume data  
cluster1::> volume offline -vserver vs1 -volume data
```

```
cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-  
active
```

vserver	volume	state	junction-path	junction-active
vs1	data	offline	-	-
vs1	home4	online	/eng/home	true
vs1	sales	online	/sales	true

**Display volume mount and junction point information**

You can display information about mounted volumes for storage virtual machines (SVMs) and the junction points to which the volumes are mounted. You can also determine which volumes are not mounted to a junction point. You can use this information to understand and manage your SVM namespace.

**Step**

1. Perform the desired action:

**If you want to display...**

**Enter the command...**

Summary information about mounted and unmounted volumes on the SVM	<code>volume show -vserver vserver_name -junction</code>
Detailed information about mounted and unmounted volumes on the SVM	<code>volume show -vserver vserver_name -volume volume_name -instance</code>
Specific information about mounted and unmounted volumes on the SVM	<p>a. If necessary, you can display valid fields for the <code>-fields</code> parameter by using the following command:  <code>volume show -fields ?</code></p> <p>b. Display the desired information by using the <code>-fields</code> parameter:  <code>volume show -vserver vserver_name -fields fieldname,...</code></p>

### Examples

The following example displays a summary of mounted and unmounted volumes on SVM vs1:

```
cluster1::> volume show -vserver vs1 -junction
```

Vserver	Volume	Junction Active	Junction Path	Junction Path Source
vs1	data	true	/data	RW_volume
vs1	home4	true	/eng/home	RW_volume
vs1	vs1_root	-	/	-
vs1	sales	true	/sales	RW_volume

The following example displays information about specified fields for volumes located on SVM vs2:

```

cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume    aggregate size state  type security-style junction-path
junction-parent node
-----
vs2      data1      aggr3    2GB  online RW   unix          -          -
node3
vs2      data2      aggr3    1GB  online RW   ntfs          /data2
vs2_root node3
vs2      data2_1    aggr3    8GB  online RW   ntfs          /data2/d2_1
data2    node3
vs2      data2_2    aggr3    8GB  online RW   ntfs          /data2/d2_2
data2    node3
vs2      pubs      aggr1    1GB  online RW   unix          /publications
vs2_root node1
vs2      images    aggr3    2TB  online RW   ntfs          /images
vs2_root node3
vs2      logs      aggr1    1GB  online RW   unix          /logs
vs2_root node1
vs2      vs2_root  aggr3    1GB  online RW   ntfs          /          -
node3

```

## Configure security styles

### How security styles affect data access

#### What the security styles and their effects are

There are four different security styles: UNIX, NTFS, mixed, and unified. Each security style has a different effect on how permissions are handled for data. You must understand the different effects to ensure that you select the appropriate security style for your purposes.

It is important to understand that security styles do not determine what client types can or cannot access data. Security styles only determine the type of permissions ONTAP uses to control data access and what client type can modify these permissions.

For example, if a volume uses UNIX security style, SMB clients can still access data (provided that they properly authenticate and authorize) due to the multiprotocol nature of ONTAP. However, ONTAP uses UNIX permissions that only UNIX clients can modify using native tools.

Security style	Clients that can modify permissions	Permissions that clients can use	Resulting effective security style	Clients that can access files
Unix	NFS	NFSv3 mode bits	Unix	NFS and SMB
		NFSv4.x ACLs		
NTFS	SMB	NTFS ACLs	NTFS	
Mixed	NFS or SMB	NFSv3 mode bits	UNIX	
		NFSv4.ACLs		
		NTFS ACLs	NTFS	
Unified (For infinite volumes only, in ONTAP 9.4 and earlier releases.)	NFS or SMB	NFSv3 mode bits	Unix	
		NFSv4.1 ACLs		
		NTFS ACLs	NTFS	

FlexVol volumes support UNIX, NTFS, and mixed security styles. When the security style is mixed or unified, the effective permissions depend on the client type that last modified the permissions because users set the security style on an individual basis. If the last client that modified permissions was an NFSv3 client, the permissions are UNIX NFSv3 mode bits. If the last client was an NFSv4 client, the permissions are NFSv4 ACLs. If the last client was an SMB client, the permissions are Windows NTFS ACLs.

The unified security style is only available with infinite volumes, which are no longer supported in ONTAP 9.5 and later releases. For more information, see [FlexGroup volumes management overview](#).

Beginning with ONTAP 9.2, the `show-effective-permissions` parameter to the `vserver security file-directory` command enables you to display effective permissions granted to a Windows or UNIX user on the specified file or folder path. In addition, the optional parameter `-share-name` enables you to display the effective share permission.



ONTAP initially sets some default file permissions. By default, the effective security style on all data in UNIX, mixed, and unified security style volumes is UNIX and the effective permissions type is UNIX mode bits (0755 unless specified otherwise) until configured by a client as allowed by the default security style. By default, the effective security style on all data in NTFS security style volumes is NTFS and has an ACL allowing full control to everyone.

### Where and when to set security styles

Security styles can be set on FlexVol volumes (both root or data volumes) and qtrees. Security styles can be set manually at the time of creation, inherited automatically, or changed at a later time.

### Decide which security style to use on SVMs

To help you decide which security style to use on a volume, you should consider two factors. The primary factor is the type of administrator that manages the file system. The secondary factor is the type of user or service that accesses the data on the volume.

When you configure the security style on a volume, you should consider the needs of your environment to

ensure that you select the best security style and avoid issues with managing permissions. The following considerations can help you decide:

Security style	Choose if...
UNIX	<ul style="list-style-type: none"><li>• The file system is managed by a UNIX administrator.</li><li>• The majority of users are NFS clients.</li><li>• An application accessing the data uses a UNIX user as the service account.</li></ul>
NTFS	<ul style="list-style-type: none"><li>• The file system is managed by a Windows administrator.</li><li>• The majority of users are SMB clients.</li><li>• An application accessing the data uses a Windows user as the service account.</li></ul>
Mixed	<ul style="list-style-type: none"><li>• The file system is managed by both UNIX and Windows administrators and users consist of both NFS and SMB clients.</li></ul>

#### How security style inheritance works

If you do not specify the security style when creating a new FlexVol volume or a qtree, it inherits its security style in different ways.

Security styles are inherited in the following manner:

- A FlexVol volume inherits the security style of the root volume of its containing SVM.
- A qtree inherits the security style of its containing FlexVol volume.
- A file or directory inherits the security style of its containing FlexVol volume or qtree.

#### How ONTAP preserves UNIX permissions

When files in a FlexVol volume that currently have UNIX permissions are edited and saved by Windows applications, ONTAP can preserve the UNIX permissions.

When applications on Windows clients edit and save files, they read the security properties of the file, create a new temporary file, apply those properties to the temporary file, and then give the temporary file the original file name.

When Windows clients perform a query for the security properties, they receive a constructed ACL that exactly represents the UNIX permissions. The sole purpose of this constructed ACL is to preserve the file's UNIX permissions as files are updated by Windows applications to ensure that the resulting files have the same UNIX permissions. ONTAP does not set any NTFS ACLs using the constructed ACL.

#### Manage UNIX permissions using the Windows Security tab

If you want to manipulate UNIX permissions of files or folders in mixed security-style volumes or qtrees on SVMs, you can use the Security tab on Windows clients. Alternatively, you can use applications that can query and set Windows ACLs.

- Modifying UNIX permissions

You can use the Windows Security tab to view and change UNIX permissions for a mixed security-style volume or qtree. If you use the main Windows Security tab to change UNIX permissions, you must first remove the existing ACE you want to edit (this sets the mode bits to 0) before you make your changes. Alternatively, you can use the Advanced editor to change permissions.

If mode permissions are used, you can directly change the mode permissions for the listed UID, GID, and others (everyone else with an account on the computer). For example, if the displayed UID has r-x permissions, you can change the UID permissions to rwx.

- Changing UNIX permissions to NTFS permissions

You can use the Windows Security tab to replace UNIX security objects with Windows security objects on a mixed security-style volume or qtree where the files and folders have a UNIX effective security style.

You must first remove all listed UNIX permission entries before you can replace them with the desired Windows User and Group objects. You can then configure NTFS-based ACLs on the Windows User and Group objects. By removing all UNIX security objects and adding only Windows Users and Groups to a file or folder in a mixed security-style volume or qtree, you change the effective security style on the file or folder from UNIX to NTFS.

When changing permissions on a folder, the default Windows behavior is to propagate these changes to all subfolders and files. Therefore, you must change the propagation choice to the desired setting if you do not want to propagate a change in security style to all child folders, subfolders, and files.

## Configure security styles on SVM root volumes

You configure the storage virtual machine (SVM) root volume security style to determine the type of permissions used for data on the root volume of the SVM.

### Steps

1. Use the `vserver create` command with the `-rootvolume-security-style` parameter to define the security style.

The possible options for the root volume security style are `unix`, `ntfs`, or `mixed`.

2. Display and verify the configuration, including the root volume security style of the SVM you created:

```
vserver show -vserver vserver_name
```

## Configure security styles on FlexVol volumes

You configure the FlexVol volume security style to determine the type of permissions used for data on FlexVol volumes of the storage virtual machine (SVM).

### Steps

1. Perform one of the following actions:

If the FlexVol volume...	Use the command...
Does not yet exist	<code>volume create</code> and include the <code>-security-style</code> parameter to specify the security style.



Already exists	<code>volume modify</code> and include the <code>-security-style</code> parameter to specify the security style.
----------------	--

The possible options for the FlexVol volume security style are `unix`, `ntfs`, or `mixed`.

If you do not specify a security style when creating a FlexVol volume, the volume inherits the security style of the root volume.

For more information about the `volume create` or `volume modify` commands, see [Logical storage management](#).

2. To display the configuration, including the security style of the FlexVol volume you created, enter the following command:

```
volume show -volume volume_name -instance
```

## Configure security styles on qtrees

You configure the qtree volume security style to determine the type of permissions used for data on qtrees.

### Steps

1. Perform one of the following actions:

If the qtree...	Use the command...
Does not exist yet	<code>volume qtree create</code> and include the <code>-security-style</code> parameter to specify the security style.
Already exists	<code>volume qtree modify</code> and include the <code>-security-style</code> parameter to specify the security style.

The possible options for the qtree security style are `unix`, `ntfs`, or `mixed`.

If you do not specify a security style when creating a qtree, the default security style is `mixed`.

For more information about the `volume qtree create` or `volume qtree modify` commands, see [Logical storage management](#).

2. To display the configuration, including the security style of the qtree you created, enter the following command: `volume qtree show -qtree qtree_name -instance`

## Set up file access using NFS

### Set up file access using NFS overview

You must complete a number of steps to allow clients access to files on storage virtual machines (SVMs) using NFS. There are some additional steps that are optional depending on the current configuration of your environment.

For clients to be able to access files on SVMs using NFS, you must complete the following tasks:

1. Enable the NFS protocol on the SVM.

You must configure the SVM to allow data access from clients over NFS.

2. Create an NFS server on the SVM.

An NFS server is a logical entity on the SVM that enables the SVM to serve files over NFS. You must create the NFS server and specify the NFS protocol versions you want to allow.

3. Configure export policies on the SVM.

You must configure export policies to make volumes and qtrees available to clients.

4. Configure the NFS server with the appropriate security and other settings depending on the network and storage environment.

This step might include configuring Kerberos, LDAP, NIS, name mappings, and local users.

## Secure NFS access using export policies

### How export policies control client access to volumes or qtrees

Export policies contain one or more *export rules* that process each client access request. The result of the process determines whether the client is denied or granted access and what level of access. An export policy with export rules must exist on the storage virtual machine (SVM) for clients to access data.

You associate exactly one export policy with each volume or qtree to configure client access to the volume or qtree. The SVM can contain multiple export policies. This enables you to do the following for SVMs with multiple volumes or qtrees:

- Assign different export policies to each volume or qtree of the SVM for individual client access control to each volume or qtree in the SVM.
- Assign the same export policy to multiple volumes or qtrees of the SVM for identical client access control without having to create a new export policy for each volume or qtree.

If a client makes an access request that is not permitted by the applicable export policy, the request fails with a permission-denied message. If a client does not match any rule in the export policy, then access is denied. If an export policy is empty, then all accesses are implicitly denied.

You can modify an export policy dynamically on a system running ONTAP.

### Default export policy for SVMs

Each SVM has a default export policy that contains no rules. An export policy with rules must exist before clients can access data on the SVM. Each FlexVol volume contained in the SVM must be associated with an export policy.

When you create an SVM, the storage system automatically creates a default export policy called `default` for the root volume of the SVM. You must create one or more rules for the default export policy before clients can access data on the SVM. Alternatively, you can create a custom export policy with rules. You can modify and

rename the default export policy, but you cannot delete the default export policy.

When you create a FlexVol volume in its containing SVM, the storage system creates the volume and associates the volume with the default export policy for the root volume of the SVM. By default, each volume created in the SVM is associated with the default export policy for the root volume. You can use the default export policy for all volumes contained in the SVM, or you can create a unique export policy for each volume. You can associate multiple volumes with the same export policy.

### How export rules work

Export rules are the functional elements of an export policy. Export rules match client access requests to a volume against specific parameters you configure to determine how to handle the client access requests.

An export policy must contain at least one export rule to allow access to clients. If an export policy contains more than one rule, the rules are processed in the order in which they appear in the export policy. The rule order is dictated by the rule index number. If a rule matches a client, the permissions of that rule are used and no further rules are processed. If no rules match, the client is denied access.

You can configure export rules to determine client access permissions using the following criteria:

- The file access protocol used by the client sending the request, for example, NFSv4 or SMB.
- A client identifier, for example, host name or IP address.

The maximum size for the `-clientmatch` field is 4096 characters.

- The security type used by the client to authenticate, for example, Kerberos v5, NTLM, or AUTH\_SYS.

If a rule specifies multiple criteria, the client must match all of them for the rule to apply.



Beginning with ONTAP 9.3, you can enable export policy configuration checking as a background job that records any rules violations in an error rule list. The `vserver export-policy config-checker` commands invoke the checker and display results, which you can use to verify your configuration and delete erroneous rules from the policy.

The commands only validate export configuration for host names, netgroups, and anonymous users.

### Example

The export policy contains an export rule with the following parameters:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

The client access request is sent using the NFSv3 protocol and the client has the IP address 10.1.17.37.

Even though the client access protocol matches, the IP address of the client is in a different subnet from the one specified in the export rule. Therefore, client matching fails and this rule does not apply to this client.

## Example

The export policy contains an export rule with the following parameters:

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

The client access request is sent using the NFSv4 protocol and the client has the IP address 10.1.16.54.

The client access protocol matches and the IP address of the client is in the specified subnet. Therefore, client matching is successful and this rule applies to this client. The client gets read-write access regardless of its security type.

## Example

The export policy contains an export rule with the following parameters:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

Client #1 has the IP address 10.1.16.207, sends an access request using the NFSv3 protocol, and authenticated with Kerberos v5.

Client #2 has the IP address 10.1.16.211, sends an access request using the NFSv3 protocol, and authenticated with AUTH\_SYS.

The client access protocol and IP address matches for both clients. The read-only parameter allows read-only access to all clients regardless of the security type they authenticated with. Therefore both clients get read-only access. However, only client #1 gets read-write access because it used the approved security type Kerberos v5 to authenticate. Client #2 does not get read-write access.

## Manage clients with an unlisted security type

When a client presents itself with a security type that is not listed in an access parameter of an export rule, you have the choice of either denying access to the client or mapping it to the anonymous user ID instead by using the option `none` in the access parameter.

A client might present itself with a security type that is not listed in an access parameter because it was authenticated with a different security type or was not authenticated at all (security type AUTH\_NONE). By default, the client is automatically denied access to that level. However, you can add the option `none` to the access parameter. As a result, clients with an unlisted security style are mapped to the anonymous user ID instead. The `-anon` parameter determines what user ID is assigned to those clients. The user ID specified for the `-anon` parameter must be a valid user that is configured with permissions you deem appropriate for the anonymous user.

Valid values for the `-anon` parameter range from 0 to 65535.

User ID assigned to <code>-anon</code>	Resulting handling of client access requests
0 - 65533	The client access request is mapped to the anonymous user ID and gets access depending on the permissions configured for this user.
65534	The client access request is mapped to the user <code>nobody</code> and gets access depending on the permissions configured for this user. This is the default.
65535	The access request from any client is denied when mapped to this ID and the client presents itself with security type <code>AUTH_NONE</code> . The access request from clients with user ID 0 is denied when mapped to this ID and the client presents itself with any other security type.

When using the option `none`, it is important to remember that the read-only parameter is processed first. Consider the following guidelines when configuring export rules for clients with unlisted security types:

Read-only includes <code>none</code>	Read-write includes <code>none</code>	Resulting access for clients with unlisted security types
No	No	Denied
No	Yes	Denied because read-only is processed first
Yes	No	Read-only as anonymous
Yes	Yes	Read-write as anonymous

### Example

The export policy contains an export rule with the following parameters:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule any`
- `-anon 70`

Client #1 has the IP address 10.1.16.207, sends an access request using the NFSv3 protocol, and authenticated with Kerberos v5.

Client #2 has the IP address 10.1.16.211, sends an access request using the NFSv3 protocol, and authenticated with `AUTH_SYS`.

Client #3 has the IP address 10.1.16.234, sends an access request using the NFSv3 protocol, and did not authenticate (meaning security type AUTH\_NONE).

The client access protocol and IP address matches for all three clients. The read-only parameter allows read-only access to clients with their own user ID that authenticated with AUTH\_SYS. The read-only parameter allows read-only access as the anonymous user with user ID 70 to clients that authenticated using any other security type. The read-write parameter allows read-write access to any security type, but in this case only applies to clients already filtered by the read-only rule.

Therefore, clients #1 and #3 get read-write access only as the anonymous user with user ID 70. Client #2 gets read-write access with its own user ID.

### Example

The export policy contains an export rule with the following parameters:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys, none`
- `-rwrule none`
- `-anon 70`

Client #1 has the IP address 10.1.16.207, sends an access request using the NFSv3 protocol, and authenticated with Kerberos v5.

Client #2 has the IP address 10.1.16.211, sends an access request using the NFSv3 protocol, and authenticated with AUTH\_SYS.

Client #3 has the IP address 10.1.16.234, sends an access request using the NFSv3 protocol, and did not authenticate (meaning security type AUTH\_NONE).

The client access protocol and IP address matches for all three clients. The read-only parameter allows read-only access to clients with their own user ID that authenticated with AUTH\_SYS. The read-only parameter allows read-only access as the anonymous user with user ID 70 to clients that authenticated using any other security type. The read-write parameter allows read-write access only as the anonymous user.

Therefore, client #1 and client #3 get read-write access only as the anonymous user with user ID 70. Client #2 gets read-only access with its own user ID but is denied read-write access.

### How security types determine client access levels

The security type that the client authenticated with plays a special role in export rules. You must understand how the security type determines the levels of access the client gets to a volume or qtree.

The three possible access levels are as follows:

1. Read-only
2. Read-write
3. Superuser (for clients with user ID 0)

Because the access level by security type is evaluated in this order, you must observe the following rules when

constructing access level parameters in export rules:

For a client to get access level...	These access parameters must match the client's security type...
Normal user read-only	Read-only ( <code>-rorule</code> )
Normal user read-write	Read-only ( <code>-rorule</code> ) and read-write ( <code>-rwrule</code> )
Superuser read-only	Read-only ( <code>-rorule</code> ) and <code>-superuser</code>
Superuser read-write	Read-only ( <code>-rorule</code> ) and read-write ( <code>-rwrule</code> ) and <code>-superuser</code>

The following are valid security types for each of these three access parameters:

- `any`
- `none`
- `never`

This security type is not valid for use with the `-superuser` parameter.

- `krb5`
- `krb5i`
- `krb5p`
- `ntlm`
- `sys`

When matching a client's security type against each of the three access parameters, there are three possible outcomes:

If the client's security type...	Then the client...
Matches the one specified in the access parameter.	Gets access for that level with its own user ID.
Does not match the one specified, but the access parameter includes the option <code>none</code> .	Gets access for that level but as the anonymous user with the user ID specified by the <code>-anon</code> parameter.
Does not match the one specified and the access parameter does not include the option <code>none</code> .	Does not get any access for that level. This does not apply to the <code>-superuser</code> parameter because it always includes <code>none</code> even when not specified.

### Example

The export policy contains an export rule with the following parameters:

- `-protocol nfs3`

- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule sys, krb5`
- `-superuser krb5`

Client #1 has the IP address 10.1.16.207, has user ID 0, sends an access request using the NFSv3 protocol, and authenticated with Kerberos v5.

Client #2 has the IP address 10.1.16.211, has user ID 0, sends an access request using the NFSv3 protocol, and authenticated with AUTH\_SYS.

Client #3 has the IP address 10.1.16.234, has user ID 0, sends an access request using the NFSv3 protocol, and did not authenticate (AUTH\_NONE).

The client access protocol and IP address matches all three clients. The read-only parameter allows read-only access to all clients regardless of security type. The read-write parameter allows read-write access to clients with their own user ID that authenticated with AUTH\_SYS or Kerberos v5. The superuser parameter allows superuser access to clients with user ID 0 that authenticated with Kerberos v5.

Therefore, client #1 gets superuser read-write access because it matches all three access parameters. Client #2 gets read-write access but not superuser access. Client #3 gets read-only access but not superuser access.

#### **Manage superuser access requests**

When you configure export policies, you need to consider what you want to happen if the storage system receives a client access request with user ID 0, meaning as a superuser, and set up your export rules accordingly.

In the UNIX world, a user with the user ID 0 is known as the superuser, typically called root, who has unlimited access rights on a system. Using superuser privileges can be dangerous for several reasons, including breach of system and data security.

By default, ONTAP maps clients presenting with user ID 0 to the anonymous user. However, you can specify the `-superuser` parameter in export rules to determine how to handle clients presenting with user ID 0 depending on their security type. The following are valid options for the `-superuser` parameter:

- `any`
- `none`

This is the default setting if you do not specify the `-superuser` parameter.

- `krb5`
- `ntlm`
- `sys`

There are two different ways how clients presenting with user ID 0 are handled, depending on the `-superuser` parameter configuration:



If the <code>-superuser</code> parameter and the client's security type...	Then the client...
Match	Gets superuser access with user ID 0.
Do not match	Gets access as the anonymous user with the user ID specified by the <code>-anon</code> parameter and its assigned permissions. This is regardless of whether the read-only or read-write parameter specifies the option <code>none</code> .

If a client presents with user ID 0 to access a volume with NTFS security style and the `-superuser` parameter is set to `none`, ONTAP uses the name mapping for the anonymous user to obtain the proper credentials.

### Example

The export policy contains an export rule with the following parameters:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-anon 127`

Client #1 has the IP address 10.1.16.207, has user ID 746, sends an access request using the NFSv3 protocol, and authenticated with Kerberos v5.

Client #2 has the IP address 10.1.16.211, has user ID 0, sends an access request using the NFSv3 protocol, and authenticated with AUTH\_SYS.

The client access protocol and IP address matches for both clients. The read-only parameter allows read-only access to all clients regardless of the security type they authenticated with. However, only client #1 gets read-write access because it used the approved security type Kerberos v5 to authenticate.

Client #2 does not get superuser access. Instead, it gets mapped to anonymous because the `-superuser` parameter is not specified. This means it defaults to `none` and automatically maps user ID 0 to anonymous. Client #2 also only gets read-only access because its security type did not match the read-write parameter.

### Example

The export policy contains an export rule with the following parameters:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-superuser krb5`
- `-anon 0`

Client #1 has the IP address 10.1.16.207, has user ID 0, sends an access request using the NFSv3 protocol, and authenticated with Kerberos v5.

Client #2 has the IP address 10.1.16.211, has user ID 0, sends an access request using the NFSv3 protocol, and authenticated with AUTH\_SYS.

The client access protocol and IP address matches for both clients. The read-only parameter allows read-only access to all clients regardless of the security type they authenticated with. However, only client #1 gets read-write access because it used the approved security type Kerberos v5 to authenticate. Client #2 does not get read-write access.

The export rule allows superuser access for clients with user ID 0. Client #1 gets superuser access because it matches the user ID and security type for the read-only and `-superuser` parameters. Client #2 does not get read-write or superuser access because its security type does not match the read-write parameter or the `-superuser` parameter. Instead, client #2 is mapped to the anonymous user, which in this case has the user ID 0.

### How ONTAP uses export policy caches

To improve system performance, ONTAP uses local caches to store information such as host names and netgroups. This enables ONTAP to process export policy rules more quickly than retrieving the information from external sources. Understanding what the caches are and what they do can help you troubleshoot client access issues.

You configure export policies to control client access to NFS exports. Each export policy contains rules, and each rule contains parameters to match the rule to clients requesting access. Some of these parameters require ONTAP to contact an external source, such as DNS or NIS servers, to resolve objects such as domain names, host names, or netgroups.

These communications with external sources take a small amount of time. To increase performance, ONTAP reduces the amount of time it takes to resolve export policy rule objects by storing information locally on each node in several caches.

Cache name	Type of information stored
Access	Mappings of clients to corresponding export policies
Name	Mappings of UNIX user names to corresponding UNIX user IDs
ID	Mappings of UNIX user IDs to corresponding UNIX user IDs and extended UNIX group IDs
Host	Mappings of host names to corresponding IP addresses
Netgroup	Mappings of netgroups to corresponding IP addresses of members
Showmount	List of exported directories from SVM namespace

If you change information on the external name servers in your environment after ONTAP retrieved and stored it locally, the caches might now contain outdated information. Although ONTAP refreshes caches automatically after certain time periods, different caches have different expiration and refresh times and algorithms.

Another possible reason for caches to contain outdated information is when ONTAP attempts to refresh cached information but encounters a failure when attempting to communicate with name servers. If this happens, ONTAP continues to use the information currently stored in the local caches to prevent client disruption.

As a result, client access requests that are supposed to succeed might fail, and client access requests that are supposed to fail might succeed. You can view and manually flush some of the export policy caches when troubleshooting such client access issues.

#### **How the access cache works**

ONTAP uses an access cache to store the results of export policy rule evaluation for client access operations to a volume or qtree. This results in performance improvements because the information can be retrieved much faster from the access cache than going through the export policy rule evaluation process every time a client sends an I/O request.

Whenever an NFS client sends an I/O request to access data on a volume or qtree, ONTAP must evaluate each I/O request to determine whether to grant or deny the I/O request. This evaluation involves checking every export policy rule of the export policy associated with the volume or qtree. If the path to the volume or qtree involves crossing one or more junction points, this might require performing this check for multiple export policies along the path.

Note that this evaluation occurs for every I/O request sent from an NFS client, such as read, write, list, copy and other operations; not just for initial mount requests.

After ONTAP has identified the applicable export policy rules and decided whether to allow or deny the request, ONTAP then creates an entry in the access cache to store this information.

When an NFS client sends an I/O request, ONTAP notes the IP address of the client, the ID of the SVM, and the export policy associated with the target volume or qtree, and first checks the access cache for a matching entry. If a matching entry exists in the access cache, ONTAP uses the stored information to allow or deny the I/O request. If a matching entry does not exist, ONTAP then goes through the normal process of evaluating all applicable policy rules as explained above.

Access cache entries that are not actively used are not refreshed. This reduces unnecessary and wasteful communication with external name servers.

Retrieving the information from the access cache is much faster than going through the entire export policy rule evaluation process for every I/O request. Therefore, using the access cache greatly improves performance by reducing the overhead of client access checks.

#### **How access cache parameters work**

Several parameters control the refresh periods for entries in the access cache. Understanding how these parameters work enables you to modify them to tune the access cache and balance performance with how recent the stored information is.

The access cache stores entries consisting of one or more export rules that apply to clients attempting to access volumes or qtrees. These entries are stored for a certain amount of time before they are refreshed. The

refresh time is determined by access cache parameters and depends on the type of access cache entry.

You can specify access cache parameters for individual SVMs. This allows the parameters to differ according to SVM access requirements. Access cache entries that are not actively used are not refreshed, which reduces unnecessary and wasteful communication with external name servers.

Access cache entry type	Description	Refresh period in seconds
Positive entries	Access cache entries that have not resulted in access denial to clients.	Minimum: 300 Maximum: 86,400 Default: 3,600
Negative entries	Access cache entries that have resulted in access denial to clients.	Minimum: 60 Maximum: 86,400 Default: 3,600

### Example

An NFS client attempts to access a volume on a cluster. ONTAP matches the client to an export policy rule and determines that the client gets access based on the export policy rule configuration. ONTAP stores the export policy rule in the access cache as a positive entry. By default, ONTAP keeps the positive entry in the access cache for one hour (3,600 seconds), and then automatically refreshes the entry to keep the information current.

To prevent the access cache from filling up unnecessarily, there is an additional parameter to clear existing access cache entries that have not been used for a certain time period to decide client access. This `-harvest -timeout` parameter has an allowed range of 60 through 2,592,000 seconds and a default setting of 86,400 seconds.

### Remove an export policy from a qtree

If you decide you do not want a specific export policy assigned to a qtree any longer, you can remove the export policy by modifying the qtree to inherit the export policy of the containing volume instead. You can do this by using the `volume qtree modify` command with the `-export-policy` parameter and an empty name string ("").

### Steps

1. To remove an export policy from a qtree, enter the following command:

```
volume qtree modify -vserver vserver_name -qtree-path  
/vol/volume_name/qtree_name -export-policy ""
```

2. Verify that the qtree was modified accordingly:

```
volume qtree show -qtree qtree_name -fields export-policy
```

### Validate qtree IDs for qtree file operations

ONTAP can perform an optional additional validation of qtree IDs. This validation ensures

that client file operation requests use a valid qtree ID and that clients can only move files within the same qtree. You can enable or disable this validation by modifying the `-validate-qtrees-export` parameter. This parameter is enabled by default.

### About this task

This parameter is only effective when you have assigned an export policy directly to one or more qtrees on the storage virtual machine (SVM).

### Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Perform one of the following actions:

If you want qtree ID validation to be...	Enter the following command...
Enabled	<pre>vserver nfs modify -vserver vserver_name -validate-qtrees-export enabled</pre>
Disabled	<pre>vserver nfs modify -vserver vserver_name -validate-qtrees-export disabled</pre>

3. Return to the admin privilege level:

```
set -privilege admin
```

### Export policy restrictions and nested junctions for FlexVol volumes

If you configured export policies to set a less restrictive policy on a nested junction but a more restrictive policy on a higher level junction, access to the lower level junction might fail.

You should ensure that higher level junctions have less restrictive export policies than lower level junctions.

### Using Kerberos with NFS for strong security

#### ONTAP support for Kerberos

Kerberos provides strong secure authentication for client/server applications. Authentication provides verification of user and process identities to a server. In the ONTAP environment, Kerberos provides authentication between storage virtual machines (SVMs) and NFS clients.

In ONTAP 9, the following Kerberos functionality is supported:

- Kerberos 5 authentication with integrity checking (krb5i)

Krb5i uses checksums to verify the integrity of each NFS message transferred between client and server. This is useful both for security reasons (for example, to ensure that data has not been tampered with) and for data integrity reasons (for example, to prevent data corruption when using NFS over unreliable networks).

- Kerberos 5 authentication with privacy checking (krb5p)

Krb5p uses checksums to encrypt all the traffic between client and the server. This is more secure and also incurs more load.

- 128-bit and 256-bit AES encryption

Advanced Encryption Standard (AES) is an encryption algorithm for securing electronic data. ONTAP now supports AES with 128-bit keys (AES-128) and AES with 256-bit keys (AES-256) encryption for Kerberos for stronger security.

- SVM-level Kerberos realm configurations

SVM administrators can now create Kerberos realm configurations at the SVM level. This means that SVM administrators no longer have to rely on the cluster administrator for Kerberos realm configuration and can create individual Kerberos realm configurations in a multi-tenancy environment.

### Requirements for configuring Kerberos with NFS

Before you configure Kerberos with NFS on your system, you must verify that certain items in your network and storage environment are properly configured.



The steps to configure your environment depend on what version and type of client operating system, domain controller, Kerberos, DNS, etc., that you are using. Documenting all these variables is beyond the scope of this document. For more information, see the respective documentation for each component.

For a detailed example of how to set up ONTAP and Kerberos 5 with NFSv3 and NFSv4 in an environment using Windows Server 2008 R2 Active Directory and Linux hosts, see technical report 4073.

The following items should be configured first:

### Network environment requirements

- Kerberos

You must have a working Kerberos setup with a key distribution center (KDC), such as Windows Active Directory based Kerberos or MIT Kerberos.

NFS servers must use `nfs` as the primary component of their machine principal.

- Directory service

You must use a secure directory service in your environment, such as Active Directory or OpenLDAP, that is configured to use LDAP over SSL/TLS.

- NTP

You must have a working time server running NTP. This is necessary to prevent Kerberos authentication failure due to time skew.

- Domain name resolution (DNS)

Each UNIX client and each SVM LIF must have a proper service record (SRV) registered with the KDC under forward and reverse lookup zones. All participants must be properly resolvable via DNS.

- User accounts

Each client must have a user account in the Kerberos realm. NFS servers must use “nfs” as the primary component of their machine principal.

## **NFS client requirements**

- NFS

Each client must be properly configured to communicate over the network using NFSv3 or NFSv4.

Clients must support RFC1964 and RFC2203.

- Kerberos

Each client must be properly configured to use Kerberos authentication, including the following details:

- Encryption for TGS communication is enabled.
  - AES-256 for strongest security.
- The most secure encryption type for TGT communication is enabled.
- The Kerberos realm and domain are configured correctly.
- GSS is enabled.

When using machine credentials:

- Do not run `gssd` with the `-n` parameter.
  - Do not run `kinit` as the root user.
- Each client must use the most recent and updated operating system version.

This provides the best compatibility and reliability for AES encryption with Kerberos.

- DNS

Each client must be properly configured to use DNS for correct name resolution.

- NTP

Each client must be synchronizing with the NTP server.

- Host and domain information

Each client's `/etc/hosts` and `/etc/resolv.conf` files must contain the correct host name and DNS information, respectively.

- Keytab files

Each client must have a keytab file from the KDC. The realm must be in uppercase letters. The encryption type must be AES-256 for strongest security.

- Optional: For best performance, clients benefit from having at least two network interfaces: one for communicating with the local area network and one for communicating with the storage network.

## Storage system requirements

- NFS license

The storage system must have a valid NFS license installed.

- CIFS license

The CIFS license is optional. It is only required for checking Windows credentials when using multiprotocol name mapping. It is not required in a strict UNIX-only environment.

- SVM

You must have at least one SVM configured on the system.

- DNS on the SVM

You must have configured DNS on each SVM.

- NFS server

You must have configured NFS on the SVM.

- AES encryption

For strongest security, you must configure the NFS server to allow only AES-256 encryption for Kerberos.

- SMB server

If you are running a multiprotocol environment, you must have configured SMB on the SVM. The SMB server is required for multiprotocol name mapping.

- Volumes

You must have a root volume and at least one data volume configured for use by the SVM.

- Root volume

The root volume of the SVM must have the following configuration:

Name	Setting
Security style	UNIX
UID	root or ID 0



Name	Setting
GID	root or ID 0
UNIX permissions	777

In contrast to the root volume, data volumes can have either security style.

- UNIX groups

The SVM must have the following UNIX groups configured:

Group name	Group ID
daemon	1
root	0
pcuser	65534 (created automatically by ONTAP when you create the SVM)

- UNIX users

The SVM must have the following UNIX users configured:

User name	User ID	Primary group ID	Comment
nfs	500	0	Required for GSS INIT phase The first component of the NFS client user SPN is used as the user.
pcuser	65534	65534	Required for NFS and CIFS multiprotocol use Created and added to the pcuser group automatically by ONTAP when you create the SVM.
root	0	0	Required for mounting

The nfs user is not required if a Kerberos-UNIX name mapping exists for the SPN of the NFS client user.

- Export policies and rules

You must have configured export policies with the necessary export rules for the root and data volumes and qtrees. If all volumes of the SVM are accessed over Kerberos, you can set the export rule options `-rorule`, `-rwrule`, and `-superuser` for the root volume to `krb5`, `krb5i`, or `krb5p`.

- Kerberos-UNIX name mapping

If you want the user identified by the NFS client user SPN to have root permissions, you must create a name mapping to root.

## Related information

[NetApp Technical Report 4073: Secure Unified Authentication](#)

[NetApp Interoperability Matrix Tool](#)

[System administration](#)

[Logical storage management](#)

## Specify the user ID domain for NFSv4

To specify the user ID domain, you can set the `-v4-id-domain` option.

### About this task

By default, ONTAP uses the NIS domain for NFSv4 user ID mapping, if one is set. If an NIS domain is not set, the DNS domain is used. You might need to set the user ID domain if, for example, you have multiple user ID domains. The domain name must match the domain configuration on the domain controller. It is not required for NFSv3.

### Step

1. Enter the following command:

```
vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
```

## Configure name services

### How ONTAP name service switch configuration works

ONTAP stores name service configuration information in a table that is the equivalent of the `/etc/nsswitch.conf` file on UNIX systems. You must understand the function of the table and how ONTAP uses it so that you can configure it appropriately for your environment.

The ONTAP name service switch table determines which name service sources ONTAP consults in which order to retrieve information for a certain type of name service information. ONTAP maintains a separate name service switch table for each SVM.

### Database types

The table stores a separate name service list for each of the following database types:

Database type	Defines name service sources for...	Valid sources are...
hosts	Converting host names to IP addresses	files, dns

Database type	Defines name service sources for...	Valid sources are...
group	Looking up user group information	files, nis, ldap
passwd	Looking up user information	files, nis, ldap
netgroup	Looking up netgroup information	files, nis, ldap
namemap	Mapping user names	files, ldap

## Source types

The sources specify which name service source to use for retrieving the appropriate information.

Specify source type...	To look up information in...	Managed by the command families...
files	Local source files	<pre>vserver services name- service unix-user vserver services name-service unix-group  vserver services name- service netgroup  vserver services name- service dns hosts</pre>
nis	External NIS servers as specified in the NIS domain configuration of the SVM	<pre>vserver services name- service nis-domain</pre>
ldap	External LDAP servers as specified in the LDAP client configuration of the SVM	<pre>vserver services name- service ldap</pre>
dns	External DNS servers as specified in the DNS configuration of the SVM	<pre>vserver services name- service dns</pre>

Even if you plan to use NIS or LDAP for both data access and SVM administration authentication, you should still include `files` and configure local users as a fallback in case NIS or LDAP authentication fails.

## Protocols used to access external sources

To access the servers for external sources, ONTAP uses the following protocols:

External name service source	Protocol used for access
NIS	UDP
DNS	UDP
LDAP	TCP

### Example

The following example displays the name service switch configuration for the SVM svm\_1:

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
```

Vserver	Database	Source	Order
svm_1	hosts	files, dns	
svm_1	group	files	
svm_1	passwd	files	
svm_1	netgroup	nis, files	

To look up IP addresses for hosts, ONTAP first consults local source files. If the query does not return any results, DNS servers are checked next.

To look up user or group information, ONTAP consults only local sources files. If the query does not return any results, the lookup fails.

To look up netgroup information, ONTAP first consults external NIS servers. If the query does not return any results, the local netgroup file is checked next.

There are no name service entries for name mapping in the table for the SVM svm\_1. Therefore, ONTAP consults only local source files by default.

### Related information

[NetApp Technical Report 4668: Name Services Best Practices Guide](#)

### Use LDAP

#### LDAP Overview

An LDAP (Lightweight Directory Access Protocol) server enables you to centrally maintain user information. If you store your user database on an LDAP server in your environment, you can configure your storage system to look up user information in your existing LDAP database.

- Before configuring LDAP for ONTAP, you should verify that your site deployment meets best practices for LDAP server and client configuration. In particular, the following conditions must be met:

- The domain name of the LDAP server must match the entry on the LDAP client.
- The LDAP user password hash types supported by the LDAP server must include those supported by ONTAP:
  - CRYPT (all types) and SHA-1 (SHA, SSHA).
  - Beginning with ONTAP 9.8, SHA-2 hashes (SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384, and SSHA-512) are also supported.
- If the LDAP server requires session security measures, you must configure them in the LDAP client.

The following session security options are available:

- LDAP signing (provides data integrity checking) and LDAP signing and sealing (provides data integrity checking and encryption)
- START TLS
- LDAPS (LDAP over TLS or SSL)
- To enable signed and sealed LDAP queries, the following services must be configured:
  - LDAP servers must support the GSSAPI (Kerberos) SASL mechanism.
  - LDAP servers must have DNS A/AAAA records as well as PTR records set up on the DNS server.
  - Kerberos servers must have SRV records present on the DNS server.
- To enable START TLS or LDAPS, the following points should be considered.
  - It is a NetApp best practice to use Start TLS rather than LDAPS.
  - If LDAPS is used, the LDAP server must be enabled for TLS or for SSL in ONTAP 9.5 and later. SSL is not supported in ONTAP 9.0-9.4.
  - A certificate server must already be configured in the domain.
- To enable LDAP referral chasing (in ONTAP 9.5 and later), the following conditions must be satisfied:
  - Both domains should be configured with one of the following trust relationships:
    - Two-way
    - One-way, where the primary trusts the referral domain
    - Parent-child
  - DNS must be configured to resolve all referred server names.
  - Domain passwords should be same to authenticate when `--bind-as-cifs-server` set to true.

The following configurations are not supported with LDAP referral chasing.



- For all ONTAP versions:
  - LDAP clients on an admin SVM
- For ONTAP 9.8 and earlier (they are supported in 9.9.1 and later):
  - LDAP signing and sealing (the `-session-security` option)
  - Encrypted TLS connections (the `-use-start-tls` option)
  - Communications over LDAPS port 636 (the `-use-ldaps-for-ad-ldap` option)

- Beginning with ONTAP 9.11.1, you can use [LDAP fast bind for nsswitch authentication](#).

- You must enter an LDAP schema when configuring the LDAP client on the SVM.

In most cases, one of the default ONTAP schemas will be appropriate. However, if the LDAP schema in your environment differs from these, you must create a new LDAP client schema for ONTAP before creating the LDAP client. Consult with your LDAP administrator about requirements for your environment.

- Using LDAP for host name resolution is not supported.

For additional information, see [NetApp Technical Report 4835: How to Configure LDAP in ONTAP](#).

## LDAP signing and sealing concepts

Beginning with ONTAP 9, you can configure signing and sealing to enable LDAP session security on queries to an Active Directory (AD) server. You must configure the NFS server security settings on the storage virtual machine (SVM) to correspond to those on the LDAP server.

Signing confirms the integrity of the LDAP payload data using secret key technology. Sealing encrypts the LDAP payload data to avoid transmitting sensitive information in clear text. An *LDAP Security Level* option indicates whether the LDAP traffic needs to be signed, signed and sealed, or neither. The default is `none`. `test`

LDAP signing and sealing on SMB traffic is enabled on the SVM with the `-session-security-for-ad -ldap` option to the `vserver cifs security modify` command.

## LDAPS concepts

You must understand certain terms and concepts about how ONTAP secures LDAP communication. ONTAP can use START TLS or LDAPS for setting up authenticated sessions between Active Directory-integrated LDAP servers or UNIX-based LDAP servers.

## Terminology

There are certain terms that you should understand about how ONTAP uses LDAPS to secure LDAP communication.

- **LDAP**

(Lightweight Directory Access Protocol) A protocol for accessing and managing information directories. LDAP is used as an information directory for storing objects such as users, groups, and netgroups. LDAP also provides directory services that manage these objects and fulfill LDAP requests from LDAP clients.

- **SSL**

(Secure Sockets Layer) A protocol developed for sending information securely over the Internet. It has been deprecated in favor of TLS. SSL is not supported in ONTAP 9.0-9.4.

- **TLS**

(Transport Layer Security) An IETF standards track protocol that is based on the earlier SSL specifications. It is the successor to SSL.

- **LDAPS (LDAP over SSL or TLS)**

A protocol that uses TLS or SSL to secure communication between LDAP clients and LDAP servers. The terms *LDAP over SSL* and *LDAP over TLS* are sometimes used interchangeably; TLS is supported by ONTAP 9 and later, SSL is supported by ONTAP 9.5 and later.

- In ONTAP 9.5-9.8, LDAPS can only be enabled on port 636. To do so, use the `-use-ldaps-for-ad-ldap` parameter with the `vserver cifs security modify` command.
- Beginning with ONTAP 9.9.1, LDAPS can be enabled on any port, although port 636 remains the default. To do so, set the `-ldaps-enabled` parameter to `true` and specify the desired `-port` parameter. For more information, see the `vserver services name-service ldap client create` man page



It is a NetApp best practice to use Start TLS rather than LDAPS.

## • Start TLS

(Also known as *start\_tls*, *STARTTLS*, and *StartTLS*) A mechanism to provide secure communication by using the TLS protocols.

ONTAP uses STARTTLS for securing LDAP communication, and uses the default LDAP port (389) to communicate with the LDAP server. The LDAP server must be configured to allow connections over LDAP port 389; otherwise, LDAP TLS connections from the SVM to the LDAP server fail.

## How ONTAP uses LDAPS

ONTAP supports TLS server authentication, which enables the SVM LDAP client to confirm the LDAP server's identity during the bind operation. TLS-enabled LDAP clients can use standard techniques of public-key cryptography to check that a server's certificate and public ID are valid and have been issued by a certificate authority (CA) listed in the client's list of trusted CAs.

LDAP supports STARTTLS to encrypt communications using TLS. STARTTLS begins as a plaintext connection over the standard LDAP port (389), and that connection is then upgraded to TLS.

ONTAP supports the following:

- LDAPS for SMB-related traffic between the Active Directory-integrated LDAP servers and the SVM
- LDAPS for LDAP traffic for name mapping and other UNIX information

Either Active Directory-integrated LDAP servers or UNIX-based LDAP servers can be used to store information for LDAP name mapping and other UNIX information, such as users, groups, and netgroups.

- Self-signed root CA certificates

When using an Active-Directory integrated LDAP, the self-signed root certificate is generated when the Windows Server Certificate Service is installed in the domain. When using an UNIX-based LDAP server for LDAP name mapping, the self-signed root certificate is generated and saved by using means appropriate to that LDAP application.

By default, LDAPS is disabled.

## Enable LDAP RFC2307bis support

If you want to use LDAP and require the additional capability to use nested group

memberships, you can configure ONTAP to enable LDAP RFC2307bis support.

### What you'll need

You must have created a copy of one of the default LDAP client schemas that you want to use.

### About this task

In LDAP client schemas, group objects use the `memberUid` attribute. This attribute can contain multiple values and lists the names of the users that belong to that group. In RFC2307bis enabled LDAP client schemas, group objects use the `uniqueMember` attribute. This attribute can contain the full distinguished name (DN) of another object in the LDAP directory. This enables you to use nested groups because groups can have other groups as members.

The user should not be a member of more than 256 groups including nested groups. ONTAP ignores any groups over the 256 group limit.

By default, RFC2307bis support is disabled.



RFC2307bis support is enabled automatically in ONTAP when an LDAP client is created with the MS-AD-BIS schema.

For additional information, see [NetApp Technical Report 4835: How to Configure LDAP in ONTAP](#).

### Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Modify the copied RFC2307 LDAP client schema to enable RFC2307bis support:

```
vserver services name-service ldap client schema modify -vserver vserver_name  
-schema schema-name -enable-rfc2307bis true
```

3. Modify the schema to match the object class supported in the LDAP server:

```
vserver services name-service ldap client schema modify -vserver vserver-name  
-schema schema_name -group-of-unique-names-object-class object_class
```

4. Modify the schema to match the attribute name supported in the LDAP server:

```
vserver services name-service ldap client schema modify -vserver vserver-name  
-schema schema_name -unique-member-attribute attribute_name
```

5. Return to the admin privilege level:

```
set -privilege admin
```

### Configuration options for LDAP directory searches

You can optimize LDAP directory searches, including user, group, and netgroup information, by configuring the ONTAP LDAP client to connect to LDAP servers in the most appropriate way for your environment. You need to understand when the default LDAP base and scope search values suffice and which parameters to specify when



custom values are more appropriate.

LDAP client search options for user, group, and netgroup information can help avoid failed LDAP queries, and therefore failed client access to storage systems. They also help ensure that the searches are as efficient as possible to avoid client performance issues.

### Default base and scope search values

The LDAP base is the default base DN that the LDAP client uses to perform LDAP queries. All searches, including user, group, and netgroup searches, are done using the base DN. This option is appropriate when your LDAP directory is relatively small and all relevant entries are located in the same DN.

If you do not specify a custom base DN, the default is `root`. This means that each query searches the entire directory. Although this maximizes the chances of success of the LDAP query, it can be inefficient and result in significantly decreased performance with large LDAP directories.

The LDAP base scope is the default search scope that the LDAP client uses to perform LDAP queries. All searches, including user, group, and netgroup searches, are done using the base scope. It determines whether the LDAP query searches only the named entry, entries one level below the DN, or the entire subtree below the DN.

If you do not specify a custom base scope, the default is `subtree`. This means that each query searches the entire subtree below the DN. Although this maximizes the chances of success of the LDAP query, it can be inefficient and result in significantly decreased performance with large LDAP directories.

### Custom base and scope search values

Optionally, you can specify separate base and scope values for user, group, and netgroup searches. Limiting the search base and scope of queries this way can significantly improve performance because it limits the search to a smaller subsection of the LDAP directory.

If you specify custom base and scope values, they override the general default search base and scope for user, group, and netgroup searches. The parameters to specify custom base and scope values are available at the advanced privilege level.

LDAP client parameter...	Specifies custom...
<code>-base-dn</code>	Base DN for all LDAP searches Multiple values can be entered if needed (for example, if LDAP referral chasing is enabled in ONTAP 9.5 and later releases).
<code>-base-scope</code>	Base scope for all LDAP searches
<code>-user-dn</code>	Base DN for all LDAP user searches This parameter also applies to user name-mapping searches.
<code>-user-scope</code>	Base scope for all LDAP user searches This parameter also applies to user name-mapping searches.
<code>-group-dn</code>	Base DN for all LDAP group searches

<code>-group-scope</code>	Base scope for all LDAP group searches
<code>-netgroup-dn</code>	Base DN for all LDAP netgroup searches
<code>-netgroup-scope</code>	Base scope for all LDAP netgroup searches

### Multiple custom base DN values

If your LDAP directory structure is more complex, it might be necessary for you to specify multiple base DN values to search multiple parts of your LDAP directory for certain information. You can specify multiple DN values for the `user`, `group`, and `netgroup` DN parameters by separating them with a semicolon (;) and enclosing the entire DN search list with double quotes ("). If a DN contains a semicolon, you must add an escape character (\) immediately before the semicolon in the DN.

Note that the scope applies to the entire list of DN values specified for the corresponding parameter. For example, if you specify a list of three different user DN values and subtree for the `user` scope, then LDAP user searches search the entire subtree for each of the three specified DN values.

Beginning with ONTAP 9.5, you can also specify LDAP *referral chasing*, which allows the ONTAP LDAP client to refer look-up requests to other LDAP servers if an LDAP referral response is not returned by the primary LDAP server. The client uses that referral data to retrieve the target object from the server described in the referral data. To search for objects present in the referred LDAP servers, the `base-dn` of the referred objects can be added to the `base-dn` as part of LDAP client configuration. However, referred objects are only looked up when referral chasing is enabled (using the `-referral-enabled true` option) during LDAP client creation or modification.

### Improve performance of LDAP directory netgroup-by-host searches

If your LDAP environment is configured to allow `netgroup-by-host` searches, you can configure ONTAP to take advantage of this and perform `netgroup-by-host` searches. This can significantly speed up `netgroup` searches and reduce possible NFS client access issues due to latency during `netgroup` searches.

#### What you'll need

Your LDAP directory must contain a `netgroup.byhost` map.

Your DNS servers should contain both forward (A) and reverse (PTR) lookup records for NFS clients.

When you specify IPv6 addresses in `netgroups`, you must always shorten and compress each address as specified in RFC 5952.

#### About this task

NIS servers store `netgroup` information in three separate maps called `netgroup`, `netgroup.byuser`, and `netgroup.byhost`. The purpose of the `netgroup.byuser` and `netgroup.byhost` maps is to speed up `netgroup` searches. ONTAP can perform `netgroup-by-host` searches on NIS servers for improved mount response times.

By default, LDAP directories do not have such a `netgroup.byhost` map like NIS servers. It is possible, though, with the help of third-party tools, to import a NIS `netgroup.byhost` map into LDAP directories to enable fast `netgroup-by-host` searches. If you have configured your LDAP environment to allow `netgroup-by-`

host searches, you can configure the ONTAP LDAP client with the `netgroup.byhost` map name, DN, and search scope for faster `netgroup-by-host` searches.

Receiving the results for `netgroup-by-host` searches faster enables ONTAP to process export rules faster when NFS clients request access to exports. This reduces the chance of delayed access due to `netgroup` search latency issues.

## Steps

1. Obtain the exact full distinguished name of the NIS `netgroup.byhost` map you imported into your LDAP directory.

The map DN can vary depending on the third-party tool you used for import. For best performance, you should specify the exact map DN.

2. Set the privilege level to advanced: `set -privilege advanced`
3. Enable `netgroup-by-host` searches in the LDAP client configuration of the storage virtual machine (SVM):  

```
vserver services name-service ldap client modify -vserver vserver_name -client -config config_name -is-netgroup-byhost-enabled true -netgroup-byhost-dn netgroup-by-host_map_distinguished_name -netgroup-byhost-scope netgroup-by-host_search_scope
```

`-is-netgroup-byhost-enabled {true|false}` enables or disables `netgroup-by-host` search for LDAP directories. The default is `false`.

`-netgroup-byhost-dn netgroup-by-host_map_distinguished_name` specifies the distinguished name of the `netgroup.byhost` map in the LDAP directory. It overrides the base DN for `netgroup-by-host` searches. If you do not specify this parameter, ONTAP uses the base DN instead.

`-netgroup-byhost-scope {base|onelevel|subtree}` specifies the search scope for `netgroup-by-host` searches. If you do not specify this parameter, the default is `subtree`.

If the LDAP client configuration does not exist yet, you can enable `netgroup-by-host` searches by specifying these parameters when creating a new LDAP client configuration using the `vserver services name-service ldap client create` command.



Beginning with ONTAP 9.2, the field `-ldap-servers` replaces the field `-servers`. This new field can take either a hostname or an IP address for the LDAP server.

4. Return to the admin privilege level: `set -privilege admin`

## Example

The following command modifies the existing LDAP client configuration named “`ldap_corp`” to enable `netgroup-by-host` searches using the `netgroup.byhost` map named “`nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com`” and the default search scope `subtree`:

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1 -client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost -dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

## After you finish

The `netgroup.byhost` and `netgroup` maps in the directory must be kept in sync at all times to avoid client access issues.

### Related information

[IETF RFC 5952: A Recommendation for IPv6 Address Text Representation](#)

### Use LDAP fast bind for nsswitch authentication

Beginning with ONTAP 9.11.1, you can take advantage of LDAP *fast bind* functionality (also known as *concurrent bind*) for faster and simpler client authentication requests. To use this functionality, the LDAP server must support fast bind functionality.

#### About this task

Without fast bind, ONTAP uses LDAP simple bind to authenticate admin users with the LDAP server. With this authentication method, ONTAP sends a user or group name to the LDAP server, receives the stored hash password, and compares the server hash code with the hash passcode generated locally from the user password. If they are identical, ONTAP grants login permission.

With fast bind functionality, ONTAP sends only user credentials (user name and password) to the LDAP server through a secure connection. The LDAP server then validates these credentials and instructs ONTAP to grant login permissions.

One advantage of fast bind is that there is no need for ONTAP to support every new hashing algorithm supported by LDAP servers, because password hashing is performed by the LDAP server.

[Learn about using fast bind.](#)

You can use existing LDAP client configurations for LDAP fast bind. However, it is strongly recommended that the LDAP client be configured for TLS or LDAPS; otherwise, the password is sent over the wire in plain text.

To enable LDAP fast bind in an ONTAP environment, you must satisfy these requirements:

- ONTAP admin users must be configured on an LDAP server that supports fast bind.
- The ONTAP SVM must be configured for LDAP in the name services switch (nsswitch) database.
- ONTAP admin user and group accounts must be configured for nsswitch authentication using fast bind.

#### Steps

1. Confirm with your LDAP administrator that LDAP fast bind is supported on the LDAP server.
2. Ensure that ONTAP admin user credentials are configured on the LDAP server.
3. Verify that the admin or data SVM is configured correctly for LDAP fast bind.
  - a. To confirm that the LDAP fast bind server is listed in the LDAP client configuration, enter:

```
vserver services name-service ldap client show
```

[Learn about LDAP client configuration.](#)

- b. To confirm that `ldap` is one of the configured sources for the `nsswitch passwd` database, enter:

```
vserver services name-service ns-switch show
```

[Learn about nsswitch configuration.](#)

4. Ensure that admin users are authenticating with nsswitch and that LDAP fast bind authentication is enabled in their accounts.

- For existing users, enter `security login modify` and verify the following parameter settings:

```
-authentication-method nsswitch
```

```
-is-ldap-fastbind true
```

- For new admin users, see [Enable LDAP or NIS account access](#).

## Display LDAP statistics

Beginning with ONTAP 9.2, you can display LDAP statistics for storage virtual machines (SVMs) on a storage system to monitor the performance and diagnose issues.

### What you'll need

- You must have configured an LDAP client on the SVM.
- You must have identified LDAP objects from which you can view data.

### Step

1. View the performance data for counter objects:

```
statistics show
```

### Examples

The following example shows the performance data for object `secd_external_service_op`:

```
cluster::*> statistics show -vserver vserverName -object
secd_external_service_op -instance "vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1"
```

```
Object: secd_external_service_op
Instance: vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1
Start-time: 4/13/2016 22:15:38
End-time: 4/13/2016 22:15:38
Scope: vserverName
```

Counter	Value
instance_name	vserverName:LDAP (NIS & Name Mapping):GetUserInfoFromName: 1.1.1.1
last_modified_time	1460610787
node_name	nodeName
num_not_found_responses	1
num_request_failures	1
num_requests_sent	1
num_responses_received	1
num_successful_responses	0
num_timeouts	0
operation	GetUserInfoFromName
process_name	secd
request_latency	52131us

## Configure name mappings

### Configure name mappings overview

ONTAP uses name mapping to map SMB identities to UNIX identities, Kerberos identities to UNIX identities, and UNIX identities to SMB identities. It needs this information to obtain user credentials and provide proper file access regardless of whether they are connecting from an NFS client or a SMB client.

There are two exceptions where you do not have to use name mapping:

- You configure a pure UNIX environment and do not plan to use SMB access or NTFS security style on volumes.
- You configure the default user to be used instead.

In this scenario, name mapping is not required because instead of mapping every individual client credential all client credentials are mapped to the same default user.

Note that you can use name mapping only for users, not for groups.

However, you can map a group of individual users to a specific user. For example, you can map all AD users that start or end with the word SALES to a specific UNIX user and to the user's UID.

### How name mapping works

When ONTAP has to map credentials for a user, it first checks the local name mapping database and LDAP server for an existing mapping. Whether it checks one or both and in which order is determined by the name service configuration of the SVM.

- For Windows to UNIX mapping

If no mapping is found, ONTAP checks whether the lowercase Windows user name is a valid user name in the UNIX domain. If this does not work, it uses the default UNIX user provided that it is configured. If the default UNIX user is not configured and ONTAP cannot obtain a mapping this way either, mapping fails and an error is returned.

- For UNIX to Windows mapping

If no mapping is found, ONTAP tries to find a Windows account that matches the UNIX name in the SMB domain. If this does not work, it uses the default SMB user, provided that it is configured. If the default SMB user is not configured and ONTAP cannot obtain a mapping this way either, mapping fails and an error is returned.

Machine accounts are mapped to the specified default UNIX user by default. If no default UNIX user is specified, machine account mappings fail.

- Beginning with ONTAP 9.5, you can map machine accounts to users other than the default UNIX user.
- In ONTAP 9.4 and earlier, you cannot map machine accounts to other users.

Even if name mappings for machine accounts are defined, the mappings are ignored.

### Multidomain searches for UNIX user to Windows user name mappings

ONTAP supports multidomain searches when mapping UNIX users to Windows users. All discovered trusted domains are searched for matches to the replacement pattern until a matching result is returned. Alternatively, you can configure a list of preferred trusted domains, which is used instead of the discovered trusted domain list and is searched in order until a matching result is returned.

### How domain trusts affect UNIX user to Windows user name mapping searches

To understand how multidomain user name mapping works, you must understand how domain trusts work with ONTAP. Active Directory trust relationships with the SMB server's home domain can be a bidirectional trust or can be one of two types of unidirectional trusts, either an inbound trust or an outbound trust. The home domain is the domain to which the SMB server on the SVM belongs.

- *Bidirectional trust*

With bidirectional trusts, both domains trust each other. If the SMB server's home domain has a bidirectional trust with another domain, the home domain can authenticate and authorize a user belonging to the trusted domain and vice versa.

UNIX user to Windows user name mapping searches can be performed only on domains with bidirectional trusts between the home domain and the other domain.

- *Outbound trust*

With an outbound trust, the home domain trusts the other domain. In this case, the home domain can authenticate and authorize a user belonging to the outbound trusted domain.

A domain with an outbound trust with the home domain is *not* searched when performing UNIX user to Windows user name mapping searches.


- *Inbound trust*

With an inbound trust, the other domain trusts the SMB server's home domain. In this case, the home domain cannot authenticate or authorize a user belonging to the inbound trusted domain.

A domain with an inbound trust with the home domain is *not* searched when performing UNIX user to Windows user name mapping searches.

### How wildcards (\*) are used to configure multidomain searches for name mapping

Multidomain name mapping searches are facilitated by the use of wildcards in the domain section of the Windows user name. The following table illustrates how to use wildcards in the domain part of a name mapping entry to enable multidomain searches:

Pattern	Replacement	Result
root	*\\administrator	The UNIX user "root" is mapped to the user named "administrator". All trusted domains are searched in order until the first matching user named "administrator" is found.
*	*\\*	Valid UNIX users are mapped to the corresponding Windows users. All trusted domains are searched in order until the first matching user with that name is found.  <div style="border: 1px solid gray; padding: 5px; display: inline-block;">  The pattern *\\* is only valid for name mapping from UNIX to Windows, not the other way around.         </div>

### How multidomain name searches are performed

You can choose one of two methods for determining the list of trusted domains used for multidomain name searches:

- Use the automatically discovered bidirectional trust list compiled by ONTAP
- Use the preferred trusted domain list that you compile



If a UNIX user is mapped to a Windows user with a wildcard used for the domain section of the user name, the Windows user is looked up in all the trusted domains as follows:

- If a preferred trusted-domain list is configured, the mapped Windows user is looked up in this search list only, in order.
- If a preferred list of trusted domains is not configured, then the Windows user is looked up in all the bidirectional trusted domains of the home domain.
- If there are no bidirectionally trusted domains for the home domain, the user is looked up in the home domain.

If a UNIX user is mapped to a Windows user without a domain section in the user name, the Windows user is looked up in the home domain.

### Name mapping conversion rules

An ONTAP system keeps a set of conversion rules for each SVM. Each rule consists of two pieces: a *pattern* and a *replacement*. Conversions start at the beginning of the appropriate list and perform a substitution based on the first matching rule. The pattern is a UNIX-style regular expression. The replacement is a string containing escape sequences representing subexpressions from the pattern, as in the UNIX `sed` program.

### Create a name mapping

You can use the `vserver name-mapping create` command to create a name mapping. You use name mappings to enable Windows users to access UNIX security style volumes and the reverse.

#### About this task

For each SVM, ONTAP supports up to 12,500 name mappings for each direction.

#### Step

1. Create a name mapping:

```
vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-unix|unix-win} -position integer -pattern text -replacement text
```



The `-pattern` and `-replacement` statements can be formulated as regular expressions. You can also use the `-replacement` statement to explicitly deny a mapping to the user by using the null replacement string " " (the space character). See the `vserver name-mapping create` man page for details.

When Windows-to-UNIX mappings are created, any SMB clients that have open connections to the ONTAP system at the time the new mappings are created must log out and log back in to see the new mappings.

### Examples

The following command creates a name mapping on the SVM named `vs1`. The mapping is a mapping from UNIX to Windows at position 1 in the priority list. The mapping maps the UNIX user `johnd` to the Windows user `ENG\JohnDoe`.

```
vs1::> vsserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

The following command creates another name mapping on the SVM named vs1. The mapping is a mapping from Windows to UNIX at position 1 in the priority list. Here the pattern and replacement include regular expressions. The mapping maps every CIFS user in the domain ENG to users in the LDAP domain associated with the SVM.

```
vs1::> vsserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\\1"
```

The following command creates another name mapping on the SVM named vs1. Here the pattern includes "\$" as an element in the Windows user name that must be escaped. The mapping maps the windows user ENG\john\$ops to UNIX user john\_ops.

```
vs1::> vsserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

### Configure the default user

You can configure a default user to use if all other mapping attempts fail for a user, or if you do not want to map individual users between UNIX and Windows. Alternatively, if you want authentication of non-mapped users to fail, you should not configure a default user.

### About this task

For CIFS authentication, if you do not want to map each Windows user to an individual UNIX user, you can instead specify a default UNIX user.

For NFS authentication, if you do not want to map each UNIX user to an individual Windows user, you can instead specify a default Windows user.

### Step

1. Perform one of the following actions:

If you want to...	Enter the following command...
Configure the default UNIX user	<pre>vsserver cifs options modify -default-unix-user user_name</pre>
Configure the default Windows user	<pre>vsserver nfs modify -default-win-user user_name</pre>

## Commands for managing name mappings

There are specific ONTAP commands for managing name mappings.

If you want to...	Use this command...
Create a name mapping	<code>vserver name-mapping create</code>
Insert a name mapping at a specific position	<code>vserver name-mapping insert</code>
Display name mappings	<code>vserver name-mapping show</code>
Exchange the position of two name mappings NOTE: A swap is not allowed when name-mapping is configured with an ip-qualifier entry.	<code>vserver name-mapping swap</code>
Modify a name mapping	<code>vserver name-mapping modify</code>
Delete a name mapping	<code>vserver name-mapping delete</code>
Validate the correct name mapping	<code>vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1</code>

See the man page for each command for more information.

## Enable access for Windows NFS clients

ONTAP supports file access from Windows NFSv3 clients. This means that clients running Windows operating systems with NFSv3 support can now access files on NFSv3 exports on the cluster. To successfully use this functionality, you must properly configure the storage virtual machine (SVM) and be aware of certain requirements and limitations.

### What you'll need

NFSv3 must be enabled on the SVM.

### About this task

By default, Windows NFSv3 client support is disabled.

Windows NFSv3 clients do not support the network status monitor (NSM) protocol. As a result, Windows NFSv3 client sessions might experience disruptions during storage failover and volume move operations.

### Steps

1. Enable Windows NFSv3 client support:

```
vserver nfs modify -vserver vserver_name -v3-ms-dos-client enabled
```

2. On all SVMs that support Windows NFSv3 clients, disable the `-enable-ejukebox` and `-v3-connection-drop` parameters: `vserver nfs modify -vserver vserver_name -enable-ejukebox false -v3-connection-drop disabled`

Windows NFSv3 clients can now mount exports on the storage system.

3. Ensure that each Windows NFSv3 client uses hard mounts by specifying the `-o mtype=hard` option.

This is required to ensure reliable mounts.

```
mount -o mtype=hard \\10.53.33.10\vol\vol1 z:\
```

## Enable the display of NFS exports on NFS clients

NFS clients can use the `showmount -e` command to see a list of exports available from an ONTAP NFS server. This can help users identify the file system they want to mount.

Beginning with ONTAP 9.2, ONTAP allows NFS clients to view the export list by default. In earlier releases, the `showmount` option of the `vserver nfs modify` command must be enabled explicitly. For viewing the export list, NFSv3 should be enabled on the SVM.

### Example

The following command shows the `showmount` feature on the SVM named `vs1`:

```
cluster1 : : > vserver nfs show -vserver vs1 -fields showmount
vserver showmount
-----
vs1      enabled
```

The following command executed on an NFS client displays the list of exports on an NFS server with the IP address 10.63.21.9:

```
showmount -e 10.63.21.9
Export list for 10.63.21.9:
/unix      (everyone)
/unix/unix1 (everyone)
/unix/unix2 (everyone)
/          (everyone)
```

## Manage file access using NFS

### Enable or disable NFSv3

You can enable or disable NFSv3 by modifying the `-v3` option. This allows file access for clients using the NFSv3 protocol. By default, NFSv3 is enabled.

### Step

1. Perform one of the following actions:

If you want to...	Enter the command...
Enable NFSv3	<code>vserver nfs modify -vserver vserver_name -v3 enabled</code>
Disable NFSv3	<code>vserver nfs modify -vserver vserver_name -v3 disabled</code>

### Enable or disable NFSv4.0

You can enable or disable NFSv4.0 by modifying the `-v4.0` option. This allows file access for clients using the NFSv4.0 protocol. In ONTAP 9.9.1, NFSv4.0 is enabled by default; in earlier releases, it is disabled by default.

#### Step

1. Perform one of the following actions:

If you want to...	Enter the following command...
Enable NFSv4.0	<code>vserver nfs modify -vserver vserver_name -v4.0 enabled</code>
Disable NFSv4.0	<code>vserver nfs modify -vserver vserver_name -v4.0 disabled</code>

### Enable or disable NFSv4.1

You can enable or disable NFSv4.1 by modifying the `-v4.1` option. This allows file access for clients using the NFSv4.1 protocol. In ONTAP 9.9.1, NFSv4.1 is enabled by default; in earlier releases, it is disabled by default.

#### Step

1. Perform one of the following actions:

If you want to...	Enter the following command...
Enable NFSv4.1	<code>vserver nfs modify -vserver vserver_name -v4.1 enabled</code>
Disable NFSv4.1	<code>vserver nfs modify -vserver vserver_name -v4.1 disabled</code>

### Enable or disable pNFS

pNFS improves performance by allowing NFS clients to perform read/write operations on

storage devices directly and in parallel, bypassing the NFS server as a potential bottleneck. To enable or disable pNFS (parallel NFS), you can modify the `-v4.1-pnfs` option.

If the ONTAP release is...	The pNFS default is...
9.8 or later	disabled
9.7 or earlier	enabled

### What you'll need

NFSv4.1 support is required to be able to use pNFS.

If you want to enable pNFS, you must first disable NFS referrals. They cannot both be enabled at the same time.

If you use pNFS with Kerberos on SVMs, you must enable Kerberos on every LIF on the SVM.

### Step

1. Perform one of the following actions:

If you want to...	Enter the command...
Enable pNFS	<code>vserver nfs modify -vserver vserver_name -v4.1-pnfs enabled</code>
Disable pNFS	<code>vserver nfs modify -vserver vserver_name -v4.1-pnfs disabled</code>

### Control NFS access over TCP and UDP

You can enable or disable NFS access to storage virtual machines (SVMs) over TCP and UDP by modifying the `-tcp` and `-udp` parameters, respectively. This enables you to control whether NFS clients can access data over TCP or UDP in your environment.

#### About this task

These parameters only apply to NFS. They do not affect auxiliary protocols. For example, if NFS over TCP is disabled, mount operations over TCP still succeed. To completely block TCP or UDP traffic, you can use export policy rules.



You must turn off the SnapDiff RPC Server before you disable TCP for NFS to avoid a command failed error. You can disable TCP by using the command `vserver snapdiff-rpc-server off -vserver vserver name`.

### Step

1. Perform one of the following actions:

If you want NFS access to be...	Enter the command...
---------------------------------	----------------------

Enabled over TCP	<code>vserver nfs modify -vserver vserver_name -tcp enabled</code>
Disabled over TCP	<code>vserver nfs modify -vserver vserver_name -tcp disabled</code>
Enabled over UDP	<code>vserver nfs modify -vserver vserver_name -udp enabled</code>
Disabled over UDP	<code>vserver nfs modify -vserver vserver_name -udp disabled</code>

### Control NFS requests from nonreserved ports

You can reject NFS mount requests from nonreserved ports by enabling the `-mount -rootonly` option. To reject all NFS requests from nonreserved ports, you can enable the `-nfs-rootonly` option.

#### About this task

By default, the option `-mount-rootonly` is enabled.

By default, the option `-nfs-rootonly` is disabled.

These options do not apply to the NULL procedure.

#### Step

1. Perform one of the following actions:

If you want to...	Enter the command...
Allow NFS mount requests from nonreserved ports	<code>vserver nfs modify -vserver vserver_name -mount -rootonly disabled</code>
Reject NFS mount requests from nonreserved ports	<code>vserver nfs modify -vserver vserver_name -mount -rootonly enabled</code>
Allow all NFS requests from nonreserved ports	<code>vserver nfs modify -vserver vserver_name -nfs -rootonly disabled</code>
Reject all NFS requests from nonreserved ports	<code>vserver nfs modify -vserver vserver_name -nfs -rootonly enabled</code>

### Handle NFS access to NTFS volumes or qtrees for unknown UNIX users

If ONTAP cannot identify UNIX users attempting to connect to volumes or qtrees with NTFS security style, it therefore cannot explicitly map the user to a Windows user. You can configure ONTAP to either deny access to such users for stricter security or map them to a default Windows user to ensure a minimum level of access for all users.

## What you'll need

A default Windows user must be configured if you want to enable this option.

## About this task

If a UNIX user tries to access volumes or qtrees with NTFS security style, the UNIX user must first be mapped to a Windows user so that ONTAP can properly evaluate the NTFS permissions. However, if ONTAP cannot look up the name of the UNIX user in the configured user information name service sources, it cannot explicitly map the UNIX user to a specific Windows user. You can decide how to handle such unknown UNIX users in the following ways:

- Deny access to unknown UNIX users.

This enforces stricter security by requiring explicit mapping for all UNIX users to gain access to NTFS volumes or qtrees.

- Map unknown UNIX users to a default Windows user.

This provides less security but more convenience by ensuring that all users get a minimum level of access to NTFS volumes or qtrees through a default Windows user.

## Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Perform one of the following actions:

If you want the default Windows user for unknown UNIX users...	Enter the command...
Enabled	<pre>vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user enabled</pre>
Disabled	<pre>vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user disabled</pre>

3. Return to the admin privilege level:

```
set -privilege admin
```

## Considerations for clients that mount NFS exports using a nonreserved port

The `-mount-rootonly` option must be disabled on a storage system that must support clients that mount NFS exports using a nonreserved port even when the user is logged in as root. Such clients include Hummingbird clients and Solaris NFS/IPv6 clients.

If the `-mount-rootonly` option is enabled, ONTAP does not allow NFS clients that use nonreserved ports, meaning ports with numbers higher than 1,023, to mount NFS exports.



## Perform stricter access checking for netgroups by verifying domains

By default, ONTAP performs an additional verification when evaluating client access for a netgroup. The additional check ensures that the client's domain matches the domain configuration of the storage virtual machine (SVM). Otherwise, ONTAP denies client access.

### About this task

When ONTAP evaluates export policy rules for client access and an export policy rule contains a netgroup, ONTAP must determine whether a client's IP address belongs to the netgroup. For this purpose, ONTAP converts the client's IP address to a host name using DNS and obtains a fully qualified domain name (FQDN).

If the netgroup file only lists a short name for the host and the short name for the host exists in multiple domains, it is possible for a client from a different domain to obtain access without this check.

To prevent this, ONTAP compares the domain that was returned from DNS for the host against the list of DNS domain names configured for the SVM. If it matches, access is allowed. If it does not match, access is denied.

This verification is enabled by default. You can manage it by modifying the `-netgroup-dns-domain-search` parameter, which is available at the advanced privilege level.

### Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Perform the desired action:

If you want domain verification for netgroups to be...	Enter...
Enabled	<pre>vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search enabled</pre>
Disabled	<pre>vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search disabled</pre>

3. Set the privilege level to admin:

```
set -privilege admin
```

## Modify ports used for NFSv3 services

The NFS server on the storage system uses services such as mount daemon and Network Lock Manager to communicate with NFS clients over specific default network ports. In most NFS environments the default ports work correctly and do not require modification, but if you want to use different NFS network ports in your NFSv3 environment, you can do so.

## What you'll need

Changing NFS ports on the storage system requires that all NFS clients reconnect to the system, so you should communicate this information to your users in advance of making the change.

## About this task

You can set the ports used by the NFS mount daemon, Network Lock Manager, Network Status Monitor, and NFS quota daemon services for each storage virtual machine (SVM). The port number change affects NFS clients accessing data over both TCP and UDP.

Ports for NFSv4 and NFSv4.1 cannot be changed.

## Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Disable access to NFS:

```
vserver nfs modify -vserver vserver_name -access false
```

3. Set the NFS port for the specific NFS service:

```
vserver nfs modify -vserver vserver_name nfs_port_parameter port_number
```

NFS port parameter	Description	Default port
-mountd-port	NFS mount daemon	635
-nlm-port	Network Lock Manager	4045
-nsm-port	Network Status Monitor	4046
-rquotad-port	NFS quota daemon	4049

Besides the default port, the allowed range of port numbers is 1024 through 65535. Each NFS service must use a unique port.

4. Enable access to NFS:

```
vserver nfs modify -vserver vserver_name -access true
```

5. Use the `network connections listening show` command to verify the port number changes.

6. Return to the admin privilege level:

```
set -privilege admin
```

## Example

The following commands set the NFS Mount Daemon port to 1113 on the SVM named vs1:

```

vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
        them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -access false

vs1::*> vserver nfs modify -vserver vs1 -mountd-port 1113

vs1::*> vserver nfs modify -vserver vs1 -access true


vs1::*> network connections listening show
Vserver Name      Interface Name:Local Port      Protocol/Service
-----
Node: cluster1-01
Cluster          cluster1-01_clus_1:7700        TCP/ctlopcp
vs1              data1:4046                    TCP/sm
vs1              data1:4046                    UDP/sm
vs1              data1:4045                    TCP/nlm-v4
vs1              data1:4045                    UDP/nlm-v4
vs1              data1:1113                    TCP/mount
vs1              data1:1113                    UDP/mount
...
vs1::*> set -privilege admin

```

## Commands for managing NFS servers

There are specific ONTAP commands for managing NFS servers.

If you want to...	Use this command...
Create an NFS server	<code>vserver nfs create</code>
Display NFS servers	<code>vserver nfs show</code>
Modify an NFS server	<code>vserver nfs modify</code>
Delete an NFS server	<code>vserver nfs delete</code>

<p>Hide the <code>.snapshot</code> directory listing under NFSv3 mount points</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Explicit access to the <code>.snapshot</code> directory will still be allowed even if the option is enabled.</p> </div>	<p><code>vserver nfs</code> commands with the <code>-v3-hide-snapshot</code> option enabled</p>
---	---

See the man page for each command for more information.

**Troubleshoot name service issues**

When clients experience access failures due to name service issues, you can use the `vserver services name-service getxxbyyy` command family to manually perform various name service lookups and examine the details and results of the lookup to help with troubleshooting.

**About this task**

- For each command, you can specify the following:
  - Name of the node or storage virtual machine (SVM) to perform the lookup on.
 

This enables you to test name service lookups for a specific node or SVM to narrow the search for a potential name service configuration issue.
  - Whether to show the source used for the lookup.
 

This enables you to check whether the correct source was used.
- ONTAP selects the service for performing the lookup based on the configured name service switch order.
- These commands are available at the advanced privilege level.

**Steps**

1. Perform one of the following actions:

To retrieve the...	Use the command...
IP address of a host name	<pre>vserver services name-service getxxbyyy getaddrinfo vserver services name- service getxxbyyy gethostbyname (IPv4 addresses only)</pre>
Members of a group by group ID	<pre>vserver services name-service getxxbyyy getgrbygid</pre>
Members of a group by group name	<pre>vserver services name-service getxxbyyy getgrbyname</pre>

List of groups a user belongs to	<code>vserver services name-service getxxbyyy getgrlist</code>
Host name of an IP address	<code>vserver services name-service getxxbyyy getnameinfo vserver services name- service getxxbyyy gethostbyaddr (IPv4 addresses only)</code>
User information by user name	<code>vserver services name-service getxxbyyy getpwbyname</code> You can test name resolution of RBAC users by specifying the <code>-use-rbac</code> parameter as <code>true</code> .
User information by user ID	<code>vserver services name-service getxxbyyy getpwbyuid</code> You can test name resolution of RBAC users by specifying the <code>-use-rbac</code> parameter as <code>true</code> .
Netgroup membership of a client	<code>vserver services name-service getxxbyyy netgrp</code>
Netgroup membership of a client using <code>netgroup-by-host</code> search	<code>vserver services name-service getxxbyyy netgrpbyhost</code>

The following example shows a DNS lookup test for the SVM vs1 by attempting to obtain the IP address for the host `acast1.eng.example.com`:

```
cluster1::*> vserver services name-service getxxbyyy getaddrinfo -vserver
vs1 -hostname acast1.eng.example.com -address-family all -show-source true
Source used for lookup: DNS
Host name: acast1.eng.example.com
Canonical Name: acast1.eng.example.com
IPv4: 10.72.8.29
```

The following example shows a NIS lookup test for the SVM vs1 by attempting to retrieve user information for a user with the UID 501768:

```

cluster1::*> vserver services name-service getxxbyyy getpwbyuid -vserver
vs1 -userID 501768 -show-source true
Source used for lookup: NIS
pw_name: jsmith
pw_passwd: $1$y8rA4XX7$/DDOXAvC2PC/IsNFozfIN0
pw_uid: 501768
pw_gid: 501768
pw_gecos:
pw_dir: /home/jsmith
pw_shell: /bin/bash

```

The following example shows an LDAP lookup test for the SVM vs1 by attempting to retrieve user information for a user with the name ldap1:

```

cluster1::*> vserver services name-service getxxbyyy getpwbyname -vserver
vs1 -username ldap1 -use-rbac false -show-source true
Source used for lookup: LDAP
pw_name: ldap1
pw_passwd: {crypt}JSPM6yc/ilIX6
pw_uid: 10001
pw_gid: 3333
pw_gecos: ldap1 user
pw_dir: /u/ldap1
pw_shell: /bin/csh

```

The following example shows a netgroup lookup test for the SVM vs1 by attempting to find out whether the client dnshost0 is a member of the netgroup lnetgroup136:

```

cluster1::*> vserver services name-service getxxbyyy netgrp -vserver vs1
-netgroup lnetgroup136 -client dnshost0 -show-source true
Source used for lookup: LDAP
dnshost0 is a member of lnetgroup136

```

1. Analyze the results of the test you performed and take the necessary action.

If the...	Check the...
Host name or IP address lookup failed or yielded incorrect results	DNS configuration
Lookup queried an incorrect source	Name service switch configuration

User or group lookup failed or yielded incorrect results	Name service switch configuration Source configuration (local files, NIS domain, LDAP client)  Network configuration (for example, LIFs and routes)
Host name lookup failed or timed out, and the DNS server does not resolve DNS short names (for example, host1)	DNS configuration for top-level domain (TLD) queries. You can disable TLD queries using the <code>-is-tld-query-enabled false</code> option to the <code>vserver services name-service dns modify</code> command.

### Related information

[NetApp Technical Report 4668: Name Services Best Practices Guide](#)

### Verify name service connections

Beginning with ONTAP 9.2, you can check DNS and LDAP name servers to verify that they are connected to ONTAP. These commands are available at the admin privilege level.

#### About this task

You can check for a valid DNS or LDAP name service configuration on an as-needed basis using the name service configuration checker. This validation check can be initiated at the command line or in System Manager.

For DNS configurations, all servers are tested and need to be working for the configuration to be considered valid. For LDAP configurations, as long as any server is up, the configuration is valid. The name service commands apply the configuration checker unless the `skip-config-validation` field is true (the default is false).

#### Step

1. Use the appropriate command to check a name service configuration. The UI displays the status of the configured servers.

To check...	Use this command...
DNS configuration status	<code>vserver services name-service dns check</code>
LDAP configuration status	<code>vserver services name-service ldap check</code>

```
cluster1::> vserver services name-service dns check -vserver vs0
```

```

Vserver          Name Server      Status  Status Details
-----
vs0              10.11.12.13     up      Response time (msec): 55
vs0              10.11.12.14     up      Response time (msec): 70
vs0              10.11.12.15     down    Connection refused.
+-----+

```

```
cluster1::> vserver services name-service ldap check -vserver vs0
```

```

| Vserver: vs0
| Client Configuration Name: c1
| LDAP Status: up
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".

```

Configuration validation is successful if at least one of the configured servers (name-servers/ldap-servers) is reachable and providing the service. A warning is shown if some of the servers are not reachable.

### Commands for managing name service switch entries

You can manage name service switch entries by creating, displaying, modifying, and deleting them.

If you want to...	Use this command...
Create a name service switch entry	<code>vserver services name-service ns-switch create</code>
Display name service switch entries	<code>vserver services name-service ns-switch show</code>
Modify a name service switch entry	<code>vserver services name-service ns-switch modify</code>
Delete a name service switch entry	<code>vserver services name-service ns-switch delete</code>

See the man page for each command for more information.

### Related information

[NetApp Technical Report 4668: Name Services Best Practices Guide](#)

### Commands for managing name service cache

You can manage name service cache by modifying the time to live (TTL) value. The TTL value determines how long name service information is persistent in cache.



<b>If you want to modify the TTL value for...</b>	<b>Use this command...</b>
Unix users	<code>vserver services name-service cache unix-user settings</code>
Unix groups	<code>vserver services name-service cache unix-group settings</code>
Unix netgroups	<code>vserver services name-service cache netgroups settings</code>
Hosts	<code>vserver services name-service cache hosts settings</code>
Group membership	<code>vserver services name-service cache group-membership settings</code>

### Related information

[ONTAP 9 Commands](#)

### Commands for managing name mappings

There are specific ONTAP commands for managing name mappings.

<b>If you want to...</b>	<b>Use this command...</b>
Create a name mapping	<code>vserver name-mapping create</code>
Insert a name mapping at a specific position	<code>vserver name-mapping insert</code>
Display name mappings	<code>vserver name-mapping show</code>
Exchange the position of two name mappings NOTE: A swap is not allowed when name-mapping is configured with an ip-qualifier entry.	<code>vserver name-mapping swap</code>
Modify a name mapping	<code>vserver name-mapping modify</code>
Delete a name mapping	<code>vserver name-mapping delete</code>
Validate the correct name mapping	<code>vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1</code>

See the man page for each command for more information.

### Commands for managing local UNIX users

There are specific ONTAP commands for managing local UNIX users.

If you want to...	Use this command...
Create a local UNIX user	<code>vserver services name-service unix-user create</code>
Load local UNIX users from a URI	<code>vserver services name-service unix-user load-from-uri</code>
Display local UNIX users	<code>vserver services name-service unix-user show</code>
Modify a local UNIX user	<code>vserver services name-service unix-user modify</code>
Delete a local UNIX user	<code>vserver services name-service unix-user delete</code>

See the man page for each command for more information.

### Commands for managing local UNIX groups

There are specific ONTAP commands for managing local UNIX groups.

If you want to...	Use this command...
Create a local UNIX group	<code>vserver services name-service unix-group create</code>
Add a user to a local UNIX group	<code>vserver services name-service unix-group adduser</code>
Load local UNIX groups from a URI	<code>vserver services name-service unix-group load-from-uri</code>
Display local UNIX groups	<code>vserver services name-service unix-group show</code>
Modify a local UNIX group	<code>vserver services name-service unix-group modify</code>
Delete a user from a local UNIX group	<code>vserver services name-service unix-group deluser</code>
Delete a local UNIX group	<code>vserver services name-service unix-group delete</code>

See the man page for each command for more information.

## Limits for local UNIX users, groups, and group members

ONTAP introduced limits for the maximum number of UNIX users and groups in the cluster, and commands to manage these limits. These limits can help avoid performance issues by preventing administrators from creating too many local UNIX users and groups in the cluster.

There is a limit for the combined number of local UNIX user groups and group members. There is a separate limit for local UNIX users. The limits are cluster-wide. Each of these new limits is set to a default value that you can modify up to a preassigned hard limit.

Database	Default limit	Hard limit
Local UNIX users	32,768	65,536
Local UNIX groups and group members	32,768	65,536

## Manage limits for local UNIX users and groups

There are specific ONTAP commands for managing limits for local UNIX users and groups. Cluster administrators can use these commands to troubleshoot performance issues in the cluster believed to be related to excessive numbers of local UNIX users and groups.

### About this task

These commands are available to the cluster administrator at the advanced privilege level.

### Step

1. Perform one of the following actions:

If you want to...	Use the command...
Display information about local UNIX user limits	<code>vserver services unix-user max-limit show</code>
Display information about local UNIX group limits	<code>vserver services unix-group max-limit show</code>
Modify local UNIX user limits	<code>vserver services unix-user max-limit modify</code>
Modify local UNIX group limits	<code>vserver services unix-group max-limit modify</code>

See the man page for each command for more information.

## Commands for managing local netgroups

You can manage local netgroups by loading them from a URI, verifying their status across nodes, displaying them, and deleting them.

If you want to...	Use the command...
Load netgroups from a URI	<code>vserver services name-service netgroup load</code>
Verify the status of netgroups across nodes	<code>vserver services name-service netgroup status</code> Available at the advanced privilege level and higher.
Display local netgroups	<code>vserver services name-service netgroup file show</code>
Delete a local netgroup	<code>vserver services name-service netgroup file delete</code>

See the man page for each command for more information.

## Commands for managing NIS domain configurations

There are specific ONTAP commands for managing NIS domain configurations.

If you want to...	Use this command...
Create a NIS domain configuration	<code>vserver services name-service nis-domain create</code>
Display NIS domain configurations	<code>vserver services name-service nis-domain show</code>
Display binding status of a NIS domain configuration	<code>vserver services name-service nis-domain show-bound</code>
Display NIS statistics	<code>vserver services name-service nis-domain show-statistics</code> Available at the advanced privilege level and higher.
Clear NIS statistics	<code>vserver services name-service nis-domain clear-statistics</code> Available at the advanced privilege level and higher.
Modify a NIS domain configuration	<code>vserver services name-service nis-domain modify</code>
Delete a NIS domain configuration	<code>vserver services name-service nis-domain delete</code>
Enable caching for netgroup-by-host searches	<code>vserver services name-service nis-domain netgroup-database config modify</code> Available at the advanced privilege level and higher.

See the man page for each command for more information.

## Commands for managing LDAP client configurations

There are specific ONTAP commands for managing LDAP client configurations.



SVM administrators cannot modify or delete LDAP client configurations that were created by cluster administrators.

If you want to...	Use this command...
Create an LDAP client configuration	<code>vserver services name-service ldap client create</code>
Display LDAP client configurations	<code>vserver services name-service ldap client show</code>
Modify an LDAP client configuration	<code>vserver services name-service ldap client modify</code>
Change the LDAP client BIND password	<code>vserver services name-service ldap client modify-bind-password</code>
Delete an LDAP client configuration	<code>vserver services name-service ldap client delete</code>

See the man page for each command for more information.

## Commands for managing LDAP configurations

There are specific ONTAP commands for managing LDAP configurations.

If you want to...	Use this command...
Create an LDAP configuration	<code>vserver services name-service ldap create</code>
Display LDAP configurations	<code>vserver services name-service ldap show</code>
Modify an LDAP configuration	<code>vserver services name-service ldap modify</code>
Delete an LDAP configuration	<code>vserver services name-service ldap delete</code>

See the man page for each command for more information.

## Commands for managing LDAP client schema templates

There are specific ONTAP commands for managing LDAP client schema templates.



SVM administrators cannot modify or delete LDAP client schemas that were created by cluster administrators.

If you want to...	Use this command...
-------------------	---------------------

Copy an existing LDAP schema template	<code>vserver services name-service ldap client schema copy</code> Available at the advanced privilege level and higher.
Display LDAP schema templates	<code>vserver services name-service ldap client schema show</code>
Modify an LDAP schema template	<code>vserver services name-service ldap client schema modify</code> Available at the advanced privilege level and higher.
Delete an LDAP schema template	<code>vserver services name-service ldap client schema delete</code> Available at the advanced privilege level and higher.

See the man page for each command for more information.

### Commands for managing NFS Kerberos interface configurations

There are specific ONTAP commands for managing NFS Kerberos interface configurations.

If you want to...	Use this command...
Enable NFS Kerberos on a LIF	<code>vserver nfs kerberos interface enable</code>
Display NFS Kerberos interface configurations	<code>vserver nfs kerberos interface show</code>
Modify an NFS Kerberos interface configuration	<code>vserver nfs kerberos interface modify</code>
Disable NFS Kerberos on a LIF	<code>vserver nfs kerberos interface disable</code>

See the man page for each command for more information.

### Commands for managing NFS Kerberos realm configurations

There are specific ONTAP commands for managing NFS Kerberos realm configurations.

If you want to...	Use this command...
Create an NFS Kerberos realm configuration	<code>vserver nfs kerberos realm create</code>
Display NFS Kerberos realm configurations	<code>vserver nfs kerberos realm show</code>

If you want to...	Use this command...
Modify an NFS Kerberos realm configuration	<code>vserver nfs kerberos realm modify</code>
Delete an NFS Kerberos realm configuration	<code>vserver nfs kerberos realm delete</code>

See the man page for each command for more information.

### Commands for managing export policies

There are specific ONTAP commands for managing export policies.

If you want to...	Use this command...
Display information about export policies	<code>vserver export-policy show</code>
Rename an export policy	<code>vserver export-policy rename</code>
Copy an export policy	<code>vserver export-policy copy</code>
Delete an export policy	<code>vserver export-policy delete</code>

See the man page for each command for more information.

### Commands for managing export rules

There are specific ONTAP commands for managing export rules.

If you want to...	Use this command...
Create an export rule	<code>vserver export-policy rule create</code>
Display information about export rules	<code>vserver export-policy rule show</code>
Modify an export rule	<code>vserver export-policy rule modify</code>
Delete an export rule	<code>vserver export-policy rule delete</code>



If you have configured multiple identical export rules matching different clients, be sure to keep them in sync when managing export rules.

See the man page for each command for more information.

## Configure the NFS credential cache

### Reasons for modifying the NFS credential cache time-to-live

ONTAP uses a credential cache to store information needed for user authentication for NFS export access to provide faster access and improve performance. You can configure how long information is stored in the credential cache to customize it for your environment.

There are several scenarios when modifying the NFS credential cache time-to-live (TTL) can help resolve issues. You should understand what these scenarios are as well as the consequences of making these modifications.

### Reasons

Consider changing the default TTL under the following circumstances:

Issue	Remedial action
The name servers in your environment are experiencing performance degradation due to a high load of requests from ONTAP.	Increase the TTL for cached positive and negative credentials to reduce the number of requests from ONTAP to name servers.
The name server administrator made changes to allow access to NFS users that were previously denied.	Decrease the TTL for cached negative credentials to reduce the time NFS users have to wait for ONTAP to request fresh credentials from external name servers so they can get access.
The name server administrator made changes to deny access to NFS users that were previously allowed.	Reduce the TTL for cached positive credentials to reduce the time before ONTAP requests fresh credentials from external name servers so the NFS users are now denied access.

### Consequences

You can modify the length of time individually for caching positive and negative credentials. However, you should be aware of both the advantages and disadvantages of doing so.

If you...	The advantage is...	The disadvantage is...
Increase the positive credential cache time	ONTAP sends requests for credentials to name servers less frequently, reducing the load on name servers.	It takes longer to deny access to NFS users that previously were allowed access but are not anymore.
Decrease the positive credential cache time	It takes less time to deny access to NFS users that previously were allowed access but are not anymore.	ONTAP sends requests for credentials to name servers more frequently, increasing the load on name servers.



If you...	The advantage is...	The disadvantage is...
Increase the negative credential cache time	ONTAP sends requests for credentials to name servers less frequently, reducing the load on name servers.	It takes longer to grant access to NFS users that previously were not allowed access but are now.
Decrease the negative credential cache time	It takes less time to grant access to NFS users that previously were not allowed access but are now.	ONTAP sends requests for credentials to name servers more frequently, increasing the load on name servers.

### Configure the time-to-live for cached NFS user credentials

You can configure the length of time that ONTAP stores credentials for NFS users in its internal cache (time-to-live, or TTL) by modifying the NFS server of the storage virtual machine (SVM). This enables you to alleviate certain issues related to high load on name servers or changes in credentials affecting NFS user access.

#### About this task

These parameters are available at the advanced privilege level.

#### Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Perform the desired action:

If you want to modify the TTL for cached...	Use the command...
Positive credentials	<pre>vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live</pre> <p>The TTL is measured in milliseconds. The default is 24 hours (86,400,000 milliseconds). The allowed range for this value is 1 minute (60000 milliseconds) through 7 days (604,800,000 milliseconds).</p>
Negative credentials	<pre>vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live</pre> <p>The TTL is measured in milliseconds. The default is 2 hours (7,200,000 milliseconds). The allowed range for this value is 1 minute (60000 milliseconds) through 7 days (604,800,000 milliseconds).</p>

3. Return to the admin privilege level:

```
set -privilege admin
```

## Manage export policy caches

### Flush export policy caches

ONTAP uses several export policy caches to store information related to export policies for faster access. Flushing export policy caches manually (`vserver export-policy cache flush`) removes potentially outdated information and forces ONTAP to retrieve current information from the appropriate external resources. This can help resolve a variety of issues related to client access to NFS exports.

#### About this task

Export policy cache information might be outdated due to the following reasons:

- A recent change to export policy rules
- A recent change to host name records in name servers
- A recent change to netgroup entries in name servers
- Recovering from a network outage that prevented netgroups from being fully loaded

#### Steps

1. If you do not have name service cache enabled, perform one of the following actions in advance privilege mode:

If you want to flush...	Enter the command...
All export policy caches (except for showmount)	<pre>vserver export-policy cache flush -vserver vserver_name</pre>
The export policy rules access cache	<pre>vserver export-policy cache flush -vserver vserver_name -cache access</pre> You can include the optional <code>-node</code> parameter to specify the node on which you want to flush the access cache.
The host name cache	<pre>vserver export-policy cache flush -vserver vserver_name -cache host</pre>
The netgroup cache	<pre>vserver export-policy cache flush -vserver vserver_name -cache netgroup</pre> Processing of netgroups is resource intensive. You should only flush the netgroup cache if you are trying to resolve a client access issue that is caused by a stale netgroup.
The showmount cache	<pre>vserver export-policy cache flush -vserver vserver_name -cache showmount</pre>

2. If name service cache is enabled, perform one of the following actions:

If you want to flush...	Enter the command...
The export policy rules access cache	<code>vserver export-policy cache flush -vserver vserver_name -cache access</code> You can include the optional <code>-node</code> parameter to specify the node on which you want to flush the access cache.
The host name cache	<code>vserver services name-service cache hosts forward-lookup delete-all</code>
The netgroup cache	<code>vserver services name-service cache netgroups ip-to-netgroup delete-all</code> <code>vserver services name-service cache netgroups members delete-all</code> Processing of netgroups is resource intensive. You should only flush the netgroup cache if you are trying to resolve a client access issue that is caused by a stale netgroup.
The showmount cache	<code>vserver export-policy cache flush -vserver vserver_name -cache showmount</code>

#### Display the export policy netgroup queue and cache

ONTAP uses the netgroup queue when importing and resolving netgroups and it uses the netgroup cache to store the resulting information. When troubleshooting export policy netgroup related issues, you can use the `vserver export-policy netgroup queue show` and `vserver export-policy netgroup cache show` commands to display the status of the netgroup queue and the contents of the netgroup cache.

#### Step

1. Perform one of the following actions:

To display the export policy netgroup...	Enter the command...
Queue	<code>vserver export-policy netgroup queue show</code>
Cache	<code>vserver export-policy netgroup cache show -vserver vserver_name</code>

See the man page for each command for more information.

## Check whether a client IP address is a member of a netgroup

When troubleshooting NFS client access issues related to netgroups, you can use the `vserver export-policy netgroup check-membership` command to help determine whether a client IP is a member of a certain netgroup.

### About this task

Checking netgroup membership enables you to determine whether ONTAP is aware that a client is or is not member of a netgroup. It also lets you know whether the ONTAP netgroup cache is in a transient state while refreshing netgroup information. This information can help you understand why a client might be unexpectedly granted or denied access.

### Step

1. Check the netgroup membership of a client IP address: `vserver export-policy netgroup check-membership -vserver vserver_name -netgroup netgroup_name -client-ip client_ip`

The command can return the following results:

- The client is a member of the netgroup.

This was confirmed through a reverse lookup scan or a netgroup-by-host search.

- The client is a member of the netgroup.

It was found in the ONTAP netgroup cache.

- The client is not a member of the netgroup.

- The membership of the client cannot yet be determined because ONTAP is currently refreshing the netgroup cache.

Until this is done, membership cannot be explicitly ruled in or out. Use the `vserver export-policy netgroup queue show` command to monitor the loading of the netgroup and retry the check after it is finished.

### Example

The following example checks whether a client with the IP address 172.17.16.72 is a member of the netgroup mercury on the SVM vs1:

```
cluster1::> vserver export-policy netgroup check-membership -vserver vs1
-netgroup mercury -client-ip 172.17.16.72
```

### Optimize access cache performance

You can configure several parameters to optimize the access cache and find the right balance between performance and how current the information stored in the access cache is.

### About this task

When you configure the access cache refresh periods, keep the following in mind:

- Higher values mean entries stay longer in the access cache.

The advantage is better performance because ONTAP spends less resources on refreshing access cache entries. The disadvantage is that if export policy rules change and access cache entries become stale as a result, it takes longer to update them. As a result, clients that should get access might get denied, and clients that should get denied might get access.

- Lower values mean ONTAP refreshes access cache entries more often.

The advantage is that entries are more current and clients are more likely to be correctly granted or denied access. The disadvantage is a decrease in performance because ONTAP spends more resources refreshing access cache entries.

## Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Perform the desired action:

To modify the...	Enter...
Refresh period for positive entries	<code>vserver export-policy access-cache config modify-all-vservers -refresh -period-positive timeout_value</code>
Refresh period for negative entries	<code>vserver export-policy access-cache config modify-all-vservers -refresh -period-negative timeout_value</code>
Timeout period for old entries	<code>vserver export-policy access-cache config modify-all-vservers -harvest -timeout timeout_value</code>

3. Verify the new parameter settings:

```
vserver export-policy access-cache config show-all-vservers
```

4. Return to the admin privilege level:

```
set -privilege admin
```

## Manage file locks

### About file locking between protocols

File locking is a method used by client applications to prevent a user from accessing a file previously opened by another user. How ONTAP locks files depends on the protocol of the client.

If the client is an NFS client, locks are advisory; if the client is an SMB client, locks are mandatory.

Because of differences between the NFS and SMB file locks, an NFS client might fail to access a file previously opened by an SMB application.

The following occurs when an NFS client attempts to access a file locked by an SMB application:

- In mixed or NTFS volumes, file manipulation operations such as `rm`, `rmdir`, and `mv` can cause the NFS application to fail.
- NFS read and write operations are denied by SMB deny-read and deny-write open modes, respectively.
- NFS write operations fail when the written range of the file is locked with an exclusive SMB bytelock.

In UNIX security-style volumes, NFS unlink and rename operations ignore SMB lock state and allow access to the file. All other NFS operations on UNIX security-style volumes honor SMB lock state.

### How ONTAP treats read-only bits

The read-only bit is set on a file-by-file basis to reflect whether a file is writable (disabled) or read-only (enabled).

SMB clients that use Windows can set a per-file read-only bit. NFS clients do not set a per-file read-only bit because NFS clients do not have any protocol operations that use a per-file read-only bit.

ONTAP can set a read-only bit on a file when an SMB client that uses Windows creates that file. ONTAP can also set a read-only bit when a file is shared between NFS clients and SMB clients. Some software, when used by NFS clients and SMB clients, requires the read-only bit to be enabled.

For ONTAP to keep the appropriate read and write permissions on a file shared between NFS clients and SMB clients, it treats the read-only bit according to the following rules:

- NFS treats any file with the read-only bit enabled as if it has no write permission bits enabled.
- If an NFS client disables all write permission bits and at least one of those bits had previously been enabled, ONTAP enables the read-only bit for that file.
- If an NFS client enables any write permission bit, ONTAP disables the read-only bit for that file.
- If the read-only bit for a file is enabled and an NFS client attempts to discover permissions for the file, the permission bits for the file are not sent to the NFS client; instead, ONTAP sends the permission bits to the NFS client with the write permission bits masked.
- If the read-only bit for a file is enabled and an SMB client disables the read-only bit, ONTAP enables the owner's write permission bit for the file.
- Files with the read-only bit enabled are writable only by root.



Changes to file permissions take effect immediately on SMB clients, but might not take effect immediately on NFS clients if the NFS client enables attribute caching.

### How ONTAP differs from Windows on handling locks on share path components

Unlike Windows, ONTAP does not lock each component of the path to an open file while the file is open. This behavior also affects SMB share paths.

Because ONTAP does not lock each component of the path, it is possible to rename a path component above the open file or share, which can cause problems for certain applications, or can cause the share path in the

SMB configuration to be invalid. This can cause the share to be inaccessible.

To avoid issues caused by renaming path components, you can apply Windows Access Control List (ACL) security settings that prevent users or applications from renaming critical directories.

Learn more about [How to prevent directories from being renamed while clients are accessing them](#).

### Display information about locks

You can display information about the current file locks, including what types of locks are held and what the lock state is, details about byte-range locks, sharelock modes, delegation locks, and opportunistic locks, and whether locks are opened with durable or persistent handles.

#### About this task

The client IP address cannot be displayed for locks established through NFSv4 or NFSv4.1.

By default, the command displays information about all locks. You can use command parameters to display information about locks for a specific storage virtual machine (SVM) or to filter the command's output by other criteria.

The `vserver locks show` command displays information about four types of locks:

- Byte-range locks, which lock only a portion of a file.
- Share locks, which lock open files.
- Opportunistic locks, which control client-side caching over SMB.
- Delegations, which control client-side caching over NFSv4.x.

By specifying optional parameters, you can determine important information about each lock type. See the man page for the command for more information.

#### Step

1. Display information about locks by using the `vserver locks show` command.

#### Examples

The following example displays summary information for an NFSv4 lock on a file with the path `/vol1/file1`. The sharelock access mode is `write-deny_none`, and the lock was granted with write delegation:

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path                LIF          Protocol  Lock Type  Client
-----
-----
vol1    /vol1/file1                lif1         nfsv4     share-level -
                Sharelock Mode: write-deny_none
                delegation  -
                Delegation Type: write
```

The following example displays detailed oplock and sharelock information about the SMB lock on a file with the path /data2/data2\_2/intro.pptx. A durable handle is granted on the file with a share lock access mode of write-deny\_none to a client with an IP address of 10.3.1.3. A lease oplock is granted with a batch oplock level:

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx
```

```

    Vserver: vs1
      Volume: data2_2
    Logical Interface: lif2
      Object Path: /data2/data2_2/intro.pptx
      Lock UUID: 553cf484-7030-4998-88d3-1125adbbba0b7
    Lock Protocol: cifs
      Lock Type: share-level
  Node Holding Lock State: node3
      Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
      Bytelock is Mandatory: -
      Bytelock is Exclusive: -
      Bytelock is Superlock: -
        Bytelock is Soft: -
          Oplock Level: -
  Shared Lock Access Mode: write-deny_none
    Shared Lock is Soft: false
      Delegation Type: -
        Client Address: 10.3.1.3
          SMB Open Type: durable
            SMB Connect State: connected
  SMB Expiration Time (Secs): -
    SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

```

    Vserver: vs1
      Volume: data2_2
    Logical Interface: lif2
      Object Path: /data2/data2_2/test.pptx
      Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
    Lock Protocol: cifs
      Lock Type: op-lock
  Node Holding Lock State: node3
      Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
      Bytelock is Mandatory: -
      Bytelock is Exclusive: -
```



```

Bytelock is Superlock: -
    Bytelock is Soft: -
        Oplock Level: batch
Shared Lock Access Mode: -
    Shared Lock is Soft: -
        Delegation Type: -
            Client Address: 10.3.1.3
            SMB Open Type: -
                SMB Connect State: connected
SMB Expiration Time (Secs): -
    SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

```

### Breaking locks

When file locks are preventing client access to files, you can display information about currently held locks, and then break specific locks. Examples of scenarios in which you might need to break locks include debugging applications.

#### About this task

The `vserver locks break` command is available only at the advanced privilege level and higher. The man page for the command contains detailed information.

#### Steps

1. To find the information you need to break a lock, use the `vserver locks show` command.

The man page for the command contains detailed information.

2. Set the privilege level to advanced:

```
set -privilege advanced
```

3. Perform one of the following actions:

If you want to break a lock by specifying...	Enter the command...
The SVM name, volume name, LIF name, and file path	<code>vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif</code>
The lock ID	<code>vserver locks break -lockid UUID</code>

4. Return to the admin privilege level:

```
set -privilege admin
```

## How FPolicy first-read and first-write filters work with NFS

NFS clients experience high response time during high traffic of read/write requests when the FPolicy is enabled using an external FPolicy server with read/write operations as monitored events. For NFS clients, the use of first-read and first-write filters in the FPolicy reduces the number of FPolicy notifications and improves performance.

In NFS, the client does I/O on a file by fetching its handle. This handle might remain valid across reboots of the server and the client. Therefore, the client is free to cache the handle and send requests on it without retrieving handles again. In a regular session, lots of reads/write requests are sent to the file server. If notifications are generated for all these requests, it might result in the following issues:

- A larger load due to additional notification processing, and higher response time.
- A large number of notifications being sent to the FPolicy server even though the server unaffected by all of the notifications.

After receiving the first read/write request from a client for a particular file, a cache entry is created and the read/write count is incremented. This request is marked as the first-read/write operation, and an FPolicy event is generated. Before you plan and create your FPolicy filters for an NFS client, you should understand the basics of how FPolicy filters work.

- First-read: Filters the client read requests for first-read.

When this filter is used for NFS events, the `-file-session-io-grouping-count` and `-file-session-io-grouping-duration` settings determine the first-read request for which FPolicy is processed.

- First-write: Filters the client write requests for first-write.

When this filter is used for NFS events, the `-file-session-io-grouping-count` and `-file-session-io-grouping-duration` settings determine the first-write request for which FPolicy is processed.

The following options are added in NFS servers database.

```
file-session-io-grouping-count: Number of I/O Ops on a File to Be Clubbed
and Considered as One Session
for Event Generation
file-session-io-grouping-duration: Duration for Which I/O Ops on a File to
Be Clubbed and Considered as
One Session for Event Generation
```

## Modify the NFSv4.1 server implementation ID

The NFSv4.1 protocol includes a server implementation ID that documents the server domain, name, and date. You can modify the server implementation ID default values. Changing the default values can be useful, for example, when gathering usage statistics or troubleshooting interoperability issues. For more information, see RFC 5661.

### About this task

The default values for the three options are as follows:

Option	Option name	Default value
NFSv4.1 Implementation ID Domain	-v4.1-implementation -domain	netapp.com
NFSv4.1 Implementation ID Name	-v4.1-implementation-name	Cluster version name
NFSv4.1 Implementation ID Date	-v4.1-implementation-date	Cluster version date

## Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Perform one of the following actions:

If you want to modify the NFSv4.1 implementation ID...	Enter the command...
Domain	<pre>vserver nfs modify -v4.1 -implementation-domain domain</pre>
Name	<pre>vserver nfs modify -v4.1 -implementation-name name</pre>
Date	<pre>vserver nfs modify -v4.1 -implementation-date date</pre>

3. Return to the admin privilege level:

```
set -privilege admin
```

## Manage NFSv4 ACLs

### Benefits of enabling NFSv4 ACLs

There are many benefits to enabling NFSv4 ACLs.

The benefits of enabling NFSv4 ACLs include the following:

- Finer-grained control of user access for files and directories
- Better NFS security
- Improved interoperability with CIFS
- Removal of the NFS limitation of 16 groups per user

## How NFSv4 ACLs work

A client using NFSv4 ACLs can set and view ACLs on files and directories on the system. When a new file or subdirectory is created in a directory that has an ACL, the new file or subdirectory inherits all ACL Entries (ACEs) in the ACL that have been tagged with the appropriate inheritance flags.

When a file or directory is created as the result of an NFSv4 request, the ACL on the resulting file or directory depends on whether the file creation request includes an ACL or only standard UNIX file access permissions, and whether the parent directory has an ACL:

- If the request includes an ACL, that ACL is used.
- If the request includes only standard UNIX file access permissions but the parent directory has an ACL, the ACEs in the parent directory's ACL are inherited by the new file or directory as long as the ACEs have been tagged with the appropriate inheritance flags.



A parent ACL is inherited even if `-v4.0-acl` is set to `off`.

- If the request includes only standard UNIX file access permissions and the parent directory does not have an ACL, the client file mode is used to set standard UNIX file access permissions.
- If the request includes only standard UNIX file access permissions and the parent directory has a non-inheritable ACL, the new object is created only with mode bits.



If the `-chown-mode` parameter has been set to `restricted` with commands in the `vserver nfs` or `vserver export-policy` rule families, file ownership can be changed by the superuser only, even if the on-disk permissions set with NFSv4 ACLs allow a non-root user to change the file ownership. For more information, see the relevant man pages.

## Enable or disable modification of NFSv4 ACLs

When ONTAP receives a `chmod` command for a file or directory with an ACL, by default the ACL is retained and modified to reflect the mode bit change. You can disable the `-v4-acl-preserve` parameter to change the behavior if you want the ACL to be dropped instead.

### About this task

When using unified security style, this parameter also specifies whether NTFS file permissions are preserved or dropped when a client sends a `chmod`, `chgroup`, or `chown` command for a file or directory.

The default for this parameter is enabled.

### Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Perform one of the following actions:

If you want to...	Enter the following command...
-------------------	--------------------------------

Enable retention and modification of existing NFSv4 ACLs (default)	<code>vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled</code>
Disable retention and drop NFSv4 ACLs when changing mode bits	<code>vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled</code>

3. Return to the admin privilege level:

```
set -privilege admin
```

#### How ONTAP uses NFSv4 ACLs to determine whether it can delete a file

To determine whether it can delete a file, ONTAP uses a combination of the file's DELETE bit, and the containing directory's DELETE\_CHILD bit. For more information, see the NFS 4.1 RFC 5661.

#### Enable or disable NFSv4 ACLs

To enable or disable NFSv4 ACLs, you can modify the `-v4.0-acl` and `-v4.1-acl` options. These options are disabled by default.

#### About this task

The `-v4.0-acl` or `-v4.1-acl` option controls the setting and viewing of NFSv4 ACLs; it does not control enforcement of these ACLs for access checking.

#### Step

1. Perform one of the following actions:

If you want to...	Then...
Enable NFSv4.0 ACLs	Enter the following command:  <code>vserver nfs modify -vserver vserver_name -v4.0-acl enabled</code>
Disable NFSv4.0 ACLs	Enter the following command:  <code>vserver nfs modify -vserver vserver_name -v4.0-acl disabled</code>
Enable NFSv4.1 ACLs	Enter the following command:  <code>vserver nfs modify -vserver vserver_name -v4.1-acl enabled</code>

Disable NFSv4.1 ACLs

Enter the following command:

```
vserver nfs modify -vserver vserver_name -v4.1-acl disabled
```

### Modify the maximum ACE limit for NFSv4 ACLs

You can modify the maximum number of allowed ACEs for each NFSv4 ACL by modifying the parameter `-v4-acl-max-aces`. By default, the limit is set to 400 ACEs for each ACL. Increasing this limit can help ensure successful migration of data with ACLs containing over 400 ACEs to storage systems running ONTAP.

#### About this task

Increasing this limit might impact performance for clients accessing files with NFSv4 ACLs.

#### Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Modify the maximum ACE limit for NFSv4 ACLs:

```
vserver nfs modify -v4-acl-max-aces max_ace_limit
```

The valid range of

`max_ace_limit` is 192 to 1024.

3. Return to the admin privilege level:

```
set -privilege admin
```

### Manage NFSv4 file delegations

#### Enable or disable NFSv4 read file delegations

To enable or disable NFSv4 read file delegations, you can modify the `-v4.0-read-delegation` or `-v4.1-read-delegation` option. By enabling read file delegations, you can eliminate much of the message overhead associated with the opening and closing of files.

#### About this task

By default, read file delegations are disabled.

The disadvantage of enabling read file delegations is that the server and its clients must recover delegations after the server reboots or restarts, a client reboots or restarts, or a network partition occurs.

#### Step

1. Perform one of the following actions:

If you want to...	Then...
Enable NFSv4 read file delegations	Enter the following command:  <pre>vserver nfs modify -vserver vserver_name -v4.0 -read-delegation enabled</pre>
Enable NFSv4.1 read file delegations	Enter the following command:  <pre>+ vserver nfs modify -vserver vserver_name -v4.1 -read-delegation enabled</pre>
Disable NFSv4 read file delegations	Enter the following command:  <pre>vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled</pre>
Disable NFSv4.1 read file delegations	Enter the following command:  <pre>vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled</pre>

## Result

The file delegation options take effect as soon as they are changed. There is no need to reboot or restart NFS.

### Enable or disable NFSv4 write file delegations

To enable or disable write file delegations, you can modify the `-v4.0-write-delegation` or `-v4.1-write-delegation` option. By enabling write file delegations, you can eliminate much of the message overhead associated with file and record locking in addition to opening and closing of files.

### About this task

By default, write file delegations are disabled.

The disadvantage of enabling write file delegations is that the server and its clients must perform additional tasks to recover delegations after the server reboots or restarts, a client reboots or restarts, or a network partition occurs.

### Step

1. Perform one of the following actions:

If you want to...	Then...
Enable NFSv4 write file delegations	Enter the following command:  <pre>vserver nfs modify -vserver vserver_name -v4.0 -write-delegation enabled</pre>

If you want to...	Then...
Enable NFSv4.1 write file delegations	Enter the following command: <code>vserver nfs modify -vserver vserver_name -v4.1 -write-delegation enabled</code>
Disable NFSv4 write file delegations	Enter the following command: <code>vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled</code>
Disable NFSv4.1 write file delegations	Enter the following command: <code>vserver nfs modify -vserver vserver_name -v4.1 -write-delegation disabled</code>

## Result

The file delegation options take effect as soon as they are changed. There is no need to reboot or restart NFS.

## Configure NFSv4 file and record locking

### About NFSv4 file and record locking

For NFSv4 clients, ONTAP supports the NFSv4 file-locking mechanism, maintaining the state of all file locks under a lease-based model.

[NetApp Technical Report 3580: NFSv4 Enhancements and Best Practices Guide Data ONTAP Implementation](#)

### Specify the NFSv4 locking lease period

To specify the NFSv4 locking lease period (that is, the time period in which ONTAP irrevocably grants a lock to a client), you can modify the `-v4-lease-seconds` option. Shorter lease periods speed up server recovery while longer lease periods are beneficial for servers handling a very large amount of clients.

### About this task

By default, this option is set to 30. The minimum value for this option is 10. The maximum value for this option is the locking grace period, which you can set with the `locking.lease_seconds` option.

### Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Enter the following command:

```
vserver nfs modify -vserver vserver_name -v4-lease-seconds number_of_seconds
```

3. Return to the admin privilege level:

```
set -privilege admin
```



## Specify the NFSv4 locking grace period

To specify the NFSv4 locking grace period (that is, the time period in which clients attempt to reclaim their locking state from ONTAP during server recovery), you can modify the `-v4-grace-seconds` option.

### About this task

By default, this option is set to 45.

### Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Enter the following command:

```
vserver nfs modify -vserver vserver_name -v4-grace-seconds number_of_seconds
```

3. Return to the admin privilege level:

```
set -privilege admin
```

## How NFSv4 referrals work

When you enable NFSv4 referrals, ONTAP provides “intra-SVM” referrals to NFSv4 clients. Intra-SVM referral is when a cluster node receiving the NFSv4 request refers the NFSv4 client to another logical interface (LIF) on the storage virtual machine (SVM).

The NFSv4 client should access the path that received the referral at the target LIF from that point onward. The original cluster node provides such a referral when it determines that there exists a LIF in the SVM that is resident on the cluster node on which the data volume resides, thereby enabling the clients faster access to the data and avoiding extra cluster communication.

## Enable or disable NFSv4 referrals

You can enable NFSv4 referrals on storage virtual machines (SVMs) by enabling the options `-v4-fsid-change` and `-v4.0-referrals` or `-v4.1-referrals`. Enabling NFSV4 referrals can result in faster data access for NFSv4 clients that support this feature.

### What you'll need

If you want to enable NFS referrals, you must first disable parallel NFS. You cannot enable both at the same time.

### Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Perform one of the following actions:

If you want to...	Enter the command...
Enable NFSv4 referrals	<code>vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.0-referrals enabled</code>
Disable NFSv4 referrals	<code>vserver nfs modify -vserver vserver_name -v4.0 -referrals disabled</code>
Enable NFSv4.1 referrals	<code>vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.1-referrals enabled</code>
Disable NFSv4.1 referrals	<code>vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled</code>

3. Return to the admin privilege level:

```
set -privilege admin
```

## Display NFS statistics

You can display NFS statistics for storage virtual machines (SVMs) on the storage system to monitor performance and diagnose issues.

### Steps

1. Use the `statistics catalog object show` command to identify the NFS objects from which you can view data.

```
statistics catalog object show -object nfs*
```

2. Use the `statistics start` and optional `statistics stop` commands to collect a data sample from one or more objects.

3. Use the `statistics show` command to view the sample data.

### Example: Monitoring NFSv3 performance

The following example shows performance data for the NFSv3 protocol.

The following command starts data collection for a new sample:

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

The following command shows data from the sample by specifying counters that show the number of successful read and write requests versus the total number of read and write requests:

```
vs1::> statistics show -sample-id nfs_sample -counter
read_total|write_total|read_success|write_success
```

```
Object: nfsv3
Instance: vs1
Start-time: 2/11/2013 15:38:29
End-time: 2/11/2013 15:38:41
Cluster: cluster1
```

Counter	Value
read_success	40042
read_total	40042
write_success	1492052
write_total	1492052

## Related information

[Performance monitoring setup](#)

## Display DNS statistics

You can display DNS statistics for storage virtual machines (SVMs) on the storage system to monitor performance and diagnose issues.

### Steps

1. Use the `statistics catalog object show` command to identify the DNS objects from which you can view data.

```
statistics catalog object show -object external_service_op*
```

2. Use the `statistics start` and `statistics stop` commands to collect a data sample from one or more objects.
3. Use the `statistics show` command to view the sample data.

### Monitoring DNS statistics

The following examples show performance data for DNS queries. The following commands start data collection for a new sample:

```
vs1::*> statistics start -object external_service_op -sample-id
dns_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
dns_sample2
```

The following command displays data from the sample by specifying counters that display the number of DNS queries sent versus the number of DNS queries received, failed, or timed out:

```
vs1::*> statistics show -sample-id dns_sample1 -counter
num_requests_sent|num_responses_received|num_successful_responses|num_time
outs|num_request_failures|num_not_found_responses
```

```
Object: external_service_op
Instance: vs1:DNS:Query:10.72.219.109
Start-time: 3/8/2016 11:15:21
End-time: 3/8/2016 11:16:52
Elapsed-time: 91s
Scope: vs1
```

Counter	Value
num_not_found_responses	0
num_request_failures	0
num_requests_sent	1
num_responses_received	1
num_successful_responses	1
num_timeouts	0

6 entries were displayed.

The following command displays data from the sample by specifying counters that display the number of times a specific error was received for a DNS query on the particular server:

```
vs1::*> statistics show -sample-id dns_sample2 -counter
server_ip_address|error_string|count
```

```
Object: external_service_op_error
Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109
Start-time: 3/8/2016 11:23:21
End-time: 3/8/2016 11:24:25
Elapsed-time: 64s
Scope: vs1
```

Counter	Value
count	1
error_string	NXDOMAIN
server_ip_address	10.72.219.109

3 entries were displayed.

## Related information

[Performance monitoring setup](#)

## Display NIS statistics

You can display NIS statistics for storage virtual machines (SVMs) on the storage system to monitor performance and diagnose issues.

### Steps

1. Use the `statistics catalog object show` command to identify the NIS objects from which you can view data.

```
statistics catalog object show -object external_service_op*
```

2. Use the `statistics start` and `statistics stop` commands to collect a data sample from one or more objects.
3. Use the `statistics show` command to view the sample data.

### Monitoring NIS statistics

The following examples display performance data for NIS queries. The following commands start data collection for a new sample:

```
vs1::*> statistics start -object external_service_op -sample-id  
nis_sample1  
vs1::*> statistics start -object external_service_op_error -sample-id  
nis_sample2
```

The following command displays data from the sample by specifying counters that show the number of NIS queries sent versus the number of NIS queries received, failed, or timed out:

```
vs1::*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses
```

```
Object: external_service_op
Instance: vs1:NIS:Query:10.227.13.221
Start-time: 3/8/2016 11:27:39
End-time: 3/8/2016 11:27:56
Elapsed-time: 17s
Scope: vs1
```

Counter	Value
num_not_found_responses	0
num_request_failures	1
num_requests_sent	2
num_responses_received	1
num_successful_responses	1
num_timeouts	0

6 entries were displayed.

The following command displays data from the sample by specifying counters that show the number of times a specific error was received for a NIS query on the particular server:

```
vs1::*> statistics show -sample-id nis_sample2 -counter
server_ip_address|error_string|count
```

```
Object: external_service_op_error
Instance: vs1:NIS:Query:YP_NOTFOUND:10.227.13.221
Start-time: 3/8/2016 11:33:05
End-time: 3/8/2016 11:33:10
Elapsed-time: 5s
Scope: vs1
```

Counter	Value
count	1
error_string	YP_NOTFOUND
server_ip_address	10.227.13.221

3 entries were displayed.

## Related information

[Performance monitoring setup](#)

## Support for VMware vStorage over NFS

ONTAP supports certain VMware vStorage APIs for Array Integration (VAAI) features in an NFS environment.

### Supported features

The following features are supported:

- Copy offload

Enables an ESXi host to copy virtual machines or virtual machine disks (VMDKs) directly between the source and destination data store location without involving the host. This conserves ESXi host CPU cycles and network bandwidth. Copy offload preserves space efficiency if the source volume is sparse.

- Space reservation

Guarantees storage space for a VMDK file by reserving space for it.

### Limitations

VMware vStorage over NFS has the following limitations:

- Copy offload operations can fail in the following scenarios:
  - While running wafliron on the source or destination volume because it temporarily takes the volume offline
  - While moving either the source or destination volume
  - While moving either the source or destination LIF
  - While performing takeover or giveback operations
  - While performing switchover or switchback operations
- Server-side copy can fail due to file handle format differences in the following scenario:

You attempt to copy data from SVMs that have currently or had previously exported qtrees to SVMs that have never had exported qtrees. To work around this limitation, you can export at least one qtree on the destination SVM.

### Related information

[What VAAI offloaded operations are supported by Data ONTAP?](#)

### Enable or disable VMware vStorage over NFS

You can enable or disable support for VMware vStorage over NFS on storage virtual machines (SVMs) by using the `vserver nfs modify` command.

### About this task

By default, support for VMware vStorage over NFS is disabled.

### Steps

1. Display the current vStorage support status for SVMs:

```
vserver nfs show -vserver vserver_name -instance
```

2. Perform one of the following actions:

If you want to...	Enter the following command...
Enable VMware vStorage support	<pre>vserver nfs modify -vserver vserver_name -vstorage enabled</pre>
Disable VMware vStorage support	<pre>vserver nfs modify -vserver vserver_name -vstorage disabled</pre>

### After you finish

You must install the NFS Plug-in for VMware VAAI before you can use this functionality. For more information, see *Installing the NetApp NFS Plug-in for VMware VAAI*.

### Related information

[NetApp Documentation: NetApp NFS Plug-in for VMware VAAI](#)

### Enable or disable rquota support

ONTAP supports the remote quota protocol version 1 (rquota v1). The rquota protocol enables NFS clients to obtain quota information for users from a remote machine. You can enable rquota on storage virtual machines (SVMs) by using the `vserver nfs modify` command.

### About this task

By default, rquota is disabled.

### Step

1. Perform one of the following actions:

If you want to...	Enter the following command...
Enable rquota support for SVMs	<pre>vserver nfs modify -vserver vserver_name -rquota enable</pre>
Disable rquota support for SVMs	<pre>vserver nfs modify -vserver vserver_name -rquota disable</pre>

For more information about quotas, see [Logical storage management](#).

### NFSv3 and NFSv4 performance improvement by modifying the TCP transfer size

You can improve the performance of NFSv3 and NFSv4 clients connecting to storage systems over a high-latency network by modifying the TCP maximum transfer size.

When clients access storage systems over a high-latency network, such as a wide area network (WAN) or



metro area network (MAN) with a latency over 10 milliseconds, you might be able to improve the connection performance by modifying the TCP maximum transfer size. Clients accessing storage systems in a low-latency network, such as a local area network (LAN), can expect little to no benefit from modifying these parameters. If the throughput improvement does not outweigh the latency impact, you should not use these parameters.

To determine whether your storage environment would benefit from modifying these parameters, you should first conduct a comprehensive performance evaluation of a poorly performing NFS client. Review whether the low performance is because of excessive round trip latency and small request on the client. Under these conditions, the client and server cannot fully use the available bandwidth because they spend the majority of their duty cycles waiting for small requests and responses to be transmitted over the connection.

By increasing the NFSv3 and NFSv4 request size, the client and server can use the available bandwidth more effectively to move more data per unit time; therefore, increasing the overall efficiency of the connection.

Keep in mind that the configuration between the storage system and the client might vary. The storage system and the client supports maximum size of 1 MB for transfer operations. However, if you configure the storage system to support 1 MB maximum transfer size but the client only supports 64 KB, then the mount transfer size is limited to 64 KB or less.

Before modifying these parameters, you must be aware that it results in additional memory consumption on the storage system for the period of time necessary to assemble and transmit a large response. The more high-latency connections to the storage system, the higher the additional memory consumption. Storage systems with high memory capacity might experience very little effect from this change. Storage systems with low memory capacity might experience noticeable performance degradation.

The successful use of these parameter relies on the ability to retrieve data from multiple nodes of a cluster. The inherent latency of the cluster network might increase the overall latency of the response. Overall latency tends to increase when using these parameters. As a result, latency sensitive workloads might show negative impact.

### Modify the NFSv3 and NFSv4 TCP maximum transfer size

You can modify the `-tcp-max-xfer-size` option to configure maximum transfer sizes for all TCP connections using the NFSv3 and NFSv4.x protocols.

#### About this task

You can modify these options individually for each storage virtual machine (SVM).

Beginning with ONTAP 9, the `v3-tcp-max-read-size` and `v3-tcp-max-write-size` options are obsolete. You must use the `-tcp-max-xfer-size` option instead.

#### Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Perform one of the following actions:

If you want to...	Enter the command...
Modify the NFSv3 or NFSv4 TCP maximum transfer size	<pre>vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size</pre>

Option	Range	Default
<code>-tcp-max-xfer-size</code>	8192 to 1048576 bytes	65536 bytes



The maximum transfer size that you enter must be a multiple of 4 KB (4096 bytes). Requests that are not properly aligned negatively affect performance.

- Use the `vserver nfs show -fields tcp-max-xfer-size` command to verify the changes.
- If any clients use static mounts, unmount and remount for the new parameter size to take effect.

### Example

The following command sets the NFSv3 and NFSv4.x TCP maximum transfer size to 1048576 bytes on the SVM named vs1:

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

### Configure the number of group IDs allowed for NFS users

By default, ONTAP supports up to 32 group IDs when handling NFS user credentials using Kerberos (RPCSEC\_GSS) authentication. When using AUTH\_SYS authentication, the default maximum number of group IDs is 16, as defined in RFC 5531. You can increase the maximum up to 1,024 if you have users who are members of more than the default number of groups.

#### About this task

If a user has more than the default number of group IDs in their credentials, the remaining group IDs are truncated and the user might receive errors when attempting to access files from the storage system. You should set the maximum number of groups, per SVM, to a number that represents the maximum groups in your environment.

The following table shows the two parameters of the `vserver nfs modify` command that determine the maximum number of group IDs in three sample configurations:

Parameters	Settings	Resulting group IDs limit
<code>-extended-groups-limit</code>	32	RPCSEC_GSS: 32
<code>-auth-sys-extended-groups</code>	disabled	AUTH_SYS: 16
	These are the default settings.	
<code>-extended-groups-limit</code>	256	RPCSEC_GSS: 256
<code>-auth-sys-extended-groups</code>	disabled	AUTH_SYS: 16

<code>-extended-groups-limit</code>	512	RPCSEC_GSS: 512
<code>-auth-sys-extended-groups</code>	enabled	AUTH_SYS: 512



Some older NFS clients might not be compatible with AUTH\_SYS extended groups.

### Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Perform the desired action:

If you want to set the maximum number of allowed auxiliary groups...	Enter the command...
Only for RPCSEC_GSS and leave AUTH_SYS set to the default value of 16	<code>vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups disabled</code>
For both RPCSEC_GSS and AUTH_SYS	<code>vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups enabled</code>

3. Verify the `-extended-groups-limit` value and verify whether AUTH\_SYS is using extended groups:

```
vserver nfs show -vserver vserver_name -fields auth-sys-extended-groups,extended-groups-limit
```

4. Return to the admin privilege level:

```
set -privilege admin
```

### Example

The following example enables extended groups for AUTH\_SYS authentication and sets the maximum number of extended groups to 512 for both AUTH\_SYS and RPCSEC\_GSS authentication. These changes are made only for clients who access the SVM named vs1:

```

vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
        them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -auth-sys-extended-groups enabled
-extended-groups-limit 512

vs1::*> vserver nfs show -vserver vs1 -fields auth-sys-extended-
groups,extended-groups-limit
vserver auth-sys-extended-groups extended-groups-limit
-----
vs1      enabled                    512

vs1::*> set -privilege admin

```

### Control root user access to NTFS security-style data

You can configure ONTAP to allow NFS clients access to NTFS security-style data and NTFS clients to access NFS security-style data. When using NTFS security style on an NFS data store, you must decide how to treat access by the root user and configure the storage virtual machine (SVM) accordingly.

#### About this task

When a root user accesses NTFS security-style data, you have two options:

- Map the root user to a Windows user like any other NFS user and manage access according to NTFS ACLs.
- Ignore NTFS ACLs and provide full access to root.

#### Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Perform the desired action:

If you want the root user to...	Enter the command...
Be mapped to a Windows user	<code>vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled</code>
Bypass the NT ACL check	<code>vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled</code>

By default, this parameter is disabled.

If this parameter is enabled but there is no name mapping for the root user, ONTAP uses a default SMB administrator credential for auditing.

3. Return to the admin privilege level:

```
set -privilege admin
```

## Appendix: Supported NFS versions and clients

### Appendix: Supported NFS versions and clients

Before you can use NFS in your network, you need to know which NFS versions and clients ONTAP supports.

This table notes when major and minor NFS protocol versions are supported by default in ONTAP. Support by default does not indicate that this is the earliest version of ONTAP supporting that NFS protocol.

Version	Enabled by default
NFSv3	Yes
NFSv4.0	Yes, beginning with ONTAP 9.9.1
NFSv4.1	Yes, beginning with ONTAP 9.9.1
NFSv4.2	Yes, beginning with ONTAP 9.9.1
pNFS	No

For the latest information about which NFS clients ONTAP supports, see the Interoperability Matrix.

[NetApp Interoperability Matrix Tool](#)

### NFSv4.0 functionality supported by ONTAP

ONTAP supports all the mandatory functionality in NFSv4.0 except the SPKM3 and LIPKEY security mechanisms.

The following NFSV4 functionality is supported:

- **COMPOUND**

Allows a client to request multiple file operations in a single remote procedure call (RPC) request.

- **File delegation**

Allows the server to delegate file control to some types of clients for read and write access.

- **Pseudo-fs**

Used by NFSv4 servers to determine mount points on the storage system. There is no mount protocol in

NFSv4.

- **Locking**

Lease-based. There are no separate Network Lock Manager (NLM) or Network Status Monitor (NSM) protocols in NFSv4.

For more information about the NFSv4.0 protocol, see RFC 3530.

### Limitations of ONTAP support for NFSv4

You should be aware of several limitations of ONTAP support for NFSv4.

- The delegation feature is not supported by every client type.
- In ONTAP 9.4 and earlier releases, names with non-ASCII characters on volumes other than UTF8 volumes are rejected by the storage system.

In ONTAP 9.5 and later releases, volumes created with the utf8mb4 language setting and mounted using NFS v4 are no longer subject to this restriction.

- All file handles are persistent; the server does not give volatile file handles.
- Migration and replication are not supported.
- NFSv4 clients are not supported with read-only load-sharing mirrors.

ONTAP routes NFSv4 clients to the source of the load-sharing mirror for direct read and write access.

- Named attributes are not supported.
- All recommended attributes are supported, except for the following:

- archive
- hidden
- homogeneous
- mimetype
- quota\_avail\_hard
- quota\_avail\_soft
- quota\_used
- system
- time\_backup



Although it does not support the `quota*` attributes, ONTAP does support user and group quotas through the RQUOTA side band protocol.

### ONTAP support for NFSv4.1

Beginning with ONTAP 9.8, `nconnect` functionality is available by default when NFSv4.1 is enabled.

Earlier NFS client implementations use only a single TCP connection with a mount. In ONTAP, a single TCP connection can become a bottleneck with increasing IOPS. However, an nconnect-enabled client can have multiple TCP connections (up to 16) associated with a single NFS mount. Such an NFS client multiplexes file operations onto multiple TCP connections in a round-robin fashion and thus obtains higher throughput from the available network bandwidth. Nconnect is recommended for NFSv3 and NFSv4.1 mounts only.

See your NFS client documentation to confirm whether nconnect is supported in your client version.

NFSv4.1 is enabled by default in ONTAP 9.9.1 and later. In earlier releases, you can enable it by specifying the `-v4.1` option and setting it to `enabled` when creating an NFS server on the storage virtual machine (SVM).

ONTAP does not support NFSv4.1 directory and file level delegations.

## ONTAP support for NFSv4.2

Beginning with ONTAP 9.8, the NFSv4.2 protocol is supported to allow access for NFSv4.2 clients.

NFSv4.2 is enabled by default in ONTAP 9.9.1 and later. In ONTAP 9.8, you can enable v4.2 by specifying the `-v4.1` option and setting it to `enabled` when creating an NFS server on the storage virtual machine (SVM). Enabling NFSv4.1 also enables clients to use the NFSv4.1 features while mounted as v4.2.

The following NFSv4.2 optional features are supported:

- Beginning with ONTAP 9.9.1, Mandatory Access Control (MAC) labelled NFS is supported when NFSv4.2 is enabled.
- Additional NFSv4.2 optional features will be added in a later ONTAP release.

### Enable NFS v4.2 security labels

Beginning with ONTAP 9.9.1, NFS security labels can be enabled. They are disabled by default.

With NFS v4.2 security labels, ONTAP NFS servers are Mandatory Access Control (MAC) aware, storing and retrieving `sec_label` attributes sent by clients.

For more information, see [RFC7240](#)



NFS v4.2 security labels are not currently supported for NDMP dump operations. If security labels are encountered on files or directories, the dump fails.

### Steps

1. Change the privilege setting to advanced:

```
set -privilege advanced
```

2. Enable security labels:

```
vserver nfs modify -vserver svm_name -v4.2-seclabel enabled
```

## ONTAP support for parallel NFS

ONTAP supports parallel NFS (pNFS). The pNFS protocol offers performance

improvements by giving clients direct access to the data of a set of files distributed across multiple nodes of a cluster. It helps clients locate the optimal path to a volume.

### **Use of hard mounts**

When troubleshooting mounting problems, you need to be sure that you are using the correct mount type. NFS supports two mount types: soft mounts and hard mounts. You should use only hard mounts for reliability reasons.

You should not use soft mounts, especially when there is a possibility of frequent NFS timeouts. Race conditions can occur as a result of these timeouts, which can lead to data corruption.

## **Appendix: NFS and SMB file and directory naming dependencies**

### **Appendix: NFS and SMB file and directory naming dependencies**

File and directory naming conventions depend on both the network clients' operating systems and the file-sharing protocols, in addition to language settings on the ONTAP cluster and clients.

The operating system and the file-sharing protocols determine the following:

- Characters a file name can use
- Case-sensitivity of a file name

ONTAP supports multi-byte characters in file, directory, and qtree names, depending on the ONTAP release.

### **Characters a file or directory name can use**

If you are accessing a file or directory from clients with different operating systems, you should use characters that are valid in both operating systems.

For example, if you use UNIX to create a file or directory, do not use a colon (:) in the name because the colon is not allowed in MS-DOS file or directory names. Because restrictions on valid characters vary from one operating system to another, see the documentation for your client operating system for more information about prohibited characters.

### **Case-sensitivity of file and directory names in a multiprotocol environment**

File and directory names are case-sensitive for NFS clients and case-insensitive but case-preserving for SMB clients. You must understand what the implications are in a multiprotocol environment and the actions you might need to take when specifying the path while creating SMB shares and when accessing data within the shares.

If an SMB client creates a directory named `testdir`, both SMB and NFS clients display the file name as `testdir`. However, if an SMB user later tries to create a directory name `TESTDIR`, the name is not allowed because, to the SMB client, that name currently exists. If an NFS user later creates a directory named `TESTDIR`, NFS and SMB clients display the directory name differently, as follows:

- On NFS clients, you see both directory names as they were created, for example `testdir` and `TESTDIR`, because directory names are case-sensitive.



- SMB clients use the 8.3 names to distinguish between the two directories. One directory has the base file name. Additional directories are assigned an 8.3 file name.
  - On SMB clients, you see `testdir` and `TESTDI~1`.
  - ONTAP creates the `TESTDI~1` directory name to differentiate the two directories.

In this case, you must use the 8.3 name when specifying a share path while creating or modifying a share on a storage virtual machine (SVM).

Similarly for files, if an SMB client creates `test.txt`, both SMB and NFS clients display the file name as `test.txt`. However, if an SMB user later tries to create `Test.txt`, the name is not allowed because, to the SMB client, that name currently exists. If an NFS user later creates a file named `Test.txt`, NFS and SMB clients display the file name differently, as follows:

- On NFS clients, you see both file names as they were created, `test.txt` and `Test.txt`, because file names are case-sensitive.
- SMB clients use the 8.3 names to distinguish between the two files. One file has the base file name. Additional files are assigned an 8.3 file name.
  - On SMB clients, you see `test.txt` and `TEST~1.TXT`.
  - ONTAP creates the `TEST~1.TXT` file name to differentiate the two files.



If you have enabled or modified character mapping using the Vserver CIFS character-mapping commands, a normally case-insensitive Windows lookup becomes case-sensitive.

### How ONTAP creates file and directory names

ONTAP creates and maintains two names for files or directories in any directory that has access from an SMB client: the original long name and a name in 8.3 format.

For file or directory names that exceed the eight character name or the three character extension limit (for files), ONTAP generates an 8.3-format name as follows:

- It truncates the original file or directory name to six characters, if the name exceeds six characters.
- It appends a tilde (~) and a number, one through five, to file or directory names that are no longer unique after being truncated.

If it runs out of numbers because there are more than five similar names, it creates a unique name that bears no relation to the original name.

- In the case of files, it truncates the file name extension to three characters.

For example, if an NFS client creates a file named `specifications.html`, the 8.3 format file name created by ONTAP is `specif~1.htm`. If this name already exists, ONTAP uses a different number at the end of the file name. For example, if an NFS client then creates another file named `specifications_new.html`, the 8.3 format of `specifications_new.html` is `specif~2.htm`.

### How ONTAP handles multi-byte file, directory, and qtree names

Beginning with ONTAP 9.5, support for 4-byte UTF-8 encoded names enables the creation and display of file, directory, and tree names that include Unicode supplementary

characters outside the Basic Multilingual Plane (BMP). In earlier releases, these supplementary characters did not display correctly in multiprotocol environments.

To enable support for 4-byte UTF-8 encoded names, a new *utf8mb4* language code is available for the `vserver` and `volume` command families.

- You must create a new volume in one of the following ways:
- Setting the volume `-language` option explicitly:

```
volume create -language utf8mb4 {...}
```

- Inheriting the volume `-language` option from an SVM that has been created with or modified for the option:

```
vserver [create|modify] -language utf8mb4 {...}``volume create {...}
```

- You cannot modify existing volumes for *utf8mb4* support; you must create a new *utf8mb4*-ready volume, and then migrate the data using client-based copy tools.

You can update SVMs for *utf8mb4* support, but existing volumes retain their original language codes.



LUN names with 4-byte UTF-8 characters are not currently supported.

- Unicode character data is typically represented in Windows file systems applications using the 16-bit Unicode Transformation Format (UTF-16) and in NFS file systems using the 8-bit Unicode Transformation Format (UTF-8).

In releases prior to ONTAP 9.5, names including UTF-16 supplementary characters that were created by Windows clients were correctly displayed to other Windows clients but were not translated correctly to UTF-8 for NFS clients. Similarly, names with UTF-8 supplementary characters by created NFS clients were not translated correctly to UTF-16 for Windows clients.

- When you create file names on systems running ONTAP 9.4 or earlier that contain valid or invalid supplementary characters, ONTAP rejects the file name and returns an invalid file name error.

To avoid this issue, use only BMP characters in file names and avoid using supplementary characters, or upgrade to ONTAP 9.5 or later.

Unicode characters are allowed in `qtree` names.

- You can use either the `volume qtree` command family or System Manager to set or modify `qtree` names.
- `qtree` names can include multi-byte characters in Unicode format, such as Japanese and Chinese characters.
- In releases before ONTAP 9.5, only BMP characters (that is, those that could be represented in 3 bytes) were supported.



In releases before ONTAP 9.5, the junction-path of the `qtree`'s parent volume can contain `qtree` and directory names with Unicode characters. The `volume show` command displays these names correctly when the parent volume has a UTF-8 language setting. However, if the parent volume language is not one of the UTF-8 language settings, some parts of the junction-path are displayed using a numeric NFS alternate name.

- In 9.5 and later releases, 4-byte characters are supported in qtree names, provided that the qtree is in a volume enabled for utf8mb4.

## Configure character mapping for SMB file name translation on volumes

NFS clients can create file names that contain characters that are not valid for SMB clients and certain Windows applications. You can configure character mapping for file name translation on volumes to allow SMB clients to access files with NFS names that would otherwise not be valid.

### About this task

When files created by NFS clients are accessed by SMB clients, ONTAP looks at the name of the file. If the name is not a valid SMB file name (for example, if it has an embedded colon ":" character), ONTAP returns the 8.3 file name that is maintained for each file. However, this causes problems for applications that encode important information into long file names.

Therefore, if you are sharing a file between clients on different operating systems, you should use characters in the file names that are valid in both operating systems.

However, if you have NFS clients that create file names containing characters that are not valid file names for SMB clients, you can define a map that converts the invalid NFS characters into Unicode characters that both SMB and certain Windows applications accept. For example, this functionality supports the CATIA MCAD and Mathematica applications as well as other applications that have this requirement.

You can configure character mapping on a volume-by-volume basis.

You must keep the following in mind when configuring character mapping on a volume:

- Character mapping is not applied across junction points.

You must explicitly configure character mapping for each junction volume.

- You must make sure that the Unicode characters that are used to represent invalid or illegal characters are characters that do not normally appear in file names; otherwise, unwanted mappings occur.

For example, if you try to map a colon (:) to a hyphen (-) but the hyphen (-) was used in the file name correctly, a Windows client trying to access a file named "a-b" would have its request mapped to the NFS name of "a:b" (not the desired outcome).

- After applying character mapping, if the mapping still contains an invalid Windows character, ONTAP falls back to Windows 8.3 file names.
- In FPolicy notifications, NAS audit logs, and security trace messages, the mapped file names are shown.
- When a SnapMirror relation of type DP is created, the source volume's character mapping is not replicated on the destination DP volume.
- Case sensitivity: Because the mapped Windows names turn into NFS names, the lookup of the names follows NFS semantics. That includes the fact that NFS lookups are case-sensitive. This means that the applications accessing mapped shares must not rely on Windows case-insensitive behavior. However, the 8.3 name is available, and that is case-insensitive.
- Partial or invalid mappings: After mapping a name to return to clients doing directory enumeration ("dir"), the resulting Unicode name is checked for Windows validity. If that name still has invalid characters in it, or if it is otherwise invalid for Windows (e.g. it ends in "." or blank) the 8.3 name is returned instead of the invalid name.

## Step

### 1. Configure character mapping:

```
vserver cifs character-mapping create -vserver vserver_name -volume  
volume_name -mapping mapping_text, ...
```

The mapping consists of a list of source-target character pairs separated by “:”. The characters are Unicode characters entered using hexadecimal digits. For example: 3C:E03C.

The first value of each `mapping_text` pair that is separated by a colon is the hexadecimal value of the NFS character you want to translate, and the second value is the Unicode value that SMB uses. The mapping pairs must be unique (a one-to-one mapping should exist).

- Source mapping

The following table shows the permissible Unicode character set for source mapping:

Unicode character	Printed character	Description
0x01-0x19	Not applicable	Non-printing control characters
0x5C	\	Backslash
0x3A	:	Colon
0x2A	*	Asterisk
0x3F	?	Question mark
0x22	"	Quotation mark
0x3C	<	Less than
0x3E	>	Greater than
0x7C		Vertical line
0xB1	±	Plus-minus sign

- Target mapping

You can specify target characters in the “Private Use Area” of Unicode in the following range: U+E0000...U+F8FFF.

## Example

The following command creates a character mapping for a volume named “data” on storage virtual machine (SVM) vs1:

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show
```

```
Vserver          Volume Name  Character Mapping
-----
vs1              data        3c:e17c, 3e:f17d, 2a:f745
```

### Commands for managing character mappings for SMB file name translation

You can manage character mapping by creating, modifying, displaying information about, or deleting file character mappings used for SMB file name translation on FlexVol volumes.

If you want to...	Use this command...
Create new file character mappings	<code>vserver cifs character-mapping create</code>
Display information about file character mappings	<code>vserver cifs character-mapping show</code>
Modify existing file character mappings	<code>vserver cifs character-mapping modify</code>
Delete file character mappings	<code>vserver cifs character-mapping delete</code>

For more information, see the man page for each command.

## Manage NFS over RDMA

### NFS over RDMA

NFS over RDMA utilizes RDMA adapters, allowing data to be copied directly between storage system memory and host system memory, circumventing CPU interruptions and overhead.

NFS over RDMA configurations are designed for customers with latency sensitive or high-bandwidth workloads such as machine learning and analytics. NVIDIA has extended NFS over RDMA to enable GPU Direct Storage (GDS). GDS further accelerates GPU-enabled workloads by bypassing the CPU and main memory altogether using RDMA to transfer data between the storage system and GPU memory directly.

In ONTAP 9.10.1, this configuration is only supported for the NFSv4.0 protocol when used with the Mellanox CX-5 or CX-6 adapter, which provides support for RDMA using version 2 of the RoCE protocol. GDS is only supported using NVIDIA Tesla- and Ampere-family GPUs with Mellanox NIC cards and MOFED software. NFS over RDMA support is limited to node-local traffic only. Standard FlexVols or FlexGroups where all constituents are on the same node are supported and must be accessed from a LIF on the same node. NFS mount sizes higher than 64k result in unstable performance with NFS over RDMA configurations.

## Requirements

- Storage systems must be running ONTAP 9.10.1
- Both nodes in the HA pair must be the same version
- Storage system controllers must have RDMA support (currently A400, A700, and A800)
- Storage appliance configured with RDMA-supported hardware (e.g. Mellanox CX-5 or CX-6)
- Data LIFs must be configured to support RDMA.
- Clients must be using Mellanox RDMA-capable NIC cards and Mellanox OFED (MOFED) network software.

## Next Steps

- [Configure NICs for NFS over RDMA](#)
- [Configure LIFs for NFS over RDMA](#)
- [NFS settings for NFS over RDMA](#)

## Further reading

- [RFC 7530: NFS Version 4 Protocol](#)
- [RFC 8166: Remote Direct Memory Access Transport for Remote Procedure Call Version 1](#)
- [RFC 8167: Bidirectional Remote Procedure Call on RPC-over-RDMA Transports](#)
- [RFC 8267: NFS Upper-Layer Binding to RPC-over-RDMA version 1](#)

## Configure NICs for NFS over RDMA

NFS over RDMA requires NIC configuration for both the client system and storage platform.

### Storage platform configuration

An X1148 RDMA adapter needs to be installed on the server. If you are using an HA configuration, you must have a corresponding X1148 adapter on the failover partner so RDMA service can continue during failover. The NIC must be ROCE capable.

Beginning with ONTAP 9.10.1, you can view a list of RDMA offload protocols with the command:

```
network port show -rdma-protocols roce
```

### Client system configuration

Clients must be using Mellanox RDMA-capable NIC cards (e.g. X1148) and Mellanox OFED network software. Consult Mellanox documentation for supported models and versions. Although the client and server can be directly connected, the use of switches is recommended due to improved failover performance with a switch.

The client, server, and any switches, and all ports on switches must be configured using Jumbo frames. Also ensure that priority flow-control is in effect on any switches.

Once this configuration is confirmed, you can mount the NFS.

## Steps

1. Check if RDMA access is enabled on the NFS server with the command:

```
vserver nfs show-vserver vserver_name
```

By default, `-rdma` should be enabled. If it is not, enable RDMA access on the NFS server:

```
vserver nfs modify -vserver vserver_name -rdma enabled
```

## 2. Mount the client via NFSv4.0 over RDMA:

- a. The input for the `proto` parameter depends on the server IP protocol version. If it is v4, use `proto=rdma`. If it is v6, use `proto=rdma6`.
- b. Specify the NFS target port as `port=20049` instead of the standard port of 2049:

```
mount -o vers=4,minorversion=0,proto=rdma,port=20049 Server_IP_address  
:/volume_path mount_point
```

## 3. **OPTIONAL:** If you need to unmount the client, run the command `umount mount_path`

## Configure LIFs for NFS over RDMA

To utilize NFS over RDMA, you must configure your LIFs to be RDMA compatible. Both the LIF and its failover pair must be RDMA capable.

Beginning with ONTAP 9.10.1, there is a new `-rdma_protocols` parameter on the network interface commands where you can configure support, along with setting an appropriate service policy.

### Procedure to create a new LIF

#### 1. Create a LIF:

```
network interface create -vserver SVM_name -lif lif_name -service-policy  
service_policy_name -home-node node_name -home-port port_name {-address  
IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall-policy  
policy_name -auto-revert {true|false} -rdma-protocols roce
```

- a. The service policy must be either `default-data-files` or a custom policy that includes the `data-nfs` network interface service.
- b. The `-rdma-protocols` parameter accepts a list, which is by default empty. When `roce` is added as a value, the LIF can only be configured on ports supporting RoCE offload, affecting both LIF migration and failover.

### Procedure to modify a LIF

1. You can check the status of your LIFs with the `network interface show` command. The service policy must include the `data-nfs` network interface service. The `-rdma-protocols` list should include `roce`. If either of these conditions are untrue, modify the LIF.
2. To modify the LIF, run:

```
network interface modify vserver SVM_name -lif lif_name -service-policy  
service_policy_name -home-node node_name -home-port port_name {-address  
IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall-policy  
policy_name -auto-revert {true|false} -rdma-protocols roce
```



Modifying a LIF to require a particular offload protocol when the LIF is not currently assigned to a port that supports that protocol will produce an error.

## More Information

[Create a LIF](#)

## Modify the NFS configuration

In most cases, you will not need to modify the configuration of the NFS-enabled vserver for NFS over RDMA.

If you are, however, dealing with issues related to Mellanox chips and LIF migration, you should increase the NFSv4 locking grace period. By default, the grace period is set to 45 seconds. Beginning with ONTAP 9.10.1, the grace period can go as high as 180 seconds.

### Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Enter the following command:

```
vserver nfs modify -vserver vserver_name -v4-grace-seconds number_of_seconds
```

For more about this task, see [Specifying the NFSv4 locking grace period](#).

## Configure SMB with the CLI

### SMB configuration overview with the CLI

You can use ONTAP 9 CLI commands to configure SMB client access to files contained in a new volume or qtree in a new or existing SVM.



*SMB* (Server Message Block) refers to modern dialects of the Common Internet File System (CIFS) protocol. You will still see *CIFS* in the ONTAP command-line interface (CLI) and in OnCommand management tools.

Use these procedures if you want to configure SMB access to a volume or qtree in the following way:

- You want to use SMB version 2 or later.
- You want to serve SMB clients only, not NFS clients (not a multiprotocol configuration).
- NTFS file permissions will be used to secure the new volume.
- You have cluster administrator privileges, not SVM administrator privileges.

Cluster administrator privileges are required to create SVMs and LIFs. SVM administrator privileges are sufficient for other SMB configuration tasks.

- You want to use the CLI, not System Manager or an automated scripting tool.



To use System Manager to configure NAS multiprotocol access, see [Provision NAS storage for both Windows and Linux using both NFS and SMB](#).

- You want to use best practices, not explore every available option.

Details about command syntax are available from CLI help and ONTAP man pages.

If you want details about the range of ONTAP SMB protocol capabilities, consult the [SMB reference overview](#).

### Other ways to do this in ONTAP

To perform these tasks with...	Refer to...
The redesigned System Manager (available with ONTAP 9.7 and later)	<a href="#">Provision NAS storage for Windows servers using SMB</a>
System Manager Classic (available with ONTAP 9.7 and earlier)	<a href="#">SMB configuration overview</a>

## SMB configuration workflow

Configuring SMB involves assessing physical storage and networking requirements, and then choosing a workflow that is specific to your goal; configuring SMB access to a new or existing SVM, or adding a volume or qtree to an existing SVM that is already fully configured for SMB access.

## Preparation

### Assess physical storage requirements

Before provisioning SMB storage for clients, you must ensure that there is sufficient space in an existing aggregate for the new volume. If there is not, you can add disks to an existing aggregate or create a new aggregate of the desired type.

### Steps

1. Display available space in existing aggregates: `storage aggregate show`

If there is an aggregate with sufficient space, record its name in the worksheet.

```

cluster::> storage aggregate show
Aggregate      Size Available Used% State  #Vols  Nodes  RAID Status
-----
aggr_0        239.0GB   11.13GB   95% online    1 node1  raid_dp,
normal
aggr_1        239.0GB   11.13GB   95% online    1 node1  raid_dp,
normal
aggr_2        239.0GB   11.13GB   95% online    1 node2  raid_dp,
normal
aggr_3        239.0GB   11.13GB   95% online    1 node2  raid_dp,
normal
aggr_4        239.0GB   238.9GB   95% online    5 node3  raid_dp,
normal
aggr_5        239.0GB   239.0GB   95% online    4 node4  raid_dp,
normal

6 entries were displayed.

```

2. If there are no aggregates with sufficient space, add disks to an existing aggregate by using the `storage aggregate add-disks` command, or create a new aggregate by using the `storage aggregate create` command.

## Assess networking requirements

Before providing SMB storage to clients, you must verify that networking is correctly configured to meet the SMB provisioning requirements.

### Before you begin

The following cluster networking objects must be configured:

- Physical and logical ports
- Broadcast domains
- Subnets (if required)
- IPspaces (as required, in addition to the default IPspace)
- Failover groups (as required, in addition to the default failover group for each broadcast domain)
- External firewalls

### Steps

1. Display the available physical and virtual ports: `network port show`
  - When possible, you should use the port with the highest speed for the data network.
  - All components in the data network must have the same MTU setting for best performance.
2. If you are planning to use a subnet name to allocate the IP address and network mask value for a LIF, verify that the subnet exists and has sufficient addresses available: `network subnet show`

Subnets contain a pool of IP addresses that belong to the same layer 3 subnet. Subnets are created by using the `network subnet create` command.

3. Display available IPspaces: `network ipspace show`

You can use the default IPspace or a custom IPspace.

4. If you want to use IPv6 addresses, verify that IPv6 is enabled on the cluster: `network options ipv6 show`

If required, you can enable IPv6 by using the `network options ipv6 modify` command.

## Decide where to provision new SMB storage capacity

Before you create a new SMB volume or qtree, you must decide whether to place it in a new or existing SVM, and how much configuration the SVM requires. This decision determines your workflow.

### Choices

- If you want to provision a volume or qtree on a new SVM, or on an existing SVM that has SMB enabled but not configured, complete the steps in both “Configuring SMB access to an SVM” and “Adding storage capacity to an SMB-enabled SVM”.

[Configuring SMB access to an SVM](#)

[Configuring SMB client access to shared storage](#)

You might choose to create a new SVM if one of the following is true:

- You are enabling SMB on a cluster for the first time.
- You have existing SVMs in a cluster in which you do not want to enable SMB support.
- You have one or more SMB-enabled SVMs in a cluster, and you want one of the following connections:
  - To a different Active Directory forest or workgroup.
  - To an SMB server in an isolated namespace (multi-tenancy scenario).  
You should also choose this option to provision storage on an existing SVM that has SMB enabled but not configured. This might be the case if you created the SVM for SAN access or if no protocols were enabled when the SVM was created.

After enabling SMB on the SVM, proceed to provision a volume or qtree.

- If you want to provision a volume or qtree on an existing SVM that is fully configured for SMB access, complete the steps in “Adding storage capacity to an SMB-enabled SVM”.

[Configuring SMB client access to shared storage](#)

## Worksheet for gathering SMB configuration information

The SMB configuration worksheet enables you to collect the required information to set up SMB access for clients.

You should complete one or both sections of the worksheet, depending on the decision you made about where to provision storage:

- If you are configuring SMB access to an SVM, you should complete both sections.

## Configuring SMB access to an SVM

### Configuring SMB client access to shared storage

- If you are adding storage capacity to an SMB-enabled SVM, you should complete only the second section.

### Configuring SMB client access to shared storage

The command man pages contain details about the parameters.

## Configuring SMB access to an SVM

### Parameters for creating an SVM

You supply these values with the `vserver create` command if you are creating a new SVM.

Field	Description	Your value
<code>-vserver</code>	A name you supply for the new SVM that is either a fully qualified domain name (FQDN) or follows another convention that enforces unique SVM names across a cluster.	
<code>-aggregate</code>	The name of an aggregate in the cluster with sufficient space for new SMB storage capacity.	
<code>-rootvolume</code>	A unique name you supply for the SVM root volume.	
<code>-rootvolume-security-style</code>	Use the NTFS security style for the SVM.	<code>ntfs</code>
<code>-language</code>	Use the default language setting in this workflow.	<code>C.UTF-8</code>
<code>ipospace</code>	Optional: IPspaces are distinct IP address spaces in which SVMs reside.	

### Parameters for creating a LIF

You supply these values with the `network interface create` command when you are creating LIFs.

Field	Description	Your value
<code>-lif</code>	A name you supply for the new LIF.	

Field	Description	Your value
<code>-role</code>	Use the data LIF role in this workflow.	<code>data</code>
<code>-data-protocol</code>	Use only the SMB protocol in this workflow.	<code>cifs</code>
<code>-home-node</code>	The node to which the LIF returns when the <code>network interface revert</code> command is run on the LIF.	
<code>-home-port</code>	The port or interface group to which the LIF returns when the <code>network interface revert</code> command is run on the LIF.	
<code>-address</code>	The IPv4 or IPv6 address on the cluster that will be used for data access by the new LIF.	
<code>-netmask</code>	The network mask and gateway for the LIF.	
<code>-subnet</code>	A pool of IP addresses. Used instead of <code>-address</code> and <code>-netmask</code> to assign addresses and netmasks automatically.	
<code>-firewall-policy</code>	Use the default data firewall policy in this workflow.	<code>data</code>
<code>-auto-revert</code>	Optional: Specifies whether a data LIF is automatically reverted to its home node on startup or under other circumstances. The default setting is <code>false</code> .	

### Parameters for DNS host name resolution

You supply these values with the `vserver services name-service dns create` command when you are configuring DNS.

Field	Description	Your value
<code>-domains</code>	Up to five DNS domain names.	

Field	Description	Your value
<code>-name-servers</code>	Up to three IP addresses for each DNS name server.	

### Setting up an SMB server in an Active Directory domain

#### Parameters for time service configuration

You supply these values with the `cluster time-service ntp server create` command when you are configuring time services.

Field	Description	Your value
<code>-server</code>	The host name or IP address of the NTP server for the Active Directory domain.	

#### Parameters for creating an SMB server in an Active Directory domain

You supply these values with the `vserver cifs create` command when you create a new SMB server and specify domain information.

Field	Description	Your value
<code>-vserver</code>	The name of the SVM on which to create the SMB server.	
<code>-cifs-server</code>	The name of the SMB server (up to 15 characters).	
<code>-domain</code>	The fully qualified domain name (FQDN) of the Active Directory domain to associate with the SMB server.	
<code>-ou</code>	Optional: The organizational unit within the Active Directory domain to associate with the SMB server. By default, this parameter is set to CN=Computers.	
<code>-netbios-aliases</code>	Optional: A list of NetBIOS aliases, which are alternate names to the SMB server name.	
<code>-comment</code>	Optional: A text comment for the server. Windows clients can see this SMB server description when browsing servers on the network.	

## Setting up an SMB server in a workgroup

### Parameters for creating an SMB server in a workgroup

You supply these values with the `vserver cifs create` command when you create a new SMB server and specify supported SMB versions.

Field	Description	Your value
<code>-vserver</code>	The name of the SVM on which to create the SMB server.	
<code>-cifs-server</code>	The name of the SMB server (up to 15 characters).	
<code>-workgroup</code>	The name of the workgroup (up to 15 characters).	
<code>-comment</code>	Optional: A text comment for the server. Windows clients can see this SMB server description when browsing servers on the network.	

### Parameters for creating local users

You supply these values when you create local users by using the `vserver cifs users-and-groups local-user create` command. They are required for SMB servers in workgroups and optional in AD domains.

Field	Description	Your value
<code>-vserver</code>	The name of the SVM on which to create the local user.	
<code>-user-name</code>	The name of the local user (up to 20 characters).	
<code>-full-name</code>	Optional: The user's full name. If the full name contains a space, enclose the full name within double quotation marks.	
<code>-description</code>	Optional: A description for the local user. If the description contains a space, enclose the parameter in quotation marks.	

Field	Description	Your value
<code>-is-account-disabled</code>	Optional: Specifies whether the user account is enabled or disabled. If this parameter is not specified, the default is to enable the user account.	

### Parameters for creating local groups

You supply these values when you create local groups by using the `vserver cifs users-and-groups local-group create` command. They are optional for SMB servers in AD domains and workgroups.

Field	Description	Your value
<code>-vserver</code>	The name of the SVM on which to create the local group.	
<code>-group-name</code>	The name of the local group (up to 256 characters).	
<code>-description</code>	Optional: A description for the local group. If the description contains a space, enclose the parameter in quotation marks.	

### Adding storage capacity to an SMB-enabled SVM

#### Parameters for creating a volume

You supply these values with the `volume create` command if you are creating a volume instead of a `qtree`.

Field	Description	Your value
<code>-vserver</code>	The name of a new or existing SVM that will host the new volume.	
<code>-volume</code>	A unique descriptive name you supply for the new volume.	
<code>-aggregate</code>	The name of an aggregate in the cluster with sufficient space for the new SMB volume.	
<code>-size</code>	An integer you supply for the size of the new volume.	
<code>-security-style</code>	Use the NTFS security style for this workflow.	<code>ntfs</code>



Field	Description	Your value
-junction-path	Location under root (/) where the new volume is to be mounted.	

### Parameters for creating a qtree

You supply these values with the `volume qtree create` command if you are creating a qtree instead of a volume.

Field	Description	Your value
-vserver	The name of the SVM on which the volume containing the qtree resides.	
-volume	The name of the volume that will contain the new qtree.	
-qtree	A unique descriptive name you supply for the new qtree, 64 characters or less.	
-qtree-path	The qtree path argument in the format <code>/vol/volume_name/qtree_name\&gt;</code> can be specified instead of specifying volume and qtree as separate arguments.	

### Parameters for creating SMB shares

You supply these values with the `vserver cifs share create` command.

Field	Description	Your value
-vserver	The name of the SVM on which to create the SMB share.	
-share-name	The name of the SMB share that you want to create (up to 256 characters).	
-path	The name of the path to the SMB share (up to 256 characters). This path must exist in a volume before creating the share.	

Field	Description	Your value
-share-properties	Optional: A list of share properties. The default settings are <code>oplocks</code> , <code>browsable</code> , <code>changenotify</code> , and <code>show-previous-versions</code> .	
-comment	Optional: A text comment for the server (up to 256 characters). Windows clients can see this SMB share description when browsing on the network.	

### Parameters for creating SMB share access control lists (ACLs)

You supply these values with the `vserver cifs share access-control create` command.

Field	Description	Your value
-vserver	The name of the SVM on which to create the SMB ACL.	
-share	The name of the SMB share on which to create.	
-user-group-type	The type of the user or group to add to the share's ACL. The default type is <code>windows</code>	<code>windows</code>
-user-or-group	The user or group to add to the share's ACL. If you specify the user name, you must include the user's domain using the "domain\username" format.	
-permission	Specifies the permissions for the user or group.	[ <code>No_access</code>   <code>Read</code>   <code>Change</code>   <code>Full_Control</code> ]

## Configure SMB access to an SVM

### Configure SMB access to an SVM

If you do not already have an SVM configured for SMB client access, you must either create and configure a new SVM or configure an existing SVM. Configuring SMB involves opening SVM root volume access, creating an SMB server, creating a LIF, enabling host-name resolution, configuring name services, and if desired, enabling Kerberos security.

## Create an SVM

If you do not already have at least one SVM in a cluster to provide data access to SMB clients, you must create one.

### Steps

1. Create an SVM: `vserver create -vserver vserver_name -rootvolume root_volume_name -aggregate aggregate_name -rootvolume-security-style ntfs -language C.UTF-8 -ipospace ipospace_name`
  - Use the NTFS setting for the `-rootvolume-security-style` option.
  - Use the default `C.UTF-8` `-language` option.
  - The `ipospace` setting is optional.
2. Verify the configuration and status of the newly created SVM: `vserver show -vserver vserver_name`

The `Allowed Protocols` field must include CIFS. You can edit this list later.

The `Vserver Operational State` field must display the `running` state. If it displays the `initializing` state, it means that some intermediate operation such as root volume creation failed, and you must delete the SVM and re-create it.

### Examples

The following command creates an SVM for data access in the IPspace `ipospaceA`:

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style ntfs -language C.UTF-8 -ipospace ipospaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

The following command shows that an SVM was created with a root volume of 1 GB, and it was started automatically and is in `running` state. The root volume has a default export policy that does not include any rules, so the root volume is not exported upon creation.

```

cluster1::> vserver show -vserver vs1.example.com
                Vserver: vs1.example.com
                Vserver Type: data
                Vserver Subtype: default
                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                Root Volume: root_vs1
                Aggregate: aggr1
                NIS Domain: -
                Root Volume Security Style: ntfs
                LDAP Client: -
                Default Volume Language Code: C.UTF-8
                Snapshot Policy: default
                Comment:
                Quota Policy: default
                List of Aggregates Assigned: -
                Limit on Maximum Number of Volumes allowed: unlimited
                Vserver Admin State: running
                Vserver Operational State: running
                Vserver Operational State Stopped Reason: -
                Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                Disallowed Protocols: -
                QoS Policy Group: -
                Config Lock: false
                IPspace Name: ipspaceA

```

## Verify that the SMB protocol is enabled on the SVM

Before you can configure and use SMB on SVMs, you must verify that the protocol is enabled.

### About this task

This is typically done during SVM setup, but if you did not enable the protocol during setup, you can enable it later by using the `vserver add-protocols` command.



You cannot add or remove a protocol from a LIF once it is created.

You can also disable protocols on SVMs using the `vserver remove-protocols` command.

### Steps

1. Check which protocols are currently enabled and disabled for the SVM: `vserver show -vserver vserver_name -protocols`

You can also use the `vserver show-protocols` command to view the currently enabled protocols on all SVMs in the cluster.

2. If necessary, enable or disable a protocol:

- To enable the SMB protocol: `vserver add-protocols -vserver vserver_name -protocols cifs`
- To disable a protocol: `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]`

3. Confirm that the enabled and disabled protocols were updated correctly: `vserver show -vserver vserver_name -protocols`

### Example

The following command displays which protocols are currently enabled and disabled (allowed and disallowed) on the SVM named vs1:

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols           Disallowed Protocols
-----           -
vs1.example.com   cifs                         nfs, fcp, iscsi, ndmp
```

The following command allows access over SMB by adding `cifs` to the list of enabled protocols on the SVM named vs1:

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols cifs
```

### Open the export policy of the SVM root volume

The default export policy of the SVM root volume must include a rule to allow all clients open access through SMB. Without such a rule, all SMB clients are denied access to the SVM and its volumes.

#### About this task

When a new SVM is created, a default export policy (called default) is created automatically for the root volume of the SVM. You must create one or more rules for the default export policy before clients can access data on the SVM.

You should verify that all SMB access is open in the default export policy, and later restrict access to individual volumes by creating custom export policies for individual volumes or qtrees.

#### Steps

1. If you are using an existing SVM, check the default root volume export policy: `vserver export-policy rule show`

The command output should be similar to the following:

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance
```

```
                Vserver: vs1.example.com
                Policy Name: default
                Rule Index: 1
                Access Protocol: cifs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                RO Access Rule: any
                RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                Superuser Security Types: any
                Honor SetUID Bits in SETATTR: true
                Allow Creation of Devices: true
```

If such a rule exists that allows open access, this task is complete. If not, proceed to the next step.

2. Create an export rule for the SVM root volume: `vserver export-policy rule create -vserver vserver_name -policyname default -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`
3. Verify rule creation by using the `vserver export-policy rule show` command.

## Results

Any SMB client can now access any volume or qtree created on the SVM.

## Create a LIF

A LIF is an IP address associated with a physical or logical port. If there is a component failure, a LIF can fail over to or be migrated to a different physical port, thereby continuing to communicate with the network.

### Before you begin

- The underlying physical or logical network port must have been configured to the administrative `up` status.
- If you are planning to use a subnet name to allocate the IP address and network mask value for a LIF, the subnet must already exist.

Subnets contain a pool of IP addresses that belong to the same layer 3 subnet. They are created using the `network subnet create` command.

- The mechanism for specifying the type of traffic handled by a LIF has changed. For ONTAP 9.5 and earlier, LIFs used roles to specify the type of traffic it would handle. Beginning with ONTAP 9.6, LIFs use service policies to specify the type of traffic it would handle.

### About this task

- You can create both IPv4 and IPv6 LIFs on the same network port.
- If you have a large number of LIFs in your cluster, you can verify the LIF capacity supported on the cluster by using the `network interface capacity show` command and the LIF capacity supported on each

node by using the `network interface capacity details show` command (at the advanced privilege level).

- Beginning with ONTAP 9.7, if other LIFs already exist for the SVM in the same subnet, you do not need to specify the home port of the LIF. ONTAP automatically chooses a random port on the specified home node in the same broadcast domain as the other LIFs already configured in the same subnet.

Beginning with ONTAP 9.4, FC-NVMe is supported. If you are creating an FC-NVMe LIF you should be aware of the following:

- The NVMe protocol must be supported by the FC adapter on which the LIF is created.
- FC-NVMe can be the only data protocol on data LIFs.
- One LIF handling management traffic must be configured for every storage virtual machine (SVM) supporting SAN.
- NVMe LIFs and namespaces must be hosted on the same node.
- Only one NVMe LIF handling data traffic can be configured per SVM

## Steps

### 1. Create a LIF:

```
network interface create -vserver vserver_name -lif lif_name -role data -data
-protocol cifs -home-node node_name -home-port port_name {-address IP_address
-netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto
-revert {true|false}
```

#### ONTAP 9.5 and earlier

```
network interface create -vserver vserver_name -lif lif_name -role data -data
-protocol cifs -home-node node_name -home-port port_name {-address IP_address
-netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto
-revert {true|false}
```

#### ONTAP 9.6 and later

```
network interface create -vserver vserver_name -lif lif_name -service-policy
service_policy_name -home-node node_name -home-port port_name {-address
IP_address -netmask IP_address | -subnet-name subnet_name} -firewall-policy
data -auto-revert {true|false}
```

- The `-role` parameter is not required when creating a LIF using a service policy (beginning with ONTAP 9.6).
- The `-data-protocol` parameter must be specified when the LIF is created, and cannot be modified later without destroying and re-creating the data LIF.

The `-data-protocol` parameter is not required when creating a LIF using a service policy (beginning with ONTAP 9.6).

- `-home-node` is the node to which the LIF returns when the `network interface revert` command is run on the LIF.

You can also specify whether the LIF should automatically revert to the home-node and home-port with the `-auto-revert` option.

- `-home-port` is the physical or logical port to which the LIF returns when the `network interface revert` command is run on the LIF.
- You can specify an IP address with the `-address` and `-netmask` options, or you enable allocation from a subnet with the `-subnet_name` option.
- When using a subnet to supply the IP address and network mask, if the subnet was defined with a gateway, a default route to that gateway is added automatically to the SVM when a LIF is created using that subnet.
- If you assign IP addresses manually (without using a subnet), you might need to configure a default route to a gateway if there are clients or domain controllers on a different IP subnet. The `network route create man` page contains information about creating a static route within an SVM.
- For the `-firewall-policy` option, use the same default data as the LIF role.

You can create and add a custom firewall policy later if desired.

- `-auto-revert` allows you to specify whether a data LIF is automatically reverted to its home node under circumstances such as startup, changes to the status of the management database, or when the network connection is made. The default setting is `false`, but you can set it to `false` depending on network management policies in your environment.

## 2. Verify that the LIF was created successfully:

```
network interface show
```

## 3. Verify that the configured IP address is reachable:

To verify an...	Use...
IPv4 address	<code>network ping</code>
IPv6 address	<code>network ping6</code>

## Examples

The following command creates a LIF and specifies the IP address and network mask values using the `-address` and `-netmask` parameters:

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol cifs -home-node node-4 -home-port elc -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

The following command creates a LIF and assigns IP address and network mask values from the specified subnet (named `client1_sub`):



```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol cifs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

The following command shows all the LIFs in cluster-1. Data LIFs datalif1 and datalif3 are configured with IPv4 addresses, and datalif4 is configured with an IPv6 address:

```
network interface show
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is
Home						
cluster-1	cluster_mgmt	up/up	192.0.2.3/24	node-1	e1a	
true						
node-1	clus1	up/up	192.0.2.12/24	node-1	e0a	
true						
	clus2	up/up	192.0.2.13/24	node-1	e0b	
true						
	mgmt1	up/up	192.0.2.68/24	node-1	e1a	
true						
node-2	clus1	up/up	192.0.2.14/24	node-2	e0a	
true						
	clus2	up/up	192.0.2.15/24	node-2	e0b	
true						
	mgmt1	up/up	192.0.2.69/24	node-2	e1a	
true						
vs1.example.com						
	datalif1	up/down	192.0.2.145/30	node-1	e1c	
true						
vs3.example.com						
	datalif3	up/up	192.0.2.146/30	node-2	e0c	
true						
	datalif4	up/up	2001::2/64	node-2	e0c	
true						

5 entries were displayed.

The following command shows how to create a NAS data LIF that is assigned with the default-data-files service policy:

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

## Enable DNS for host-name resolution

You can use the `vserver services name-service dns` command to enable DNS on an SVM, and configure it to use DNS for host-name resolution. Host names are resolved using external DNS servers.

### Before you begin

A site-wide DNS server must be available for host name lookups.

You should configure more than one DNS server to avoid a single-point-of-failure. The `vserver services name-service dns create` command issues a warning if you enter only one DNS server name.

### About this task

The *Network Management Guide* contains information about configuring dynamic DNS on the SVM.

### Steps

1. Enable DNS on the SVM: `vserver services name-service dns create -vserver vserver_name -domains domain_name -name-servers ip_addresses -state enabled`

The following command enables external DNS server servers on the SVM vs1:

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```



Beginning with ONTAP 9.2, the `vserver services name-service dns create` command performs an automatic configuration validation and reports an error message if ONTAP cannot contact the name server.

2. Display the DNS domain configurations by using the `vserver services name-service dns show` command. ``

The following command displays the DNS configurations for all SVMs in the cluster:

```
vserver services name-service dns show
```

Vserver	State	Domains	Name Servers
cluster1	enabled	example.com	192.0.2.201, 192.0.2.202
vs1.example.com	enabled	example.com	192.0.2.201, 192.0.2.202

The following command displays detailed DNS configuration information for SVM vs1:

```
vserver services name-service dns show -vserver vs1.example.com
      Vserver: vs1.example.com
      Domains: example.com
      Name Servers: 192.0.2.201, 192.0.2.202
      Enable/Disable DNS: enabled
      Timeout (secs): 2
      Maximum Attempts: 1
```

3. Validate the status of the name servers by using the `vserver services name-service dns check` command.

The `vserver services name-service dns check` command is available beginning with ONTAP 9.2.

```
vserver services name-service dns check -vserver vs1.example.com
```

Vserver	Name Server	Status	Status Details
vs1.example.com	10.0.0.50	up	Response time (msec): 2
vs1.example.com	10.0.0.51	up	Response time (msec): 2

## Set up an SMB server in an Active Directory domain

### Configure time services

Before creating an SMB server in an Active Domain controller, you must ensure that the cluster time and the time on the domain controllers of the domain to which the SMB server will belong matches to within five minutes.

### About this task

You should configure cluster NTP services to use the same NTP servers for time synchronization that the Active Directory domain uses.

Beginning with ONTAP 9.5, you can set up your NTP server with symmetric authentication.

### Steps

1. Configure time services by using the `cluster time-service ntp server create` command.
  - To configure time services without symmetric authentication enter the following command: `cluster time-service ntp server create -server server_ip_address`
  - To configure time services with symmetric authentication, enter the following command: `cluster time-service ntp server create -server server_ip_address -key-id key_id`  
`cluster time-service ntp server create -server 10.10.10.1 cluster time-service ntp server create -server 10.10.10.2`



- Verify that time services are set up correctly by using the `cluster time-service ntp server show` command.

```
cluster time-service ntp server show
```

```
Server                               Version
-----                               -
10.10.10.1                           auto
10.10.10.2                           auto
```

### Commands for managing symmetric authentication on NTP servers

Beginning with ONTAP 9.5, Network Time Protocol (NTP) version 3 is supported. NTPv3 includes symmetric authentication using SHA-1 keys which increases network security.

To do this...	Use this command...
Configure an NTP server without symmetric authentication	<code>cluster time-service ntp server create -server server_name</code>
Configure an NTP server with symmetric authentication	<code>cluster time-service ntp server create -server server_ip_address -key-id key_id</code>
Enable symmetric authentication for an existing NTP server An existing NTP server can be modified to enable authentication by adding the required key-id.	<code>cluster time-service ntp server modify -server server_name -key-id key_id</code>
Configure a shared NTP key	<code>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</code> <div style="margin-top: 10px;">  <p>Shared keys are referred to by an ID. The ID, its type, and value must be identical on both the node and the NTP server</p> </div>
Configure an NTP server with an unknown key ID	<code>cluster time-service ntp server create -server server_name -key-id key_id</code>
Configure a server with a key ID not configured on the NTP server.	<code>cluster time-service ntp server create -server server_name -key-id key_id</code> <div style="margin-top: 10px;">  <p>The key ID, type, and value must be identical to the key ID, type, and value configured on the NTP server.</p> </div>

To do this...	Use this command...
Disable symmetric authentication	<pre>cluster time-service ntp server modify -server server_name -authentication disabled</pre>

### Create an SMB server in an Active Directory domain

You can use the `vserver cifs create` command to create an SMB server on the SVM and specify the Active Directory (AD) domain to which it belongs.

#### Before you begin

The SVM and LIFs that you are using to serve data must have been configured to allow the SMB protocol. The LIFs must be able to connect to the DNS servers that are configured on the SVM and to an AD domain controller of the domain to which you want to join the SMB server.

Any user who is authorized to create machine accounts in the AD domain to which you are joining the SMB server can create the SMB server on the SVM. This can include users from other domains.

Beginning with ONTAP 9.7, your AD administrator can provide you with a URI to a keytab file as an alternative to providing you with a name and password to a privileged Windows account. When you receive the URI, include it in the `-keytab-uri` parameter with the `vserver cifs` commands.

#### About this task

When creating an SMB server in an Activity Directory domain:

- You must use the fully qualified domain name (FQDN) when specifying the domain.
- The default setting is to add the SMB server machine account to the Active Directory CN=Computer object.
- You can choose to add the SMB server to a different organizational unit (OU) by using the `-ou` option.
- You can optionally choose to add a comma-delimited list of one or more NetBIOS aliases (up to 200) for the SMB server.

Configuring NetBIOS aliases for an SMB server can be useful when you are consolidating data from other file servers to the SMB server and want the SMB server to respond to the original servers' names.

The `vserver cifs` man pages contain additional optional parameters and naming requirements.



Beginning with ONTAP 9.1, you can enable SMB version 2.0 to connect to a domain controller (DC). Doing so is necessary if you have disabled SMB 1.0 on domain controllers. Beginning with ONTAP 9.2, SMB 2.0 is enabled by default.

Beginning with ONTAP 9.8, you can specify that connections to domain controllers be encrypted. ONTAP requires encryption for domain controller communications when the `-encryption-required-for-dc-connection` option is set to `true`; the default is `false`. When the option is set, only the SMB3 protocol will be used for ONTAP-DC connections, because encryption is only supported by SMB3. .

[SMB management](#) contains more information about SMB server configuration options.

#### Steps

1. Verify that SMB is licensed on your cluster: `system license show -package cifs`

If it is not, contact your sales representative.

A CIFS license is not required if the SMB server will be used for authentication only.

2. Create the SMB server in an AD domain: `vserver cifs create -vserver vserver_name -cifs -server smb_server_name -domain FQDN [-ou organizational_unit] [-netbios-aliases NetBIOS_name, ...] [-keytab-uri {(ftp|http)://hostname|IP_address}] [-comment text]`

When joining a domain, this command might take several minutes to finish.

The following command creates the SMB server “smb\_server01” in the domain “example.com”:

```
cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
smb_server01 -domain example.com
```

The following command creates the SMB server “smb\_server02” in the domain “mydomain.com” and authenticates the ONTAP administrator with a keytab file:

```
cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server
smb_server02 -domain mydomain.com -keytab-uri
http://admin.mydomain.com/ontap1.keytab
```

3. Verify the SMB server configuration by using the `vserver cifs show` command.

In this example, the command output shows that an SMB server named “SMB\_SERVER01” was created on SVM vs1.example.com, and was joined to the “example.com” domain.

```
cluster1::> vserver cifs show -vserver vs1

                                Vserver: vs1.example.com
                CIFS Server NetBIOS Name: SMB_SERVER01
    NetBIOS Domain/Workgroup Name: EXAMPLE
                Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                Authentication Style: domain
    CIFS Server Administrative Status: up
                CIFS Server Description: -
                List of NetBIOS Aliases: -
```

4. If desired, enable encrypted communication with the domain controller (ONTAP 9.8 and later): `vserver cifs security modify -vserver svm_name -encryption-required-for-dc-connection true`

## Examples

The following command creates a SMB server named “smb\_server02” on SVM vs2.example.com in the “example.com” domain. The machine account is created in the “OU=eng,OU=corp,DC=example,DC=com” container. The SMB server is assigned a NetBIOS alias.

```
cluster1::> vserver cifs create -vserver vs2.example.com -cifs-server
smb_server02 -domain example.com -ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01

cluster1::> vserver cifs show -vserver vs1
                                Vserver: vs2.example.com
                                CIFS Server NetBIOS Name: SMB_SERVER02
                                NetBIOS Domain/Workgroup Name: EXAMPLE
                                Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                                Authentication Style: domain
                                CIFS Server Administrative Status: up
                                CIFS Server Description: -
                                List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

The following command enables a user from a different domain, in this case an administrator of a trusted domain, to create a SMB server named “smb\_server03” on SVM vs3.example.com. The `-domain` option specifies the name of the home domain (specified in the DNS configuration) in which you want to create the SMB server. The `username` option specifies the administrator of the trusted domain.

- Home domain: example.com
- Trusted domain: trust.lab.com
- Username for the trusted domain: Administrator1

```
cluster1::> vserver cifs create -vserver vs3.example.com -cifs-server
smb_server03 -domain example.com

Username: Administrator1@trust.lab.com
Password: . . .
```

### Create keytab files for SMB authentication

Beginning with ONTAP 9.7, ONTAP supports SVM authentication with Active Directory (AD) servers using keytab files. AD administrators generate a keytab file and make it available to ONTAP administrators as a uniform resource identifier (URI), which is supplied when `vserver cifs` commands require Kerberos authentication with the AD domain.

AD administrators can create the keytab files using the standard Windows Server `ktpass` command. The command should be run on the primary domain where authentication is required. The `ktpass` command can be used to generate keytab files only for primary domain users; keys generated using trusted-domain users are not supported.

Keytab files are generated for specific ONTAP admin users. As long as the admin user's password does not change, the keys generated for the specific encryption type and domain will not change. Therefore, a new keytab file is required whenever the admin user's password is changed.

The following encryption types are supported:

- AES256-SHA1
- DES-CBC-MD5



ONTAP does not support DES-CBC-CRC encryption type.

- RC4-HMAC

AES256 is the highest encryption type and should be used if enabled on the ONTAP system.

Keytab files can be generated by specifying either the admin password or by using a randomly-generated password. However, at any given time only one password option can be used, because a private key specific to the admin user is needed at the AD server for decrypting the keys inside the keytab file. Any change in the private key for a specific admin will invalidate the keytab file.

## Set up an SMB server in a workgroup

### Set up an SMB server in a workgroup overview

Setting up an SMB server as a member in a workgroup consists of creating the SMB server, and then creating local users and groups.

You can configure an SMB server in a workgroup when the Microsoft Active Directory domain infrastructure is not available.

An SMB server in workgroup mode supports only NTLM authentication and does not support Kerberos authentication.

### Create an SMB server in a workgroup

You can use the `vserver cifs create` command to create an SMB server on the SVM and specify the workgroup to which it belongs.

### Before you begin

The SVM and LIFs that you are using to serve data must have been configured to allow the SMB protocol. The LIFs must be able to connect to the DNS servers that are configured on the SVM.

### About this task

SMB servers in workgroup mode do not support the following SMB features:

- SMB3 Witness protocol
- SMB3 CA shares
- SQL over SMB
- Folder Redirection
- Roaming Profiles



- Group Policy Object (GPO)
- Volume Snapshot Service (VSS)

The `vserver cifs` man pages contain additional optional configuration parameters and naming requirements.

### Steps

1. Verify that SMB is licensed on your cluster: `system license show -package cifs`

If it is not, contact your sales representative.

A CIFS license is not required if the SMB server will be used for authentication only.

2. Create the SMB server in a workgroup: `vserver cifs create -vserver vserver_name -cifs -server cifs_server_name -workgroup workgroup_name [-comment text]`

The following command creates the SMB server “smb\_server01” in the workgroup “workgroup01”:

```
cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
SMB_SERVER01 -workgroup workgroup01
```

3. Verify the SMB server configuration by using the `vserver cifs show` command.

In the following example, the command output shows that a SMB server named “smb\_server01” was created on SVM vs1.example.com in the workgroup “workgroup01”:

```
cluster1::> vserver cifs show -vserver vs0

                                Vserver: vs1.example.com
                                CIFS Server NetBIOS Name: SMB_SERVER01
                                NetBIOS Domain/Workgroup Name: workgroup01
                                Fully Qualified Domain Name: -
                                Organizational Unit: -
                                Default Site Used by LIFs Without Site Membership: -
                                Workgroup Name: workgroup01
                                Authentication Style: workgroup
                                CIFS Server Administrative Status: up
                                CIFS Server Description:
                                List of NetBIOS Aliases: -
```

### After you finish

For a CIFS server in a workgroup, you must create local users, and optionally local groups, on the SVM.

### Related information

[SMB management](#)

## Create local user accounts

You can create a local user account that can be used to authorize access to data contained in the SVM over an SMB connection. You can also use local user accounts for authentication when creating an SMB session.

### About this task

Local user functionality is enabled by default when the SVM is created.

When you create a local user account, you must specify a user name and you must specify the SVM with which to associate the account.

The `vserver cifs users-and-groups local-user` man pages contain details about optional parameters and naming requirements.

### Steps

1. Create the local user: `vserver cifs users-and-groups local-user create -vserver vserver_name -user-name user_name optional_parameters`

The following optional parameters might be useful:

- `-full-name`

The users's full name.

- `-description`

A description for the local user.

- `-is-account-disabled {true|false}`

Specifies whether the user account is enabled or disabled. If this parameter is not specified, the default is to enable the user account.

The command prompts for the local user's password.

2. Enter a password for the local user, and then confirm the password.
3. Verify that the user was successfully created: `vserver cifs users-and-groups local-user show -vserver vserver_name`

### Example

The following example creates a local user "SMB\_SERVER01\sue", with a full name "Sue Chang", associated with SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-user create -vserver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"
```

Enter the password:

Confirm the password:

```
cluster1::> vserver cifs users-and-groups local-user show
Vserver  User Name                Full Name  Description
-----  -
vs1      SMB_SERVER01\Administrator    Built-in administrator
account
vs1      SMB_SERVER01\sue              Sue Chang
```

### Create local groups

You can create local groups that can be used for authorizing access to data associated with the SVM over an SMB connection. You can also assign privileges that define what user rights or capabilities a member of the group has.

#### About this task

Local group functionality is enabled by default when the SVM is created.

When you create a local group, you must specify a name for the group and you must specify the SVM with which to associate the group. You can specify a group name with or without the local domain name, and you can optionally specify a description for the local group. You cannot add a local group to another local group.

The `vserver cifs users-and-groups local-group man` pages contain details about optional parameters and naming requirements.

#### Steps

1. Create the local group: `vserver cifs users-and-groups local-group create -vserver vserver_name -group-name group_name`

The following optional parameter might be useful:

- `-description`

A description for the local group.

2. Verify that the group was successfully created: `vserver cifs users-and-groups local-group show -vserver vserver_name`

#### Example

The following example creates a local group "SMB\_SERVER01\engineering" associated with SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group create -vserver
vs1.example.com -group-name SMB_SERVER01\engineering
```

```
cluster1::> vserver cifs users-and-groups local-group show -vserver
vs1.example.com
```

Vserver	Group Name	Description
vs1.example.com	BUILTIN\Administrators	Built-in Administrators group
vs1.example.com	BUILTIN\Backup Operators	Backup Operators group
vs1.example.com	BUILTIN\Power Users	Restricted administrative privileges
vs1.example.com	BUILTIN\Users	All users
vs1.example.com	SMB_SERVER01\engineering	
vs1.example.com	SMB_SERVER01\sales	

### After you finish

You must add members to the new group.

### Manage local group membership

You can manage local group membership by adding and removing local or domain users, or adding and removing domain groups. This is useful if you want to control access to data based on access controls placed on the group, or if you want users to have privileges associated with that group.

### About this task

If you no longer want a local user, domain user, or domain group to have access rights or privileges based on membership in a group, you can remove the member from the group.

You must keep the following in mind when adding members to a local group:

- You cannot add users to the special *Everyone* group.
- You cannot add a local group to another local group.
- To add a domain user or group to a local group, ONTAP must be able to resolve the name to a SID.

You must keep the following in mind when removing members from a local group:

- You cannot remove members from the special *Everyone* group.
- To remove a member from a local group, ONTAP must be able to resolve their name to a SID.

### Steps

1. Add a member to or remove a member from a group.

- **Add a member:** `vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[,...]`

You can specify a comma-delimited list of local users, domain users, or domain groups to add to the

specified local group.

- **Remove a member:** `vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[,...]`

You can specify a comma-delimited list of local users, domain users, or domain groups to remove from the specified local group.

## Examples

The following example adds a local user “SMB\_SERVER01\sue” to the local group “SMB\_SERVER01\engineering” on SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver vs1.example.com -group-name SMB_SERVER01\engineering -member-names SMB_SERVER01\sue
```

The following example removes the local users “SMB\_SERVER01\sue” and “SMB\_SERVER01\james” from the local group “SMB\_SERVER01\engineering” on SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-group remove-members -vserver vs1.example.com -group-name SMB_SERVER\engineering -member-names SMB_SERVER\sue,SMB_SERVER\james
```

## Verify enabled SMB versions

Your ONTAP 9 release determines which SMB versions are enabled by default for connections with clients and domain controllers. You should verify that the SMB server supports the clients and functionality required in your environment.

### About this task

For connections with both clients and domain controllers, you should enable SMB 2.0 and later whenever possible. For security reasons, you should avoid using SMB 1.0, and you should disable it if you have verified that it is not required in your environment.

In ONTAP 9, SMB versions 2.0 and later are enabled by default for client connections, but the version of SMB 1.0 enabled by default depends on your ONTAP release.

- Beginning with ONTAP 9.1 P8, SMB 1.0 can be disabled on SVMs.

The `-smb1-enabled` option to the `vserver cifs options modify` command enables or disables SMB 1.0.

- Beginning with ONTAP 9.3, it is disabled by default on new SVMs.

If your SMB server is in an Active Directory (AD) domain, you can enable SMB 2.0 to connect to a domain controller (DC) beginning with ONTAP 9.1. Doing so is necessary if you have disabled SMB 1.0 on DCs. Beginning with ONTAP 9.2, SMB 2.0 is enabled by default for DC connections.



If `-smb1-enabled-for-dc-connections` is set to `false` while `-smb1-enabled` is set to `true`, ONTAP denies SMB 1.0 connections as the client, but continues to accept inbound SMB 1.0 connections as the server.

**SMB management** contains details about supported SMB versions and functionality.

### Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Verify which SMB versions are enabled: `vserver cifs options show`

You can scroll down the list to view the SMB versions enabled for client connections, and if you are configuring an SMB server in an AD domain, for AD domain connections.

3. Enable or disable the SMB protocol for client connections as required:

- To enable an SMB version: `vserver cifs options modify -vserver vserver_name smb_version true`

- To disable an SMB version: `vserver cifs options modify -vserver vserver_name smb_version false`

Possible values for `smb_version`:

- `-smb1-enabled`
- `-smb2-enabled`
- `-smb3-enabled`
- `-smb31-enabled`

The following command enables SMB 3.1 on SVM `vs1.example.com`:

```
cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31-enabled true
```

4. If your SMB server is in an Active Directory domain, enable or disable the SMB protocol for DC connections as required:

- To enable an SMB version: `vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections true`

- To disable an SMB version: `vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections false`

5. Return to the admin privilege level: `set -privilege admin`

### Map the SMB server on the DNS server

Your site's DNS server must have an entry pointing the SMB server name, and any NetBIOS aliases, to the IP address of the data LIF so that Windows users can map a drive to the SMB server name.

### Before you begin

You must have administrative access to your site's DNS server. If you do not have administrative access, you

must ask the DNS administrator to perform this task.

### About this task

If you use NetBIOS aliases for the SMB server name, it is a best practice to create DNS server entry points for each alias.

### Steps

1. Log in to the DNS server.
2. Create forward (A - Address record) and reverse (PTR - Pointer record) lookup entries to map the SMB server name to the IP address of the data LIF.
3. If you use NetBIOS aliases, create an Alias canonical name (CNAME resource record) lookup entry to map each alias to the IP address of the SMB server's data LIF.

### Results

After the mapping is propagated across the network, Windows users can map a drive to the SMB server name or its NetBIOS aliases.

## Configure SMB client access to shared storage

### Configure SMB client access to shared storage

To provide SMB client access to shared storage on an SVM, you must create a volume or qtree to provide a storage container, and then create or modify a share for that container. You can then configure share and file permissions, and test access from client systems.

### Before you begin

- SMB must be completely set up on the SVM.
- Any updates to your name services configuration must be complete.
- Any additions or modifications to an Active Directory domain or workgroup configuration must be complete.

### Create a volume or qtree storage container

#### Create a volume

You can create a volume and specify its junction point and other properties by using the `volume create` command.

### Before you begin

The SVM security style must be NTFS, and SMB should be set up and running.

### About this task

A volume must include a *junction path* for its data to be made available to clients. You can specify the junction path when you create a new volume. If you create a volume without specifying a junction path, you must *mount* the volume in the SVM namespace using the `volume mount` command.

### Steps

1. Create the volume with a junction point: `volume create -vserver vservice_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style ntfs -junction-path junction_path`

The choices for `-junction-path` are the following:

- Directly under root, for example, `/new_vol`

You can create a new volume and specify that it be mounted directly to the SVM root volume.

- Under an existing directory, for example, `/existing_dir/new_vol`

You can create a new volume and specify that it be mounted to an existing volume (in an existing hierarchy), expressed as a directory.

If you want to create a volume in a new directory (in a new hierarchy under a new volume), for example, `/new_dir/new_vol`, then you must first create a new parent volume that is junctioned to the SVM root volume. You would then create the new child volume in the junction path of the new parent volume (new directory).

2. Verify that the volume was created with the desired junction point: `volume show -vserver vserver_name -volume volume_name -junction`

### Examples

The following command creates a new volume named `users1` on the SVM `vs1.example.com` and the aggregate `aggr1`. The new volume is made available at `/users`. The volume is 750 GB in size, and its volume guarantee is of type `volume` (by default).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction

```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1.example.com	users1	true	/users	RW_volume

The following command creates a new volume named "home4" on the SVM "vs1.example.com" and the aggregate "aggr1". The directory `/eng/` already exists in the namespace for the `vs1` SVM, and the new volume is made available at `/eng/home`, which becomes the home directory for the `/eng/` namespace. The volume is 750 GB in size, and its volume guarantee is of type `volume` (by default).



```

cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction

```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1.example.com	home4	true	/eng/home	RW_volume

### Create a qtree

You can create a qtree to contain your data and specify its properties by using the `volume qtree create` command.

### Before you begin

- The SVM and the volume that will contain the new qtree must already exist.
- The SVM security style must be NTFS, and SMB should be set up and running.

### Steps

1. Create the qtree: `volume qtree create -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path } -security-style ntfs`

You can specify the volume and qtree as separate arguments or specify the qtree path argument in the format `/vol/volume_name/_qtree_name`.

2. Verify that the qtree was created with the desired junction path: `volume qtree show -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path }`

### Example

The following example creates a qtree named `qt01` located on SVM `vs1.example.com` that has a junction path `/vol/data1`:

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style ntfs
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01
```

```
          Vserver Name: vs1.example.com
          Volume Name: data1
          Qtree Name: qt01
Actual (Non-Junction) Qtree Path: /vol/data1/qt01
          Security Style: ntfs
          Oplock Mode: enable
          Unix Permissions: ---rwxr-xr-x
          Qtree Id: 2
          Qtree Status: normal
          Export Policy: default
Is Export Policy Inherited: true
```

## Requirements and considerations for creating an SMB share

Before creating an SMB share, you must understand requirements for share paths and share properties, particularly for home directories.

Creating an SMB share entails specifying a directory path structure (using the `-path` option in the `vserver cifs share create` command) that clients will access. The directory path corresponds to the junction path for a volume or qtree that you created in the SVM namespace. The directory path and corresponding junction path must exist before creating your share.

Share paths have the following requirements:

- A directory path name can be up to 255 characters long.
- If there is a space in the path name, the entire string must be put in quotes (for example, `"/new volume/mount here"`).
- If the UNC path (`\\servername\sharename\filepath`) of the share contains more than 256 characters (excluding the initial `\\` in the UNC path), then the **Security** tab in the Windows Properties box is unavailable.

This is a Windows client issue rather than an ONTAP issue. To avoid this issue, do not create shares with UNC paths with more than 256 characters.

Share property defaults can be changed:

- The default initial properties for all shares are `oplocks`, `browsable`, `changenotify`, and `show-previous-versions`.
- It is optional to specify share properties when you create a share.

However, if you do specify share properties when you create the share, the defaults are not used. If you use the `-share-properties` parameter when you create a share, you must specify all of the share properties that you want to apply to the share using a comma-delimited list.

- To designate a home directory share, use the `homedirectory` property.

This feature enables you to configure a share that maps to different directories based on the user that connects to it and a set of variables. Instead of having to create separate shares for each user, you can configure a single share with a few home directory parameters to define a user's relationship between an entry point (the share) and their home directory (a directory on the SVM).



You cannot add or remove this property after creating the share.

Home directory shares have the following requirements:

- Before creating SMB home directories, you must add at least one home directory search path by using the `vserver cifs home-directory search-path add` command.
- Home directory shares specified by the value of `homedirectory` on the `-share-properties` parameter must include the `%w` (Windows user name) dynamic variable in the share name.

The share name can additionally contain the `%d` (domain name) dynamic variable (for example, `%d/%w`) or a static portion in the share name (for example, `home1_%w`).

- If the share is used by administrators or users to connect to other users' home directories (using options to the `vserver cifs home-directory modify` command), the dynamic share name pattern must be preceded by a tilde (`~`).

[SMB management](#) and `vserver cifs share` man pages have additional information.

## Create an SMB share

You must create an SMB share before you can share data from an SMB server with SMB clients. When you create a share, you can set share properties, such as designating the share as a home directory. You can also customize the share by configuring optional settings.

### Before you begin

The directory path for the volume or `qtree` must exist in the SVM namespace before creating the share.

### About this task

When you create a share, the default share ACL (default share permissions) is `Everyone / Full Control`. After testing access to the share, you should remove the default share ACL and replace it with a more secure alternative.

### Steps

1. If necessary, create the directory path structure for the share.

The `vserver cifs share create` command checks the path specified in the `-path` option during share creation. If the specified path does not exist, the command fails.

2. Create an SMB share associated with the specified SVM: `vserver cifs share create -vserver`

```
vserver_name -share-name share_name -path path [-share-properties
share_properties,...] [other_attributes] [-comment text]
```

3. Verify that the share was created: `vserver cifs share show -share-name share_name`

## Examples

The following command creates an SMB share named "SHARE1" on SVM `vs1.example.com`. Its directory path is `/users`, and it is created with default properties.

```
cluster1::> vserver cifs share create -vserver vs1.example.com -share-name
SHARE1 -path /users

cluster1::> vserver cifs share show -share-name SHARE1
```

Vserver	Share	Path	Properties	Comment	ACL
vs1.example.com	SHARE1	/users	oplocks	-	Everyone / Full Control
			browsable		
			changenotify		
			show-previous-versions		

## Verify SMB client access

You should verify that you have configured SMB correctly by accessing and writing data to the share. You should test access using the SMB server name and any NetBIOS aliases.

### Steps

1. Log in to a Windows client.
2. Test access using the SMB server name:
  - a. In Windows Explorer, map a drive to the share in the following format: `\\SMB_Server_Name\Share_Name`

If the mapping is not successful, it is possible that the DNS mapping has not yet propagated throughout the network. You must test access using the SMB server name later.

If the SMB server is named `vs1.example.com` and the share is named `SHARE1`, you should enter the following: `\\vs0.example.com\SHARE1`

- b. On the newly created drive, create a test file, and then delete the file.

You have verified write access to the share using the SMB server name.

3. Repeat Step 2 for any NetBIOS aliases.

## Create SMB share access control lists

Configuring share permissions by creating access control lists (ACLs) for SMB shares enables you to control the level of access to a share for users and groups.

### Before you begin

You must have decided which users or groups will be given access to the share.

### About this task

You can configure share-level ACLs by using local or domain Windows user or group names.

Before creating a new ACL, you should delete the default share ACL `Everyone / Full Control`, which poses a security risk.

In workgroup mode, the local domain name is the SMB server name.

### Steps

1. Delete the default share ACL:  
`vserver cifs share access-control delete -vserver vserver_name -share share_name -user-or-group everyone`
2. Configure the new ACL:

If you want to configure ACLs by using a...	Enter the command...
Windows user	<pre>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_domain_name\\user_name -permission access_right</pre>
Windows group	<pre>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_group_name -permission access_right</pre>

3. Verify that the ACL applied to the share is correct by using the `vserver cifs share access-control show` command.

### Example

The following command gives `Change` permissions to the “Sales Team” Windows group for the “sales” share on the “vs1.example.com” SVM:

```

cluster1::> vsserver cifs share access-control create -vsserver
vs1.example.com -share sales -user-or-group "Sales Team" -permission
Change

cluster1::> vsserver cifs share access-control show

```

Vserver	Share Name	User/Group Name	User/Group Type	Access Permission
vs1.example.com	c\$	BUILTIN\Administrators	windows	Full_Control
vs1.example.com	sales	DOMAIN\"Sales Team"	windows	Change

The following commands give Change permission to the local Windows group named "Tiger Team" and Full\_Control permission to the local Windows user named "Sue Chang" for the "datavol5" share on the "vs1" SVM:

```

cluster1::> vsserver cifs share access-control create -vsserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vsserver cifs share access-control create -vsserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vsserver cifs share access-control show -vsserver vs1

```

Vserver	Share Name	User/Group Name	User/Group Type	Access Permission
vs1	c\$	BUILTIN\Administrators	windows	Full_Control
vs1	datavol5	DOMAIN\"Tiger Team"	windows	Change
vs1	datavol5	DOMAIN\"Sue Chang"	windows	Full_Control

### Configure NTFS file permissions in a share

To enable file access to the users or groups who have access to a share, you must configure NTFS file permissions on files and directories in that share from a Windows client.

### Before you begin

The administrator performing this task must have sufficient NTFS permissions to change permissions on the selected objects.

### About this task

[SMB management](#) and your Windows documentation contain information about how to set standard and advanced NTFS permissions.

### Steps

1. Log in to a Windows client as an administrator.
2. From the **Tools** menu in Windows Explorer, select **Map network drive**.
3. Complete the **Map Network Drive** box:
  - a. Select a **Drive** letter.
  - b. In the **Folder** box, type the SMB server name containing the share that contains the data to which you want to apply permissions and the name of the share.

If your SMB server name is SMB\_SERVER01 and your share is named "SHARE1", you would enter \\SMB\_SERVER01\SHARE1.



You can specify the IP address of the data interface for the SMB server instead of the SMB server name.

- c. Click **Finish**.

The drive you selected is mounted and ready with the Windows Explorer window displaying files and folders contained within the share.

4. Select the file or directory for which you want to set NTFS file permissions.
5. Right-click the file or directory, and then select **Properties**.
6. Select the **Security** tab.

The Security tab displays the list of users and groups for which NTFS permission are set. The Permissions for <Object> box displays a list of Allow and Deny permissions in effect for the selected user or group.

7. Click **Edit**.

The Permissions for <Object> box opens.

8. Perform the desired actions:

If you want to....	Do the following...
Set standard NTFS permissions for a new user or group	<ol style="list-style-type: none"><li>a. Click <b>Add</b>.  The Select User, Computers, Service Accounts, or Groups window opens.</li><li>b. In the <b>Enter the object names to select</b> box, type the name of the user or group on which you want to add NTFS permission.</li><li>c. Click <b>OK</b>.</li></ol>

If you want to....	Do the following...
Change or remove standard NTFS permissions from a user or group	In the <b>Group or user names</b> box, select the user or group that you want to change or remove.

9. Perform the desired actions:

If you want to...	Do the following
Set standard NTFS permissions for a new or existing user or group	In the <b>Permissions for &lt;Object&gt;</b> box, select the <b>Allow</b> or <b>Deny</b> boxes for the type of access that you want to allow or not allow for the selected user or group.
Remove a user or group	Click <b>Remove</b> .



If some or all of the standard permission boxes are not selectable, it is because the permissions are inherited from the parent object. The **Special permissions** box is not selectable. If it is selected, it means that one or more of the granular advanced rights has been set for the selected user or group.

10. After you finish adding, removing, or editing NTFS permissions on that object, click **OK**.

### Verify user access

You should test that the users you configured can access the SMB share and the files it contains.

### Steps

1. On a Windows client, log in as one of the users who now has access to the share.
2. From the **Tools** menu in Windows Explorer, select **Map network drive**.
3. Complete the **Map Network Drive** box:
  - a. Select a **Drive** letter.
  - b. In the **Folder** box, type the share name you will provide to users.

If your SMB server name is SMB\_SERVER01 and your share is named "SHARE1", you would enter \\SMB\_SERVER01\share1.

- c. Click **Finish**.

The drive you selected is mounted and ready with the Windows Explorer window displaying files and folders contained within the share.

4. Create a test file, verify that it exists, write text to it, and then remove the test file.

## Manage SMB with the CLI



## SMB reference overview

ONTAP file access features are available for the SMB protocol. You can enable a CIFS server, create shares, and enable Microsoft services.



*SMB* (Server Message Block) refers to modern dialects of the Common Internet File System (CIFS) protocol. You will still see *CIFS* in the ONTAP command-line interface (CLI) and in OnCommand management tools.

You should use these procedures under the following circumstances:

- You want to understand the range of ONTAP SMB protocol capabilities.
- You want to perform less common configuration and maintenance tasks, not basic SMB configuration.
- You want to use the command-line interface (CLI), not System Manager or an automated scripting tool.

## SMB server support

### SMB server support overview

You can enable and configure SMB servers on storage virtual machines (SVMs) to let SMB clients access files on your cluster.

- Each data SVM in the cluster can be bound to exactly one Active Directory domain.
- Data SVMs do not need to be bound to the same domain.
- Multiple SVMs can be bound to the same domain.

You must configure the SVMs and LIFs that you are using to serve data before you can create an SMB server. If your data network is not flat, you might also need to configure IPspaces, broadcast domains, and subnets. The *Network Management Guide* contains details.

### Related information

[Network management](#)

[Modify SMB servers](#)

[System administration](#)

### Supported SMB versions and functionality

Server Message Block (SMB) is a remote file-sharing protocol used by Microsoft Windows clients and servers. In ONTAP 9, all SMB versions are supported; however, default SMB 1.0 support depends on your ONTAP version. You should verify that the ONTAP SMB server supports the clients and functionality required in your environment.

The latest information about which SMB clients and domain controllers ONTAP supports is available in the *Interoperability Matrix Tool*.

SMB 2.0 and later versions are enabled by default for ONTAP 9 SMB servers, and can be enabled or disabled as needed. The following table shows SMB 1.0 support and default configuration.

SMB 1.0 functionality:	In these ONTAP 9 releases:			
	9.0	9.1	9.2	9.3 and later
Is enabled by default	Yes	Yes	Yes	No
Can be enabled or disabled	No	Yes*9.1 P8 or later required.	Yes	Yes



Default settings for SMB 1.0 and 2.0 connections to domain controllers also depend on the ONTAP version. More information is available in the `vserver cifs security modify man` page. For environments with existing CIFS servers running SMB 1.0, you should migrate to a later SMB version as soon as possible to prepare for security and compliance enhancements. Contact your NetApp representative for details.

The following table shows which SMB features are supported in each SMB version. Some SMB features are enabled by default and some require additional configuration.

This functionality:	Requires enablement:	Is supported in ONTAP 9 for these SMB versions:					
		1.0	2.0	2.1	3.0	3.1.1	
Legacy SMB 1.0 functionality		X	X	X	X	X	
Durable handles			X	X	X	X	
Compounded operations			X	X	X	X	
Asynchronous operations			X	X	X	X	
Increased read and write buffer sizes			X	X	X	X	
Increased scalability			X	X	X	X	
SMB signing	X	X	X	X	X	X	

<b>This functionality:</b>	<b>Requires enablement:</b>	<b>Is supported in ONTAP 9 for these SMB versions:</b>				
Alternate Data Stream (ADS) file format	X	X	X	X	X	X
Large MTU (enabled by default beginning with ONTAP 9.7)	X			X	X	X
Lease oplocks				X	X	X
Continuously available shares	X				X	X
Persistent handles					X	X
Witness					X	X
SMB encryption: AES-128-CCM	X				X	X
Scale out (required by CA shares)					X	X
Transparent failover					X	X
SMB Multichannel (beginning with ONTAP 9.4)	X				X	X
Preauthentication integrity						X
Cluster client failover v.2 (CCFv2)						X

This functionality:	Requires enablement:	Is supported in ONTAP 9 for these SMB versions:				
SMB encryption: AES-128-GCM (beginning with ONTAP 9.1)	X					X

**Related information**

[Using SMB signing to enhance network security](#)

[Setting the SMB server minimum authentication security level](#)

[Configuring required SMB encryption on SMB servers for data transfers over SMB](#)

[NetApp Technical Report 4543: SMB Protocol Best Practices](#)

[NetApp Interoperability](#)

**Unsupported Windows features**

Before you use CIFS in your network, you need to be aware of certain Windows features that ONTAP does not support.

ONTAP does not support the following Windows features:

- Encrypted File System (EFS)
- Logging of NT File System (NTFS) events in the change journal
- Microsoft File Replication Service (FRS)
- Microsoft Windows Indexing Service
- Remote storage through Hierarchical Storage Management (HSM)
- Quota management from Windows clients
- Windows quota semantics
- The LMHOSTS file
- NTFS native compression

**Configure NIS or LDAP name services on the SVM**

With SMB access, user mapping to a UNIX user is always performed, even when accessing data in an NTFS security-style volume. If you map Windows users to corresponding UNIX users whose information is stored in NIS or LDAP directory stores, or if you use LDAP for name mapping, you should configure these name services during SMB setup.

**Before you begin**

You must have customized your name services database configuration to match your name service infrastructure.

### About this task

SVMs use the name services ns-switch databases to determine the order in which to look up the sources for a given name service database. The ns-switch source can be any combination of “files”, “nis”, or “ldap”. For the groups database, ONTAP attempts to get the group memberships from all configured sources and then uses the consolidated group membership information for access checks. If one of these sources is unavailable at the time of obtaining UNIX group information, ONTAP cannot get the complete UNIX credentials and subsequent access checks might fail. Therefore, you must always check that all ns-switch sources are configured for the group database in the ns-switch settings.

The default is to have the SMB server map all Windows users to the default UNIX user that is stored in the local `passwd` database. If you want to use the default configuration, configuring NIS or LDAP UNIX user and group name services or LDAP user mapping is optional for SMB access.

### Steps

1. If UNIX user, group, and netgroup information is managed by NIS name services, configure NIS name services:
  - a. Determine the current ordering of name services by using the `vserver services name-service ns-switch show` command.

In this example, the three databases (`group`, `passwd`, and `netgroup`) that can use `nis` as a name service source are using only `files` as a source.

```
vserver services name-service ns-switch show -vserver vs1
```

Vserver	Database	Enabled	Source Order
vs1	hosts	true	dns, files
vs1	group	true	files
vs1	passwd	true	files
vs1	netgroup	true	files
vs1	namemap	true	files

You must add the `nis` source to the `group` and `passwd` databases, and optionally to the `netgroup` database.

- b. Adjust the name service ns-switch database ordering as desired by using the `vserver services name-service ns-switch modify` command.

For best performance, you should not add a name service to a name service database unless you plan on configuring that name service on the SVM.

If you modify the configuration for more than one name service database, you must run the command separately for each name service database that you want to modify.

In this example, `nis` and `files` are configured as sources for the `group` and `passwd` databases, in

that order. The rest of the name service databases are unchanged.

```
vserver services name-service ns-switch modify -vserver vs1 -database group
-sources nis,files
vserver services name-service ns-switch modify -vserver
vs1 -database passwd -sources nis,files
```

- c. Verify that the ordering of name services is correct by using the `vserver services name-service ns-switch show` command.

```
vserver services name-service ns-switch show -vserver vs1
```

Vserver	Database	Enabled	Source Order
vs1	hosts	true	dns, files
vs1	group	true	nis, files
vs1	passwd	true	nis, files
vs1	netgroup	true	files
vs1	namemap	true	files

- d. Create the NIS name service configuration:

```
vserver services name-service nis-domain create -vserver vserver_name
-domain NIS_domain_name -servers NIS_server_IPaddress,... -active true+
```

```
vserver services name-service nis-domain create -vserver vs1 -domain
example.com -servers 10.0.0.60 -active true
```



Beginning with ONTAP 9.2, the field `-nis-servers` replaces the field `-servers`. This new field can take either a hostname or an IP address for the NIS server.

- e. Verify that the NIS name service is properly configured and active: `vserver services name-service nis-domain show vserver vserver_name`

```
vserver services name-service nis-domain show vserver vs1
```

Vserver	Domain	Active	Server
vs1	example.com	true	10.0.0.60

2. If UNIX user, group, and netgroup information or name mapping is managed by LDAP name services, configure LDAP name services by using the information located [NFS management](#).

## How ONTAP name service switch configuration works

ONTAP stores name service configuration information in a table that is the equivalent of the `/etc/nsswitch.conf` file on UNIX systems. You must understand the function of the table and how ONTAP uses it so that you can configure it appropriately for your environment.

The ONTAP name service switch table determines which name service sources ONTAP consults in which order to retrieve information for a certain type of name service information. ONTAP maintains a separate name service switch table for each SVM.

### Database types

The table stores a separate name service list for each of the following database types:

Database type	Defines name service sources for...	Valid sources are...
hosts	Converting host names to IP addresses	files, dns
group	Looking up user group information	files, nis, ldap
passwd	Looking up user information	files, nis, ldap
netgroup	Looking up netgroup information	files, nis, ldap
namemap	Mapping user names	files, ldap

### Source types

The sources specify which name service source to use for retrieving the appropriate information.

Specify source type...	To look up information in...	Managed by the command families...
files	Local source files	<code>vserver services name-service unix-user vserver services name-service unix-group</code>  <code>vserver services name-service netgroup</code>  <code>vserver services name-service dns hosts</code>
nis	External NIS servers as specified in the NIS domain configuration of the SVM	<code>vserver services name-service nis-domain</code>

Specify source type...	To look up information in...	Managed by the command families...
ldap	External LDAP servers as specified in the LDAP client configuration of the SVM	vserver services name-service ldap
dns	External DNS servers as specified in the DNS configuration of the SVM	vserver services name-service dns

Even if you plan to use NIS or LDAP for both data access and SVM administration authentication, you should still include `files` and configure local users as a fallback in case NIS or LDAP authentication fails.

### Protocols used to access external sources

To access the servers for external sources, ONTAP uses the following protocols:

External name service source	Protocol used for access
NIS	UDP
DNS	UDP
LDAP	TCP

### Example

The following example displays the name service switch configuration for the SVM `svm_1`:

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
Source
Vserver      Database      Order
-----
svm_1        hosts         files,
              dns
svm_1        group         files
svm_1        passwd        files
svm_1        netgroup      nis,
              files
```

To look up user or group information, ONTAP consults only local sources `files`. If the query does not return any results, the lookup fails.

To look up `netgroup` information, ONTAP first consults external NIS servers. If the query does not return any results, the local `netgroup` file is checked next.

There are no name service entries for name mapping in the table for the SVM `svm_1`. Therefore, ONTAP consults only local source `files` by default.



## Manage SMB servers

### Modify SMB servers

You can move a SMB server from a workgroup to an Active Directory domain, from a workgroup to another workgroup, or from an Active Directory domain to a workgroup by using the `vserver cifs modify` command.

#### About this task

You can also modify other attributes of the SMB server, such as the SMB server name and administrative status. See the man page for details.

#### Choices

- Move the SMB server from a workgroup to an Active Directory domain:
  - a. Set the administrative status of the SMB server to down.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- b. Move the SMB server from the workgroup to an Active Directory domain: `vserver cifs modify -vserver vserver_name -domain domain_name`

```
Cluster1::>vserver cifs modify -vserver vs1 -domain example.com
```

In order to create an Active Directory machine account for the SMB server, you must supply the name and password of a Windows account with sufficient privileges to add computers to the `ou=example` ou container within the `example.com` domain.

Beginning with ONTAP 9.7, your AD administrator can provide you with a URI to a keytab file as an alternative to providing you with a name and password to a privileged Windows account. When you receive the URI, include it in the `-keytab-uri` parameter with the `vserver cifs` commands.

- Move the SMB server from a workgroup to another workgroup:
  - a. Set the administrative status of the SMB server to down.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- b. Modify the workgroup for the SMB server: `vserver cifs modify -vserver vserver_name -workgroup new_workgroup_name`

```
Cluster1::>vserver cifs modify -vserver vs1 -workgroup workgroup2
```

- Move the SMB server from an Active Directory domain to a workgroup:
  - a. Set the administrative status of the SMB server to down.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- b. Move the SMB server from the Active Directory domain to a workgroup: `vserver cifs modify -vserver vserver_name -workgroup workgroup_name`

```
cluster1::> vserver cifs modify -vserver vs1 -workgroup workgroup1
```



To enter workgroup mode, all domain-based features must be disabled and their configuration removed automatically by the system, including continuously-available shares, shadow copies, and AES. However, domain-configured share ACLs such as "EXAMPLE.COM\userName" will not work properly, but cannot be removed by ONTAP. Remove these share ACLs as soon as possible using external tools after the command completes. If AES is enabled, you may be asked to supply the name and password of a Windows account with sufficient privileges to disable it in the "EXAMPLE.COM" domain.

- Modify other attributes by using the appropriate parameter of the `vserver cifs modify` command.

## Use options to customize SMB servers

### Available SMB server options

It is useful to know what options are available when considering how to customize the SMB server. Although some options are for general use on the SMB server, several are used to enable and configure specific SMB functionality. SMB server options are controlled with the `vserver cifs options modify` option.

The following list specifies the SMB server options that are available at the admin privilege level:

- **Configuring the SMB session timeout value**

Configuring this option enables you to specify the number of seconds of idle time before an SMB session is disconnected. An idle session is a session in which a user does not have any files or directories opened on the client. The default value is 900 seconds.

- **Configuring the default UNIX user**

Configuring this option enables you to specify the default UNIX user that the SMB server uses. ONTAP automatically creates a default user named "pcuser" (with a UID of 65534), creates a group named "pcuser" (with a GID of 65534), and adds the default user to the "pcuser" group. When you create a SMB server, ONTAP automatically configures "pcuser" as the default UNIX user.

- **Configuring the guest UNIX user**

Configuring this option enables you to specify the name of a UNIX user to which users who log in from untrusted domains are mapped, which allows a user from an untrusted domain to connect to the SMB server. By default, this option is not configured (there is no default value); therefore, the default is to not allow users from untrusted domains to connect to the SMB server.

- **Enabling or disabling read grant execution for mode bits**

Enabling or disabling this option enables you to specify whether to allow SMB clients to run executable files with UNIX mode bits to which they have read access, even when the UNIX executable bit is not set. This option is disabled by default.

- **Enabling or disabling the ability to delete read-only files from NFS clients**

Enabling or disabling this option determines whether to allow NFS clients to delete files or folders with the read-only attribute set. NTFS delete semantics does not allow the deletion of a file or folder when the read-only attribute is set. UNIX delete semantics ignores the read-only bit, using the parent directory permissions instead to determine whether a file or folder can be deleted. The default setting is `disabled`, which results in NTFS delete semantics.

- **Configuring Windows Internet Name Service server addresses**

Configuring this option enables you to specify a list of Windows Internet Name Service (WINS) server addresses as a comma-delimited list. You must specify IPv4 addresses. IPv6 addresses are not supported. There is no default value.

The following list specifies the SMB server options that are available at the advanced privilege level:

- **Granting UNIX group permissions to CIFS users**

Configuring this option determines whether the incoming CIFS user who is not the owner of the file can be granted the group permission. If the CIFS user is not the owner of the UNIX security-style file and this parameter is set to `true`, then the group permission is granted for the file. If the CIFS user is not the owner of the UNIX security-style file and this parameter is set to `false`, then the normal UNIX rules are applicable to grant the file permission. This parameter is applicable to UNIX security-style files that have permission set as `mode bits` and is not applicable to files with the NTFS or NFSv4 security mode. The default setting is `false`.

- **Enabling or disabling SMB 1.0**

SMB 1.0 is disabled by default on an SVM for which a SMB server is created in ONTAP 9.3.



Beginning ONTAP 9.3, SMB 1.0 is disabled by default for new SMB servers created in ONTAP 9.3. You should migrate to a later SMB version as soon as possible to prepare for security and compliance enhancements. Contact your NetApp representative for details.

- **Enabling or disabling SMB 2.x**

SMB 2.0 is the minimum SMB version that supports LIF failover. If you disable SMB 2.x, ONTAP also automatically disables SMB 3.X.

SMB 2.0 is supported only on SVMs. The option is enabled by default on SVMs

- **Enabling or disabling SMB 3.0**

SMB 3.0 is the minimum SMB version that supports continuously available shares. Windows Server 2012 and Windows 8 are the minimum Windows versions that support SMB 3.0.

SMB 3.0 is supported only on SVMs. The option is enabled by default on SVMs

- **Enabling or disabling SMB 3.1**

Windows 10 is the only Windows version that supports SMB 3.1.

SMB 3.1 is supported only on SVMs. The option is enabled by default on SVMs

- **Enabling or disabling ODX copy offload**

ODX copy offload is used automatically by Windows clients that support it. This option is enabled by default.

- **Enabling or disabling the direct-copy mechanism for ODX copy offload**

The direct-copy mechanism increases the performance of the copy offload operation when Windows clients try to open the source file of a copy in a mode that prevents the file being changed while the copy is in progress. By default, the direct copy mechanism is enabled.

- **Enabling or disabling automatic node referrals**

With automatic node referrals, the SMB server automatically refers clients to a data LIF local to the node that hosts the data accessed through the requested share.

- **Enabling or disabling export policies for SMB**

This option is disabled by default.

- **Enabling or disabling using junction points as reparse points**

If this option is enabled, the SMB server exposes junction points to SMB clients as reparse points. This option is valid only for SMB 2.x or SMB 3.0 connections. This option is enabled by default.

This option is supported only on SVMs. The option is enabled by default on SVMs

- **Configuring the number of maximum simultaneous operations per TCP connection**

The default value is 255.

- **Enabling or disabling local Windows users and groups functionality**

This option is enabled by default.

- **Enabling or disabling local Windows users authentication**

This option is enabled by default.

- **Enabling or disabling VSS shadow copy functionality**

ONTAP uses the shadow copy functionality to perform remote backups of data stored using the Hyper-V over SMB solution.

This option is supported only on SVMs, and only for Hyper-V over SMB configurations. The option is enabled by default on SVMs

- **Configuring the shadow copy directory depth**

Configuring this option enables you to define the maximum depth of directories on which to create shadow

copies when using the shadow copy functionality.

This option is supported only on SVMs, and only for Hyper-V over SMB configurations. The option is enabled by default on SVMs

- **Enabling or disabling multidomain search capabilities for name mapping**

If enabled, when a UNIX user is mapped to a Windows domain user by using a wildcard (\*) in the domain portion of the Windows user name (for example, \*\\joe), ONTAP searches for the specified user in all of the domains with bidirectional trusts to the home domain. The home domain is the domain that contains the SMB server's computer account.

As an alternative to searching all of the bidirectionally trusted domains, you can configure a list of preferred trusted domains. If this option is enabled and a preferred list is configured, the preferred list is used to perform multidomain name mapping searches.

The default is to enable multidomain name mapping searches.

- **Configuring the file system sector size**

Configuring this option enables you to configure the file system sector size in bytes that ONTAP reports to SMB clients. There are two valid values for this option: 4096 and 512. The default value is 4096. You might need to set this value to 512 if the Windows application supports only a sector size of 512 bytes.

- **Enabling or disabling Dynamic Access Control**

Enabling this option enables you to secure objects on the SMB server by using Dynamic Access Control (DAC), including using auditing to stage central access policies and using Group Policy Objects to implement central access policies. The option is disabled by default.

This option is supported only on SVMs.

- **Setting the access restrictions for non-authenticated sessions (restrict anonymous)**

Setting this option determines what the access restrictions are for non-authenticated sessions. The restrictions are applied to anonymous users. By default, there are no access restrictions for anonymous users.

- **Enabling or disabling the presentation of NTFS ACLs on volumes with UNIX effective security (UNIX security-style volumes or mixed security-style volumes with UNIX effective security)**

Enabling or disabling this option determines how file security on files and folders with UNIX security is presented to SMB clients. If enabled, ONTAP presents files and folders in volumes with UNIX security to SMB clients as having NTFS file security with NTFS ACLs. If disabled, ONTAP presents volumes with UNIX security as FAT volumes, with no file security. By default, volumes are presented as having NTFS file security with NTFS ACLs.

- **Enabling or disabling the SMB fake open functionality**

Enabling this functionality improves SMB 2.x and SMB 3.0 performance by optimizing how ONTAP makes open and close requests when querying for attribute information on files and directories. By default, the SMB fake open functionality is enabled. This option is useful only for connections that are made with SMB 2.x or later.

- **Enabling or disabling the UNIX extensions**

Enabling this option enables UNIX extensions on a SMB server. UNIX extensions allow POSIX/UNIX style security to be displayed through the SMB protocol. By default this option is disabled.

If you have UNIX-based SMB clients, such as Mac OSX clients, in your environment, you should enable UNIX extensions. Enabling UNIX extensions allows the SMB server to transmit POSIX/UNIX security information over SMB to the UNIX-based client, which then translates the security information into POSIX/UNIX security.

- **Enabling or disabling support for short name searches**

Enabling this option allows the SMB server to perform searches on short names. A search query with this option enabled tries to match 8.3 file names along with long file names. The default value for this parameter is `false`.

- **Enabling or disabling support for automatic advertisement of DFS capabilities**

Enabling or disabling this option determines whether SMB servers automatically advertise DFS capabilities to SMB 2.x and SMB 3.0 clients that connect to shares. ONTAP uses DFS referrals in the implementation of symbolic links for SMB access. If enabled, the SMB server always advertises DFS capabilities regardless of whether symbolic link access is enabled. If disabled, the SMB server advertises DFS capabilities only when the clients connect to shares where symbolic link access is enabled.

- **Configuring the maximum number of SMB credits**

Beginning with ONTAP 9.4, configuring the `-max-credits` option allows you to limit the number of credits to be granted on an SMB connection when clients and server are running SMB version 2 or later. The default value is 128.

- **Enabling or disabling support for SMB Multichannel**

Enabling the `-is-multichannel-enabled` option in ONTAP 9.4 and later releases allows the SMB server to establish multiple connections for a single SMB session when appropriate NICs are deployed on the cluster and its clients. Doing so improves throughput and fault tolerance. The default value for this parameter is `false`.

When SMB Multichannel is enabled, you can also specify the following parameters:

- The maximum number of connections allowed per Multichannel session. The default value for this parameter is 32.
- The maximum number of network interfaces advertised per Multichannel session. The default value for this parameter is 256.

## Configuring SMB server options

You can configure SMB server options at any time after you have created a SMB server on a storage virtual machine (SVM).

### Step

1. Perform the desired action:

If you want to configure SMB server options...	Enter the command...
At admin-privilege level	<code>vserver cifs options modify -vserver vserver_name options</code>
At advanced-privilege level	<ul style="list-style-type: none"> <li>a. <code>set -privilege advanced</code></li> <li>b. <code>vserver cifs options modify -vserver vserver_name options</code></li> <li>c. <code>set -privilege admin</code></li> </ul>

For more information about configuring SMB server options, see the man page for the `vserver cifs options modify` command.

### Configure the grant UNIX group permission to SMB users

You can configure this option to grant group permissions to access files or directories even if the incoming SMB user is not the owner of the file.

#### Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Configure the grant UNIX group permission as appropriate:

If you want to	Enter the command
Enable the access to the files or directories to get group permissions even if the user is not the owner of the file	<code>vserver cifs options modify -grant-unix-group-perms-to-others true</code>
Disable the access to the files or directories to get group permissions even if the user is not the owner of the file	<code>vserver cifs options modify -grant-unix-group-perms-to-others false</code>

3. Verify that the option is set to the desired value: `vserver cifs options show -fields grant-unix-group-perms-to-others`
4. Return to the admin privilege level: `set -privilege admin`

### Configure access restrictions for anonymous users

By default, an anonymous, unauthenticated user (also known as the *null user*) can access certain information on the network. You can use a SMB server option to configure access restrictions for the anonymous user.

#### About this task

The `-restrict-anonymous` SMB server option corresponds to the `RestrictAnonymous` registry entry in Windows.

Anonymous users can list or enumerate certain types of system information from Windows hosts on the

network, including user names and details, account policies, and share names. You can control access for the anonymous user by specifying one of three access restriction settings:

Value	Description
<code>no-restriction</code> (default)	Specifies no access restrictions for anonymous users.
<code>no-enumeration</code>	Specifies that only enumeration is restricted for anonymous users.
<code>no-access</code>	Specifies that access is restricted for anonymous users.

### Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Configure the restrict anonymous setting: `vserver cifs options modify -vserver vserver_name -restrict-anonymous {no-restriction|no-enumeration|no-access}`
3. Verify that the option is set to the desired value: `vserver cifs options show -vserver vserver_name`
4. Return to the admin privilege level: `set -privilege admin`

### Related information

[Available SMB server options](#)

### Manage how file security is presented to SMB clients for UNIX security-style data

#### Manage how file security is presented to SMB clients for UNIX security-style data overview

You can choose how you want to present file security to SMB clients for UNIX security-style data by enabling or disabling the presentation of NTFS ACLs to SMB clients. There are advantages with each setting, which you should understand to choose the setting best suited for your business requirements.

By default, ONTAP presents UNIX permissions on UNIX security-style volumes to SMB clients as NTFS ACLs. There are scenarios where this is desirable, including the following:

- You want to view and edit UNIX permissions by using the **Security** tab in the Windows Properties box.

You cannot modify permissions from a Windows client if the operation is not permitted by the UNIX system. For example, you cannot change the ownership of a file you do not own, because the UNIX system does not permit this operation. This restriction prevents SMB clients from bypassing UNIX permissions set on the files and folders.

- Users are editing and saving files on the UNIX security-style volume by using certain Windows applications, for example Microsoft Office, where ONTAP must preserve UNIX permissions during save operations.
- There are certain Windows applications in your environment that expect to read NTFS ACLs on files they use.



Under certain circumstances, you might want to disable the presentation of UNIX permissions as NTFS ACLs. If this functionality is disabled, ONTAP presents UNIX security-style volumes as FAT volumes to SMB clients. There are specific reasons why you might want to present UNIX security-style volumes as FAT volumes to SMB clients:

- You only change UNIX permissions by using mounts on UNIX clients.

The Security tab is not available when a UNIX security-style volume is mapped on an SMB client. The mapped drive appears to be formatted with the FAT file system, which has no file permissions.

- You are using applications over SMB that set NTFS ACLs on accessed files and folders, which can fail if the data resides on UNIX security-style volumes.

If ONTAP reports the volume as FAT, the application does not try to change an ACL.

## Related information

[Configuring security styles on FlexVol volumes](#)

[Configuring security styles on qtrees](#)

## Enable or disable the presentation of NTFS ACLs for UNIX security-style data

You can enable or disable the presentation of NTFS ACLs to SMB clients for UNIX security-style data (UNIX security-style volumes and mixed security-style volumes with UNIX effective security).

### About this task

If you enable this option, ONTAP presents files and folders on volumes with effective UNIX security style to SMB clients as having NTFS ACLs. If you disable this option, the volumes are presented as FAT volumes to SMB clients. The default is to present NTFS ACLs to SMB clients.

### Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Configure the UNIX NTFS ACL option setting: `vserver cifs options modify -vserver vserver_name -is-unix-nt-acl-enabled {true|false}`
3. Verify that the option is set to the desired value: `vserver cifs options show -vserver vserver_name`
4. Return to the admin privilege level: `set -privilege admin`

## How ONTAP preserves UNIX permissions

When files in a FlexVol volume that currently have UNIX permissions are edited and saved by Windows applications, ONTAP can preserve the UNIX permissions.

When applications on Windows clients edit and save files, they read the security properties of the file, create a new temporary file, apply those properties to the temporary file, and then give the temporary file the original file name.

When Windows clients perform a query for the security properties, they receive a constructed ACL that exactly represents the UNIX permissions. The sole purpose of this constructed ACL is to preserve the file's UNIX permissions as files are updated by Windows applications to ensure that the resulting files have the same

UNIX permissions. ONTAP does not set any NTFS ACLs using the constructed ACL.

## Manage UNIX permissions using the Windows Security tab

If you want to manipulate UNIX permissions of files or folders in mixed security-style volumes or qtrees on SVMs, you can use the Security tab on Windows clients. Alternatively, you can use applications that can query and set Windows ACLs.

- Modifying UNIX permissions

You can use the Windows Security tab to view and change UNIX permissions for a mixed security-style volume or qtree. If you use the main Windows Security tab to change UNIX permissions, you must first remove the existing ACE you want to edit (this sets the mode bits to 0) before you make your changes. Alternatively, you can use the Advanced editor to change permissions.

If mode permissions are used, you can directly change the mode permissions for the listed UID, GID, and others (everyone else with an account on the computer). For example, if the displayed UID has r-x permissions, you can change the UID permissions to rwx.

- Changing UNIX permissions to NTFS permissions

You can use the Windows Security tab to replace UNIX security objects with Windows security objects on a mixed security-style volume or qtree where the files and folders have a UNIX effective security style.

You must first remove all listed UNIX permission entries before you can replace them with the desired Windows User and Group objects. You can then configure NTFS-based ACLs on the Windows User and Group objects. By removing all UNIX security objects and adding only Windows Users and Groups to a file or folder in a mixed security-style volume or qtree, you change the effective security style on the file or folder from UNIX to NTFS.

When changing permissions on a folder, the default Windows behavior is to propagate these changes to all subfolders and files. Therefore, you must change the propagation choice to the desired setting if you do not want to propagate a change in security style to all child folders, subfolders, and files.

## Manage SMB server security settings

### How ONTAP handles SMB client authentication

Before users can create SMB connections to access data contained on the SVM, they must be authenticated by the domain to which the SMB server belongs. The SMB server supports two authentication methods, Kerberos and NTLM (NTLMv1 or NTLMv2). Kerberos is the default method used to authenticate domain users.

### Kerberos authentication

ONTAP supports Kerberos authentication when creating authenticated SMB sessions.

Kerberos is the primary authentication service for Active Directory. The Kerberos server, or Kerberos Key Distribution Center (KDC) service, stores and retrieves information about security principles in the Active Directory. Unlike the NTLM model, Active Directory clients who want to establish a session with another computer, such the SMB server, contact a KDC directly to obtain their session credentials.

## NTLM authentication

NTLM client authentication is done using a challenge response protocol based on shared knowledge of a user-specific secret based on a password.

If a user creates an SMB connection using a local Windows user account, authentication is done locally by the SMB server using NTLMv2.

### Guidelines for SMB server security settings in an SVM disaster recovery configuration

Before creating an SVM that is configured as a disaster recovery destination where the identity is not preserved (the `-identity-preserve` option is set to `false` in the SnapMirror configuration), you should know about how SMB server security settings are managed on the destination SVM.

- Non-default SMB server security settings are not replicated to the destination.

When you create a SMB server on the destination SVM, all SMB server security settings are set to default values. When the SVM disaster recovery destination is initialized, updated, or resynced, the SMB server security settings on the source are not replicated to the destination.

- You must manually configure non-default SMB server security settings.

If you have non-default SMB server security settings configured on the source SVM, you must manually configure these same settings on the destination SVM after the destination becomes read-write (after the SnapMirror relationship is broken).

### Display information about SMB server security settings

You can display information about SMB server security settings on your storage virtual machines (SVMs). You can use this information to verify that the security settings are correct.

#### About this task

A displayed security setting can be the default value for that object or a non-default value that is configured either by using the ONTAP CLI or by using Active Directory group policy objects (GPOs).

Do not use the `vserver cifs security show` command for SMB servers in workgroup mode, because some of the options are not valid.

#### Step

1. Perform one of the following actions:

If you want display information about...	Enter the command...
All security settings on a specified SVM	<pre>vserver cifs security show -vserver vserver_name</pre>

If you want display information about...	Enter the command...
A specific security setting or settings on the SVM	<code>vserver cifs security show -vserver _vserver_name_ -fields [fieldname,...]</code> You can enter <code>-fields ?</code> to determine what fields you can use.

### Example

The following example shows all security settings for SVM vs1:

```
cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                Kerberos Clock Skew:           5 minutes
                Kerberos Ticket Age:            10 hours
                Kerberos Renewal Age:           7 days
                Kerberos KDC Timeout:           3 seconds
                Is Signing Required:            false
                Is Password Complexity Required: true
                Use start_tls For AD LDAP connection: false
                Is AES Encryption Enabled:       false
                LM Compatibility Level:          lm-ntlm-ntlmv2-krb
                Is SMB Encryption Required:       false
                Client Session Security:         none
                SMB1 Enabled for DC Connections: false
                SMB2 Enabled for DC Connections: system-default
                LDAP Referral Enabled For AD LDAP connections: false
                Use LDAPS for AD LDAP connection: false
                Encryption is required for DC Connections: false
                AES session key enabled for NetLogon channel: false
                Try Channel Binding For AD LDAP Connections: false
```

Note that the settings displayed depend on the running ONTAP version.

The following example shows the Kerberos clock skew for SVM vs1:

```
cluster1::> vserver cifs security show -vserver vs1 -fields kerberos-
clock-skew

                vserver kerberos-clock-skew
                -----
                vs1      5
```

### Related information

## Displaying information about GPO configurations

### Enable or disable required password complexity for local SMB users

Required password complexity provides enhanced security for local SMB users on your storage virtual machines (SVMs). The required password complexity feature is enabled by default. You can disable it and reenable it at any time.

#### Before you begin

Local users, local groups, and local user authentication must be enabled on the CIFS server.



#### About this task

You must not use the `vserver cifs security modify` command for a CIFS server in workgroup mode because some of the options are not valid.

#### Steps

1. Perform one of the following actions:

If you want required password complexity for local SMB users to be...	Enter the command...
Enabled	<pre>vserver cifs security modify -vserver vserver_name -is-password-complexity -required true</pre>
Disabled	<pre>vserver cifs security modify -vserver vserver_name -is-password-complexity -required false</pre>

2. Verify the security setting for required password complexity: `vserver cifs security show -vserver vserver_name`

#### Example

The following example shows that required password complexity is enabled for local SMB users for SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password  
-complexity-required true  
  
cluster1::> vserver cifs security show -vserver vs1 -fields is-password-  
complexity-required  
vserver is-password-complexity-required  
-----  
vs1      true
```

#### Related information

[Displaying information about CIFS server security settings](#)

## Using local users and groups for authentication and authorization

### Requirements for local user passwords

### Changing local user account passwords

#### Modify the CIFS server Kerberos security settings

You can modify certain CIFS server Kerberos security settings, including the maximum allowed Kerberos clock skew time, the Kerberos ticket lifetime, and the maximum number of ticket renewal days.

#### About this task

Modifying CIFS server Kerberos settings by using the `vserver cifs security modify` command modifies the settings only on the single storage virtual machine (SVM) that you specify with the `-vserver vserver_name` parameter. You can centrally manage Kerberos security settings for all SVMs on the cluster belonging to the same Active Directory domain by using Active Directory group policy objects (GPOs).

#### Steps

1. Perform one or more of the following actions:

If you want to...	Enter...
Specify the maximum allowed Kerberos clock skew time in minutes.	<pre>vserver cifs security modify -vserver vserver_name -kerberos-clock-skew integer_in_minutes</pre> <p>The default setting is 5 minutes.</p>
Specify the Kerberos ticket lifetime in hours.	<pre>vserver cifs security modify -vserver vserver_name -kerberos-ticket-age integer_in_hours</pre> <p>The default setting is 10 hours.</p>
Specify the maximum number of ticket renewal days.	<pre>vserver cifs security modify -vserver vserver_name -kerberos-renew-age integer_in_days</pre> <p>The default setting is 7 days.</p>
Specify the timeout for sockets on KDCs after which all KDCs are marked as unreachable.	<pre>vserver cifs security modify -vserver vserver_name -kerberos-kdc-timeout integer_in_seconds</pre> <p>The default setting is 3 seconds.</p>

2. Verify the Kerberos security settings:

```
vserver cifs security show -vserver vserver_name
```

## Example

The following example makes the following changes to Kerberos security: “Kerberos Clock Skew” is set to 3 minutes and “Kerberos Ticket Age” is set to 8 hours for SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew
3 -kerberos-ticket-age 8

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                Kerberos Clock Skew:                3 minutes
                Kerberos Ticket Age:                 8 hours
                Kerberos Renewal Age:                 7 days
                Kerberos KDC Timeout:                 3 seconds
                Is Signing Required:                   false
                Is Password Complexity Required:       true
                Use start_tls For AD LDAP connection:  false
                Is AES Encryption Enabled:             false
                LM Compatibility Level: lm-ntlm-ntlmv2-krb
                Is SMB Encryption Required:            false
```

## Related information

[Displaying information about CIFS server security settings](#)

[Supported GPOs](#)

[Applying Group Policy Objects to CIFS servers](#)

### Set the SMB server minimum authentication security level

You can set the SMB server minimum security level, also known as the *LMCompatibilityLevel*, on your SMB server to meet your business security requirements for SMB client access. The minimum security level is the minimum level of the security tokens that the SMB server accepts from SMB clients.



#### About this task

- SMB servers in workgroup mode support only NTLM authentication. Kerberos authentication is not supported.
- *LMCompatibilityLevel* applies only to SMB client authentication, not admin authentication.

You can set the minimum authentication security level to one of four supported security levels.

Value	Description
lm-ntlm-ntlmv2-krb (default)	The storage virtual machine (SVM) accepts LM, NTLM, NTLMv2, and Kerberos authentication security.
ntlm-ntlmv2-krb	The SVM accepts NTLM, NTLMv2, and Kerberos authentication security. The SVM denies LM authentication.
ntlmv2-krb	The SVM accepts NTLMv2 and Kerberos authentication security. The SVM denies LM and NTLM authentication.
krb	The SVM accepts Kerberos authentication security only. The SVM denies LM, NTLM, and NTLMv2 authentication.

### Steps

1. Set the minimum authentication security level: `vserver cifs security modify -vserver vserver_name -lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. Verify that the authentication security level is set to the desired level: `vserver cifs security show -vserver vserver_name`

### Related information

[Enabling or disabling AES encryption for Kerberos-based communication](#)

#### Configure strong security for Kerberos-based communication by using AES encryption

For strongest security with Kerberos-based communication, you can enable AES-256 and AES-128 encryption on the SMB server. By default, when you create a SMB server on the SVM, AES encryption is disabled. You must enable it to take advantage of the strong security provided by Advanced Encryption Standard (AES) encryption.

Kerberos-related communication for SMB is used during SMB server creation on the SVM, as well as during the SMB session setup phase. The SMB server supports the following encryption types for Kerberos communication:

- RC4-HMAC
- DES
- AES 128
- AES 256

If you want to use the highest security encryption type for Kerberos communication, you should enable AES encryption for Kerberos communication on the SVM.





Intel AES New Instructions (Intel AES NI) is available in SMB 3.0, improving on the AES algorithm and accelerating data encryption with supported processor families. Beginning with SMB 3.1.1, AES-128-GCM replaces AES-128-CCM as the hash algorithm used by SMB encryption.

When the SMB server is created, the domain controller creates a computer machine account in Active Directory. At this time, the KDC becomes aware of the encryption capabilities of the particular machine account. Subsequently, a particular encryption type is selected for encrypting the service ticket that the client presents to the server during authentication.

### Related information

[Modifying the CIFS server Kerberos security settings](#)

### Enable or disable AES encryption for Kerberos-based communication

To take advantage of the strongest security with Kerberos-based communication, you can enable AES-256 and AES-128 encryption on the SMB server. If you do not want the SMB server to select the AES encryption types for Kerberos-based communication with the Active Directory (AD) KDC, you can disable AES encryption. By default, AES encryption is disabled.

### About this task

To enhance security, the storage virtual machine (SVM) changes its machine account password in the AD each time the AES security option is modified. Changing the password might require administrative AD credentials for the organizational unit (OU) that contains the machine account.

If an SVM is configured as a disaster recovery destination where the identity is not preserved (the `-identity -preserve` option is set to `false` in the SnapMirror configuration), the non-default SMB server security settings are not replicated to the destination. If you have enabled AES encryption on the source SVM, you must manually enable it on the destination SVM after the destination becomes read-write (after the SnapMirror relationship is broken).

### Steps

1. Perform one of the following actions:

If you want the AES encryption types for Kerberos communication to be...	Enter the command...
Enabled	<pre>vserver cifs security modify -vserver vserver_name -is-aes-encryption -enabled true</pre>
Disabled	<pre>vserver cifs security modify -vserver vserver_name -is-aes-encryption -enabled false</pre>

2. Verify that AES encryption is enabled or disabled as desired: `vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled`

The `is-aes-encryption-enabled` field displays `true` if AES encryption is enabled and `false` if it is

disabled.

### Example

The following example enables the AES encryption types for the CIFS server on SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-aes-encryption
-enabled true

cluster1::> vserver cifs security show -vserver vs1 -fields is-aes-
encryption-enabled
vserver  is-aes-encryption-enabled
-----
vs1      true
```

The following example enables the AES encryption types for the SMB server on SVM vs2. The administrator is prompted to enter the administrative AD credentials for the OU containing the SMB server.

```
cluster1::> vserver cifs security modify -vserver vs2 -is-aes-encryption
-enabled true

Info: In order to enable SMB AES encryption, the password for the SMB
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields is-aes-
encryption-enabled
vserver  is-aes-encryption-enabled
-----
vs2      true
```

### Use SMB signing to enhance network security

#### Use SMB signing to enhance network security overview

SMB signing helps to ensure that network traffic between the SMB server and the client is not compromised; it does this by preventing replay attacks. By default, ONTAP supports SMB signing when requested by the client. Optionally, the storage administrator can configure the SMB server to require SMB signing.

## How SMB signing policies affect communication with a CIFS server

In addition to the CIFS server SMB signing security settings, two SMB signing policies on Windows clients control the digital signing of communications between clients and the CIFS server. You can configure the setting that meets your business requirements.

Client SMB policies are controlled through Windows local security policy settings, which are configured by using the Microsoft Management Console (MMC) or Active Directory GPOs. For more information about client SMB signing and security issues, see the Microsoft Windows documentation.

Here are descriptions of the two SMB signing policies on Microsoft clients:

- `Microsoft network client: Digitally sign communications (if server agrees)`

This setting controls whether the client's SMB signing capability is enabled. It is enabled by default. When this setting is disabled on the client, the client communications with the CIFS server depends on the SMB signing setting on the CIFS server.

- `Microsoft network client: Digitally sign communications (always)`

This setting controls whether the client requires SMB signing to communicate with a server. It is disabled by default. When this setting is disabled on the client, SMB signing behavior is based on the policy setting for `Microsoft network client: Digitally sign communications (if server agrees)` and the setting on the CIFS server.



If your environment includes Windows clients configured to require SMB signing, you must enable SMB signing on the CIFS server. If you do not, the CIFS server cannot serve data to these systems.

The effective results of client and CIFS server SMB signing settings depends on whether the SMB sessions uses SMB 1.0 or SMB 2.x and later.

The following table summarizes the effective SMB signing behavior if the session uses SMB 1.0:

Client	ONTAP—signing not required	ONTAP—signing required
Signing disabled and not required	Not signed	Signed
Signing enabled and not required	Not signed	Signed
Signing disabled and required	Signed	Signed
Signing enabled and required	Signed	Signed



Older Windows SMB 1 clients and some non-Windows SMB 1 clients might fail to connect if signing is disabled on the client but required on the CIFS server.

The following table summarizes the effective SMB signing behavior if the session uses SMB 2.x or SMB 3.0:



For SMB 2.x and SMB 3.0 clients, SMB signing is always enabled. It cannot be disabled.

Client	ONTAP—signing not required	ONTAP—signing required
Signing not required	Not signed	Signed
Signing required	Signed	Signed

The following table summarizes the default Microsoft client and server SMB signing behavior:

Protocol	Hash algorithm	Can enable/disable	Can require/not require	Client default	Server default	DC default
SMB 1.0	MD5	Yes	Yes	Enabled (not required)	Disabled (not required)	Required
SMB 2.x	HMAC SHA-256	No	Yes	Not required	Not required	Required
SMB 3.0	AES-CMAC.	No	Yes	Not required	Not required	Required



Microsoft no longer recommends using Digitally sign communications (if client agrees) or Digitally sign communications (if server agrees) Group Policy settings. Microsoft also no longer recommends using the EnableSecuritySignature registry settings. These options only affect the SMB 1 behavior and can be replaced by the Digitally sign communications (always) Group Policy setting or the RequireSecuritySignature registry setting. You can also get more information from the Microsoft Blog <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>[The Basics of SMB Signing (covering both SMB1 and SMB2)]

### Performance impact of SMB signing

When SMB sessions use SMB signing, all SMB communications to and from Windows clients experience a performance impact, which affects both the clients and the server (that is, the nodes on the cluster running the SVM containing the SMB server).

The performance impact shows as increased CPU usage on both the clients and the server, although the amount of network traffic does not change.

The extent of the performance impact depends on the version of ONTAP 9 you are running. Beginning with ONTAP 9.7, a new encryption off-load algorithm can enable better performance in signed SMB traffic. SMB signing offload is enabled by default when SMB signing is enabled.

Enhanced SMB signing performance requires AES-NI offload capability. See the Hardware Universe (HWU) to verify that AES-NI offload is supported for your platform.

Further performance improvements are also possible if you are able to use SMB version 3.11 (supported with Windows 10 and Windows Server 2016), which supports the much faster GCM algorithm.

Depending on your network, ONTAP 9 version, SMB version, and SVM implementation, the performance

impact of SMB signing can vary widely; you can verify it only through testing in your network environment.

Most Windows clients negotiate SMB signing by default if it is enabled on the server. If you require SMB protection for some of your Windows clients, and if SMB signing is causing performance issues, you can disable SMB signing on any of your Windows clients that do not require protection against replay attacks. For information about disabling SMB signing on Windows clients, see the Microsoft Windows documentation.

### Recommendations for configuring SMB signing

You can configure SMB signing behavior between SMB clients and the CIFS server to meet your security requirements. The settings you choose when configuring SMB signing on your CIFS server are dependent on what your security requirements are.

You can configure SMB signing on either the client or the CIFS server. Consider the following recommendations when configuring SMB signing:

If...	Recommendation...
You want to increase the security of the communication between the client and the server	Make SMB signing required at the client by enabling the <code>Require Option (Sign always)</code> security setting on the client.
You want all SMB traffic to a certain storage virtual machine (SVM) signed	Make SMB signing required on the CIFS server by configuring the security settings to require SMB signing.

See Microsoft documentation for more information on configuring Windows client security settings.

### Guidelines for SMB signing when multiple data LIFS are configured

If you enable or disable required SMB signing on the SMB server, you should be aware of the guidelines for multiple data LIFS configurations for an SVM.

When you configure a SMB server, there might be multiple data LIFs configured. If so, the DNS server contains multiple `A` record entries for the CIFS server, all using the same SMB server host name, but each with a unique IP address. For example, a SMB server that has two data LIFs configured might have the following DNS `A` record entries:

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

The normal behavior is that upon changing the required SMB signing setting, only new connections from clients are affected by the change in the SMB signing setting. However, there is an exception to this behavior. There is a case where a client has an existing connection to a share, and the client creates a new connection to the same share after the setting is changed, while maintaining the original connection. In this case, both the new and the existing SMB connection adopt the new SMB signing requirements.

Consider the following example:

1. Client1 connects to a share without required SMB signing using the path `o:\.`

2. The storage administrator modifies the SMB server configuration to require SMB signing.
3. Client1 connects to the same share with required SMB signing using the path `s:\` (while maintaining the connection using the path `o:\`).
4. The result is that SMB signing is used when accessing data over both the `o:\` and `s:\` drives.

### Enable or disable required SMB signing for incoming SMB traffic

You can enforce the requirement for clients to sign SMB messages by enabling required SMB signing. If enabled, ONTAP accepts SMB messages only if they have valid signatures. If you want to permit SMB signing, but not require it, you can disable required SMB signing.

#### About this task

By default, required SMB signing is disabled. You can enable or disable required SMB signing at any time.

SMB signing is not disabled by default under the following circumstances:



1. Required SMB signing is enabled, and the cluster is reverted to a version of ONTAP that does not support SMB signing.
2. The cluster is subsequently upgraded to a version of ONTAP that supports SMB signing.

Under these circumstances, the SMB signing configuration that was originally configured on a supported version of ONTAP is retained through reversion and subsequent upgrade.

When you set up a storage virtual machine (SVM) disaster recovery relationship, the value that you select for the `-identity-preserve` option of the `snapmirror create` command determines the configuration details that are replicated in the destination SVM.

If you set the `-identity-preserve` option to `true` (ID-preserve), the SMB signing security setting is replicated to the destination.

If you set the `-identity-preserve` option to `false` (non-ID-preserve), the SMB signing security setting is not replicated to the destination. In this case, the CIFS server security settings on the destination are set to the default values. If you have enabled required SMB signing on the source SVM, you must manually enable required SMB signing on the destination SVM.

#### Steps

1. Perform one of the following actions:

If you want required SMB signing to be...	Enter the command...
Enabled	<code>vserver cifs security modify -vserver <i>vserver_name</i> -is-signing-required true</code>
Disabled	<code>vserver cifs security modify -vserver <i>vserver_name</i> -is-signing-required false</code>

2. Verify that required SMB signing is enabled or disabled by determining whether the value in the `Is Signing Required` field in the output of the following command is set to the desired value: `vserver cifs security show -vserver vserver_name -fields is-signing-required`

### Example

The following example enables required SMB signing for SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required
true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-
required
vserver  is-signing-required
-----  -----
vs1      true
```

### Determine whether SMB sessions are signed

You can display information about connected SMB sessions on the CIFS server. You can use this information to determine whether SMB sessions are signed. This can be helpful in determining whether SMB client sessions are connecting with the desired security settings.

### Steps

1. Perform one of the following actions:

If you want display information about...	Enter the command...
All signed sessions on a specified storage virtual machine (SVM)	<code>vserver cifs session show -vserver vserver_name -is-session-signed true</code>
Details for a signed session with a specific session ID on the SVM	<code>vserver cifs session show -vserver vserver_name -session-id integer -instance</code>

### Examples

The following command displays session information about signed sessions on SVM vs1. The default summary output does not display the “Is Session Signed” output field:

```

cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
Node:    node1
Vserver: vs1
Connection Session
ID       ID       Workstation      Windows User      Open      Idle
-----  -
3151272279  1       10.1.1.1        DOMAIN\joe        2         23s

```

The following command displays detailed session information, including whether the session is signed, on an SMB session with a session ID of 2:

```

cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
Node: node1
Vserver: vs1
Session ID: 2
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\joe
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: CIFS_ALIAS1
SMB Encryption Status: Unencrypted

```

## Related information

[Monitoring SMB signed session statistics](#)

## Monitor SMB signed session statistics

You can monitor SMB sessions statistics and determine which established sessions are signed and which are not.

### About this task

The `statistics` command at the advanced privilege level provides the `signed_sessions` counter that you can use to monitor the number of signed SMB sessions. The `signed_sessions` counter is available with the following statistics objects:



- `cifs` enables you to monitor SMB signing for all SMB sessions.
- `smb1` enables you to monitor SMB signing for SMB 1.0 sessions.
- `smb2` enables you to monitor SMB signing for SMB 2.x and SMB 3.0 sessions.



SMB 3.0 statistics are included in the output for the `smb2` object.

If you want to compare the number of signed session to the total number of sessions, you can compare output for the `signed_sessions` counter with the output for the `established_sessions` counter.

You must start a statistics sample collection before you can view the resultant data. You can view data from the sample if you do not stop data collection. Stopping data collection gives you a fixed sample. Not stopping data collection gives you the ability to get updated data that you can use to compare against previous queries. The comparison can help you identify trends.

### Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Start a data collection: `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]`

If you do not specify the `-sample-id` parameter, the command generates a sample identifier for you and defines this sample as the default sample for the CLI session. The value for `-sample-id` is a text string. If you run this command during the same CLI session and do not specify the `-sample-id` parameter, the command overwrites the previous default sample.

You can optionally specify the node on which you want to collect statistics. If you do not specify the node, the sample collects statistics for all nodes in the cluster.

3. Use the `statistics stop` command to stop collecting data for the sample.
4. View SMB signing statistics:

If you want to view information for...	Enter...
Signed sessions	<code>show -sample-id <i>sample_ID</i> -counter signed_sessions <i>node_name</i> [-node <i>node_name</i>]</code>
Signed sessions and established sessions	<code>show -sample-id <i>sample_ID</i> -counter signed_sessions established_sessions <i>node_name</i> [-node <i>node_name</i>]</code>

If you want to display information for only a single node, specify the optional `-node` parameter.

5. Return to the admin privilege level: `set -privilege admin`

### Examples

The following example shows how you can monitor SMB 2.x and SMB 3.0 signing statistics on storage virtual machine (SVM) vs1.

The following command moves to the advanced privilege level:

```
cluster1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them only  
when directed to do so by support personnel.
```

```
Do you want to continue? {y|n}: y
```

The following command starts data collection for a new sample:

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample  
-vserver vs1
```

```
Statistics collection is being started for Sample-id: smbsigning_sample
```

The following command stops the data collection for the sample:

```
cluster1::*> statistics stop -sample-id smbsigning_sample
```

```
Statistics collection is being stopped for Sample-id: smbsigning_sample
```

The following command shows signed SMB sessions and established SMB sessions by node from the sample:

```
cluster1::*> statistics show -sample-id smbSigning_sample -counter
signed_sessions|established_sessions|node_name
```

```
Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:03:04
Cluster: cluster1
```

Counter	Value
-----	-----
established_sessions	0
node_name	node1
signed_sessions	0
established_sessions	1
node_name	node2
signed_sessions	1
established_sessions	0
node_name	node3
signed_sessions	0
established_sessions	0
node_name	node4
signed_sessions	0

The following command shows signed SMB sessions for node2 from the sample:

```
cluster1::*> statistics show -sample-id smbSigning_sample -counter
signed_sessions|node_name -node node2
```

```
Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:22:43
Cluster: cluster1
```

Counter	Value
-----	-----
node_name	node2
signed_sessions	1

The following command moves back to the admin privilege level:

```
cluster1::*> set -privilege admin
```

## Related information

[Determining whether SMB sessions are signed](#)

[Performance monitoring express setup](#)

**Configure required SMB encryption on SMB servers for data transfers over SMB**

### Configure required SMB encryption on SMB servers for data transfers over SMB overview

SMB encryption for data transfers over SMB is a security enhancement that you can enable or disable on SMB servers. You can also configure the desired SMB encryption setting on a share-by-share basis through a share property setting.

By default, when you create a SMB server on the storage virtual machine (SVM), SMB encryption is disabled. You must enable it to take advantage of the enhanced security provided by SMB encryption.

To create an encrypted SMB session, the SMB client must support SMB encryption. Windows clients beginning with Windows Server 2012 and Windows 8 support SMB encryption.

SMB encryption on the SVM is controlled through two settings:

- A SMB server security option that enables the functionality on the SVM
- A SMB share property that configures the SMB encryption setting on a share-by-share basis

You can decide whether to require encryption for access to all data on the SVM or to require SMB encryption to access data only in selected shares. SVM-level settings supersede share-level settings.

The effective SMB encryption configuration depends on the combination of the two settings and is described in the following table:

<b>SMB server SMB encryption enabled</b>	<b>Share encrypt data setting enabled</b>	<b>Server-side encryption behavior</b>
True	False	Server-level encryption is enabled for all of the shares in the SVM. With this configuration, encryption happens for the entire SMB session.
True	True	Server-level encryption is enabled for all of the shares in the SVM irrespective of share-level encryption. With this configuration, encryption happens for the entire SMB session.
False	True	Share-level encryption is enabled for the specific shares. With this configuration, encryption happens from the tree connect.

SMB server SMB encryption enabled	Share encrypt data setting enabled	Server-side encryption behavior
False	False	No encryption is enabled.

SMB clients that do not support encryption cannot connect to a SMB server or share that requires encryption.

### Performance impact of SMB encryption

When SMB sessions use SMB encryption, all SMB communications to and from Windows clients experience a performance impact, which affects both the clients and the server (that is, the nodes on the cluster running the SVM that contains the SMB server).

The performance impact shows as increased CPU usage on both the clients and the server, although the amount of network traffic does not change.

The extent of the performance impact depends on the version of ONTAP 9 you are running. Beginning with ONTAP 9.7, a new encryption off-load algorithm can enable better performance in encrypted SMB traffic. SMB encryption offload is enabled by default when SMB encryption is enabled.

Enhanced SMB encryption performance requires AES-NI offload capability. See the Hardware Universe (HWU) to verify that AES-NI offload is supported for your platform.

Further performance improvements are also possible if you are able to use SMB version 3.11 (supported with Windows 10 and Windows Server 2016), which supports the much faster GCM algorithm.

Depending on your network, ONTAP 9 version, SMB version, and SVM implementation, the performance impact of SMB encryption can vary widely; you can verify it only through testing in your network environment.

SMB encryption is disabled by default on the SMB server. You should enable SMB encryption only on those SMB shares or SMB servers that require encryption. With SMB encryption, ONTAP performs additional processing of decrypting the requests and encrypting the responses for every request. SMB encryption should therefore be enabled only when necessary.

### Enable or disable required SMB encryption for incoming SMB traffic

If you want to require SMB encryption for incoming SMB traffic you can enable it on the CIFS server or at the share level. By default, SMB encryption is not required.

#### About this task

You can enable SMB encryption on the CIFS server, which applies to all shares on the CIFS server. If you do not want required SMB encryption for all shares on the CIFS server or if you want to enable required SMB encryption for incoming SMB traffic on a share-by-share basis, you can disable required SMB encryption on the CIFS server.

When you set up a storage virtual machine (SVM) disaster recovery relationship, the value you select for the `-identity-preserve` option of the `snapmirror create` command determines the configuration details that are replicated in the destination SVM.

If you set the `-identity-preserve` option to `true` (ID-preserve), the SMB encryption security setting is replicated to the destination.

If you set the `-identity-preserve` option to `false` (non-ID-preserve), the SMB encryption security setting is not replicated to the destination. In this case, the CIFS server security settings on the destination are set to the default values. If you have enabled SMB encryption on the source SVM, you must manually enable CIFS server SMB encryption on the destination.

### Steps

1. Perform one of the following actions:

If you want required SMB encryption for incoming SMB traffic on the CIFS server to be...	Enter the command...
Enabled	<pre>vserver cifs security modify -vserver vserver_name -is-smb-encryption -required true</pre>
Disabled	<pre>vserver cifs security modify -vserver vserver_name -is-smb-encryption -required false</pre>

2. Verify that required SMB encryption on the CIFS server is enabled or disabled as desired: `vserver cifs security show -vserver vserver_name -fields is-smb-encryption-required`

The `is-smb-encryption-required` field displays `true` if required SMB encryption is enabled on the CIFS server and `false` if it is disabled.

### Example

The following example enables required SMB encryption for incoming SMB traffic for the CIFS server on SVM `vs1`:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-----  -----
vs1      true
```

### Determine whether clients are connected using encrypted SMB sessions

You can display information about connected SMB sessions to determine whether clients are using encrypted SMB connections. This can be helpful in determining whether SMB client sessions are connecting with the desired security settings.

#### About this task

SMB clients sessions can have one of three encryption levels:

- unencrypted

The SMB session is not encrypted. Neither storage virtual machine (SVM)-level or share-level encryption is configured.

- partially-encrypted

Encryption is initiated when the tree-connect occurs. Share-level encryption is configured. SVM-level encryption is not enabled.

- encrypted

The SMB session is fully encrypted. SVM-level encryption is enabled. Share level encryption might or might not be enabled. The SVM-level encryption setting supersedes the share-level encryption setting.

### Steps

1. Perform one of the following actions:

If you want display information about...	Enter the command...
Sessions with a specified encryption setting for sessions on a specified SVM	<pre>vserver cifs session show -vserver vserver_name {unencrypted partially- encrypted encrypted} -instance</pre>
The encryption setting for a specific session ID on a specified SVM	<pre>vserver cifs session show -vserver vserver_name -session-id integer -instance</pre>

### Examples

The following command displays detailed session information, including the encryption setting, on an SMB session with a session ID of 2:

```

cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                Node: node1
                Vserver: vs1
                Session ID: 2
                Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                Workstation: 10.1.1.2
Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                UNIX User: pcuser
                Open Shares: 1
                Open Files: 1
                Open Other: 0
                Connected Time: 10m 43s
                Idle Time: 1m 19s
                Protocol Version: SMB3
Continuously Available: No
                Is Session Signed: true
                User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
                SMB Encryption Status: Unencrypted

```

### Monitor SMB encryption statistics

You can monitor SMB encryption statistics and determine which established sessions and share connections are encrypted and which are not.

#### About this task

The `statistics` command at the advanced privilege level provides the following counters, which you can use to monitor the number of encrypted SMB sessions and share connections:

Counter name	Descriptions
<code>encrypted_sessions</code>	Gives the number of encrypted SMB 3.0 sessions
<code>encrypted_share_connections</code>	Gives the number of encrypted shares on which a tree connect has happened
<code>rejected_unencrypted_sessions</code>	Gives the number of session setups rejected due to a lack of client encryption capability
<code>rejected_unencrypted_shares</code>	Gives the number of share mappings rejected due to a lack of client encryption capability

These counters are available with the following statistics objects:



- `cifs` enables you to monitor SMB encryption for all SMB 3.0 sessions.

SMB 3.0 statistics are included in the output for the `cifs` object. If you want to compare the number of encrypted sessions to the total number of sessions, you can compare output for the `encrypted_sessions` counter with the output for the `established_sessions` counter.



If you want to compare the number of encrypted share connections to the total number of share connections, you can compare output for the `encrypted_share_connections` counter with the output for the `connected_shares` counter.

- `rejected_unencrypted_sessions` provides the number of times an attempt has been made to establish an SMB session that requires encryption from a client that does not support SMB encryption.
- `rejected_unencrypted_shares` provides the number of times an attempt has been made to connect to an SMB share that requires encryption from a client that does not support SMB encryption.

You must start a statistics sample collection before you can view the resultant data. You can view data from the sample if you do not stop the data collection. Stopping data collection gives you a fixed sample. Not stopping data collection gives you the ability to get updated data that you can use to compare against previous queries. The comparison can help you identify trends.

## Performance management

### Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Start a data collection: `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]`

If you do not specify the `-sample-id` parameter, the command generates a sample identifier for you and defines this sample as the default sample for the CLI session. The value for `-sample-id` is a text string. If you run this command during the same CLI session and do not specify the `-sample-id` parameter, the command overwrites the previous default sample.

You can optionally specify the node on which you want to collect statistics. If you do not specify the node, the sample collects statistics for all nodes in the cluster.

3. Use the `statistics stop` command to stop collecting data for the sample.
4. View SMB encryption statistics:

If you want to view information for...	Enter...
Encrypted sessions	<code>show -sample-id sample_ID -counter encrypted_sessions node_name [-node node_name]</code>

If you want to view information for...	Enter...
Encrypted sessions and established sessions	<code>show -sample-id <i>sample_ID</i> -counter encrypted_sessions established_sessions <i>node_name</i> [-node <i>node_name</i>]</code>
Encrypted share connections	<code>show -sample-id <i>sample_ID</i> -counter encrypted_share_connections <i>node_name</i> [-node <i>node_name</i>]</code>
Encrypted share connections and connected shares	<code>show -sample-id <i>sample_ID</i> -counter encrypted_share_connections connected_shares <i>node_name</i> [-node <i>node_name</i>]</code>
Rejected unencrypted sessions	<code>show -sample-id <i>sample_ID</i> -counter rejected_unencrypted_sessions <i>node_name</i> [-node <i>node_name</i>]</code>
Rejected unencrypted share connections	<code>show -sample-id <i>sample_ID</i> -counter rejected_unencrypted_share <i>node_name</i> [-node <i>node_name</i>]</code>

If you want to display information only for a single node, specify the optional `-node` parameter.

5. Return to the admin privilege level: `set -privilege admin`

### Examples

The following example shows how you can monitor SMB 3.0 encryption statistics on storage virtual machine (SVM) `vs1`.

The following command moves to the advanced privilege level:

```
cluster1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
```

```
Do you want to continue? {y|n}: y
```

The following command starts data collection for a new sample:

```
cluster1::*> statistics start -object cifs -sample-id smbencryption_sample
-vserver vs1
Statistics collection is being started for Sample-id: smbencryption_sample
```

The following command stops data collection for that sample:

```
cluster1::~*> statistics stop -sample-id smbencryption_sample
Statistics collection is being stopped for Sample-id: smbencryption_sample
```

The following command shows encrypted SMB sessions and established SMB sessions by the node from the sample:

```
cluster2::~*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name -node node_name
```

```
Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:45
Scope: vsim2
```

Counter	Value
established_sessions	1
encrypted_sessions	1

```
2 entries were displayed
```

The following command shows the number of rejected unencrypted SMB sessions by the node from the sample:

```
clus-2::~*> statistics show -object cifs -counter
rejected_unencrypted_sessions -node node_name
```

```
Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:51
Scope: vsim2
```

Counter	Value
rejected_unencrypted_sessions	1

```
1 entry was displayed.
```

The following command shows the number of connected SMB shares and encrypted SMB shares by the node from the sample:

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name
```

```
Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:41:43
Scope: vsim2
```

Counter	Value
connected_shares	2
encrypted_share_connections	1

2 entries were displayed.

The following command shows the number of rejected unencrypted SMB share connections by the node from the sample:

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares -node node_name
```

```
Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:42:06
Scope: vsim2
```

Counter	Value
rejected_unencrypted_shares	1

1 entry was displayed.

## Related information

[Determining which statistics objects and counters are available](#)

[Performance monitoring express setup](#)

**Secure LDAP session communication**

**LDAP signing and sealing concepts**

Beginning with ONTAP 9, you can configure signing and sealing to enable LDAP session security on queries to an Active Directory (AD) server. You must configure the CIFS

server security settings on the storage virtual machine (SVM) to correspond to those on the LDAP server.

Signing confirms the integrity of the LDAP payload data using secret key technology. Sealing encrypts the LDAP payload data to avoid transmitting sensitive information in clear text. An *LDAP Security Level* option indicates whether the LDAP traffic needs to be signed, signed and sealed, or neither. The default is `none`.

LDAP signing and sealing on CIFS traffic is enabled on the SVM with the `-session-security-for-ad-ldap` option to the `vserver cifs security modify` command.

### Enable LDAP signing and sealing on the CIFS server

Before your CIFS server can use signing and sealing for secure communication with an Active Directory LDAP server, you must modify the CIFS server security settings to enable LDAP signing and sealing.

#### Before you begin

You must consult with your AD server administrator to determine the appropriate security configuration values.

#### Steps

1. Configure the CIFS server security setting that enables signed and sealed traffic with Active Directory LDAP servers: `vserver cifs security modify -vserver vserver_name -session -security-for-ad-ldap {none|sign|seal}`

You can enable signing (`sign`, data integrity), signing and sealing (`seal`, data integrity and encryption), or neither (`none`, no signing or sealing). The default value is `none`.

2. Verify that the LDAP signing and sealing security setting is set correctly: `vserver cifs security show -vserver vserver_name`



If the SVM uses the same LDAP server for querying name-mapping or other UNIX information, such as users, groups, and netgroups, then you must enable the corresponding setting with the `-session-security` option of the `vserver services name-service ldap client modify` command.

### Configure LDAP over TLS

#### Export a copy of the self-signed root CA certificate

To use LDAP over SSL/TLS for securing Active Directory communication, you must first export a copy of the Active Directory Certificate Service's self-signed root CA certificate to a certificate file and convert it to an ASCII text file. This text file is used by ONTAP to install the certificate on the storage virtual machine (SVM).

#### Before you begin

The Active Directory Certificate Service must already be installed and configured for the domain to which the CIFS server belongs. You can find information about installing and configuring Active Director Certificate Services by consulting the Microsoft TechNet Library.

Microsoft TechNet Library: [technet.microsoft.com](http://technet.microsoft.com)

## Step

1. Obtain a root CA certificate of the domain controller that is in the .pem text format.

[Microsoft TechNet Library: technet.microsoft.com](https://technet.microsoft.com)

## After you finish

Install the certificate on the SVM.

## Related information

[Microsoft TechNet Library](https://technet.microsoft.com)

## Install the self-signed root CA certificate on the SVM

If LDAP authentication with TLS is required when binding to LDAP servers, you must first install the self-signed root CA certificate on the SVM.

## About this task

When LDAP over TLS is enabled, the ONTAP LDAP client on the SVM does not support revoked certificates in ONTAP 9.0 and 9.1.

Beginning with ONTAP 9.2, all applications within ONTAP that use TLS communications can check digital certificate status using Online Certificate Status Protocol (OCSP). If OCSP is enabled for LDAP over TLS, revoked certificates are rejected and the connection fails.

## Steps

1. Install the self-signed root CA certificate:
  - a. Begin the certificate installation: `security certificate install -vserver vserver_name -type server-ca`  
  
The console output displays the following message: `Please enter Certificate: Press <Enter> when done`
  - b. Open the certificate .pem file with a text editor, copy the certificate, including the lines beginning with `-----BEGIN CERTIFICATE-----` and ending with `-----END CERTIFICATE-----`, and then paste the certificate after the command prompt.
  - c. Verify that the certificate is displayed correctly.
  - d. Complete the installation by pressing Enter.
2. Verify that the certificate is installed: `security certificate show -vserver vserver_name`

## Enable LDAP over TLS on the server

Before your SMB server can use TLS for secure communication with an Active Directory LDAP server, you must modify the SMB server security settings to enable LDAP over TLS.

Beginning with ONTAP 9.10.1, LDAP channel binding is supported by default for both Active Directory (AD) and name services LDAP connections. ONTAP will try channel binding with LDAP connections only if Start-TLS or LDAPS is enabled along with session security set to either sign or seal. To disable or reenble LDAP channel binding with AD servers, use the `-try-channel-binding-for-ad-ldap` parameter with the

`vserver cifs security modify` command.

For more information, see [2020 LDAP channel binding and LDAP signing requirements for Windows](#).

### Steps

1. Configure the SMB server security setting that allows secure LDAP communication with Active Directory LDAP servers: `vserver cifs security modify -vserver vserver_name -use-start-tls -for-ad-ldap true`
2. Verify that the LDAP over TLS security setting is set to true: `vserver cifs security show -vserver vserver_name`



If the SVM uses the same LDAP server for querying name-mapping or other UNIX information (such as users, groups, and netgroups), then you must also modify the `-use-start-tls` option by using the `vserver services name-service ldap client modify` command.

### Related information

[LDAPS concepts](#)

[NFS management](#)

### Configure SMB Multichannel for performance and redundancy

Beginning with ONTAP 9.4, you can configure SMB Multichannel to provide multiple connections between ONTAP and clients in a single SMB session. Doing so improves throughput and fault tolerance.

#### Before you begin

You can use SMB Multichannel functionality only when clients negotiate at SMB 3.0 or later versions. SMB 3.0 and later is enabled on the ONTAP SMB server by default.

#### About this task

SMB clients automatically detect and use multiple network connections if a proper configuration is identified on the ONTAP cluster.

The number of simultaneous connections in an SMB session depends on the NICs you have deployed:

- **1G NICs on client and ONTAP cluster**

The client establishes one connection per NIC and binds the session to all connections.

- **10G and larger capacity NICs on client and ONTAP cluster**

The client establishes up to four connections per NIC and binds the session to all connections. The client can establish connections on multiple 10G and larger capacity NICs.

You can also modify the following parameters (advanced privilege):

- `-max-connections-per-session`

The maximum number of connections allowed per Multichannel session. The default is 32 connections.

If you want to enable more connections than the default, you must make comparable adjustments to the client configuration, which also has a default of 32 connections.

- **-max-lifs-per-session**

The maximum number of network interfaces advertised per Multichannel session. The default is 256 network interfaces.

### Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Enable SMB Multichannel on the SMB server: `vserver cifs options modify -vserver vserver_name -is-multichannel-enabled true`
3. Verify that ONTAP is reporting SMB Multichannel sessions: `vserver cifs session show options`
4. Return to the admin privilege level: `set -privilege admin`

### Example

The following example displays information about all SMB sessions, showing multiple connections for a single session:

```
cluster1::> vserver cifs session show
Node:      node1
Vserver:  vs1
Connection Session                               Open
Idle
IDs        ID      Workstation      Windows User      Files
Time
-----
-----
138683,
138684,
138685      1      10.1.1.1        DOMAIN\
4s                                     Administrator      0
```

The following example displays detailed information about an SMB session with session-id 1:



```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
           Node: node1
           Session ID: 1
           Connection IDs: 138683,138684,138685
           Connection Count: 3
           Incoming Data LIF IP Address: 192.1.1.1
           Workstation IP Address: 10.1.1.1
           Authentication Mechanism: NTLMv1
           User Authenticated as: domain-user
           Windows User: DOMAIN\administrator
           UNIX User: root
           Open Shares: 2
           Open Files: 5
           Open Other: 0
           Connected Time: 5s
           Idle Time: 5s
           Protocol Version: SMB3
           Continuously Available: No
           Is Session Signed: false
           NetBIOS Name: -
```

## Configure default Windows user to UNIX user mappings on the SMB server

### Configure the default UNIX user

You can configure the default UNIX user to use if all other mapping attempts fail for a user, or if you do not want to map individual users between UNIX and Windows. Alternatively, if you want authentication of non-mapped users to fail, you should not configure the default UNIX user.

### About this task

By default, the name of the default UNIX user is “pcuser”, which means that, by default, user mapping to the default UNIX user is enabled. You can specify another name to use as the default UNIX user. The name that you specify must exist in the name service databases configured for the storage virtual machine (SVM). If this option is set to a null string, no one can access the CIFS server as a UNIX default user. That is, each user must have an account in the password database before they can access the CIFS server.

For a user to connect to the CIFS server using the default UNIX user account, the user must meet the following prerequisites:

- The user is authenticated.
- The user is in the CIFS server’s local Windows user database, in the CIFS server’s home domain, or in a trusted domain (if multidomain name mapping searches is enabled on the CIFS server).
- The user name is not explicitly mapped to a null string.

## Steps

1. Configure the default UNIX user:

If you want to ...	Enter ...
Use the default UNIX user "pcuser"	<pre>vserver cifs options modify -default -unix-user pcuser</pre>
Use another UNIX user account as the default user	<pre>vserver cifs options modify -default -unix-user user_name</pre>
Disable the default UNIX user	<pre>vserver cifs options modify -default -unix-user ""</pre>

```
vserver cifs options modify -default-unix-user pcuser
```

2. Verify that the default UNIX user is configured correctly: `vserver cifs options show -vserver vserver_name`

In the following example, both the default UNIX user and the guest UNIX user on SVM vs1 are configured to use UNIX user "pcuser":

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

Client Session Timeout : 900
Default Unix Group      : -
Default Unix User       : pcuser
Guest Unix User         : pcuser
Read Grants Exec       : disabled
Read Only Delete       : disabled
WINS Servers           : -
```

### Configure the guest UNIX user

Configuring the guest UNIX user option means that users who log in from untrusted domains are mapped to the guest UNIX user and can connect to the CIFS server. Alternatively, if you want authentication of users from untrusted domains to fail, you should not configure the guest UNIX user. The default is to not allow users from untrusted domains to connect to the CIFS server (the guest UNIX account is not configured).

### About this task

You should keep the following in mind when configuring the guest UNIX account:

- If the CIFS server cannot authenticate the user against a domain controller for the home domain or a trusted domain or the local database and this option is enabled, the CIFS server considers the user as a

guest user and maps the user to the specified UNIX user.

- If this option is set to a null string, the guest UNIX user is disabled.
- You must create a UNIX user to use as the guest UNIX user in one of the storage virtual machine (SVM) name service databases.
- A user logged in as a guest user is automatically is a member of the BUILTIN\guests group on the CIFS server.
- The 'homedirs-public' option applies only to authenticated users. A user logged in as a guest user does not have a home directory and cannot access other users' home directories.

## Steps

1. Perform one of the following actions:

If you want to...	Enter...
Configure the guest UNIX user	<pre>vserver cifs options modify -guest -unix-user <i>unix_name</i></pre>
Disable the guest UNIX user	<pre>vserver cifs options modify -guest -unix-user ""</pre>

```
vserver cifs options modify -guest-unix-user pcuser
```

2. Verify that the guest UNIX user is configured correctly: `vserver cifs options show -vserver vserver_name`

In the following example, both the default UNIX user and the guest UNIX user on SVM vs1 are configured to use UNIX user "pcuser":

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

Client Session Timeout : 900
Default Unix Group      : -
Default Unix User       : pcuser
Guest Unix User         : pcuser
Read Grants Exec        : disabled
Read Only Delete        : disabled
WINS Servers            : -
```

## Map the administrators group to root

If you have only CIFS clients in your environment and your storage virtual machine (SVM) was set up as a multiprotocol storage system, you must have at least one Windows account that has root privilege for accessing files on the SVM; otherwise, you cannot manage the SVM because you do not have sufficient user rights.

## About this task

If your storage system was set up as NTFS-only, however, the `/etc` directory has a file-level ACL that enables the administrators group to access the ONTAP configuration files.

## Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Configure the CIFS server option that maps the administrators group to root as appropriate:

If you want to...	Then...
Map the administrator group members to root	<code>vserver cifs options modify -vserver vserver_name -is-admin-users-mapped-to-root-enabled true</code> All accounts in the administrators group are considered root, even if you do not have an <code>/etc/usermap.cfg</code> entry mapping the accounts to root. If you create a file using an account that belongs to the administrators group, the file is owned by root when you view the file from a UNIX client.
Disable mapping the administrators group members to root	<code>vserver cifs options modify -vserver vserver_name -is-admin-users-mapped-to-root-enabled false</code> Accounts in the administrators group no longer map to root. You can only explicitly map a single user to root.

3. Verify that the option is set to the desired value: `vserver cifs options show -vserver vserver_name`
4. Return to the admin privilege level: `set -privilege admin`

## Display information about what types of users are connected over SMB sessions

You can display information about what type of users are connected over SMB sessions. This can help you ensure that only the appropriate type of user is connecting over SMB sessions on the storage virtual machine (SVM).

### About this task

The following types of users can connect over SMB sessions:

- `local-user`

Authenticated as a local CIFS user

- `domain-user`

Authenticated as a domain user (either from the CIFS server's home domain or a trusted domain)

- `guest-user`

Authenticated as a guest user

- anonymous-user

Authenticated as an anonymous or null user

## Steps

1. Determine what type of user is connected over an SMB session: `vserver cifs session show -vserver vserver_name -windows-user windows_user_name -fields windows-user,address,lif-address,user-type`

If you want to display user type information for established sessions...	Enter the following command...
For all sessions with a specified user type	<code>vserver cifs session show -vserver vserver_name -user-type {local-user domain-user guest-user anonymous-user}</code>
For a specific user	<code>vserver cifs session show -vserver vserver_name -windows-user windows_user_name -fields windows-user,address,lif-address,user-type</code>

## Examples

The following command displays session information on the user type for sessions on SVM vs1 established by user "iepubs\user1":

```
cluster1::> vserver cifs session show -vserver pub1 -windows-user
iepubs\user1 -fields windows-user,address,lif-address,user-type
node          vserver session-id connection-id lif-address  address
windows-user          user-type
-----
pub1node1 pub1      1          3439441860    10.0.0.1    10.1.1.1
IEPUBS\user1          domain-user
```

## Command options to limit excessive Windows client resource consumption

Options to the `vserver cifs options modify` command enable you to control resource consumption for Windows clients. This can be helpful if any clients are outside normal bounds of resource consumption, for example, if there are unusually high numbers of files open, sessions open, or change notify requests.

The following options to the `vserver cifs options modify` command have been added to control Windows client resource consumption. If the maximum value for any of these options is exceeded, the request is denied and an EMS message is sent. An EMS warning message is also sent when 80 percent of the configured limit for these options is reached.

- `-max-opens-same-file-per-tree`

Maximum number of opens on the same file per CIFS tree

- `-max-same-user-sessions-per-connection`

Maximum number of sessions opened by the same user per connection

- `-max-same-tree-connect-per-session`

Maximum number of tree connects on the same share per session

- `-max-watches-set-per-tree`

Maximum number of watches (also known as *change notifies*) established per tree

See the man pages for the default limits and to display the current configuration.

Beginning with ONTAP 9.4, servers running SMB version 2 or later can limit the number of outstanding requests (*SMB credits*) that the client can send to the server on a SMB connection. The management of SMB credits is initiated by the client and controlled by the server.

The maximum number of outstanding requests that can be granted on an SMB connection is controlled by the `-max-credits` option. The default value for this option is 128.

## Improve client performance with traditional and lease oplocks

### Improve client performance with traditional and lease oplocks overview

Traditional oplocks (opportunistic locks) and lease oplocks enable an SMB client in certain file-sharing scenarios to perform client-side caching of read-ahead, write-behind, and lock information. A client can then read from or write to a file without regularly reminding the server that it needs access to the file in question. This improves performance by reducing network traffic.

Lease oplocks are an enhanced form of oplocks available with the SMB 2.1 protocol and later. Lease oplocks allow a client to obtain and preserve client caching state across multiple SMB opens originating from itself.

Oplocks can be controlled in two ways:

- By a share property, using the `vserver cifs share create` command when the share is created, or the `vserver share properties` command after creation.
- By a qtree property, using the `volume qtree create` command when the qtree is created, or the `volume qtree oplock` commands after creation.

### Write cache data-loss considerations when using oplocks

Under some circumstances, if a process has an exclusive oplock on a file and a second process attempts to open the file, the first process must invalidate cached data and flush writes and locks. The client must then relinquish the oplock and access to the file. If there is a network failure during this flush, cached write data might be lost.

- Data-loss possibilities

Any application that has write-cached data can lose that data under the following set of circumstances:

- The connection is made using SMB 1.0.
- It has an exclusive oplock on the file.
- It is told to either break that oplock or close the file.
- During the process of flushing the write cache, the network or target system generates an error.

- Error handling and write completion

The cache itself does not have any error handling—the applications do. When the application makes a write to the cache, the write is always completed. If the cache, in turn, makes a write to the target system over a network, it must assume that the write is completed because if it does not, the data is lost.

### **Enable or disable oplocks when creating SMB shares**

Oplocks allow clients to lock files and cache content locally, which can increase performance for file operations. Oplocks are enabled on SMB shares residing on storage virtual machines (SVMs). In some circumstances, you might want to disable oplocks. You can enable or disable oplocks on a share-by-share basis.



#### **About this task**

If oplocks are enabled on the volume containing a share but the oplock share property for that share is disabled, oplocks are disabled for that share. Disabling oplocks on a share takes precedence over the volume oplock setting. Disabling oplocks on the share disables both opportunistic and lease oplocks.

You can specify other share properties in addition to specifying the oplock share property by using a comma-delimited list. You can also specify other share parameters.

#### **Steps**

1. Perform the applicable action:

If you want to...	Then...
<p>Enable oplocks on a share during share creation</p>	<p>Enter the following command: <code>vserver cifs share create -vserver _vserver_name_ -share-name share_name -path path_to_share -share-properties [oplocks, ...]</code></p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>If you want the share to have only the default share properties, which are <code>oplocks</code>, <code>browsable</code>, and <code>changenotify</code> enabled, you do not have to specify the <code>-share-properties</code> parameter when creating an SMB share. If you want any combination of share properties other than the default, then you must specify the <code>-share-properties</code> parameter with the list of share properties to use for that share.</p> </div>
<p>Disable oplocks on a share during share creation</p>	<p>Enter the following command: <code>vserver cifs share create -vserver _vserver_name_ -share-name _share_name_ -path _path_to_share_ -share-properties [other_share_property, ...]</code></p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>When disabling oplocks, you must specify a list of share properties when creating the share, but you should not specify the <code>oplocks</code> property.</p> </div>

## Related information

[Enabling or disabling oplocks on existing SMB shares](#)

[Monitoring oplock status](#)

### Commands for enabling or disabling oplocks on volumes and qtrees

Oplocks allow clients to lock files and cache content locally, which can increase performance for file operations. You need to know the commands for enabling or disabling oplocks on volumes or qtrees. You also must know when you can enable or disable oplocks on volumes and qtrees.

- Oplocks are enabled on volumes by default.
- You cannot disable oplocks when you create a volume.
- You can enable or disable oplocks on existing volumes for SVMs at any time.



- You can enable oplocks on qtrees for SVMs.

The oplock mode setting is a property of qtree ID 0, the default qtree that all volumes have. If you do not specify an oplock setting when creating a qtree, the qtree inherits the oplock setting of the parent volume, which is enabled by default. However, if you do specify an oplock setting on the new qtree, it takes precedence over the oplock setting on the volume.

If you want to...	Use this command...
Enable oplocks on volumes or qtrees	<code>volume qtree oplocks with the -oplock-mode parameter set to enable</code>
Disable oplocks on volumes or qtrees	<code>volume qtree oplocks with the -oplock-mode parameter set to disable</code>

### Related information

[Monitoring oplock status](#)

### Enable or disable oplocks on existing SMB shares


Oplocks are enabled on SMB shares on storage virtual machines (SVMs) by default. Under some circumstances, you might want to disable oplocks; alternatively, if you have previously disabled oplocks on a share, you might want to reenables oplocks.

### About this task

If oplocks are enabled on the volume containing a share, but the oplock share property for that share is disabled, oplocks are disabled for that share. Disabling oplocks on a share takes precedence over enabling oplocks on the volume. Disabling oplocks on the share, disables both opportunistic and lease oplocks. You can enable or disable oplocks on existing shares at any time.

### Step

1. Perform the applicable action:

If you want to...	Then...
Enable oplocks on a share by modifying an existing share	<p>Enter the following command: <code>vserver cifs share properties add -vserver <i>vserver_name</i> -share-name <i>share_name</i> -share-properties oplocks</code></p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p> You can specify additional share properties to add by using a comma-delimited list.</p> </div> <p>Newly added properties are appended to the existing list of share properties. Any share properties that you have previously specified remain in effect.</p>

If you want to...	Then...
Disable oplocks on a share by modifying an existing share	<p data-bbox="841 163 1430 300">Enter the following command: <code>vserver cifs share properties remove -vserver <i>vserver_name</i> -share-name <i>share_name</i> -share-properties oplocks</code></p> <div data-bbox="873 369 927 426" style="border: 1px solid black; border-radius: 50%; width: 33px; height: 33px; display: flex; align-items: center; justify-content: center; margin: 10px 0;"> <span data-bbox="889 380 911 411" style="font-size: 20px; font-weight: bold;">i</span> </div> <p data-bbox="987 348 1390 447">You can specify additional share properties to remove by using a comma-delimited list.</p> <p data-bbox="841 495 1471 625">Share properties that you remove are deleted from the existing list of share properties; however, previously configured share properties that you do not remove remain in effect.</p>

### Examples

The following command enables oplocks for the share named “Engineering” on storage virtual machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver      Share      Properties
-----
vs1          Engineering oplocks
              browsable
              changenotify
              showsnapshot
```

The following command disables oplocks for the share named “Engineering” on SVM vs1:

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver      Share      Properties
-----
vs1          Engineering browsable
              changenotify
              showsnapshot
```

### Related information

[Enabling or disabling oplocks when creating SMB shares](#)

## Monitoring oplock status

### Adding or removing share properties on an existing SMB share

#### Monitor oplock status

You can monitor and display information about oplock status. You can use this information to determine which files have oplocks, what the oplock level and oplock state level are, and whether oplock leasing is used. You can also determine information about locks that you might need to break manually.

#### About this task

You can display information about all oplocks in summary form or in a detailed list form. You can also use optional parameters to display information about a smaller subset of existing locks. For example, you can specify that the output return only locks with the specified client IP address or with the specified path.

You can display the following information about traditional and lease oplocks:

- SVM, node, volume, and LIF on which the oplock is established
- Lock UUID
- IP address of the client with the oplock
- Path at which the oplock is established
- Lock protocol (SMB) and type (oplock)
- Lock state
- Oplock level
- Connection state and SMB expiration time
- Open Group ID if a lease oplock is granted

See the `vserver oplocks show` man page for a detailed description of each parameter.

#### Steps

1. Display oplock status by using the `vserver locks show` command.

#### Examples

The following command displays default information about all locks. The oplock on the displayed file is granted with a `read-batch` oplock level:

```
cluster1::> vserver locks show
```

```
Vserver: vs0
```

Volume	Object Path	LIF	Protocol	Lock Type	Client
vol1	/vol1/notes.txt	node1_data1			
			cifs	share-level	192.168.1.5
	Sharelock Mode: read_write-deny_delete				
				op-lock	192.168.1.5
	Oplock Level: read-batch				

The following example displays more detailed information about the lock on a file with the path `/data2/data2_2/intro.pptx`. A lease oplock is granted on the file with a `batch` oplock level to a client with an IP address of `10.3.1.3`:



When displaying detailed information, the command provides separate output for oplock and sharelock information. This example only shows the output from the oplock section.

```

cluster1::> vserver lock show -instance -path /data2/data2_2/intro.pptx

          Vserver: vs1
            Volume: data2_2
Logical Interface: lif2
      Object Path: /data2/data2_2/intro.pptx
        Lock UUID: ff1cbf29-bfef-4d91-ae06-062bf69212c3
      Lock Protocol: cifs
        Lock Type: op-lock
Node Holding Lock State: node3
      Lock State: granted
Bytelock Starting Offset: -
  Number of Bytes Locked: -
    Bytelock is Mandatory: -
    Bytelock is Exclusive: -
    Bytelock is Superlock: -
      Bytelock is Soft: -
        Oplock Level: batch
Shared Lock Access Mode: -
  Shared Lock is Soft: -
    Delegation Type: -
      Client Address: 10.3.1.3
        SMB Open Type: -
          SMB Connect State: connected
SMB Expiration Time (Secs): -
      SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

```

## Related information

[Enabling or disabling oplocks when creating SMB shares](#)

[Enabling or disabling oplocks on existing SMB shares](#)

[Commands for enabling or disabling oplocks on volumes and qtrees](#)

## Apply Group Policy Objects to SMB servers

### Apply Group Policy Objects to SMB servers overview

Your SMB server supports Group Policy Objects (GPOs), a set of rules known as *group policy attributes* that apply to computers in an Active Directory environment. You can use GPOs to centrally manage settings for all storage virtual machines (SVMs) on the cluster belonging to the same Active Directory domain.

When GPOs are enabled on your SMB server, ONTAP sends LDAP queries to the Active Directory server requesting GPO information. If there are GPO definitions that are applicable to your SMB server, the Active Directory server returns the following GPO information:

- GPO name
- Current GPO version
- Location of the GPO definition
- Lists of UUIDs (universally unique identifiers) for GPO policy sets

### Related information

[Securing file access by using Dynamic Access Control \(DAC\)](#)

[SMB and NFS auditing and security tracing](#)

### Supported GPOs

Although not all Group Policy Objects (GPOs) are applicable to your CIFS-enabled storage virtual machines (SVMs), SVMs can recognize and process the relevant set of GPOs.

The following GPOs are currently supported on SVMs:

- Advanced audit policy configuration settings:

Object access: Central Access Policy staging

Specifies the type of events to be audited for central access policy (CAP) staging, including the following settings:

- Do not audit
- Audit only success events
- Audit only failure events
- Audit both success and failure events



If any of the three audit options are set (audit only success events, audit only failure events, audit both success and failure events), ONTAP audits both success and failure events.

Set by using the `Audit Central Access Policy Staging` setting in the `Advanced Audit Policy Configuration/Audit Policies/Object Access` GPO.



To use advanced audit policy configuration GPO settings, auditing must be configured on the CIFS-enabled SVM to which you want to apply these setting. If auditing is not configured on the SVM, the GPO settings will not be applied and will be dropped.

- Registry settings:
  - Group Policy refresh interval for CIFS-enabled SVM

Set by using the `Registry` GPO.

- Group Policy refresh random offset

Set by using the `Registry` GPO.

- Hash publication for BranchCache

The Hash Publication for BranchCache GPO corresponds to the BranchCache operating mode. The following three supported operating modes are supported:

- Per-share
- All-shares
- Disabled  
Set by using the `Registry` GPO.

- Hash version support for BranchCache

The following three hash version settings are supported:

- BranchCache version 1
- BranchCache version 2
- BranchCache versions 1 and 2  
Set by using the `Registry` GPO.



To use BranchCache GPO settings, BranchCache must be configured on the CIFS-enabled SVM to which you want to apply these setting. If BranchCache is not configured on the SVM, the GPO settings will not be applied and will be dropped.

- Security settings

- Audit policy and event log

- Audit logon events

Specifies the type of logon events to be audited, including the following settings:

- Do not audit
- Audit only success events
- Audit on failure events
- Audit both success and failure events  
Set by using the `Audit logon events` setting in the `Local Policies/Audit Policy` GPO.



If any of the three audit options are set (audit only success events, audit only failure events, audit both success and failure events), ONTAP audits both success and failure events.

- Audit object access

Specifies the type of object access to be audited, including the following settings:

- Do not audit
- Audit only success events
- Audit on failure events
- Audit both success and failure events

Set by using the `Audit object access` setting in the `Local Policies/Audit Policy GPO`.



If any of the three audit options are set (audit only success events, audit only failure events, audit both success and failure events), ONTAP audits both success and failure events.

- **Log retention method**

Specifies the audit log retention method, including the following settings:

- **Overwrite the event log when size of the log file exceeds the maximum log size**
- **Do not overwrite the event log (clear log manually)**

Set by using the `Retention method for security log` setting in the `Event Log GPO`.

- **Maximum log size**

Specifies the maximum size of the audit log.

Set by using the `Maximum security log size` setting in the `Event Log GPO`.



To use audit policy and event log GPO settings, auditing must be configured on the CIFS-enabled SVM to which you want to apply these setting. If auditing is not configured on the SVM, the GPO settings will not be applied and will be dropped.

- **File system security**

Specifies a list of files or directories on which file security is applied through a GPO.

Set by using the `File System` GPO.



The volume path to which the file system security GPO is configured must exist within the SVM.

- **Kerberos policy**

- **Maximum clock skew**

Specifies maximum tolerance in minutes for computer clock synchronization.

Set by using the `Maximum tolerance for computer clock synchronization` setting in the `Account Policies/Kerberos Policy GPO`.

- **Maximum ticket age**

Specifies maximum lifetime in hours for user ticket.

Set by using the `Maximum lifetime for user ticket` setting in the `Account Policies/Kerberos Policy GPO`.

- **Maximum ticket renew age**

Specifies maximum lifetime in days for user ticket renewal.



Set by using the `Maximum lifetime for user ticket renewal` setting in the `Account Policies/Kerberos Policy` GPO.

- User rights assignment (privilege rights)

- Take ownership

Specifies the list of users and groups that have the right to take ownership of any securable object.

Set by using the `Take ownership of files or other objects` setting in the `Local Policies/User Rights Assignment` GPO.

- Security privilege

Specifies the list of users and groups that can specify auditing options for object access of individual resources, such as files, folders, and Active Directory objects.

Set by using the `Manage auditing and security log` setting in the `Local Policies/User Rights Assignment` GPO.

- Change notify privilege (bypass traverse checking)

Specifies the list of users and groups that can traverse directory trees even though the users and groups might not have permissions on the traversed directory.

The same privilege is required for users to receive notifications of changes to files and directories. Set by using the `Bypass traverse checking` setting in the `Local Policies/User Rights Assignment` GPO.

- Registry values

- Signing required setting

Specifies whether required SMB signing is enabled or disabled.

Set by using the `Microsoft network server: Digitally sign communications (always)` setting in the `Security Options` GPO.

- Restrict anonymous

Specifies what the restrictions for anonymous users are and includes the following three GPO settings:

- No enumeration of Security Account Manager (SAM) accounts:

This security setting determines what additional permissions are granted for anonymous connections to the computer. This option is displayed as `no-enumeration` in ONTAP if it is enabled.

Set by using the `Network access: Do not allow anonymous enumeration of SAM accounts` setting in the `Local Policies/Security Options` GPO.

- No enumeration of SAM accounts and shares

This security setting determines whether anonymous enumeration of SAM accounts and shares is allowed. This option is displayed as `no-enumeration` in ONTAP if it is enabled.

Set by using the `Network access: Do not allow anonymous enumeration of SAM accounts and shares` setting in the `Local Policies/Security Options` GPO.

- **Restrict anonymous access to shares and named pipes**

This security setting restricts anonymous access to shares and pipes. This option is displayed as `no-access` in ONTAP if it is enabled.

Set by using the `Network access: Restrict anonymous access to Named Pipes and Shares` setting in the `Local Policies/Security Options` GPO.

When displaying information about defined and applied group policies, the `Resultant restriction for anonymous user output` field provides information about the resultant restriction of the three restrict anonymous GPO settings. The possible resultant restrictions are as follows:

- `no-access`

The anonymous user is denied access to the specified shares and named pipes, and cannot use enumeration of SAM accounts and shares. This resultant restriction is seen if the `Network access: Restrict anonymous access to Named Pipes and Shares` GPO is enabled.

- `no-enumeration`

The anonymous user has access to the specified shares and named pipes, but cannot use enumeration of SAM accounts and shares. This resultant restriction is seen if both of the following conditions are met:

- **The `Network access: Restrict anonymous access to Named Pipes and Shares` GPO is disabled.**
- **Either the `Network access: Do not allow anonymous enumeration of SAM accounts and shares` GPO is enabled or the `Network access: Do not allow anonymous enumeration of SAM accounts and shares` GPO is disabled.**

- `no-restriction`

The anonymous user has full access and can use enumeration. This resultant restriction is seen if both of the following conditions are met:

- **The `Network access: Restrict anonymous access to Named Pipes and Shares` GPO is disabled.**
- **Both the `Network access: Do not allow anonymous enumeration of SAM accounts and shares` GPO is disabled and the `Network access: Do not allow anonymous enumeration of SAM accounts and shares` GPO is disabled.**

- **Restricted Groups**

You can configure restricted groups to centrally manage membership of either built-in or user-defined groups. When you apply a restricted group through a group policy, the membership of a CIFS server local group is automatically set to match the membership-list settings defined in the applied group policy.

Set by using the `Restricted Groups` GPO.

- Central access policy settings

Specifies a list of central access policies. Central access policies and the associated central access policy rules determine access permissions for multiple files on the SVM.

### Related information

[Enabling or disabling GPO support on a CIFS server](#)

[Securing file access by using Dynamic Access Control \(DAC\)](#)

[SMB and NFS auditing and security tracing](#)

[Modifying the CIFS server Kerberos security settings](#)

[Using BranchCache to cache SMB share content at a branch office](#)

[Using SMB signing to enhance network security](#)

[Configuring bypass traverse checking](#)

[Configuring access restrictions for anonymous users](#)

### Requirements for using GPOs with your SMB server

To use Group Policy Objects (GPOs) with your SMB server, your system must meet several requirements.

- SMB must be licensed on the cluster.
- A SMB server must be configured and joined to a Windows Active Directory domain.
- The SMB server admin status must be on.
- GPOs must be configured and applied to the Windows Active Directory Organizational Unit (OU) containing the SMB server computer object.
- GPO support must be enabled on the SMB server.

### Enable or disable GPO support on a CIFS server

You can enable or disable Group Policy Object (GPO) support on a CIFS server. If you enable GPO support on a CIFS server, the applicable GPOs that are defined on the group policy—the policy that is applied to the organizational unit (OU) that contains the CIFS server computer object—are applied to the CIFS server.



#### About this task

GPOs cannot be enabled on CIFS servers in workgroup mode.

### Steps

1. Perform one of the following actions:

If you want to...	Enter the command...
Enable GPOs	<code>vserver cifs group-policy modify -vserver vserver_name -status enabled</code>
Disable GPOs	<code>vserver cifs group-policy modify -vserver vserver_name -status disabled</code>

2. Verify that GPO support is in the desired state: `vserver cifs group-policy show -vserver +vserver_name_`

Group Policy Status for CIFS servers in workgroup mode is displayed as “disabled”.

### Example

The following example enables GPO support on storage virtual machine (SVM) vs1:

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled

cluster1::> vserver cifs group-policy show -vserver vs1

          Vserver: vs1
Group Policy Status: enabled
```

### Related information

[Supported GPOs](#)

[Requirements for using GPOs with your CIFS server](#)

[How GPOs are updated on the CIFS server](#)

[Manually updating GPO settings on the CIFS server](#)

[Displaying information about GPO configurations](#)

**How GPOs are updated on the SMB server**

**How GPOs are updated on the CIFS server overview**

By default, ONTAP retrieves and applies Group Policy Object (GPO) changes every 90 minutes. Security settings are refreshed every 16 hours. If you want to update GPOs to apply new GPO policy settings before ONTAP automatically updates them, you can trigger a manual update on a CIFS server with an ONTAP command.

- By default, all GPOs are verified and updated as needed every 90 minutes.

This interval is configurable and can be set using the `Refresh interval` and `Random offset` GPO settings.

ONTAP queries Active Directory for changes to GPOs. If the GPO version numbers recorded in Active

Directory are higher than those on the CIFS server, ONTAP retrieves and applies the new GPOs. If the version numbers are the same, GPOs on the CIFS server are not updated.

- Security Settings GPOs are refreshed every 16 hours.

ONTAP retrieves and applies Security Settings GPOs every 16 hours, whether or not these GPOs have changed.



The 16-hour default value cannot be changed in the current ONTAP version. It is a Windows client default setting.

- All GPOs can be updated manually with an ONTAP command.

This command simulates the Windows `gpupdate.exe /force` command.

### Related information

[Manually updating GPO settings on the CIFS server](#)

### What to do if GPO updates are failing

Under some circumstances, Group Policy Object (GPO) updates from Windows 2012 domain controllers might fail, which leads to nothing being visible under the `Central Access Policy Settings` section of the output for the `vserver cifs group-policy show-defined` command. You should know how to correct this issue if it occurs.

Underlying cause	Remedy
<p>When ONTAP attempts to connect to the Windows 2012 domain controller to perform the GPO update, the connection might fail with the error <code>error 0xc00000bd (NT STATUS_DUPLICATE_NAME)</code>.</p> <p>This error occurs when the server name used to make the connection is different from the NetBIOS name of the CIFS server. There are various reasons this might occur, including the use of aliases. Additionally, ONTAP pads the NetBIOS name used when connecting to the domain controller to make the name length equal to 15 characters. This can make it appear that the CIFS server name and the NetBIOS name are different.</p>	<ol style="list-style-type: none"><li>1. Disable NetBIOS name checking on the Windows server by adding the following registry key with the value set to 1:  <code>"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\DisableStrictNameChecking"</code>  To learn more about this registry key, contact <a href="#">Microsoft Support</a>.</li><li>2. Reboot the domain controller.</li></ol>

### Manually updating GPO settings on the CIFS server

If you want to update Group Policy Object (GPO) settings on your CIFS server immediately, you can manually update the settings. You can update only changed settings or you can force an update for all settings, including the settings that were applied previously but have not changed.

## Step

1. Perform the appropriate action:

If you want to update...	Enter the command...
Changed GPO settings	<code>vserver cifs group-policy update -vserver vserver_name</code>
All GPO settings	<code>vserver cifs group-policy update -vserver vserver_name -force-reapply -all-settings true</code>

## Related information

[How GPOs are updated on the CIFS server](#)

### Display information about GPO configurations

You can display information about Group Policy Object (GPO) configurations that are defined in Active Directory and about GPO configurations applied to the CIFS server.

### About this task

You can display information about all GPO configurations defined in the Active Directory of the domain to which the CIFS server belongs, or you can display information only about GPO configurations applied to a CIFS server.

## Steps

1. Display information about GPO configurations by performing one of the following actions:

If you want to display information about all Group Policy configurations...	Enter the command...
Defined in Active Directory	<code>vserver cifs group-policy show-defined -vserver vserver_name</code>
Applied to a CIFS-enabled storage virtual machine (SVM)	<code>vserver cifs group-policy show-applied -vserver vserver_name</code>

## Example

The following example displays the GPO configurations defined in the Active Directory to which the CIFS-enabled SVM named vs1 belongs:

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
-----
      GPO Name: Default Domain Policy
      Level: Domain
```

```
Status: enabled
Advanced Audit Settings:
  Object Access:
    Central Access Policy Staging: failure
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
  Hash Publication Mode for BranchCache: per-share
  Hash Version Support for BranchCache : version1
Security Settings:
  Event Audit and Event Log:
    Audit Logon Events: none
    Audit Object Access: success
    Log Retention Method: overwrite-as-needed
    Max Log Size: 16384
File Security:
  /voll/home
  /voll/dir1
Kerberos:
  Max Clock Skew: 5
  Max Ticket Age: 10
  Max Renew Age: 7
Privilege Rights:
  Take Ownership: usr1, usr2
  Security Privilege: usr1, usr2
  Change Notify: usr1, usr2
Registry Values:
  Signing Required: false
Restrict Anonymous:
  No enumeration of SAM accounts: true
  No enumeration of SAM accounts and shares: false
  Restrict anonymous access to shares and named pipes: true
  Combined restriction for anonymous user: no-access
Restricted Groups:
  gpr1
  gpr2
Central Access Policy Settings:
  Policies: cap1
           cap2

GPO Name: Resultant Set of Policy
Status: enabled
Advanced Audit Settings:
  Object Access:
    Central Access Policy Staging: failure
Registry Settings:
```

```

Refresh Time Interval: 22
Refresh Random Offset: 8
Hash Publication for Mode BranchCache: per-share
Hash Version Support for BranchCache: version1
Security Settings:
  Event Audit and Event Log:
    Audit Logon Events: none
    Audit Object Access: success
    Log Retention Method: overwrite-as-needed
    Max Log Size: 16384
  File Security:
    /voll/home
    /voll/dirl
  Kerberos:
    Max Clock Skew: 5
    Max Ticket Age: 10
    Max Renew Age: 7
  Privilege Rights:
    Take Ownership: usr1, usr2
    Security Privilege: usr1, usr2
    Change Notify: usr1, usr2
  Registry Values:
    Signing Required: false
  Restrict Anonymous:
    No enumeration of SAM accounts: true
    No enumeration of SAM accounts and shares: false
    Restrict anonymous access to shares and named pipes: true
    Combined restriction for anonymous user: no-access
  Restricted Groups:
    gpr1
    gpr2
Central Access Policy Settings:
  Policies: cap1
           cap2

```

The following example displays the GPO configurations applied to the CIFS-enabled SVM vs1:

```

cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
-----
  GPO Name: Default Domain Policy
    Level: Domain
    Status: enabled
Advanced Audit Settings:

```



```
Object Access:
  Central Access Policy Staging: failure
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
  Hash Publication Mode for BranchCache: per-share
  Hash Version Support for BranchCache: all-versions
Security Settings:
  Event Audit and Event Log:
    Audit Logon Events: none
    Audit Object Access: success
    Log Retention Method: overwrite-as-needed
    Max Log Size: 16384
  File Security:
    /voll/home
    /voll/dirl
  Kerberos:
    Max Clock Skew: 5
    Max Ticket Age: 10
    Max Renew Age: 7
  Privilege Rights:
    Take Ownership: usr1, usr2
    Security Privilege: usr1, usr2
    Change Notify: usr1, usr2
  Registry Values:
    Signing Required: false
  Restrict Anonymous:
    No enumeration of SAM accounts: true
    No enumeration of SAM accounts and shares: false
    Restrict anonymous access to shares and named pipes: true
    Combined restriction for anonymous user: no-access
  Restricted Groups:
    gpr1
    gpr2
Central Access Policy Settings:
  Policies: cap1
    cap2

GPO Name: Resultant Set of Policy
  Level: RSOP
Advanced Audit Settings:
  Object Access:
    Central Access Policy Staging: failure
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
```

```
Hash Publication Mode for BranchCache: per-share
Hash Version Support for BranchCache: all-versions
Security Settings:
  Event Audit and Event Log:
    Audit Logon Events: none
    Audit Object Access: success
    Log Retention Method: overwrite-as-needed
    Max Log Size: 16384
  File Security:
    /vol1/home
    /vol1/dir1
  Kerberos:
    Max Clock Skew: 5
    Max Ticket Age: 10
    Max Renew Age: 7
  Privilege Rights:
    Take Ownership: usr1, usr2
    Security Privilege: usr1, usr2
    Change Notify: usr1, usr2
  Registry Values:
    Signing Required: false
  Restrict Anonymous:
    No enumeration of SAM accounts: true
    No enumeration of SAM accounts and shares: false
    Restrict anonymous access to shares and named pipes: true
    Combined restriction for anonymous user: no-access
  Restricted Groups:
    gpr1
    gpr2
  Central Access Policy Settings:
    Policies: cap1
           cap2
```

## Related information

[Enabling or disabling GPO support on a CIFS server](#)

### Display detailed information about restricted group GPOs

You can display detailed information about restricted groups that are defined as Group Policy Objects (GPOs) in Active Directory and that are applied to the CIFS server.

### About this task

By default, the following information is displayed:

- Group policy name
- Group policy version

- Link

Specifies the level in which the group policy is configured. Possible output values include the following:

- Local when the group policy is configured in ONTAP
  - Site when the group policy is configured at the site level in the domain controller
  - Domain when the group policy is configured at the domain level in the domain controller
  - OrganizationalUnit when the group policy is configured at the Organizational Unit (OU) level in the domain controller
  - RSOP for the resultant set of policies derived from all the group policies defined at various levels
- Restricted group name
  - The users and groups who belong to and who do not belong to the restricted group
  - The list of groups to which the restricted group is added

A group can be a member of groups other than the groups listed here.

### Step

1. Display information about all restricted group GPOs by performing one of the following actions:

If you want to display information about all restricted group GPOs...	Enter the command...
Defined in Active Directory	<pre>vserver cifs group-policy restricted- group show-defined -vserver vserver_name</pre>
Applied to a CIFS server	<pre>vserver cifs group-policy restricted- group show-applied -vserver vserver_name</pre>

### Example

The following example displays information about restricted group GPOs defined in the Active Directory domain to which the CIFS-enabled SVM named vs1 belongs:

```
cluster1::> vserver cifs group-policy restricted-group show-defined
-vserver vs1
```

```
Vserver: vs1
```

```
-----
```

```
Group Policy Name: gp01
Version: 16
Link: OrganizationalUnit
Group Name: group1
Members: user1
MemberOf: EXAMPLE\group9
```

```
Group Policy Name: Resultant Set of Policy
Version: 0
Link: RSOP
Group Name: group1
Members: user1
MemberOf: EXAMPLE\group9
```

The following example displays information about restricted groups GPOs applied to the CIFS-enabled SVM vs1:

```
cluster1::> vserver cifs group-policy restricted-group show-applied
-vserver vs1
```

```
Vserver: vs1
```

```
-----
```

```
Group Policy Name: gp01
Version: 16
Link: OrganizationalUnit
Group Name: group1
Members: user1
MemberOf: EXAMPLE\group9
```

```
Group Policy Name: Resultant Set of Policy
Version: 0
Link: RSOP
Group Name: group1
Members: user1
MemberOf: EXAMPLE\group9
```

## Related information

## Displaying information about GPO configurations

### Display information about central access policies

You can display detailed information about the central access policies that are defined in Active Directory. You can also display information about the central access policies that are applied to the CIFS server through group policy objects (GPOs).

#### About this task

By default, the following information is displayed:

- SVM name
- Name of the central access policy
- SID
- Description
- Creation time
- Modification time
- Member rules



CIFS servers in workgroup mode are not displayed because they do not support GPOs.

#### Step

1. Display information about central access policies by performing one of the following actions:

If you want to display information about all central access policies...	Enter the command...
Defined in Active Directory	<code>vserver cifs group-policy central-access-policy show-defined -vserver <i>vserver_name</i></code>
Applied to a CIFS server	<code>vserver cifs group-policy central-access-policy show-applied -vserver <i>vserver_name</i></code>

#### Example

The following example displays information for all the central access policies that are defined in Active Directory:

```
cluster1::> vserver cifs group-policy central-access-policy show-defined
```

```
Vserver  Name          SID
-----  -
-----  -
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
      Description: policy #1
      Creation Time: Tue Oct 22 09:34:13 2013
      Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
      Description: policy #2
      Creation Time: Tue Oct 22 10:28:20 2013
      Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                        r2
```

The following example displays information for all the central access policies that are applied to the storage virtual machines (SVMs) on the cluster:

```
cluster1::> vserver cifs group-policy central-access-policy show-applied
```

```
Vserver  Name          SID
-----  -
-----  -
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
      Description: policy #1
      Creation Time: Tue Oct 22 09:34:13 2013
      Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
      Description: policy #2
      Creation Time: Tue Oct 22 10:28:20 2013
      Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                        r2
```

## Related information

## Securing file access by using Dynamic Access Control (DAC)

### Displaying information about GPO configurations

### Displaying information about central access policy rules

#### Display information about central access policy rules

You can display detailed information about central access policy rules that are associated with central access policies defined in Active Directory. You can also display information about central access policies rules that are applied to the CIFS server through central access policy GPOs (group policy objects).

#### About this task

You can display detailed information about defined and applied central access policy rules. By default, the following information is displayed:

- Vserver name
- Name of the central access rule
- Description
- Creation time
- Modification time
- Current permissions
- Proposed permissions
- Target resources

**Table 1. Step**

<b>If you want to display information about all central access policy rules associated with central access policies...</b>	<b>Enter the command...</b>
Defined in Active Directory	<pre>vserver cifs group-policy central- access-rule show-defined -vserver vserver_name</pre>
Applied to a CIFS server	<pre>vserver cifs group-policy central- access-rule show-applied -vserver vserver_name</pre>

#### Example

The following example displays information for all central access policy rules associated with central access policies defined in Active Directory:

```
cluster1::> vserver cifs group-policy central-access-rule show-defined
```

```
Vserver      Name
-----
vs1          r1
             Description: rule #1
             Creation Time: Tue Oct 22 09:33:48 2013
             Modification Time: Tue Oct 22 09:33:48 2013
             Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
             Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1          r2
             Description: rule #2
             Creation Time: Tue Oct 22 10:27:57 2013
             Modification Time: Tue Oct 22 10:27:57 2013
             Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
             Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

The following example displays information for all central access policy rules associated with central access policies applied to storage virtual machines (SVMs) on the cluster:

```
cluster1::> vserver cifs group-policy central-access-rule show-applied
```

```
Vserver      Name
-----
vs1          r1
             Description: rule #1
             Creation Time: Tue Oct 22 09:33:48 2013
             Modification Time: Tue Oct 22 09:33:48 2013
             Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
             Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1          r2
             Description: rule #2
             Creation Time: Tue Oct 22 10:27:57 2013
             Modification Time: Tue Oct 22 10:27:57 2013
             Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
             Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

## Related information

[Securing file access by using Dynamic Access Control \(DAC\)](#)

[Displaying information about GPO configurations](#)

[Displaying information about central access policies](#)



## Commands for managing SMB servers computer account passwords

You need to know the commands for changing, resetting, and disabling passwords, and for configuring automatic update schedules. You can also configure a schedule on the SMB server to update it automatically.

If you want to...	Use this command...
Change or reset the domain account password and you know the password	<code>vserver cifs domain password change</code>
Reset the domain account password and you do not know the password	<code>vserver cifs domain password reset</code>
Configure SMB servers for automatic computer account password changes	<code>vserver cifs domain password schedule modify -vserver vserver_name -is-schedule-enabled true</code>
Disable automatic computer account password changes on SMB servers	<code>vserver cifs domain password schedule modify -vserver vs1 -is-schedule-enabled false</code>

See the man page for each command for more information.

## Manage domain controller connections

### Display information about discovered servers

You can display information related to discovered LDAP servers and domain controllers on your CIFS server.

### Step

1. To display information related to discovered servers, enter the following command: `vserver cifs domain discovered-servers show`

### Example

The following example shows discovered servers for SVM vs1:

```
cluster1::> vserver cifs domain discovered-servers show
```

```
Node: node1  
Vserver: vs1
```

Domain Name	Type	Preference	DC-Name	DC-Address	Status
example.com	MS-LDAP	adequate	DC-1	1.1.3.4	OK
example.com	MS-LDAP	adequate	DC-2	1.1.3.5	OK
example.com	MS-DC	adequate	DC-1	1.1.3.4	OK
example.com	MS-DC	adequate	DC-2	1.1.3.5	OK

## Related information

[Resetting and rediscovering servers](#)

[Stopping or starting the CIFS server](#)

### Reset and rediscover servers

Resetting and rediscovering servers on your CIFS server allows the CIFS server to discard stored information about LDAP servers and domain controllers. After discarding server information, the CIFS server reacquires current information about these external servers. This can be useful when the connected servers are not responding appropriately.

### Steps

1. Enter the following command: `vserver cifs domain discovered-servers reset-servers -vserver vserver_name`
2. Display information about the newly rediscovered servers: `vserver cifs domain discovered-servers show -vserver vserver_name`

### Example

The following example resets and rediscovers servers for storage virtual machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs domain discovered-servers reset-servers -vserver vs1
```

```
cluster1::> vserver cifs domain discovered-servers show
```

```
Node: node1  
Vserver: vs1
```

Domain Name	Type	Preference	DC-Name	DC-Address	Status
example.com	MS-LDAP	adequate	DC-1	1.1.3.4	OK
example.com	MS-LDAP	adequate	DC-2	1.1.3.5	OK
example.com	MS-DC	adequate	DC-1	1.1.3.4	OK
example.com	MS-DC	adequate	DC-2	1.1.3.5	OK

## Related information

[Displaying information about discovered servers](#)

[Stopping or starting the CIFS server](#)

## Manage domain controller discovery

Beginning with ONTAP 9.3, you can modify the default process by which domain controllers (DCs) are discovered. This enables you to limit discovery to your site or to a pool of preferred DCs, which can lead to performance improvements depending on the environment.

### About this task

By default, the dynamic discovery process discovers all available DCs, including any preferred DCs, all DCs in the local site, and all remote DCs. This configuration can lead to latency in authentication and accessing shares in certain environments. If you have already determined the pool of DCs that you want to use, or if the remote DCs are inadequate or inaccessible, you can change the discovery method.

In ONTAP 9.3 and later releases, the `discovery-mode` parameter of the `cifs domain discovered-servers` command enables you to select one of the following discovery options:

- All DCs in the domain are discovered.
- Only DCs in the local site are discovered.

The `default-site` parameter for the SMB server must be defined to use this mode.

- Server discovery is not performed, the SMB server configuration depends only on preferred DCs.

To use this mode, you must first define the preferred DCs for the SMB server.

## Step

1. Specify the desired discovery option: `vserver cifs domain discovered-servers discovery-mode modify -vserver vserver_name -mode {all|site|none}`

Options for the `mode` parameter:

- `all`

Discover all available DCs (default).

- `site`

Limit DC discovery to your site.

- `none`

Use only preferred DCs and not perform discovery.

### Add preferred domain controllers

ONTAP automatically discovers domain controllers through DNS. Optionally, you can add one or more domain controllers to the list of preferred domain controllers for a specific domain.

#### About this task

If a preferred domain controller list already exists for the specified domain, the new list is merged with the existing list.

#### Step

1. To add to the list of preferred domain controllers, enter the following command:

```
vserver cifs domain preferred-dc add -vserver vserver_name -domain domain_name
-preferred-dc IP_address, ...+
```

`-vserver vserver_name` specifies the storage virtual machine (SVM) name.

`-domain domain_name` specifies the fully qualified Active Directory name of the domain to which the specified domain controllers belong.

`-preferred-dc IP_address,...` specifies one or more IP addresses of the preferred domain controllers, as a comma-delimited list, in order of preference.

#### Example

The following command adds domain controllers 172.17.102.25 and 172.17.102.24 to the list of preferred domain controllers that the SMB server on SVM vs1 uses to manage external access to the `cifs.lab.example.com` domain.

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

#### Related information

[Commands for managing preferred domain controllers](#)

## Commands for managing preferred domain controllers

You need to know the commands for adding, displaying, and removing preferred domain controllers.

If you want to...	Use this command...
Add a preferred domain controller	<code>vserver cifs domain preferred-dc add</code>
Display preferred domain controllers	<code>vserver cifs domain preferred-dc show</code>
Remove a preferred domain controller	<code>vserver cifs domain preferred-dc remove</code>

See the man page for each command for more information.

### Related information

[Adding preferred domain controllers](#)

### Enable SMB2 connections to domain controllers

Beginning with ONTAP 9.1, you can enable SMB version 2.0 to connect to a domain controller. Doing so is necessary if you have disabled SMB 1.0 on domain controllers. Beginning with ONTAP 9.2, SMB2 is enabled by default.

### About this task

The `smb2-enabled-for-dc-connections` command option enables the system default for the release of ONTAP you are using. The system default for ONTAP 9.1 is enabled for SMB 1.0 and disabled for SMB 2.0. The system default for ONTAP 9.2 is enabled for SMB 1.0 and enabled for SMB 2.0. If the domain controller cannot negotiate SMB 2.0 initially, it uses SMB 1.0.

SMB 1.0 can be disabled from ONTAP to a domain controller. In ONTAP 9.1, if SMB 1.0 has been disabled, SMB 2.0 must be enabled in order to communicate with a domain controller.



If `-smb1-enabled-for-dc-connections` is set to `false` while `-smb1-enabled` is set to `true`, ONTAP denies SMB 1.0 connections as the client, but continues to accept inbound SMB 1.0 connections as the server. See the topic, *Enabling and disabling SMB versions* in this guide.

### Steps

1. Before changing SMB security settings, verify which SMB versions are enabled: `vserver cifs security show`
2. Scroll down the list to see the SMB versions.
3. Perform the appropriate command, using the `smb2-enabled-for-dc-connections` option.

If you want SMB2 to be...	Enter the command...
Enabled	<code>vserver cifs security modify -vserver <i>vserver_name</i> -smb2-enabled-for-dc-connections true</code>

If you want SMB2 to be...	Enter the command...
Disabled	<pre>vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc -connections false</pre>

## Related information

[Supported SMB versions and functionality](#)

### Enable encrypted connections to domain controllers

Beginning with ONTAP 9.8, you can specify that connections to domain controllers be encrypted.

#### About this task

ONTAP requires encryption for domain controller (DC) communications when the `-encryption-required-for-dc-connection` option is set to `true`; the default is `false`. When the option is set, only the SMB3 protocol will be used for ONTAP-DC connections, because encryption is only supported by SMB3.

When encrypted DC communications are required, the `-smb2-enabled-for-dc-connections` option is ignored, because ONTAP only negotiates SMB3 connections. If a DC doesn't support SMB3 and encryption, ONTAP will not connect with it.

#### Step

1. Enable encrypted communication with the DC: 

```
vserver cifs security modify -vserver svm_name -encryption-required-for-dc-connection true
```

## Use null sessions to access storage in non-Kerberos environments

### Use null sessions to access storage in non-Kerberos environments overview

Null session access provides permissions for network resources, such as storage system data, and to client-based services running under the local system. A null session occurs when a client process uses the "system" account to access a network resource. Null session configuration is specific to non-Kerberos authentication.

#### How the storage system provides null session access

Because null session shares do not require authentication, clients that require null session access must have their IP addresses mapped on the storage system.

By default, unmapped null session clients can access certain ONTAP system services, such as share enumeration, but they are restricted from accessing any storage system data.



ONTAP supports Windows RestrictAnonymous registry setting values with the `-restrict-anonymous` option. This enables you to control the extent to which unmapped null users can view or access system resources. For example, you can disable share enumeration and access to the IPC\$ share (the hidden named pipe share). The `vserver cifs options modify` and `vserver cifs options show man` pages provide more information about the `-restrict-anonymous` option.

Unless otherwise configured, a client running a local process that requests storage system access through a null session is a member only of nonrestrictive groups, such as “everyone”. To limit null session access to selected storage system resources, you might want to create a group to which all null session clients belong; creating this group enables you to restrict storage system access and to set storage system resource permissions that apply specifically to null session clients.

ONTAP provides a mapping syntax in the `vserver name-mapping` command set to specify the IP address of clients allowed access to storage system resources using a null user session. After you create a group for null users, you can specify access restrictions for storage system resources and resource permissions that apply only to null sessions. Null user is identified as anonymous logon. Null users do not have access to any home directory.

Any null user accessing the storage system from a mapped IP address is granted mapped user permissions. Consider appropriate precautions to prevent unauthorized access to storage systems mapped with null users. For maximum protection, place the storage system and all clients requiring null user storage system access on a separate network, to eliminate the possibility of IP address “spoofing”.

## Related information

[Configuring access restrictions for anonymous users](#)

### Grant null users access to file system shares

You can allow access to your storage system resources by null session clients by assigning a group to be used by null session clients and recording the IP addresses of null session clients to add to the storage system’s list of clients allowed to access data using null sessions.

### Steps

1. Use the `vserver name-mapping create` command to map the null user to any valid windows user, with an IP qualifier.

The following command maps the null user to user1 with a valid host name google.com:

```
vserver name-mapping create -direction win-unix -position 1 -pattern
"ANONYMOUS LOGON" -replacement user1 - hostname google.com
```

The following command maps the null user to user1 with a valid IP address 10.238.2.54/32:

```
vserver name-mapping create -direction win-unix -position 2 -pattern
"ANONYMOUS LOGON" -replacement user1 -address 10.238.2.54/32
```

2. Use the `vserver name-mapping show` command to confirm the name mapping.

```
vserver name-mapping show

Vserver:    vs1
Direction: win-unix
Position Hostname          IP Address/Mask
-----
1          -              10.72.40.83/32      Pattern: anonymous logon
                                      Replacement: user1
```

3. Use the `vserver cifs options modify -win-name-for-null-user` command to assign Windows membership to the null user.

This option is applicable only when there is a valid name mapping for the null user.

```
vserver cifs options modify -win-name-for-null-user user1
```

4. Use the `vserver cifs options show` command to confirm the mapping of the null user to the Windows user or group.

```
vserver cifs options show

Vserver :vs1

Map Null User to Windows User of Group: user1
```

## Manage NetBIOS aliases for SMB servers

### Manage NetBIOS aliases for SMB servers overview

NetBIOS aliases are alternative names for your SMB server that SMB clients can use when connecting to the SMB server. Configuring NetBIOS aliases for a SMB server can be useful when you are consolidating data from other file servers to the SMB server and want the SMB server to respond to the original file servers' names.

You can specify a list of NetBIOS aliases when you create the SMB server or at any time after you create the SMB server. You can add or remove NetBIOS aliases from the list at any time. You can connect to the SMB server using any of the names in the NetBIOS alias list.

### Related information

[Displaying information about NetBIOS over TCP connections](#)



## Add a list of NetBIOS aliases to the SMB server

If you want SMB clients to connect to the SMB server by using an alias, you can create a list of NetBIOS aliases, or you can add NetBIOS aliases to an existing list of NetBIOS aliases.

### About this task

- The NetBIOS alias name can be 15 up to characters in length.
- You can configure up to 200 NetBIOS aliases on the SMB server.
- The following characters are not allowed:

```
@ # * ( ) = + [ ] | ; : " , < > \ / ?
```

### Steps

1. Add the NetBIOS aliases:

```
vserver cifs add-netbios-aliases -vserver vserver_name -netbios-aliases  
NetBIOS_alias,...
```

```
vserver cifs add-netbios-aliases -vserver vs1 -netbios-aliases  
alias_1,alias_2,alias_3
```

- You can specify one or more NetBIOS aliases by using a comma-delimited list.
- The specified NetBIOS aliases are added to the existing list.
- A new list of NetBIOS aliases is created if the list is currently empty.

2. Verify that the NetBIOS aliases were added correctly: `vserver cifs show -vserver vserver_name -display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1
```

```
Server Name: CIFS_SERVER
```

```
NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

### Related information

[Removing NetBIOS aliases from the NetBIOS alias list](#)

[Displaying the list of NetBIOS aliases on CIFS servers](#)

### Remove NetBIOS aliases from the NetBIOS alias list

If you do not need specific NetBIOS aliases for a CIFS server, you can remove those NetBIOS aliases from the list. You can also remove all NetBIOS aliases from the list.

### About this task

You can remove more than one NetBIOS alias by using a comma-delimited list. You can remove all of the NetBIOS aliases on a CIFS server by specifying `-` as the value for the `-netbios-aliases` parameter.

## Steps

1. Perform one of the following actions:

If you want to remove...	Enter...
Specific NetBIOS aliases from the list	<pre>vserver cifs remove-netbios-aliases -vserver _vserver_name_ -netbios -aliases _NetBIOS_alias_,...</pre>
All NetBIOS aliases from the list	<pre>vserver cifs remove-netbios-aliases -vserver vserver_name -netbios-aliases -</pre>

```
vserver cifs remove-netbios-aliases -vserver vs1 -netbios-aliases alias_1
```

2. Verify that the specified NetBIOS aliases were removed: `vserver cifs show -vserver vserver_name -display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1  
  
Server Name: CIFS_SERVER  
NetBIOS Aliases: ALIAS_2, ALIAS_3
```

## Display the list of NetBIOS aliases on CIFS servers

You can display the list of NetBIOS aliases. This can be useful when you want to determine the list of names over which SMB clients can make connections to the CIFS server.

### Step

1. Perform one of the following actions:

If you want to display information about...	Enter...
A CIFS server's NetBIOS aliases	<pre>vserver cifs show -display-netbios -aliases</pre>
The list of NetBIOS aliases as part of the detailed CIFS server information	<pre>vserver cifs show -instance</pre>

The following example displays information about a CIFS server's NetBIOS aliases:

```
vserver cifs show -display-netbios-aliases
```

```
Vserver: vs1
```

```
Server Name: CIFS_SERVER
```

```
NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

The following example displays the list of NetBIOS aliases as part of the detailed CIFS server information:

```
vserver cifs show -instance
```

```

                                Vserver: vs1
                                CIFS Server NetBIOS Name: CIFS_SERVER
                                NetBIOS Domain/Workgroup Name: EXAMPLE
                                Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                                Authentication Style: domain
                                CIFS Server Administrative Status: up
                                CIFS Server Description:
                                List of NetBIOS Aliases: ALIAS_1, ALIAS_2,
ALIAS_3
```

See the man page for the commands for more information.

## Related information

[Adding a list of NetBIOS aliases to the CIFS server](#)

[Commands for managing CIFS servers](#)

### Determine whether SMB clients are connected using NetBIOS aliases

You can determine whether SMB clients are connected using NetBIOS aliases, and if so, which NetBIOS alias is used to make the connection. This can be useful when troubleshooting connection issues.

#### About this task

You must use the `-instance` parameter to display the NetBIOS alias (if any) associated with an SMB connection. If the CIFS server name or an IP address is used to make the SMB connection, the output for the `NetBIOS Name` field is `-` (hyphen).

#### Step

1. Perform the desired action:

If you want to display NetBIOS information for...	Enter...
SMB connections	<code>vserver cifs session show -instance</code>

If you want to display NetBIOS information for...	Enter...
Connections using a specified NetBIOS alias:	<pre>vserver cifs session show -instance -netbios-name netbios_name</pre>

The following example displays information about the NetBIOS alias used to make the SMB connection with session ID 1:

```
vserver cifs session show -session-id 1 -instance
```

```

Node: nodel
Vserver: vs1
Session ID: 1
Connection ID: 127834
Incoming Data LIF IP Address: 10.1.1.25
Workstation: 10.2.2.50
Authentication Mechanism: NTLMv2
Windows User: EXAMPLE\user1
UNIX User: user1
Open Shares: 2
Open Files: 2
Open Other: 0
Connected Time: 1d 1h 10m 5s
Idle Time: 22s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: ALIAS1
SMB Encryption Status: Unencrypted
```

## Manage miscellaneous SMB server tasks

### Stop or start the CIFS server

You can stop the CIFS server on a SVM, which can be useful when performing tasks while users are not accessing data over SMB shares. You can restart SMB access by starting the CIFS server. By stopping the CIFS server, you can also modify the protocols allowed on the storage virtual machine (SVM).

#### Steps

1. Perform one of the following actions:

If you want to...	Enter the command...
Stop the CIFS server	<code>vserver cifs stop -vserver vserver_name [-foreground {true false}]</code>
Start the CIFS server	<code>vserver cifs start -vserver vserver_name [-foreground {true false}]</code>

`-foreground` specifies whether the command should execute in the foreground or background. If you do not enter this parameter, it is set to `true`, and the command is executed in the foreground.

2. Verify that the CIFS server administrative status is correct by using the `vserver cifs show` command.

### Example

The following commands start the CIFS server on SVM vs1:

```
cluster1::> vserver start -vserver vs1

cluster1::> vserver cifs show -vserver vs1

                                Vserver: vs1
                                CIFS Server NetBIOS Name: VS1
                                NetBIOS Domain/Workgroup Name: DOMAIN
                                Fully Qualified Domain Name: DOMAIN.LOCAL
Default Site Used by LIFs Without Site Membership:
                                Authentication Style: domain
                                CIFS Server Administrative Status: up
```

### Related information

[Displaying information about discovered servers](#)

[Resetting and rediscovering servers](#)

### Move CIFS servers to different OUs

The CIFS server create-process uses the default organizational unit (OU) `CN=Computers` during setup unless you specify a different OU. You can move CIFS servers to different OUs after setup.

### Steps

1. On the Windows server, open the **Active Directory Users and Computers** tree.
2. Locate the Active Directory object for the storage virtual machine (SVM).
3. Right-click the object and select **Move**.
4. Select the OU that you want to associate with the SVM

## Results

The SVM object is placed in the selected OU.

### Modify the dynamic DNS domain on the SVM before moving the SMB server

If you want the Active Directory-integrated DNS server to dynamically register the SMB server's DNS records in DNS when you move the SMB server to another domain, you must modify dynamic DNS (DDNS) on the storage virtual machine (SVM) before moving the SMB server.

#### Before you begin

DNS name services must be modified on the SVM to use the DNS domain that contains the service location records for the new domain that will contain the SMB server computer account. If you are using secure DDNS, you must use Active Directory-integrated DNS name servers.

#### About this task

Although DDNS (if configured on the SVM) automatically adds the DNS records for data LIFs to the new domain, the DNS records for the original domain are not automatically deleted from the original DNS server. You must delete them manually.

To complete your DDNS modifications before moving the SMB server, see the following topic:

[Configure dynamic DNS services](#)

### Join a SVM to an Active Directory domain

You can join a storage virtual machine (SVM) to an Active Directory domain without deleting the existing SMB server by modifying the domain using the `vserver cifs modify` command. You can rejoin the current domain or join a new one.

#### Before you begin

- The SVM must already have a DNS configuration.
- The DNS configuration for the SVM must be able to serve the target domain.

The DNS servers must contain the service location records (SRV) for the domain LDAP and domain controller servers.

#### About this task

- The administrative status of the CIFS server must be set to “down” to proceed with Active Directory domain modification.
- If the command completes successfully, the administrative status is automatically set to “up”.
- When joining a domain, this command might take several minutes to complete.

#### Steps

1. Join the SVM to the CIFS server domain: `vserver cifs modify -vserver vserver_name -domain domain_name -status-admin down`

For more information, see the man page for the `vserver cifs modify` command. If you need to reconfigure DNS for the new domain, see the man page for the `vserver dns modify` command.

In order to create an Active Directory machine account for the SMB server, you must supply the name and password of a Windows account with sufficient privileges to add computers to the `ou= example ou` container within the `example.com` domain.

Beginning with ONTAP 9.7, your AD administrator can provide you with a URI to a keytab file as an alternative to providing you with a name and password to a privileged Windows account. When you receive the URI, include it in the `-keytab-uri` parameter with the `vserver cifs` commands.

2. Verify that the CIFS server is in the desired Active Directory domain: `vserver cifs show`

### Example

In the following example, the SMB server “CIFSSERVER1” on SVM `vs1` joins the `example.com` domain using keytab authentication:

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status
-admin down -keytab-uri http://admin.example.com/ontap1.keytab
```

```
cluster1::> vserver cifs show
```

	Server	Status	Domain/Workgroup	Authentication
Vserver	Name	Admin	Name	Style
-----	-----	-----	-----	-----
vs1	CIFSSERVER1	up	EXAMPLE	domain

### Display information about NetBIOS over TCP connections

You can display information about NetBIOS over TCP (NBT) connections. This can be useful when troubleshooting NetBIOS-related issues.

### Step

1. Use the `vserver cifs nbtstat` command to display information about NetBIOS over TCP connections.



NetBIOS name service (NBNS) over IPv6 is not supported.

### Example

The following example shows the NetBIOS name service information displayed for “cluster1”:

```
cluster1::> vserver cifs nbtstat
```

```
Vserver: vs1
Node:    cluster1-01
Interfaces:
          10.10.10.32
          10.10.10.33
Servers:
          17.17.1.2 (active )
NBT Scope:
          [ ]
NBT Mode:
          [h]
NBT Name      NetBIOS Suffix  State   Time Left  Type
-----
CLUSTER_1    00                        wins    57
CLUSTER_1    20                        wins    57

Vserver: vs1
Node:    cluster1-02
Interfaces:
          10.10.10.35
Servers:
          17.17.1.2 (active )
CLUSTER_1    00                        wins    58
CLUSTER_1    20                        wins    58
4 entries were displayed.
```

### Commands for managing SMB servers

You need to know the commands for creating, displaying, modifying, stopping, starting, and deleting SMB servers. There are also commands to reset and rediscover servers, change or reset machine account passwords, schedule changes for machine account passwords, and add or remove NetBIOS aliases.

If you want to...	Use this command...
Create an SMB server	<code>vserver cifs create</code>
Display information about an SMB server	<code>vserver cifs show</code>
Modify an SMB server	<code>vserver cifs modify</code>
Move an SMB server to another domain	<code>vserver cifs modify</code>



Stop an SMB server	<code>vserver cifs stop</code>
Start an SMB server	<code>vserver cifs start</code>
Delete an SMB server	<code>vserver cifs delete</code>
Reset and rediscover servers for the SMB server	<code>vserver cifs domain discovered-servers reset-servers</code>
Change the SMB server's machine account password	<code>vserver cifs domain password change</code>
Reset the SMB server's machine account password	<code>vserver cifs domain password change</code>
Schedule automatic password changes for the SMB server's machine account	<code>vserver cifs domain password schedule modify</code>
Add NetBIOS aliases for the SMB server	<code>vserver cifs add-netbios-aliases</code>
Remove NetBIOS aliases for the SMB server	<code>vserver cifs remove-netbios-aliases</code>

See the man page for each command for more information.

### Related information

[What happens to local users and groups when deleting SMB servers](#)

### Enable the NetBios name service

Beginning with ONTAP 9, the NetBios name service (NBNS, sometimes called Windows Internet Name Service or WINS) is disabled by default. Previously, CIFS-enabled storage virtual machines (SVMs) sent name registration broadcasts regardless of whether WINS was enabled on a network. To limit such broadcasts to configurations where NBNS is required, you must enable NBNS explicitly for new CIFS servers.

### Before you begin

- If you are already using NBNS and you upgrade to ONTAP 9, it is not necessary to complete this task. NBNS will continue to work as before.
- NBNS is enabled over UDP (port 137).
- NBNS over IPv6 is not supported.

### Steps

1. Set the privilege level to advanced.

```
set -privilege advanced
```

2. Enable NBNS on a CIFS server.

```
vserver cifs options modify -vserver <vserver name> -is-nbns-enabled true
```

3. Return to the admin privilege level.

```
set -privilege admin
```

## Use IPv6 for SMB access and SMB services

### Requirements for using IPv6

Before you can use IPv6 on your SMB server, you need to know which versions of ONTAP and SMB support it and what the license requirements are.

### ONTAP license requirements

No special license is required for IPv6 when SMB is licensed.

### SMB protocol version requirements

- For SVMs, ONTAP supports IPv6 on all versions of the SMB protocol.



NetBIOS name service (NBNS) over IPv6 is not supported.

### Support for IPv6 with SMB access and CIFS services

If you want to use IPv6 on your CIFS server, you need to be aware of how ONTAP supports IPv6 for SMB access and network communication for CIFS services.

### Windows client and server support

ONTAP provides support for Windows servers and clients that support IPv6. The following describes Microsoft Windows client and server IPv6 support:

- Windows XP and Windows 2003 support IPv6 for SMB file sharing.

These versions provide limited support for IPv6.

- Windows 7, Windows 8, Windows Server 2008, Windows Server 2012 and later support IPv6 for both SMB file sharing and Active Directory services, including DNS, LDAP, CLDAP, and Kerberos services.

If IPv6 addresses are configured, Windows 7 and Windows Server 2008 and later releases use IPv6 by default for Active Directory services. Both NTLM and Kerberos authentication over IPv6 connections are supported.

All Windows clients supported by ONTAP can connect to SMB shares by using IPv6 addresses.

For the latest information about which Windows clients ONTAP supports, see the Interoperability Matrix.

## Interoperability Matrix



NT domains are not supported for IPv6.

### Additional CIFS services support

In addition to IPv6 support for SMB file shares and Active Directory services, ONTAP provides IPv6 support for the following:

- Client-side services, including offline folders, roaming profiles, folder redirection, and Previous Versions
- Server-side services, including Dynamic home directories (Home Directory feature), symlinks and Widelinks, BranchCache, ODX copy offload, automatic node referrals, and Previous Versions
- File access management services, including the use of Windows local users and groups for access control and rights management, setting file permissions and audit policies using the CLI, security tracing, file locks management, and monitoring SMB activity
- NAS multiprotocol auditing
- FPolicy
- Continuously available shares, Witness protocol, and Remote VSS (used with Hyper-V over SMB configurations)

### Name service and authentication service support

Communication with the following name services are supported with IPv6:

- Domain controllers
- DNS servers
- LDAP servers
- KDC servers
- NIS servers

### How CIFS servers use IPv6 to connect to external servers

To create a configuration that meets your requirements, you must be aware of how CIFS servers use IPv6 when making connections to external servers.

- Source address selection

If an attempt is made to connect to an external server, the source address selected must be of the same type as the destination address. For example, if connecting to an IPv6 address, the storage virtual machine (SVM) hosting the CIFS server must have a data LIF or management LIF that has an IPv6 address to use as the source address. Similarly, if connecting to an IPv4 address, the SVM must have a data LIF or management LIF that has an IPv4 address to use as the source address.

- For servers dynamically discovered using DNS, server discovery is performed as follows:
  - If IPv6 is disabled on the cluster, only IPv4 servers addresses are discovered.
  - If IPv6 is enabled on the cluster, both IPv4 and IPv6 server addresses are discovered. Either type might be used depending upon the suitability of the server to which the address belongs and the

availability of IPv6 or IPv4 data or management LIFs.

Dynamic server discovery is used for discovering Domain Controllers and their associated services, such as LSA, NETLOGON, Kerberos, and LDAP.

- DNS server connectivity

Whether the SVM uses IPv6 when connecting to a DNS server depends on the DNS name services configuration. If DNS services are configured to use IPv6 addresses, connections are made by using IPv6. If desired, the DNS name services configuration can use IPv4 addresses so that connections to DNS servers continue to use IPv4 addresses. Combinations of IPv4 and IPv6 addresses can be specified when configuring DNS name services.

- LDAP server connectivity

Whether the SVM uses IPv6 when connecting to an LDAP server depends on the LDAP client configuration. If the LDAP client is configured to use IPv6 addresses, connections are made by using IPv6. If desired, the LDAP client configuration can use IPv4 addresses so that connections to LDAP servers continue to use IPv4 addresses. Combinations of IPv4 and IPv6 addresses can be specified when configuring the LDAP client configuration.



The LDAP client configuration is used when configuring LDAP for UNIX user, group, and netgroup name services.

- NIS server connectivity

Whether the SVM uses IPv6 when connecting to a NIS server depends on the NIS name services configuration. If NIS services are configured to use IPv6 addresses, connections are made by using IPv6. If desired, the NIS name services configuration can use IPv4 addresses so that connections to NIS servers continue to use IPv4 addresses. Combinations of IPv4 and IPv6 addresses can be specified when configuring NIS name services.



NIS name services are used for storing and managing UNIX user, group, netgroup, and host name objects.

## Related information

[Enabling IPv6 for SMB \(cluster administrators only\)](#)

[Monitoring and displaying information about IPv6 SMB sessions](#)

### Enable IPv6 for SMB (cluster administrators only)

IPv6 networks are not enabled during cluster setup. A cluster administrator must enable IPv6 after cluster setup is complete to use IPv6 for SMB. When the cluster administrator enables IPv6, it is enabled for the entire cluster.

### Step

1. Enable IPv6: `network options ipv6 modify -enabled true`

For more information about enabling IPv6 on the cluster and configuring IPv6 LIFs, see the *Network Management Guide*.

IPv6 is enabled. IPv6 data LIFs for SMB access can be configured.

## Related information

[Monitoring and displaying information about IPv6 SMB sessions](#)

[Network management](#)

### Disable IPv6 for SMB

Even though IPv6 is enabled on the cluster using a network option, you cannot disable IPv6 for SMB by using the same command. Instead, ONTAP disables IPv6 when the cluster administrator disables the last IPv6-enabled interface on the cluster. You should communicate with the cluster administrator about management of your IPv6 enabled interfaces.

For more information about disabling IPv6 on the cluster, see the *Network Management Guide*.

## Related information

[Network management](#)

### Monitor and display information about IPv6 SMB sessions

You can monitor and display information about SMB sessions that are connected using IPv6 networks. This information is useful in determining which clients are connecting using IPv6 as well as other useful information about IPv6 SMB sessions.

#### Step

1. Perform the desired action:

If you want to determine whether...	Enter the command...
SMB sessions to a storage virtual machine (SVM) are connected using IPv6	<pre>vserver cifs session show -vserver vserver_name -instance</pre>
IPv6 is used for SMB sessions through a specified LIF address	<pre>vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address -instance</pre> <p><i>LIF_IP_address</i> is the data LIF's IPv6 address.</p>

## Set up file access using SMB

### Configure security styles

How security styles affect data access

#### What the security styles and their effects are

There are four different security styles: UNIX, NTFS, mixed, and unified. Each security style has a different effect on how permissions are handled for data. You must understand the different effects to ensure that you select the appropriate security style for your

purposes.

It is important to understand that security styles do not determine what client types can or cannot access data. Security styles only determine the type of permissions ONTAP uses to control data access and what client type can modify these permissions.

For example, if a volume uses UNIX security style, SMB clients can still access data (provided that they properly authenticate and authorize) due to the multiprotocol nature of ONTAP. However, ONTAP uses UNIX permissions that only UNIX clients can modify using native tools.

Security style	Clients that can modify permissions	Permissions that clients can use	Resulting effective security style	Clients that can access files
UNIX	NFS	NFSv3 mode bits	UNIX	NFS and SMB
		NFSv4.x ACLs	UNIX	
NTFS	SMB	NTFS ACLs	NTFS	
Mixed	NFS or SMB	NFSv3 mode bits	UNIX	
		NFSv4.x ACLs	UNIX	
NTFS ACLs	NTFS	Unified	NFS or SMB	
NFSv3 mode bits	UNIX			
NFSv4.1 ACLs	UNIX	NTFS ACLs	NTFS	
Unified (For infinite volumes only, in ONTAP 9.4 and earlier releases.)	NFS or SMB	NFSv3 mode bits	Unix	
		NFSv4.1 ACLs		NTFS ACLs

FlexVol volumes support UNIX, NTFS, and mixed security styles. When the security style is mixed or unified, the effective permissions depend on the client type that last modified the permissions because users set the security style on an individual basis. If the last client that modified permissions was an NFSv3 client, the permissions are UNIX NFSv3 mode bits. If the last client was an NFSv4 client, the permissions are NFSv4 ACLs. If the last client was an SMB client, the permissions are Windows NTFS ACLs.

The unified security style is only available with infinite volumes, which are no longer supported in ONTAP 9.5 and later releases. For more information, see [FlexGroup volumes management overview](#).

Beginning with ONTAP 9.2, the `show-effective-permissions` parameter to the `vserver security file-directory` command enables you to display effective permissions granted to a Windows or UNIX user on the specified file or folder path. In addition, the optional parameter `-share-name` enables you to display the effective share permission.



ONTAP initially sets some default file permissions. By default, the effective security style on all data in UNIX, mixed, and unified security style volumes is UNIX and the effective permissions type is UNIX mode bits (0755 unless specified otherwise) until configured by a client as allowed by the default security style. By default, the effective security style on all data in NTFS security style volumes is NTFS and has an ACL allowing full control to everyone.

2021-12-09, BURT 1443623

### Where and when to set security styles

Security styles can be set on FlexVol volumes (both root or data volumes) and qtrees. Security styles can be set manually at the time of creation, inherited automatically, or changed at a later time.

### Decide which security style to use on SVMs

To help you decide which security style to use on a volume, you should consider two factors. The primary factor is the type of administrator that manages the file system. The secondary factor is the type of user or service that accesses the data on the volume.

When you configure the security style on a volume, you should consider the needs of your environment to ensure that you select the best security style and avoid issues with managing permissions. The following considerations can help you decide:

Security style	Choose if...
UNIX	<ul style="list-style-type: none"><li>• The file system is managed by a UNIX administrator.</li><li>• The majority of users are NFS clients.</li><li>• An application accessing the data uses a UNIX user as the service account.</li></ul>
NTFS	<ul style="list-style-type: none"><li>• The file system is managed by a Windows administrator.</li><li>• The majority of users are SMB clients.</li><li>• An application accessing the data uses a Windows user as the service account.</li></ul>
Mixed	The file system is managed by both UNIX and Windows administrators and users consist of both NFS and SMB clients.

### How security style inheritance works

If you do not specify the security style when creating a new FlexVol volume or a qtree, it inherits its security style in different ways.

Security styles are inherited in the following manner:

- A FlexVol volume inherits the security style of the root volume of its containing SVM.
- A qtree inherits the security style of its containing FlexVol volume.
- A file or directory inherits the security style of its containing FlexVol volume or qtree.

## How ONTAP preserves UNIX permissions

When files in a FlexVol volume that currently have UNIX permissions are edited and saved by Windows applications, ONTAP can preserve the UNIX permissions.

When applications on Windows clients edit and save files, they read the security properties of the file, create a new temporary file, apply those properties to the temporary file, and then give the temporary file the original file name.

When Windows clients perform a query for the security properties, they receive a constructed ACL that exactly represents the UNIX permissions. The sole purpose of this constructed ACL is to preserve the file's UNIX permissions as files are updated by Windows applications to ensure that the resulting files have the same UNIX permissions. ONTAP does not set any NTFS ACLs using the constructed ACL.

## Manage UNIX permissions using the Windows Security tab

If you want to manipulate UNIX permissions of files or folders in mixed security-style volumes or qtrees on SVMs, you can use the Security tab on Windows clients. Alternatively, you can use applications that can query and set Windows ACLs.

- Modifying UNIX permissions

You can use the Windows Security tab to view and change UNIX permissions for a mixed security-style volume or qtree. If you use the main Windows Security tab to change UNIX permissions, you must first remove the existing ACE you want to edit (this sets the mode bits to 0) before you make your changes. Alternatively, you can use the Advanced editor to change permissions.

If mode permissions are used, you can directly change the mode permissions for the listed UID, GID, and others (everyone else with an account on the computer). For example, if the displayed UID has r-x permissions, you can change the UID permissions to rwx.

- Changing UNIX permissions to NTFS permissions

You can use the Windows Security tab to replace UNIX security objects with Windows security objects on a mixed security-style volume or qtree where the files and folders have a UNIX effective security style.

You must first remove all listed UNIX permission entries before you can replace them with the desired Windows User and Group objects. You can then configure NTFS-based ACLs on the Windows User and Group objects. By removing all UNIX security objects and adding only Windows Users and Groups to a file or folder in a mixed security-style volume or qtree, you change the effective security style on the file or folder from UNIX to NTFS.

When changing permissions on a folder, the default Windows behavior is to propagate these changes to all subfolders and files. Therefore, you must change the propagation choice to the desired setting if you do not want to propagate a change in security style to all child folders, subfolders, and files.



## Configure security styles on SVM root volumes

You configure the storage virtual machine (SVM) root volume security style to determine the type of permissions used for data on the root volume of the SVM.

### Steps

1. Use the `vserver create` command with the `-rootvolume-security-style` parameter to define the security style.

The possible options for the root volume security style are `unix`, `ntfs`, or `mixed`.

2. Display and verify the configuration, including the root volume security style of the SVM you created:

```
vserver show -vserver vserver_name
```

## Configure security styles on FlexVol volumes

You configure the FlexVol volume security style to determine the type of permissions used for data on FlexVol volumes of the storage virtual machine (SVM).

### Steps

1. Perform one of the following actions:

If the FlexVol volume...	Use the command...
Does not yet exist	<code>volume create</code> and include the <code>-security -style</code> parameter to specify the security style.
Already exists	<code>volume modify</code> and include the <code>-security -style</code> parameter to specify the security style.

The possible options for the FlexVol volume security style are `unix`, `ntfs`, or `mixed`.

If you do not specify a security style when creating a FlexVol volume, the volume inherits the security style of the root volume.

For more information about the `volume create` or `volume modify` commands, see [Logical storage management](#).

2. To display the configuration, including the security style of the FlexVol volume you created, enter the following command:

```
volume show -volume volume_name -instance
```

## Configure security styles on qtrees

You configure the qtree volume security style to determine the type of permissions used for data on qtrees.

### Steps

1. Perform one of the following actions:

If the qtree...	Use the command...
Does not exist yet	<code>volume qtree create</code> and include the <code>-security-style</code> parameter to specify the security style.
Already exists	<code>volume qtree modify</code> and include the <code>-security-style</code> parameter to specify the security style.

The possible options for the qtree security style are `unix`, `ntfs`, or `mixed`.

If you do not specify a security style when creating a qtree, the default security style is `mixed`.

For more information about the `volume qtree create` or `volume qtree modify` commands, see [Logical storage management](#).

- To display the configuration, including the security style of the qtree you created, enter the following command: `volume qtree show -qtree qtree_name -instance`

## Create and manage data volumes in NAS namespaces

### Create and manage data volumes in NAS namespaces overview

To manage file access in a NAS environment, you must manage data volumes and junction points on your storage virtual machine (SVM). This includes planning your namespace architecture, creating volumes with or without junction points, mounting or unmounting volumes, and displaying information about data volumes and NFS server or CIFS server namespaces.

#### Create data volumes with specified junction points

You can specify the junction point when you create a data volume. The resultant volume is automatically mounted at the junction point and is immediately available to configure for NAS access.

#### Before you begin

The aggregate in which you want to create the volume must already exist.



The following characters cannot be used in the junction path: `* # " > < | ? \`

In addition, the junction path length cannot be more than 255 characters.

#### Steps

- Create the volume with a junction point: `volume create -vserver vservers_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -junction-path junction_path`

The junction path must start with the root (`/`) and can contain both directories and junctioned volumes. The junction path does not need to contain the name of the volume. Junction paths are independent of the

volume name.

Specifying a volume security style is optional. If you do not specify a security style, ONTAP creates the volume with the same security style that is applied to the root volume of the storage virtual machine (SVM). However, the root volume's security style might not be the security style you want applied to the data volume you create. The recommendation is to specify the security style when you create the volume to minimize difficult-to-troubleshoot file-access issues.

The junction path is case insensitive; /ENG is the same as /eng. If you create a CIFS share, Windows treats the junction path as if it is case sensitive. For example, if the junction is /ENG, the path of a CIFS share must start with /ENG, not /eng.

There are many optional parameters that you can use to customize a data volume. To learn more about them, see the man pages for the `volume create` command.

2. Verify that the volume was created with the desired junction point: `volume show -vserver vserver_name -volume volume_name -junction`

### Example

The following example creates a volume named "home4" located on SVM vs1 that has a junction path /eng/home:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -volume home4 -junction
```

Vserver	Volume	Junction Active	Junction Path	Junction Path Source
vs1	home4	true	/eng/home	RW_volume

### Create data volumes without specifying junction points

You can create a data volume without specifying a junction point. The resultant volume is not automatically mounted, and is not available to configure for NAS access. You must mount the volume before you can configure SMB shares or NFS exports for that volume.

### Before you begin

The aggregate in which you want to create the volume must already exist.

### Steps

1. Create the volume without a junction point by using the following command: `volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed}`

Specifying a volume security style is optional. If you do not specify a security style, ONTAP creates the volume with the same security style that is applied to the root volume of the storage virtual machine (SVM). However, the root volume's security style might not be the security style you want applied to the data volume. The recommendation is to specify the security style when you create the volume to minimize

difficult-to-troubleshoot file-access issues.

There are many optional parameters that you can use to customize a data volume. To learn more about them, see the man pages for the `volume create` command.

2. Verify that the volume was created without a junction point: `volume show -vserver vs1 -volume volume_name -junction`

### Example

The following example creates a volume named “sales” located on SVM vs1 that is not mounted at a junction point:

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1 -junction
```

Vserver	Volume	Junction Active	Junction Path	Junction Path Source
vs1	data	true	/data	RW_volume
vs1	home4	true	/eng/home	RW_volume
vs1	vs1_root	-	/	-
vs1	sales	-	-	-

### Mount or unmount existing volumes in the NAS namespace

A volume must be mounted on the NAS namespace before you can configure NAS client access to data contained in the storage virtual machine (SVM) volumes. You can mount a volume to a junction point if it is not currently mounted. You can also unmount volumes.

#### About this task

If you unmount and offline a volume, all data within the junction point, including data in volumes with junction points contained within the unmounted volume’s namespace, are inaccessible to NAS clients.



To discontinue NAS client access to a volume, it is not sufficient to simply unmount the volume. You must offline the volume, or take other steps to ensure that client-side file handle caches are invalidated. For more information, see the following Knowledge Base article:[https://kb.netapp.com/Advice\\_and\\_Troubleshooting/Data\\_Storage\\_Software/ONTAP\\_OS/NFSv3\\_clients\\_still\\_have\\_access\\_to\\_a\\_volume\\_after\\_being\\_removed\\_from\\_the\\_namespace\\_in\\_ONTAP](https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/ONTAP_OS/NFSv3_clients_still_have_access_to_a_volume_after_being_removed_from_the_namespace_in_ONTAP)[NFSv3 clients still have access to a volume after being removed from the namespace in ONTAP]

When you unmount and offline a volume, data within the volume is not lost. Additionally, existing volume export policies and SMB shares created on the volume or on directories and junction points within the unmounted volume are retained. If you remount the unmounted volume, NAS clients can access the data contained within the volume using existing export policies and SMB shares.

### Steps

1. Perform the desired action:

If you want to...	Enter the commands...
Mount a volume	<pre>volume mount -vserver <i>svm_name</i> -volume <i>volume_name</i> -junction-path <i>junction_path</i></pre>
Unmount a volume	<pre>volume unmount -vserver <i>svm_name</i> -volume <i>volume_name</i> volume offline -vserver <i>svm_name</i> -volume <i>volume_name</i></pre>

2. Verify that the volume is in the desired mount state: `volume show -vserver vserver_name -volume volume_name -fields state,junction-path,junction-active`

### Examples

The following example mounts a volume named “sales” located on SVM vs1 to the junction point /sales:

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales
cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume   state    junction-path  junction-active
-----
vs1       data     online   /data          true
vs1       home4    online   /eng/home      true
vs1       sales    online   /sales         true
```

The following example unmounts and offlines a volume named “data” located on SVM vs1:

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume   state    junction-path  junction-active
-----
vs1       data     offline  -              -
vs1       home4    online   /eng/home      true
vs1       sales    online   /sales         true
```

### Display volume mount and junction point information

You can display information about mounted volumes for storage virtual machines (SVMs)

and the junction points to which the volumes are mounted. You can also determine which volumes are not mounted to a junction point. You can use this information to understand and manage your SVM namespace.

**Steps**

1. Perform the desired action:

If you want to display...	Enter the command...
Summary information about mounted and unmounted volumes on the SVM	<code>volume show -vserver vserver_name -junction</code>
Detailed information about mounted and unmounted volumes on the SVM	<code>volume show -vserver vserver_name -volume volume_name -instance</code>
Specific information about mounted and unmounted volumes on the SVM	<p>a. If necessary, you can display valid fields for the <code>-fields</code> parameter by using the following command: <code>volume show -fields ?</code></p> <p>b. Display the desired information by using the <code>-fields</code> parameter: <code>volume show -vserver vserver_name -fields fieldname,...</code></p>

**Examples**

The following example displays a summary of mounted and unmounted volumes on SVM vs1:

```
cluster1::> volume show -vserver vs1 -junction
Vserver      Volume      Junction
Active      Junction Path  Junction
Path Source
-----
vs1          data        true         /data         RW_volume
vs1          home4       true         /eng/home     RW_volume
vs1          vs1_root    -           /             -
vs1          sales       true         /sales        RW_volume
```

The following example displays information about specified fields for volumes located on SVM vs2:

```

cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume    aggregate size state  type security-style junction-path
junction-parent node
-----
vs2      data1      aggr3    2GB  online RW   unix          -          -
node3
vs2      data2      aggr3    1GB  online RW   ntfs          /data2
vs2_root node3
vs2      data2_1    aggr3    8GB  online RW   ntfs          /data2/d2_1
data2    node3
vs2      data2_2    aggr3    8GB  online RW   ntfs          /data2/d2_2
data2    node3
vs2      pubs      aggr1    1GB  online RW   unix          /publications
vs2_root node1
vs2      images    aggr3    2TB  online RW   ntfs          /images
vs2_root node3
vs2      logs      aggr1    1GB  online RW   unix          /logs
vs2_root node1
vs2      vs2_root  aggr3    1GB  online RW   ntfs          /          -
node3

```

## Configure name mappings

### Configure name mappings overview

ONTAP uses name mapping to map CIFS identities to UNIX identities, Kerberos identities to UNIX identities, and UNIX identities to CIFS identities. It needs this information to obtain user credentials and provide proper file access regardless of whether they are connecting from an NFS client or a CIFS client.

There are two exceptions where you do not have to use name mapping:

- You configure a pure UNIX environment and do not plan to use CIFS access or NTFS security style on volumes.
- You configure the default user to be used instead.

In this scenario, name mapping is not required because instead of mapping every individual client credential all client credentials are mapped to the same default user.

Note that you can use name mapping only for users, not for groups.

However, you can map a group of individual users to a specific user. For example, you can map all AD users that start or end with the word SALES to a specific UNIX user and to the user's UID.

## How name mapping works

When ONTAP has to map credentials for a user, it first checks the local name mapping database and LDAP server for an existing mapping. Whether it checks one or both and in which order is determined by the name service configuration of the SVM.

- For Windows to UNIX mapping

If no mapping is found, ONTAP checks whether the lowercase Windows user name is a valid user name in the UNIX domain. If this does not work, it uses the default UNIX user provided that it is configured. If the default UNIX user is not configured and ONTAP cannot obtain a mapping this way either, mapping fails and an error is returned.

- For UNIX to Windows mapping

If no mapping is found, ONTAP tries to find a Windows account that matches the UNIX name in the SMB domain. If this does not work, it uses the default SMB user, provided that it is configured. If the default CIFS user is not configured and ONTAP cannot obtain a mapping this way either, mapping fails and an error is returned.

Machine accounts are mapped to the specified default UNIX user by default. If no default UNIX user is specified, machine account mappings fail.

- Beginning with ONTAP 9.5, you can map machine accounts to users other than the default UNIX user.
- In ONTAP 9.4 and earlier, you cannot map machine accounts to other users.

Even if name mappings for machine accounts are defined, the mappings are ignored.

## Multidomain searches for UNIX user to Windows user name mappings

ONTAP supports multidomain searches when mapping UNIX users to Windows users. All discovered trusted domains are searched for matches to the replacement pattern until a matching result is returned. Alternatively, you can configure a list of preferred trusted domains, which is used instead of the discovered trusted domain list and is searched in order until a matching result is returned.

## How domain trusts affect UNIX user to Windows user name mapping searches

To understand how multidomain user name mapping works, you must understand how domain trusts work with ONTAP. Active Directory trust relationships with the CIFS server's home domain can be a bidirectional trust or can be one of two types of unidirectional trusts, either an inbound trust or an outbound trust. The home domain is the domain to which the CIFS server on the SVM belongs.

- *Bidirectional trust*

With bidirectional trusts, both domains trust each other. If the CIFS server's home domain has a bidirectional trust with another domain, the home domain can authenticate and authorize a user belonging to the trusted domain and vice versa.

UNIX user to Windows user name mapping searches can be performed only on domains with bidirectional trusts between the home domain and the other domain.



- *Outbound trust*

With an outbound trust, the home domain trusts the other domain. In this case, the home domain can authenticate and authorize a user belonging to the outbound trusted domain.

A domain with an outbound trust with the home domain is *not* searched when performing UNIX user to Windows user name mapping searches.


- *Inbound trust*

With an inbound trust, the other domain trusts the CIFS server’s home domain. In this case, the home domain cannot authenticate or authorize a user belonging to the inbound trusted domain.

A domain with an inbound trust with the home domain is *not* searched when performing UNIX user to Windows user name mapping searches.

### How wildcards (\*) are used to configure multidomain searches for name mapping

Multidomain name mapping searches are facilitated by the use of wildcards in the domain section of the Windows user name. The following table illustrates how to use wildcards in the domain part of a name mapping entry to enable multidomain searches:

Pattern	Replacement	Result
root	*\administrator	The UNIX user “root” is mapped to the user named “administrator”. All trusted domains are searched in order until the first matching user named “administrator” is found.
*	*\*	Valid UNIX users are mapped to the corresponding Windows users. All trusted domains are searched in order until the first matching user with that name is found.  <div style="border: 1px solid gray; padding: 5px; display: inline-block;">  The pattern *\* is only valid for name mapping from UNIX to Windows, not the other way around. </div>

### How multidomain name searches are performed

You can choose one of two methods for determining the list of trusted domains used for multidomain name searches:

- Use the automatically discovered bidirectional trust list compiled by ONTAP
- Use the preferred trusted domain list that you compile

If a UNIX user is mapped to a Windows user with a wildcard used for the domain section of the user name, the Windows user is looked up in all the trusted domains as follows:

- If a preferred trusted-domain list is configured, the mapped Windows user is looked up in this search list only, in order.
- If a preferred list of trusted domains is not configured, then the Windows user is looked up in all the bidirectional trusted domains of the home domain.
- If there are no bidirectionally trusted domains for the home domain, the user is looked up in the home domain.

If a UNIX user is mapped to a Windows user without a domain section in the user name, the Windows user is looked up in the home domain.

### Name mapping conversion rules

An ONTAP system keeps a set of conversion rules for each SVM. Each rule consists of two pieces: a *pattern* and a *replacement*. Conversions start at the beginning of the appropriate list and perform a substitution based on the first matching rule. The pattern is a UNIX-style regular expression. The replacement is a string containing escape sequences representing subexpressions from the pattern, as in the UNIX `sed` program.

### Create a name mapping

You can use the `vserver name-mapping create` command to create a name mapping. You use name mappings to enable Windows users to access UNIX security style volumes and the reverse.

### About this task

For each SVM, ONTAP supports up to 12,500 name mappings for each direction.

### Step

1. Create a name mapping: `vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-unix|unix-win} -position integer -pattern text -replacement text`



The `-pattern` and `-replacement` statements can be formulated as regular expressions. You can also use the `-replacement` statement to explicitly deny a mapping to the user by using the null replacement string " " (the space character). See the `vserver name-mapping create` man page for details.

When Windows-to-UNIX mappings are created, any SMB clients that have open connections to the ONTAP system at the time the new mappings are created must log out and log back in to see the new mappings.

### Examples

The following command creates a name mapping on the SVM named `vs1`. The mapping is a mapping from UNIX to Windows at position 1 in the priority list. The mapping maps the UNIX user `johnd` to the Windows user `ENG\JohnDoe`.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

The following command creates another name mapping on the SVM named vs1. The mapping is a mapping from Windows to UNIX at position 1 in the priority list. Here the pattern and replacement include regular expressions. The mapping maps every CIFS user in the domain ENG to users in the LDAP domain associated with the SVM.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\\1"
```

The following command creates another name mapping on the SVM named vs1. Here the pattern includes "\$" as an element in the Windows user name that must be escaped. The mapping maps the windows user ENG\john\$ops to UNIX user john\_ops.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

### Configure the default user

You can configure a default user to use if all other mapping attempts fail for a user, or if you do not want to map individual users between UNIX and Windows. Alternatively, if you want authentication of non-mapped users to fail, you should not configure a default user.

### About this task

For CIFS authentication, if you do not want to map each Windows user to an individual UNIX user, you can instead specify a default UNIX user.

For NFS authentication, if you do not want to map each UNIX user to an individual Windows user, you can instead specify a default Windows user.

### Steps

1. Perform one of the following actions:

If you want to...	Enter the following command...
Configure the default UNIX user	<code>vserver cifs options modify -default-unix-user <i>user_name</i></code>
Configure the default Windows user	<code>vserver nfs modify -default-win-user <i>user_name</i></code>

## Commands for managing name mappings

There are specific ONTAP commands for managing name mappings.

If you want to...	Use this command...
Create a name mapping	<code>vserver name-mapping create</code>
Insert a name mapping at a specific position	<code>vserver name-mapping insert</code>
Display name mappings	<code>vserver name-mapping show</code>
Exchange the position of two name mappings	<code>vserver name-mapping swap</code>
 A swap is not allowed when name-mapping is configured with an ip-qualifier entry.	
Modify a name mapping	<code>vserver name-mapping modify</code>
Delete a name mapping	<code>vserver name-mapping delete</code>
Validate the correct name mapping	<code>vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1</code>

See the man page for each command for more information.

## Configure multidomain name-mapping searches

### Enable or disable multidomain name mapping searches

With multidomain name mapping searches, you can use a wild card (\*) in the domain portion of a Windows name when configuring UNIX user to Windows user name mapping. Using a wild card (\*) in the domain portion of the name enables ONTAP to search all domains that have a bidirectional trust with the domain that contains the CIFS server's computer account.

### About this task

As an alternative to searching all bidirectionally trusted domains, you can configure a list of preferred trusted domains. When a list of preferred trusted domains is configured, ONTAP uses the preferred trusted domain list instead of the discovered bidirectionally trusted domains to perform multidomain name mapping searches.

- Multidomain name mapping searches are enabled by default.
- This option is available at the advanced privilege level.

## Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Perform one of the following actions:

If you want multidomain name mapping searches to be...	Enter the command...
Enabled	<pre>vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled true</pre>
Disabled	<pre>vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled false</pre>

3. Return to the admin privilege level: `set -privilege admin`

### Related information

[Available SMB server options](#)

### Reset and rediscover trusted domains

You can force the rediscovery of all the trusted domains. This can be useful when the trusted domain servers are not responding appropriately or the trust relationships have changed. Only domains with a bidirectional trust with the home domain, which is the domain containing the CIFS server's computer account, are discovered.

### Step

1. Reset and rediscover trusted domains by using the `vserver cifs domain trusts rediscover` command.

```
vserver cifs domain trusts rediscover -vserver vs1
```

### Related information

[Displaying information about discovered trusted domains](#)

### Display information about discovered trusted domains

You can display information about the discovered trusted domains for the CIFS server's home domain, which is the domain containing the CIFS server's computer account. This can be useful when you want to know which trusted domains are discovered and how they are ordered within the discovered trusted-domain list.

### About this task

Only the domains with bidirectional trusts with the home domain are discovered. Since the home domain's domain controller (DC) returns the list of trusted domains in an order determined by the DC, the order of the domains within the list cannot be predicted. By displaying the list of trusted domains, you can determine the search order for multidomain name mapping searches.

The displayed trusted domain information is grouped by node and storage virtual machine (SVM).

## Step

1. Display information about discovered trusted domains by using the `vserver cifs domain trusts show` command.

```
vserver cifs domain trusts show -vserver vs1
```

```
Node: node1
Vserver: vs1

Home Domain          Trusted Domain
-----
EXAMPLE.COM          CIFS1.EXAMPLE.COM,
                     CIFS2.EXAMPLE.COM
                     EXAMPLE.COM

Node: node2
Vserver: vs1

Home Domain          Trusted Domain
-----
EXAMPLE.COM          CIFS1.EXAMPLE.COM,
                     CIFS2.EXAMPLE.COM
                     EXAMPLE.COM
```

## Related information

[Resetting and rediscovering trusted domains](#)

### Add, remove, or replace trusted domains in preferred trusted domain lists

You can add or remove trusted domains from the preferred trusted domain list for the SMB server or you can modify the current list. If you configure a preferred trusted domain list, this list is used instead of the discovered bidirectional trusted domains when performing multidomain name mapping searches.

### About this task

- If you are adding trusted domains to an existing list, the new list is merged with the existing list with the new entries placed at the end. The trusted domains are searched in the order they appear in the trusted domain list.
- If you are removing trusted domains from the existing list and do not specify a list, the entire trusted domain list for the specified storage virtual machine (SVM) is removed.
- If you modify the existing list of trusted domains, the new list overwrites the existing list.



You should enter only bidirectionally trusted domains in the preferred trusted domain list. Even though you can enter outbound or inbound trust domains into the preferred domain list, they are not used when performing multidomain name mapping searches. ONTAP skips the entry for the unidirectional domain and moves on to the next bidirectional trusted domain in the list.

## Step

1. Perform one of the following actions:

If you want to do the following with the list of preferred trusted domains...	Use the command...
Add trusted domains to the list	<pre>vserver cifs domain name-mapping-search add -vserver _vserver_name_-trusted-domains FQDN, ...</pre>
Remove trusted domains from the list	<pre>vserver cifs domain name-mapping-search remove -vserver _vserver_name_-trusted-domains FQDN, ...]</pre>
Modify the existing list	<pre>vserver cifs domain name-mapping-search modify -vserver _vserver_name_-trusted-domains FQDN, ...</pre>

## Examples

The following command adds two trusted domains (cifs1.example.com and cifs2.example.com) to the preferred trusted domain list used by SVM vs1:

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

The following command removes two trusted domains from the list used by SVM vs1:

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

The following command modifies the trusted domain list used by SVM vs1. The new list replaces the original list:

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

## Related information

[Displaying information about the preferred trusted domain list](#)

### Display information about the preferred trusted domain list

You can display information about which trusted domains are in the preferred trusted domain list and the order in which they are searched if multidomain name mapping searches are enabled. You can configure a preferred trusted domain list as an alternative

to using the automatically discovered trusted domain list.

### Steps

1. Perform one of the following actions:

If you want to display information about the following...	Use the command...
All preferred trusted domains in the cluster grouped by storage virtual machine (SVM)	<code>vserver cifs domain name-mapping-search show</code>
All preferred trusted domains for a specified SVM	<code>vserver cifs domain name-mapping-search show -vserver <i>vserver_name</i></code>

The following command displays information about all preferred trusted domains on the cluster:

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver          Trusted Domains
-----
vs1              CIFS1.EXAMPLE.COM
```

### Related information

[Adding, removing, or replacing trusted domains in preferred trusted domain lists](#)

### Create and configure SMB shares

#### Create and configure SMB shares overview

Before users and applications can access data on the CIFS server over SMB, you must create and configure SMB shares, which is a named access point in a volume. You can customize shares by specifying share parameters and share properties. You can modify an existing share at any time.

When you create an SMB share, ONTAP creates a default ACL for the share with Full Control permissions for Everyone.

SMB shares are tied to the CIFS server on the storage virtual machine (SVM). SMB shares are deleted if either the SVM is deleted or the CIFS server with which it is associated is deleted from the SVM. If you recreate the CIFS server on the SVM, you must re-create the SMB shares.

### Related information

[Manage file access using SMB](#)

[SMB configuration for Microsoft Hyper-V and SQL Server](#)

[Configure character mapping for SMB file name translation on volumes](#)



## What the default administrative shares are

When you create a CIFS server on your storage virtual machine (SVM), three default administrative shares are automatically created. You should understand what those default shares are and how they are used.

ONTAP creates the following default administrative shares when you create the CIFS server:

- ipc\$
- admin\$
- c\$

Because shares that end with the \$ character are hidden shares, the default administrative shares are not visible from My Computer, but you can view them by using Shared Folders.

## How the ipc\$ and admin\$ default shares are used

The ipc\$ and admin\$ shares are used by ONTAP and cannot be used by Windows administrators to access data residing on the SVM.

- ipc\$ share

The ipc\$ share is a resource that shares the named pipes that are essential for communication between programs. The ipc\$ share is used during remote administration of a computer and when viewing a computer's shared resources. You cannot change the share settings, share properties, or ACLs of the ipc\$ share. You also cannot rename or delete the ipc\$ share.

- admin\$ share

The admin\$ share is used during remote administration of the SVM. The path of this resource is always the path to the SVM root. You cannot change the share settings, share properties, or ACLs for the admin\$ share. You also cannot rename or delete the admin\$ share.

## How the c\$ default share is used

The c\$ share is an administrative share that the cluster or SVM administrator can use to access and manage the SVM root volume.

The following are characteristics of the c\$ share:

- The path for this share is always the path to the SVM root volume and cannot be modified.
- The default ACL for the c\$ share is Administrator / Full Control.

This user is the BUILTIN\administrator. By default, the BUILTIN\administrator can map to the share and view, create, modify, or delete files and folders in the mapped root directory. Caution should be exercised when managing files and folders in this directory.

- You can change the c\$ share's ACL.
- You can change the c\$ share settings and share properties.
- You cannot delete the c\$ share.
- The SVM administrator can access the rest of the SVM namespace from the mapped c\$ share by crossing the namespace junctions.

- The c\$ share can be accessed by using the Microsoft Management Console.

## Related information

[Configuring advanced NTFS file permissions using the Windows Security tab](#)

### SMB share naming requirements

You should keep the ONTAP share naming requirements in mind when creating SMB shares on your SMB server.

Share naming conventions for ONTAP are the same as for Windows and include the following requirements:

- The name of each share must be unique for the SMB server.
- Share names are not case-sensitive.
- The maximum share name length is 80 characters.
- Unicode share names are supported.
- Share names ending with the \$ character are hidden shares.
- The ADMIN\$, IPC\$, and c\$ administrative shares are automatically created on every CIFS server and are reserved share names.
- You cannot use the share name ONTAP\_ADMIN\$ when creating a share.
- Share names containing spaces are supported:
  - You cannot use a space as the first character or as the last character in a share name.
  - You must enclose share names containing a space in quotation marks.



Single quotation marks are considered part of the share name and cannot be used in place of quotation marks.

- The following special characters are supported when you name SMB shares:

! @ # \$ % & ' \_ - . ~ ( ) { }

- The following special characters are not supported when you name SMB shares:

□ " / \ : ; | < > , ? \* =

### Directory case-sensitivity requirements when creating shares in a multiprotocol environment

If you create shares in an SVM where the 8.3 naming scheme is used to distinguish between directory names where there are only case differences between the names, you must use the 8.3 name in the share path to ensure that the client connects to the desired directory path.

In the following example, two directories named “testdir” and “TESTDIR” were created on a Linux client. The junction path of the volume containing the directories is /home. The first output is from a Linux client and the second output is from an SMB client.

```
ls -l
drwxrwxr-x 2 user1 group1 4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1 4096 Apr 17 11:24 TESTDIR
```

```
dir
```

```
Directory of Z:\
```

```
04/17/2015 11:23 AM <DIR> testdir
04/17/2015 11:24 AM <DIR> TESTDI~1
```

When you create a share to the second directory, you must use the 8.3 name in the share path. In this example, the share path to the first directory is `/home/testdir` and the share path to the second directory is `/home/TESTDI~1`.

### Use SMB share properties

### Use SMB share properties overview

You can customize the properties of SMB shares.

The available share properties are as follows:

Share properties	Description
oplocks	This property specifies that the share uses opportunistic locks, also known as client-side caching.
browsable	This property allows Windows clients to browse the share.
showsnapshot	This property specifies that Snapshot copies can be viewed and traversed by clients.
changenotify	This property specifies that the share supports Change Notify requests. For shares on an SVM, this is a default initial property.
attributecache	This property enables the file attribute caching on the SMB share to provide faster access of attributes. The default is to disable attribute caching. This property should be enabled only if there are clients connecting to shares over SMB 1.0. This share property is not applicable if clients are connecting to shares over SMB 2.x or SMB 3.0.

Share properties	Description
<code>continuously-available</code>	This property permits SMB clients that support it to open files in a persistent manner. Files opened this way are protected from disruptive events, such as failover and giveback.
<code>branchcache</code>	This property specifies that the share allows clients to request BranchCache hashes on the files within this share. This option is useful only if you specify “per-share” as the operating mode in the CIFS BranchCache configuration.
<code>access-based-enumeration</code>	This property specifies that <i>Access Based Enumeration</i> (ABE) is enabled on this share. ABE-filtered shared folders are visible to a user based on that individual user’s access rights, preventing the display of folders or other shared resources that the user does not have rights to access.
<code>namespace-caching</code>	This property specifies that the SMB clients connecting to this share can cache the directory enumeration results returned by the CIFS servers, which can provide better performance. By default, SMB 1 clients do not cache directory enumeration results. Because SMB 2 and SMB 3 clients cache directory enumeration results by default, specifying this share property provides performance benefits only to SMB 1 client connections.
<code>encrypt-data</code>	This property specifies that SMB encryption must be used when accessing this share. SMB clients that do not support encryption when accessing SMB data will not be able to access this share.

### Add or remove share properties on an existing SMB share

You can customize an existing SMB share by adding or removing share properties. This can be useful if you want to change the share configuration to meet changing requirements in your environment.

#### Before you begin

The share whose properties you want to modify must exist.

#### About this task

Guidelines for adding share properties:

- You can add one or more share properties by using a comma-delimited list.
- Any share properties that you have previously specified remain in effect.

Newly added properties are appended to the existing list of share properties.

- If you specify a new value for share properties that are already applied to the share, the newly specified value replaces the original value.
- You cannot remove share properties by using the `vserver cifs share properties add` command.

You can use the `vserver cifs share properties remove` command to remove share properties.

Guidelines for removing share properties:

- You can remove one or more share properties by using a comma-delimited list.
- Any share properties that you have previously specified but do not remove remain in effect.

### Steps

1. Enter the appropriate command:

If you want to...	Enter the command...
Add share properties	<pre>vserver cifs share properties add -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...</pre>
Remove share properties	<pre>vserver cifs share properties remove -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...</pre>

2. Verify the share property settings: `vserver cifs share show -vserver vserver_name -share -name share_name`

### Examples

The following command adds the `showsnapshot` share property to a share named “share1” on SVM vs1:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot

cluster1::> vserver cifs share show -vserver vs1
Vserver      Share      Path        Properties      Comment      ACL
-----      -
vs1          share1     /share1     oplocks         -            Everyone / Full
Control
                browsable
                changenotify
                showsnapshot
```

The following command removes the `browsable` share property from a share named “share2” on SVM vs1:

```
cluster1::> vsriver cifs share properties remove -vsriver vs1 -share-name
share2 -share-properties browsable
```

```
cluster1::> vsriver cifs share show -vsriver vs1
Vserver      Share      Path        Properties  Comment     ACL
-----      -
vs1          share2     /share2     oplocks    -           Everyone / Full
Control
                                changenotify
```

## Related information

[Commands for managing SMB shares](#)

### Optimize SMB user access with the force-group share setting

When you create a share from the ONTAP command line to data with UNIX effective security, you can specify that all files created by SMB users in that share belong to the same group, known as the *force-group*, which must be a predefined group in the UNIX group database. Using a force-group makes it easier to ensure that files can be accessed by SMB users belonging to various groups.

Specifying a force-group is meaningful only if the share is in a UNIX or mixed qtree. There is no need to set a force-group for shares in an NTFS volume or qtree because access to files in these shares is determined by Windows permissions, not UNIX GIDs.

If a force-group has been specified for a share, the following becomes true of the share:

- SMB users in the force-group who access this share are temporarily changed to the GID of the force-group.

This GID enables them to access files in this share that are not accessible normally with their primary GID or UID.

- All files in this share created by SMB users belong to the same force-group, regardless of the primary GID of the file owner.

When SMB users try to access a file created by NFS, the SMB users' primary GIDs determine access rights.

The force-group does not affect how NFS users access files in this share. A file created by NFS acquires the GID from the file owner. Determination of access permissions is based on the UID and primary GID of the NFS user who is trying to access the file.

Using a force-group makes it easier to ensure that files can be accessed by SMB users belonging to various groups. For example, if you want to create a share to store the company's web pages and give write access to users in the Engineering and Marketing departments, you can create a share and give write access to a force-group named "webgroup1". Because of the force-group, all files created by SMB users in this share are owned by the "webgroup1" group. In addition, users are automatically assigned the GID of the "webgroup1" group when accessing the share. As a result, all the users can write to this share without you needing to manage the access rights of the users in the Engineering and Marketing departments.

## Related information

## [Creating an SMB share with the force-group share setting](#)

### Create an SMB share with the force-group share setting

You can create an SMB share with the force-group share setting if you want SMB users that access data on volumes or qtrees with UNIX file security to be regarded by ONTAP as belonging to the same UNIX group.

#### Step

1. Create the SMB share: `vserver cifs share create -vserver vserver_name -share-name share_name -path path -force-group-for-create UNIX_group_name`

If the UNC path (`\\servername\sharename\filepath`) of the share contains more than 256 characters (excluding the initial “\” in the UNC path), then the **Security** tab in the Windows Properties box is unavailable. This is a Windows client issue rather than an ONTAP issue. To avoid this issue, do not create shares with UNC paths with more than 256 characters.

If you want to remove the force-group after the share is created, you can modify the share at any time and specify an empty string (“”) as the value for the `-force-group-for-create` parameter. If you remove the force-group by modifying the share, all existing connections to this share continue to have the previously set force-group as the primary GID.

#### Example

The following command creates a “webpages” share that is accessible on the web in the `/corp/companyinfo` directory in which all files that SMB users create are assigned to the `webgroup1` group:

```
vserver cifs share create -vserver vs1 -share-name webpages -path /corp/companyinfo -force-group-for-create webgroup1
```

#### Related information

[Optimize SMB user access with the force-group share setting](#)

#### View information about SMB shares using the MMC

You can view information about SMB shares on your SVM and perform some management tasks using the Microsoft Management Console (MMC). Before you can view the shares, you need to connect the MMC to the SVM.

#### About this task

You can perform the following tasks on shares contained within SVMs using the MMC:

- View shares
- View active sessions
- View open files
- Enumerate the list of sessions, files and tree connections in the system
- Close open files in the system
- Close open sessions
- Create/manage shares



The views displayed by the preceding capabilities are node specific and not cluster specific. Therefore, when you use the MMC to connect to the SMB server host name (that is, cifs01.domain.local), you are routed, based on how you have set up DNS, to a single LIF within your cluster.

The following functions are not supported in MMC for ONTAP:

- Creating new local users/groups
- Managing/viewing existing local users/groups
- Viewing events or performance logs
- Storage
- Services and applications

In instances where the operation is not supported, you might experience `remote procedure call failed` errors.

## FAQ: Using Windows MMC with ONTAP

### Steps

1. To open Computer Management MMC on any Windows server, in the **Control Panel**, select **Administrative Tools > Computer Management**.
2. Select **Action > Connect to another computer**.

The Select Computer dialog box appears.

3. Type the name of the storage system or click **Browse** to locate the storage system.
4. Click **OK**.

The MMC connects to the SVM.

5. In the navigation pane, click **Shared Folders > Shares**.

A list of shares on the SVM is displayed in the right display pane.

6. To display the share properties for a share, double-click the share to open the **Properties** dialog box.
7. If you cannot connect to the storage system using MMC, you can add the user to the BUILTIN\Administrators group or BUILTIN\Power Users group by using one of the following commands on the storage system:

```
cifs users-and-groups local-groups add-members -vserver <vserver_name>  
-group-name BUILTIN\Administrators -member-names <domainuser>
```

```
cifs users-and-groups local-groups add-members -vserver <vserver_name>  
-group-name "BUILTIN\Power Users" -member-names <domainuser>
```

### Commands for managing SMB shares

You use the `vserver cifs share` and `vserver cifs share properties`



commands to manage SMB shares.

If you want to...	Use this command...
Create an SMB share	<code>vserver cifs share create</code>
Display SMB shares	<code>vserver cifs share show</code>
Modify an SMB share	<code>vserver cifs share modify</code>
Delete an SMB share	<code>vserver cifs share delete</code>
Add share properties to an existing share	<code>vserver cifs share properties add</code>
Remove share properties from an existing share	<code>vserver cifs share properties remove</code>
Display information about share properties	<code>vserver cifs share properties show</code>

See the man page for each command for more information.

## Secure file access by using SMB share ACLs

### Guidelines for managing SMB share-level ACLs

You can change share-level ACLs to give users more or less access rights to the share. You can configure share-level ACLs by using either Windows users and groups or UNIX users and groups.

After you create a share, by default, the share-level ACL gives read access to the standard group named Everyone. Read access in the ACL means that all users in the domain and all trusted domains have read-only access to the share.

You can change a share-level ACL by using the Microsoft Management Console (MMC) on a Windows client or the ONTAP command line.

The following guidelines apply when you use the MMC:

- The user and group names specified must be Windows names.
- You can specify only Windows permissions.

The following guidelines apply when you use the ONTAP command line:

- The user and group names specified can be Windows names or UNIX names.

If a user and group type is not specified when creating or modifying ACLs, the default type is Windows users and groups.

- You can specify only Windows permissions.

## Create SMB share access control lists

Configuring share permissions by creating access control lists (ACLs) for SMB shares enables you to control the level of access to a share for users and groups.

### About this task

You can configure share-level ACLs by using local or domain Windows user or group names or UNIX user or group names.

Before creating a new ACL, you should delete the default share ACL `Everyone / Full Control`, which poses a security risk.

In workgroup mode, the local domain name is the SMB server name.

### Steps

1. Delete the default share ACL:  
`vserver cifs share access-control delete -vserver vserver_name -share share_name -user-or-group everyone`
2. Configure the new ACL:

If you want to configure ACLs by using a...	Enter the command...
Windows user	<pre>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_domain_name\\user_name -permission access_right</pre>
Windows group	<pre>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_group_name -permission access_right</pre>
UNIX user	<pre>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type unix-user -user-or-group UNIX_user_name -permission access_right</pre>
UNIX group	<pre>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type unix-group -user-or-group UNIX_group_name -permission access_right</pre>

3. Verify that the ACL applied to the share is correct by using the `vserver cifs share access-control show` command.

### Example

The following command gives Change permissions to the “Sales Team” Windows group for the “sales” share on the “vs1.example.com” SVM:

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "Sales Team" -permission
Change

cluster1::> vserver cifs share access-control show
      Share      User/Group      User/Group  Access
Vserver  Name          Name           Type
Permission
-----
vs1.example.com  c$            BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales         DOMAIN\"Sales Team"    windows    Change
```

The following command gives Read permission to the “engineering” UNIX group for the “eng” share on the “vs2.example.com” SVM:

```
cluster1::> vserver cifs share access-control create -vserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group eng
-permission Read

cluster1::> vserver cifs share access-control show
      Share      User/Group      User/Group  Access
Vserver  Name          Name           Type
Permission
-----
vs2.example.com  c$            BUILTIN\Administrators  windows
Full_Control
vs2.example.com  eng           engineering      unix-group  Read
```

The following commands give Change permission to the local Windows group named “Tiger Team” and Full\_Control permission to the local Windows user named “Sue Chang” for the “datavol5” share on the “vs1” SVM:

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change
```

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control
```

```
cluster1::> vserver cifs share access-control show -vserver vs1
```

Vserver	Share Name	User/Group Name	User/Group Type	Access Permission
vs1	c\$	BUILTIN\Administrators	windows	Full_Control
vs1	datavol5	DOMAIN\ "Tiger Team"	windows	Change
vs1	datavol5	DOMAIN\ "Sue Chang"	windows	Full_Control

#### Commands for managing SMB share access control lists

You need to know the commands for managing SMB access control lists (ACLs), which includes creating, displaying, modifying, and deleting them.

If you want to...	Use this command...
Create a new ACL	<code>vserver cifs share access-control create</code>
Display ACLs	<code>vserver cifs share access-control show</code>
Modify an ACL	<code>vserver cifs share access-control modify</code>
Delete an ACL	<code>vserver cifs share access-control delete</code>

#### Secure file access by using file permissions

##### Configure advanced NTFS file permissions using the Windows Security tab

You can configure standard NTFS file permissions on files and folders by using the **Windows Security** tab in the Windows Properties window.

##### Before you begin

The administrator performing this task must have sufficient NTFS permissions to change permissions on the selected objects.

### About this task

Configuring NTFS file permissions is done on a Windows host by adding entries to NTFS discretionary access control lists (DACLS) that are associated with an NTFS security descriptor. The security descriptor is then applied to NTFS files and directories. These tasks are automatically handled by the Windows GUI.

### Steps

1. From the **Tools** menu in Windows Explorer, select **Map network drive**.
2. Complete the **Map Network Drive** dialog box:
  - a. Select a **Drive** letter.
  - b. In the **Folder** box, type the CIFS server name containing the share that contains the data to which you want to apply permissions and the name of the share.

If your CIFS server name is "CIFS\_SERVER" and your share is named "share1", you should type \\CIFS\_SERVER\share1.



You can specify the IP address of the data interface for the CIFS server instead of the CIFS server name.

- c. Click **Finish**.

The drive you selected is mounted and ready with the Windows Explorer window displaying files and folders contained within the share.

3. Select the file or directory for which you want to set NTFS file permissions.
4. Right-click the file or directory, and then select **Properties**.
5. Select the **Security** tab.

The **Security** tab displays the list of users and groups for which NTFS permission are set. The **Permissions for** box displays a list of Allow and Deny permissions in effect for each user or group selected.

6. Click **Advanced**.

The Windows Properties window displays information about existing file permissions assigned to users and groups.

7. Click **Change Permissions**.

The Permissions window opens.

8. Perform the desired actions:

If you want to...	Do the following...
Set up advanced NTFS permissions for a new user or group	a. Click <b>Add</b> . b. In the <b>Enter the object name to select</b> box, type the name of the user or group that you want to add. c. Click <b>OK</b> .
Change advanced NTFS permissions from a user or group	a. In the <b>Permissions entries:</b> box, select the user or group whose advanced permissions you want to change. b. Click <b>Edit</b> .
Remove advanced NTFS permissions for a user or group	a. In the <b>Permissions entries:</b> box, select the user or group that you want to remove. b. Click <b>Remove</b> . c. Skip to Step 13.

If you are adding advanced NTFS permissions on a new user or group or changing NTFS advanced permissions on an existing user or group, the Permission Entry for <Object> box opens.

9. In the **Apply to** box, select how you want to apply this NTFS file permission entry.

If you are setting up NTFS file permissions on a single file, the **Apply to** box is not active. The **Apply to** setting defaults to **This object only**.

10. In the **Permissions** box, select the **Allow** or **Deny** boxes for the advanced permissions that you want to set on this object.

- To allow the specified access, select the **Allow** box.
  - To not allow the specified access, select the **Deny** box.
- You can set permissions on the following advanced rights:

- **Full control**

If you choose this advanced right, all other advanced rights are automatically chosen (either Allow or Deny rights).

- **Traverse folder / execute file**
- **List folder / read data**
- **Read attributes**
- **Read extended attributes**
- **Create files / write data**
- **Create folders / append data**
- **Write attributes**
- **Write extended attributes**
- **Delete subfolders and files**

- **Delete**
- **Read permissions**
- **Change permissions**
- **Take ownership**



If any of the advanced permission boxes are not selectable, it is because the permissions are inherited from the parent object.

11. If you want subfolders and files of this object to inherit these permissions, select the **Apply these permissions to objects and/or containers within this container only** box.
12. Click **OK**.
13. After you finish adding, removing, or editing NTFS permissions, specify the inheritance setting for this object:
  - Select the **Include inheritable permissions from this object's parent** box.
 

This is the default.
  - Select the **Replace all child object permissions with inheritable permissions from this object** box.
 

This setting is not present in the Permissions box if you are setting NTFS file permissions on a single file.

Be cautious when selecting this setting. This setting removes all existing permissions on all child objects and replaces them with this object's permission settings. You could inadvertently remove permissions that you did not want removed. It is especially important when setting permissions in a mixed security-style volume or qtree. If child objects have a UNIX effective security style, propagating NTFS permissions to those child objects results in ONTAP changing these objects from UNIX security style to NTFS security style, and all UNIX permissions on those child objects are replaced with NTFS permissions.
  - Select both boxes.
  - Select neither box.
14. Click **OK** to close the **Permissions** box.
15. Click **OK** to close the **Advanced Security settings for <Object>** box.

For more information about how to set advanced NTFS permissions, see your Windows documentation.

### Related information

[Configure and apply file security on NTFS files and folders using the CLI](#)

[Displaying information about file security on NTFS security-style volumes](#)

[Displaying information about file security on mixed security-style volumes](#)

[Displaying information about file security on UNIX security-style volumes](#)

## Configure NTFS file permissions using the ONTAP CLI

You can configure NTFS file permissions on files and directories using the ONTAP CLI. This enables you to configure NTFS file permissions without needing to connect to the data using an SMB share on a Windows Client.

You can configure NTFS file permissions by adding entries to NTFS discretionary access control lists (DACLS) that are associated with an NTFS security descriptor. The security descriptor is then applied to NTFS files and directories.

You can only configure NTFS file permissions using the command line. You cannot configure NFSv4 ACLs by using the CLI.

## How UNIX file permissions provide access control when accessing files over SMB

A FlexVol volume can have one of three types of security style: NTFS, UNIX, or mixed. You can access data over SMB regardless of security style; however, appropriate UNIX file permissions are needed to access data with UNIX effective security.

When data is accessed over SMB, there are several access controls used when determining whether a user is authorized to perform a requested action:

- Export permissions

Configuring export permissions for SMB access is optional.

- Share permissions
- File permissions

The following types of file permissions might be applied to the data on which the user wants to perform an action:

- NTFS
- UNIX NFSv4 ACLs
- UNIX mode bits

For data with NFSv4 ACLs or UNIX mode bits set, UNIX style permissions are used to determine file access rights to the data. The SVM administrator needs to set the appropriate file permission to ensure that users have the rights to perform the desired action.



Data in a mixed security-style volume might have either NTFS or UNIX effective security style. If the data has UNIX effective security style, then NFSv4 permissions or UNIX mode bits are used when determining file access rights to the data.

## Secure file access by using Dynamic Access Control (DAC)

### Secure file access by using Dynamic Access Control (DAC) overview

You can secure access by using Dynamic Access Control and by creating central access policies in Active Directory and applying them to files and folders on SVMs through applied Group Policy Objects (GPOs). You can configure auditing to use central access



policy staging events to see the effects of changes to central access policies before you apply them.

### **Additions to CIFS credentials**

Before Dynamic Access Control, a CIFS credential included a security principal's (the user's) identity and Windows group membership. With Dynamic Access Control, three more types of information are added to the credential—device identity, device claims, and user claims:

- Device identity

The analog of the user's identity information, except it is the identity and group membership of the device that the user is logging in from.

- Device claims

Assertions about a device security principal. For example, a device claim might be that it is a member of a specific OU.

- User claims

Assertions about a user security principal. For example, a user claim might be that their AD account is a member of a specific OU.

### **Central access policies**

Central access policies for files enable organizations to centrally deploy and manage authorization policies that include conditional expressions using user groups, user claims, device claims, and resource properties.

For example, for accessing high business impact data, a user needs to be a full time employee and only have access to the data from a managed device. Central access policies are defined in Active Directory and distributed to file servers via the GPO mechanism.

### **Central access policy staging with advanced auditing**

Central access policies can be “staged”, in which case they are evaluated in a “what-if” manner during file access checks. The results of what would have happened if the policy was in effect and how that differs from what is currently configured are logged as an audit event. In this way, administrators can use audit event logs to study the impact of an access policy change before actually putting the policy in play. After evaluating the impact of an access policy change, the policy can be deployed via GPOs to the desired SVMs.

### **Related information**

[Supported GPOs](#)

[Applying Group Policy Objects to CIFS servers](#)

[Enabling or disabling GPO support on a CIFS server](#)

[Displaying information about GPO configurations](#)

[Displaying information about central access policies](#)

[Displaying information about central access policy rules](#)

[Configuring central access policies to secure data on CIFS servers](#)

[Displaying information about Dynamic Access Control security](#)

[SMB and NFS auditing and security tracing](#)

### Supported Dynamic Access Control functionality

If you want to use Dynamic Access Control (DAC) on your CIFS server, you need to understand how ONTAP supports Dynamic Access Control functionality in Active Directory environments.

### Supported for Dynamic Access Control

ONTAP supports the following functionality when Dynamic Access Control is enabled on the CIFS server:

Functionality	Comments
Claims into the file system	Claims are simple name and value pairs that state some truth about a user. User credentials now contain claim information, and security descriptors on files can perform access checks that include claims checks. This gives administrators a finer level of control over who can access files.
Conditional expressions to file access checks	When modifying the security parameters of a file, users can now add arbitrarily complex conditional expressions to the file's security descriptor. The conditional expression can include checks for claims.
Central control of file access via central access policies	Central access policies are a kind of ACL stored in Active Directory that can be tagged to a file. Access to the file is only granted if the access checks of both the security descriptor on disk and the tagged central access policy allows access. This gives administrators the ability to control access to files from a central location (AD) without having to modify the security descriptor on disk.
Central access policy staging	Adds the ability to try out security changes without affecting actual file access, by "staging" a change to the central access policies, and seeing the effect of the change in an audit report.
Support for displaying information about central access policy security by using the ONTAP CLI	Extends the <code>vserver security file-directory show</code> command to display information about applied central access policies.
Security tracing that includes central access policies	Extends the <code>vserver security trace</code> command family to display results that include information about applied central access policies.

## Unsupported for Dynamic Access Control

ONTAP does not support the following functionality when Dynamic Access Control is enabled on the CIFS server:

Functionality	Comments
Automatic classification of NTFS file system objects	This is an extension to the Windows File Classification Infrastructure that is not supported in ONTAP.
Advanced auditing other than central access policy staging	Only central access policy staging is supported for advanced auditing.

### Considerations when using Dynamic Access Control and central access policies with CIFS servers

There are certain considerations you must keep in mind when using Dynamic Access Control (DAC) and central access policies to secure files and folders on CIFS servers.

#### NFS access can be denied to root if policy rule applies to domain\administrator user

Under certain circumstances, NFS access to root might be denied when central access policy security is applied to the data that the root user is attempting to access. The issue occurs when the central access policy contains a rule that is applied to the domain\administrator and the root account is mapped to the domain\administrator account.

Instead of applying a rule to the domain\administrator user, you should apply the rule to a group with administrative privileges, such as the domain\administrators group. In this way, you can map root to the domain\administrator account without root being impacted by this issue.

#### CIFS server's BUILTIN\Administrators group has access to resources when the applied central access policy is not found in Active Directory

It is possible that resources contained within the CIFS server have central access policies applied to them, but when the CIFS server uses the central access policy's SID to attempt to retrieve information from Active Directory, the SID does not match any existing central access policy SIDs in Active Directory. Under these circumstances, the CIFS server applies the local default recovery policy for that resource.

The local default recovery policy allows the CIFS server's BUILTIN\Administrators group access to that resource.

### Enable or disable Dynamic Access Control overview

The option that enables you to use Dynamic Access Control (DAC) to secure objects on your CIFS server is disabled by default. You must enable the option if you want to use Dynamic Access Control on your CIFS server. If you later decide that you do not want to use Dynamic Access Control to secure objects stored on the CIFS server, you can disable the option.

#### About this task

Once Dynamic Access Control is enabled, the file system can contain ACLs with Dynamic Access Control-related entries. If Dynamic Access Control is disabled, the current Dynamic Access Control entries will be

ignored, and new ones will not be allowed.

This option is available only at the advanced privilege level.

### Step

1. Set the privilege level to advanced: `set -privilege advanced`
2. Perform one of the following actions:

If you want Dynamic Access Control to be...	Enter the command...
Enabled	<code>vserver cifs options modify -vserver vserver_name -is-dac-enabled true</code>
Disabled	<code>vserver cifs options modify -vserver vserver_name -is-dac-enabled false</code>

3. Return to the administrator privilege level: `set -privilege admin`

### Related information

[Configuring central access policies to secure data on CIFS servers](#)

### Manage ACLs that contain Dynamic Access Control ACEs when Dynamic Access Control is disabled

If you have resources that have ACLs applied with Dynamic Access Control ACEs and you disable Dynamic Access Control on the storage virtual machine (SVM), you must remove the Dynamic Access Control ACEs before you can manage the non-Dynamic Access Control ACEs on that resource.

### About this task

After Dynamic Access Control is disabled, you cannot remove existing non-Dynamic Access Control ACEs or add new non-Dynamic Access Control ACEs until you have removed the existing Dynamic Access Control ACEs.

You can use whichever tool you normally use to manage ACLs to perform these steps.

### Steps

1. Determine what Dynamic Access Control ACEs are applied to the resource.
2. Remove the Dynamic Access Control ACEs from the resource.
3. Add or remove non-Dynamic Access Control ACEs as desired from the resource.

### Configure central access policies to secure data on CIFS servers

There are several steps that you must take to secure access to data on the CIFS server using central access policies, including enabling Dynamic Access Control (DAC) on the CIFS server, configuring central access policies in Active Directory, applying the central access policies to Active Directory containers with GPOs, and enabling GPOs on the CIFS server.

### Before you begin

- The Active Directory must be configured to use central access policies.
- You must have sufficient access on the Active Directory domain controllers to create central access policies and to create and apply GPOs to the containers that contain the CIFS servers.
- You must have sufficient administrative access on the storage virtual machine (SVM) to execute the necessary commands.

### About this task

Central access policies are defined and applied to group policy objects (GPOs) on Active Directory. You can consult the Microsoft TechNet Library for instructions about configuring central access policies and GPOs.

### [Microsoft TechNet Library](#)

### Steps

1. Enable Dynamic Access Control on the SVM if it is not already enabled by using the `vserver cifs options modify` command.

```
vserver cifs options modify -vserver vs1 -is-dac-enabled true
```

2. Enable group policy objects (GPOs) on the CIFS server if they are not already enabled by using the `vserver cifs group-policy modify` command.

```
vserver cifs group-policy modify -vserver vs1 -status enabled
```

3. Create central access rules and central access policies on Active Directory.
4. Create a group policy object (GPO) to deploy the central access policies on Active Directory.
5. Apply the GPO to the container where the CIFS server computer account is located.
6. Manually update the GPOs applied to the CIFS server by using the `vserver cifs group-policy update` command.

```
vserver cifs group-policy update -vserver vs1
```

7. Verify that the GPO central access policy is applied to the resources on the CIFS server by using the `vserver cifs group-policy show-applied` command.

The following example shows that the Default Domain Policy has two central access policies that are applied to the CIFS server:

```
vserver cifs group-policy show-applied
```

```
Vserver: vs1
-----
  GPO Name: Default Domain Policy
    Level: Domain
    Status: enabled
  Advanced Audit Settings:
    Object Access:
      Central Access Policy Staging: failure
  Registry Settings:
    Refresh Time Interval: 22
```

```
Refresh Random Offset: 8
Hash Publication Mode for BranchCache: per-share
Hash Version Support for BranchCache: all-versions
Security Settings:
  Event Audit and Event Log:
    Audit Logon Events: none
    Audit Object Access: success
    Log Retention Method: overwrite-as-needed
    Max Log Size: 16384
  File Security:
    /vol1/home
    /vol1/dir1
  Kerberos:
    Max Clock Skew: 5
    Max Ticket Age: 10
    Max Renew Age: 7
  Privilege Rights:
    Take Ownership: usr1, usr2
    Security Privilege: usr1, usr2
    Change Notify: usr1, usr2
  Registry Values:
    Signing Required: false
  Restrict Anonymous:
    No enumeration of SAM accounts: true
    No enumeration of SAM accounts and shares: false
    Restrict anonymous access to shares and named pipes: true
    Combined restriction for anonymous user: no-access
  Restricted Groups:
    gpr1
    gpr2
Central Access Policy Settings:
  Policies: cap1
           cap2

  GPO Name: Resultant Set of Policy
  Level: RSOP
Advanced Audit Settings:
  Object Access:
    Central Access Policy Staging: failure
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
  Hash Publication Mode for BranchCache: per-share
  Hash Version Support for BranchCache: all-versions
Security Settings:
  Event Audit and Event Log:
```

```
Audit Logon Events: none
Audit Object Access: success
Log Retention Method: overwrite-as-needed
Max Log Size: 16384
File Security:
  /voll/home
  /voll/dir1
Kerberos:
  Max Clock Skew: 5
  Max Ticket Age: 10
  Max Renew Age: 7
Privilege Rights:
  Take Ownership: usr1, usr2
  Security Privilege: usr1, usr2
  Change Notify: usr1, usr2
Registry Values:
  Signing Required: false
Restrict Anonymous:
  No enumeration of SAM accounts: true
  No enumeration of SAM accounts and shares: false
  Restrict anonymous access to shares and named pipes: true
  Combined restriction for anonymous user: no-access
Restricted Groups:
  gpr1
  gpr2
Central Access Policy Settings:
  Policies: cap1
           cap2
2 entries were displayed.
```

## Related information

[Displaying information about GPO configurations](#)

[Displaying information about central access policies](#)

[Displaying information about central access policy rules](#)

[Enabling or disabling Dynamic Access Control](#)

### Display information about Dynamic Access Control security

You can display information about Dynamic Access Control (DAC) security on NTFS volumes and on data with NTFS effective security on mixed security-style volumes. This includes information about conditional ACEs, resource ACEs, and central access policy ACEs. You can use the results to validate your security configuration or to troubleshoot file access issues.

### About this task

You must supply the name of the storage virtual machine (SVM) and the path to the data whose file or folder security information you want to display. You can display the output in summary form or as a detailed list.

### Step

1. Display file and directory security settings with the desired level of detail:

If you want to display information...	Enter the following command...
In summary form	<pre>vserver security file-directory show -vserver vserver_name -path path</pre>
With expanded detail	<pre>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</pre>
Where output is displayed with group and user SIDs	<pre>vserver security file-directory show -vserver vserver_name -path path -lookup-names false</pre>
About file and directory security for files and directories where the hexadecimal bit mask is translated to textual format	<pre>vserver security file-directory show -vserver vserver_name -path path -textual-mask true</pre>

### Examples

The following example displays Dynamic Access Control security information about the path `/vol1` in SVM `vs1`:



```

cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
          Vserver: vs1
          File Path: /vol1
    File Inode Number: 112
      Security Style: mixed
    Effective Style: ntfs
      DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attribute: -
      Unix User Id: 0
      Unix Group Id: 1
      Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
          ACLs: NTFS Security Descriptor
              Control:0xbf14
              Owner:CIFS1\Administrator
              Group:CIFS1\Domain Admins
              SACL - ACEs
                  ALL-Everyone-0xf01ff-OI|CI|SA|FA
                  RESOURCE ATTRIBUTE-Everyone-0x0

("Department_MS",TS,0x10020,"Finance")
          POLICY ID-All resources - No Write-
0x0-OI|CI
          DACL - ACEs
              ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
              ALLOW-Everyone-0x1f01ff-OI|CI
              ALLOW CALLBACK-DAC\user1-0x1200a9-
OI|CI

((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
evice.department==@Resource.Department_MS)

```

## Related information

[Displaying information about GPO configurations](#)

[Displaying information about central access policies](#)

[Displaying information about central access policy rules](#)

## Revert considerations for Dynamic Access Control

You should be aware of what happens when reverting to a version of ONTAP that does not support Dynamic Access Control (DAC) and what you must do before and after reverting.

If you want to revert the cluster to a version of ONTAP that does not support Dynamic Access Control and Dynamic Access Control is enabled on one or more the storage virtual machines (SVMs), you must do the following before reverting:

- You must disable Dynamic Access Control on all SVMs that have it enabled on the cluster.
- You must modify any auditing configurations on the cluster that contain the `cap-staging` event type to use only the `file-op` event type.

You must understand and act on some important revert considerations for files and folders with Dynamic Access Control ACEs:

- If the cluster is reverted, existing Dynamic Access Control ACEs are not removed; however, they will be ignored in file access checks.
- Since Dynamic Access Control ACEs are ignored after reversion, access to files will change on files with Dynamic Access Control ACEs.

This could allow users to access files they previously could not, or not be able to access files that they previously could.

- You should apply non-Dynamic Access Control ACEs to the affected files to restore their previous level of security.

This can be done either before reverting or immediately after reversion completes.



Since Dynamic Access Control ACEs are ignored after reversion, it is not required that you remove them when applying non-Dynamic Access Control ACEs to the affected files. However, if desired, you can manually remove them.

#### Where to find additional information about configuring and using Dynamic Access Control and central access policies

Additional resources are available to help you configure and use Dynamic Access Control and central access policies.

You can find information about how to configure Dynamic Access Control and central access policies on Active Directory in the Microsoft TechNet Library.

[Microsoft TechNet: Dynamic Access Control Scenario Overview](#)

[Microsoft TechNet: Central Access Policy Scenario](#)

The following references can help you configure the SMB server to use and support Dynamic Access Control and central access policies:

- **Using GPOs on the SMB server**

[Applying Group Policy Objects to SMB servers](#)

- **Configuring NAS auditing on the SMB server**

[SMB and NFS auditing and security tracing](#)

## Secure SMB access using export policies

### How export policies are used with SMB access

If export policies for SMB access are enabled on the CIFS server, export policies are used when controlling access to SVM volumes by SMB clients. To access data, you can create an export policy that allows SMB access and then associate the policy with the volumes containing SMB shares.

An export policy has one or more rules applied to it that specifies which clients are allowed access to the data and what authentication protocols are supported for read-only and read-write access. You can configure export policies to allow access over SMB to all clients, a subnet of clients, or a specific client and to allow authentication using Kerberos authentication, NTLM authentication, or both Kerberos and NTLM authentication when determining read-only and read-write access to data.

After processing all export rules applied to the export policy, ONTAP can determine whether the client is granted access and what level of access is granted. Export rules apply to client machines, not to Windows users and groups. Export rules do not replace Windows user and group-based authentication and authorization. Export rules provide another layer of access security in addition to share and file-access permissions. You associate exactly one export policy with each volume to configure client access to the volume. Each SVM can contain multiple export policies. This enables you to do the following for SVMs with multiple volumes:

- Assign different export policies to each volume of the SVM for individual client access control to each volume in the SVM.
- Assign the same export policy to multiple volumes of the SVM for identical client access control without having to create a new export policy for each volume.

You associate exactly one export policy to each volume to configure client access to the volume. Each SVM can contain multiple export policies. This enables you to do the following for SVMs with multiple volumes:

- Assign different export policies to each volume of the SVM for individual client access control to each volume in the SVM.
- Assign the same export policy to multiple volumes of the SVM for identical client access control without having to create a new export policy for each volume.

Each SVM has at least one export policy called “default”, which contains no rules. You cannot delete this export policy, but you can rename or modify it. Each volume on the SVM by default is associated with the default export policy. If export policies for SMB access is disabled on the SVM, the “default” export policy has no effect on SMB access.

You can configure rules that provide access to both NFS and SMB hosts and associate that rule with an export policy, which can then be associated with the volume that contains data to which both NFS and SMB hosts need access. Alternatively, if there are some volumes where only SMB clients require access, you can configure an export policy with rules that only allow access using the SMB protocol and that uses only Kerberos or NTLM (or both) for authentication for read-only and write access. The export policy is then associated to the volumes where only SMB access is desired.

If export policies for SMB is enabled and a client makes an access request that is not permitted by the applicable export policy, the request fails with a permission-denied message. If a client does not match any rule in the volume’s export policy, then access is denied. If an export policy is empty, then all accesses are implicitly denied. This is true even if the share and file permissions would otherwise permit access. This means that you must configure your export policy to minimally allow the following on volumes containing SMB shares:

- Allow access to all clients or the appropriate subset of clients
- Allow access over SMB
- Allow appropriate read-only and write access by using Kerberos or NTLM authentication (or both)

For information about configuring and managing export policies, see [NFS management](#).

### How export rules work

Export rules are the functional elements of an export policy. Export rules match client access requests to a volume against specific parameters you configure to determine how to handle the client access requests.

An export policy must contain at least one export rule to allow access to clients. If an export policy contains more than one rule, the rules are processed in the order in which they appear in the export policy. The rule order is dictated by the rule index number. If a rule matches a client, the permissions of that rule are used and no further rules are processed. If no rules match, the client is denied access.

You can configure export rules to determine client access permissions using the following criteria:

- The file access protocol used by the client sending the request, for example, NFSv4 or SMB.
- A client identifier, for example, host name or IP address.

The maximum size for the `-clientmatch` field is 4096 characters.

- The security type used by the client to authenticate, for example, Kerberos v5, NTLM, or AUTH\_SYS.

If a rule specifies multiple criteria, the client must match all of them for the rule to apply.

### Example

The export policy contains an export rule with the following parameters:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

The client access request is sent using the NFSv3 protocol and the client has the IP address 10.1.17.37.

Even though the client access protocol matches, the IP address of the client is in a different subnet from the one specified in the export rule. Therefore, client matching fails and this rule does not apply to this client.

### Example

The export policy contains an export rule with the following parameters:

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

The client access request is sent using the NFSv4 protocol and the client has the IP address 10.1.16.54.

The client access protocol matches and the IP address of the client is in the specified subnet. Therefore, client matching is successful and this rule applies to this client. The client gets read-write access regardless of its security type.

### Example

The export policy contains an export rule with the following parameters:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

Client #1 has the IP address 10.1.16.207, sends an access request using the NFSv3 protocol, and authenticated with Kerberos v5.

Client #2 has the IP address 10.1.16.211, sends an access request using the NFSv3 protocol, and authenticated with AUTH\_SYS.

The client access protocol and IP address matches for both clients. The read-only parameter allows read-only access to all clients regardless of the security type they authenticated with. Therefore both clients get read-only access. However, only client #1 gets read-write access because it used the approved security type Kerberos v5 to authenticate. Client #2 does not get read-write access.

### Examples of export policy rules that restrict or allow access over SMB

The examples show how to create export policy rules that restrict or allow access over SMB on an SVM that has export policies for SMB access enabled.

Export policies for SMB access are disabled by default. You need to configure export policy rules that restrict or allow access over SMB only if you have enabled export policies for SMB access.

### Export rule for SMB access only

The following command creates an export rule on the SVM named “vs1” that has the following configuration:

- Policy name: `cifs1`
- Index number: 1
- Client match: Matches only clients on the 192.168.1.0/24 network
- Protocol: Only enables SMB access
- Read-only access: To clients using NTLM or Kerberos authentication
- Read-write access: To clients using Kerberos authentication

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

## Export rule for SMB and NFS access

The following command creates an export rule on the SVM named "vs1" that has the following configuration:

- Policy name: cifs nfs1
- Index number: 2
- Client match: Matches all clients
- Protocol: SMB and NFS access
- Read-only access: To all clients
- Read-write access: To clients using Kerberos (NFS and SMB) or NTLM authentication (SMB)
- Mapping for UNIX user ID 0 (zero): Mapped to user ID 65534 (which typically maps to the user name nobody)
- Suid and sgid access: Allows

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs nfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule any
-rwrule krb5,ntlm -anon 65534 -allow-suid true
```

## Export rule for SMB access using NTLM only

The following command creates an export rule on the SVM named "vs1" that has the following configuration:

- Policy name: ntlm1
- Index number: 1
- Client match: Matches all clients
- Protocol: Only enables SMB access
- Read-only access: Only to clients using NTLM
- Read-write access: Only to clients using NTLM



If you configure the read-only option or the read-write option for NTLM-only access, you must use IP address-based entries in the client match option. Otherwise, you receive `access denied` errors. This is because ONTAP uses Kerberos Service Principal Names (SPN) when using a host name to check on the client's access rights. NTLM authentication does not support SPN names.

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

## Enable or disable export policies for SMB access

You can enable or disable export policies for SMB access on storage virtual machines (SVMs). Using export policies to control SMB access to resources is optional.

## Before you begin

The following are the requirements for enabling export policies for SMB:

- The client must have a “PTR” record in DNS before you create the export rules for that client.
- An additional set of “A” and “PTR” records for host names is required if the SVM provides access to NFS clients and the host name you want to use for NFS access is different from the CIFS server name.

## About this task

When setting up a new CIFS server on your SVM, the use of export policies for SMB access is disabled by default. You can enable export policies for SMB access if you want to control access based on authentication protocol or on client IP addresses or host names. You can enable or disable export policies for SMB access at any time.

## Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Enable or disable export policies:
  - Enable export policies: `vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled true`
  - Disable export policies: `vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled false`
3. Return to the admin privilege level: `set -privilege admin`

## Example

The following example enables the use of export policies to control SMB client access to resources on SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy
-enabled true

cluster1::*> set -privilege admin
```

## Secure file access by using Storage-Level Access Guard

### Secure file access by using Storage-Level Access Guard

In addition to securing access by using native file-level and export and share security, you can configure Storage-Level Access Guard, a third layer of security applied by ONTAP at the volume level. Storage-Level Access Guard applies to access from all NAS protocols to the storage object to which it is applied.

Only NTFS access permissions are supported. For ONTAP to perform security checks on UNIX users for access to data on volumes for which Storage-Level Access Guard has been applied, the UNIX user must map

to a Windows user on the SVM that owns the volume.

### **Storage-Level Access Guard behavior**

- Storage-Level Access Guard applies to all the files or all the directories in a storage object.

Because all files or directories in a volume are subject to Storage-Level Access Guard settings, inheritance through propagation is not required.

- You can configure Storage-Level Access Guard to apply to files only, to directories only, or to both files and directories within a volume.

- File and directory security

Applies to every directory and file within the storage object. This is the default setting.

- File security

Applies to every file within the storage object. Applying this security does not affect access to, or auditing of, directories.

- Directory security

Applies to every directory within the storage object. Applying this security does not affect access to, or auditing of, files.

- Storage-Level Access Guard is used to restrict permissions.

It will never give extra access permissions.

- If you view the security settings on a file or directory from an NFS or SMB client, you do not see the Storage-Level Access Guard security.

It's applied at the storage object level and stored in the metadata used to determine the effective permissions.

- Storage-level security cannot be revoked from a client, even by a system (Windows or UNIX) administrator.

It is designed to be modified by storage administrators only.

- You can apply Storage-Level Access Guard to volumes with NTFS or mixed security style.
- You can apply Storage-Level Access Guard to volumes with UNIX security style as long as the SVM containing the volume has a CIFS server configured.
- When volumes are mounted under a volume junction path and if Storage-Level Access Guard is present on that path, it will not be propagated to volumes mounted under it.
- The Storage-Level Access Guard security descriptor is replicated with SnapMirror data replication and with SVM replication.
- There is special dispensation for virus scanners.

Exceptional access is allowed to these servers to screen files and directories, even if Storage-Level Access Guard denies access to the object.

- FPolicy notifications are not sent if access is denied because of Storage-Level Access Guard.



## Order of access checks

Access to a file or directory is determined by the combined effect of the export or share permissions, the Storage-Level Access Guard permissions set on volumes, and the native file permissions applied to files and/or directories. All levels of security are evaluated to determine what the effective permissions a file or directory has. The security access checks are performed in the following order:

1. SMB share or NFS export-level permissions
2. Storage-Level Access Guard
3. NTFS file/folder access control lists (ACLs), NFSv4 ACLs, or UNIX mode bits

## Use cases for using Storage-Level Access Guard

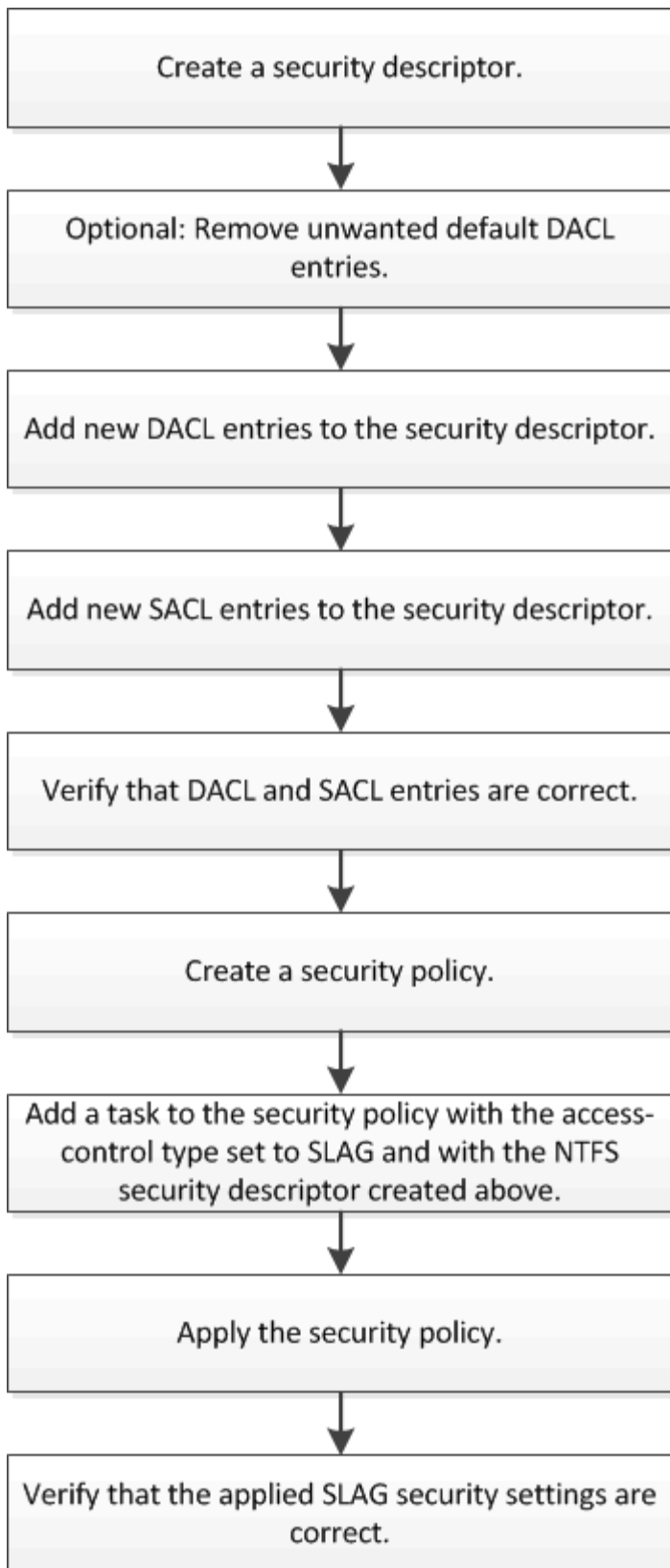
Storage-Level Access Guard provides additional security at the storage level, which is not visible from a client side; therefore, it cannot be revoked by any of the users or administrators from their desktops. There are certain use cases where the ability to control access at the storage level is beneficial.

Typical use cases for this feature include the following scenarios:

- Intellectual property protection by auditing and controlling all users' access at the storage level
- Storage for financial services companies, including banking and trading groups
- Government services with separate file storage for individual departments
- Universities protecting all student files

## Workflow to configure Storage-Level Access Guard

The workflow to configure Storage-Level Access Guard (SLAG) uses the same ONTAP CLI commands that you use to configure NTFS file permissions and auditing policies. Instead of configuring file and directory access on a designated target, you configure SLAG on the designated storage virtual machine (SVM) volume.



**Related information**

[Configuring Storage-Level Access Guard](#)

## Configure Storage-Level Access Guard

There are a number of steps you need to follow to configure Storage-Level Access Guard on a volume or qtree. Storage-Level Access Guard provides a level of access security that is set at the storage level. It provides security that applies to all accesses from all NAS protocols to the storage object to which it has been applied.

### Steps

1. Create a security descriptor by using the `vserver security file-directory ntfs create` command.

```
vserver security file-directory ntfs create -vserver vs1 -ntfs-sd sd1 vserver
security file-directory ntfs show -vserver vs1
```

```
Vserver: vs1

NTFS Security      Owner Name
Descriptor Name
-----
sd1                -
```

A security descriptor is created with the following four default DACL access control entries (ACEs):

```
Vserver: vs1
NTFS Security Descriptor Name: sd1

Account Name      Access  Access  Apply To
Type              Rights
-----
BUILTIN\Administrators
allow            full-control  this-folder, sub-folders,
files
BUILTIN\Users
allow            full-control  this-folder, sub-folders,
files
CREATOR OWNER
allow            full-control  this-folder, sub-folders,
files
NT AUTHORITY\SYSTEM
allow            full-control  this-folder, sub-folders,
files
```

If you do not want to use the default entries when configuring Storage-Level Access Guard, you can remove them prior to creating and adding your own ACEs to the security descriptor.

2. Remove any of the default DACL ACEs from the security descriptor that you do not want configured with Storage-Level Access Guard security:
  - a. Remove any unwanted DACL ACEs by using the `vserver security file-directory ntfs`

`dacl remove` command.

In this example, three default DACL ACEs are removed from the security descriptor: BUILTIN\Administrators, BUILTIN\Users, and CREATOR OWNER.

```
vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1
-access-type allow -account builtin\users vserver security file-directory
ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account
builtin\administrators vserver security file-directory ntfs dacl remove
-vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
```

- b. Verify that the DACL ACEs you do not want to use for Storage-Level Access Guard security are removed from the security descriptor by using the `vserver security file-directory ntfs dacl show` command.

In this example, the output from the command verifies that three default DACL ACEs have been removed from the security descriptor, leaving only the NT AUTHORITY\SYSTEM default DACL ACE entry:

```
vserver security file-directory ntfs dacl show -vserver vs1
```

```
Vserver: vs1
NTFS Security Descriptor Name: sd1

Account Name      Access  Access  Apply To
                  Type   Rights
-----
NT AUTHORITY\SYSTEM
                  allow   full-control  this-folder, sub-
folders, files
```

3. Add one or more DACL entries to a security descriptor by using the `vserver security file-directory ntfs dacl add` command.

In this example, two DACL ACEs are added to the security descriptor:

```
vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
-access-type allow -account example\engineering -rights full-control -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs dacl add
-vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users"
-rights read -apply-to this-folder,sub-folders,files
```

4. Add one or more SACL entries to a security descriptor by using the `vserver security file-directory ntfs sacl add` command.

In this example, two SACL ACEs are added to the security descriptor:

```
vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
-access-type failure -account "example\Domain Users" -rights read -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs sacl add
```

```
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. Verify that the DACL and SACL ACEs are configured correctly by using the `vserver security file-directory ntfs dacl show` and `vserver security file-directory ntfs sacl show` commands, respectively.

In this example, the following command displays information about DACL entries for security descriptor “sd1”:

```
vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
NTFS Security Descriptor Name: sd1

Account Name      Access  Access  Apply To
                  Type    Rights
-----
EXAMPLE\Domain Users
                  allow   read    this-folder, sub-folders,
files
EXAMPLE\engineering
                  allow   full-control  this-folder, sub-folders,
files
NT AUTHORITY\SYSTEM
                  allow   full-control  this-folder, sub-folders,
files
```

In this example, the following command displays information about SACL entries for security descriptor “sd1”:

```
vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
NTFS Security Descriptor Name: sd1

Account Name      Access  Access  Apply To
                  Type    Rights
-----
EXAMPLE\Domain Users
                  failure read    this-folder, sub-folders,
files
EXAMPLE\engineering
                  success full-control  this-folder, sub-folders,
files
```

6. Create a security policy by using the `vserver security file-directory policy create` command.

The following example creates a policy named “policy1”:

```
vserver security file-directory policy create -vserver vs1 -policy-name policy1
```

7. Verify that the policy is correctly configured by using the `vserver security file-directory policy show` command.

```
vserver security file-directory policy show
```

Vserver	Policy Name
vs1	policy1

8. Add a task with an associated security descriptor to the security policy by using the `vserver security file-directory policy-task add` command with the `-access-control` parameter set to `slag`.

Even though a policy can contain more than one Storage-Level Access Guard task, you cannot configure a policy to contain both file-directory and Storage-Level Access Guard tasks. A policy must contain either all Storage-Level Access Guard tasks or all file-directory tasks.

In this example, a task is added to the policy named “policy1”, which is assigned to security descriptor “sd1”. It is assigned to the `/datavol1` path with the access control type set to “slag”.

```
vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode propagate -ntfs-sd sd1
```

9. Verify that the task is configured correctly by using the `vserver security file-directory policy task show` command.

```
vserver security file-directory policy task show -vserver vs1 -policy-name policy1
```

```
Vserver: vs1
Policy: policy1
```

Index	File/Folder	Access	Security	NTFS	NTFS
Security	Path	Control	Type	Mode	Descriptor
Name					
1	/datavol1	slag	ntfs	propagate	sd1

10. Apply the Storage-Level Access Guard security policy by using the `vserver security file-directory apply` command.

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

The job to apply the security policy is scheduled.

11. Verify that the applied Storage-Level Access Guard security settings are correct by using the `vserver security file-directory show` command.

In this example, the output from the command shows that Storage-Level Access Guard security has been applied to the NTFS volume `/datavol1`. Even though the default DACL allowing Full Control to Everyone remains, Storage-Level Access Guard security restricts (and audits) access to the groups defined in the Storage-Level Access Guard settings.

```
vserver security file-directory show -vserver vs1 -path /datavol1
```

```

        Vserver: vs1
        File Path: /datavol1
File Inode Number: 77
        Security Style: ntfs
        Effective Style: ntfs
        DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
        ACLs: NTFS Security Descriptor
Control:0x8004
Owner: BUILTIN\Administrators
Group: BUILTIN\Administrators
DACL - ACEs
        ALLOW-Everyone-0x1f01ff
        ALLOW-Everyone-0x10000000-OI|CI|IO

Storage-Level Access Guard security
SACL (Applies to Directories):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Directories):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
SACL (Applies to Files):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Files):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

**Related information**

[Managing NTFS file security, NTFS audit policies, and Storage-Level Access Guard on SVMs using the CLI](#)

[Workflow to configure Storage-Level Access Guard](#)

[Displaying information about Storage-Level Access Guard](#)

[Removing Storage-Level Access Guard](#)



## Effective SLAG matrix

You can configure SLAG on a volume or a qtree or both. The SLAG matrix defines on which volume or qtree is the SLAG configuration applicable under various scenarios listed in the table.

	Volume SLAG in an AFS	Volume SLAG in a Snapshot copy	Qtree SLAG in an AFS	Qtree SLAG in a Snapshot copy
Volume access in an Access File System (AFS)	YES	NO	N/A	N/A
Volume access in a Snapshot copy	YES	NO	N/A	N/A
Qtree access in an AFS (when SLAG is present in the qtree)	NO	NO	YES	NO
Qtree access in an AFS (when SLAG is not present in qtree)	YES	NO	NO	NO
Qtree access in Snapshot copy (when SLAG is present in the qtree AFS)	NO	NO	YES	NO
Qtree access in Snapshot copy (when SLAG is not present in the qtree AFS)	YES	NO	NO	NO

## Display information about Storage-Level Access Guard

Storage-Level Access Guard is a third layer of security applied on a volume or qtree. Storage-Level Access Guard settings cannot be viewed by using the Windows Properties window. You must use the ONTAP CLI to view information about Storage-Level Access Guard security, which you can use to validate your configuration or to troubleshoot file access issues.

### About this task

You must supply the name of the storage virtual machine (SVM) and the path to the volume or qtree whose Storage-Level Access Guard security information you want to display. You can display the output in summary form or as a detailed list.

### Step

1. Display Storage-Level Access Guard security settings with the desired level of detail:

If you want to display information...	Enter the following command...
In summary form	<pre>vserver security file-directory show -vserver vserver_name -path path</pre>
With expanded detail	<pre>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</pre>

### Examples

The following example displays Storage-Level Access Guard security information for the NTFS security-style volume with the path `/datavol1` in SVM `vs1`:

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1
```

```

    Vserver: vs1
    File Path: /datavol1
File Inode Number: 77
    Security Style: ntfs
    Effective Style: ntfs
    DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
    Unix User Id: 0
    Unix Group Id: 0
    Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
    ACLs: NTFS Security Descriptor
        Control:0x8004
        Owner: BUILTIN\Administrators
        Group: BUILTIN\Administrators
        DACL - ACEs
            ALLOW-Everyone-0x1f01ff
            ALLOW-Everyone-0x10000000-OI|CI|IO

Storage-Level Access Guard security
SACL (Applies to Directories):
    AUDIT-EXAMPLE\Domain Users-0x120089-FA
    AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Directories):
    ALLOW-EXAMPLE\Domain Users-0x120089
    ALLOW-EXAMPLE\engineering-0x1f01ff
    ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
SACL (Applies to Files):
    AUDIT-EXAMPLE\Domain Users-0x120089-FA
    AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Files):
    ALLOW-EXAMPLE\Domain Users-0x120089
    ALLOW-EXAMPLE\engineering-0x1f01ff
    ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

The following example displays the Storage-Level Access Guard information about the mixed security-style volume at the path /datavol15 in SVM vs1. The top level of this volume has UNIX effective security. The volume has Storage-Level Access Guard security.

```

cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5

        Vserver: vs1
        File Path: /datavol5
File Inode Number: 3374
        Security Style: mixed
        Effective Style: unix
        DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 755
Unix Mode Bits in Text: rwxr-xr-x
        ACLs: Storage-Level Access Guard security
        SACL (Applies to Directories):
            AUDIT-EXAMPLE\Domain Users-0x120089-FA
            AUDIT-EXAMPLE\engineering-0x1f01ff-SA
        DACL (Applies to Directories):
            ALLOW-EXAMPLE\Domain Users-0x120089
            ALLOW-EXAMPLE\engineering-0x1f01ff
            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
        SACL (Applies to Files):
            AUDIT-EXAMPLE\Domain Users-0x120089-FA
            AUDIT-EXAMPLE\engineering-0x1f01ff-SA
        DACL (Applies to Files):
            ALLOW-EXAMPLE\Domain Users-0x120089
            ALLOW-EXAMPLE\engineering-0x1f01ff
            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

### Remove Storage-Level Access Guard

You can remove Storage-Level Access Guard on a volume or qtree if you no longer want set access security at the storage level. Removing Storage-Level Access Guard does not modify or remove regular NTFS file and directory security.

#### Steps

1. Verify that the volume or qtree has Storage-Level Access Guard configured by using the `vserver security file-directory show` command.

```
vserver security file-directory show -vserver vs1 -path /datavol2
```

```

Vserver: vs1
File Path: /datavol2
File Inode Number: 99
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
Unix User Id: 0
Unix Group Id: 0
Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
Control:0xbf14
Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
SACL - ACEs
AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
DACL - ACEs
ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

Storage-Level Access Guard security
DACL (Applies to Directories):
ALLOW-BUILTIN\Administrators-0x1f01ff
ALLOW-CREATOR OWNER-0x1f01ff
ALLOW-EXAMPLE\Domain Admins-0x1f01ff
ALLOW-EXAMPLE\Domain Users-0x120089
ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
DACL (Applies to Files):
ALLOW-BUILTIN\Administrators-0x1f01ff
ALLOW-CREATOR OWNER-0x1f01ff
ALLOW-EXAMPLE\Domain Admins-0x1f01ff
ALLOW-EXAMPLE\Domain Users-0x120089
ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

2. Remove Storage-Level Access Guard by using the `vserver security file-directory remove-slag` command.

```
vserver security file-directory remove-slag -vserver vs1 -path /datavol2
```

3. Verify that Storage-Level Access Guard has been removed from the volume or `qtree` by using the `vserver security file-directory show` command.

```
vserver security file-directory show -vserver vs1 -path /datavol2
```

```

Vserver: vs1
File Path: /datavol2
File Inode Number: 99
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
Unix User Id: 0
Unix Group Id: 0
Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
Control:0xbf14
Owner: BUILTIN\Administrators
Group: BUILTIN\Administrators
SACL - ACEs
    AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
DACL - ACEs
    ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
    ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

```

## Manage file access using SMB

### Use local users and groups for authentication and authorization

#### How ONTAP uses local users and groups

#### Local users and groups concepts

You should know what local users and groups are, and some basic information about them, before determining whether to configure and use local users and groups in your environment.

- **Local user**

A user account with a unique security identifier (SID) that has visibility only on the storage virtual machine (SVM) on which it is created. Local user accounts have a set of attributes, including user name and SID. A local user account authenticates locally on the CIFS server using NTLM authentication.

User accounts have several uses:

- Used to grant *User Rights Management* privileges to a user.
- Used to control share-level and file-level access to file and folder resources that the SVM owns.

- **Local group**

A group with a unique SID has visibility only on the SVM on which it is created. Groups contain a set of

members. Members can be local users, domain users, domain groups, and domain machine accounts. Groups can be created, modified, or deleted.

Groups have several uses:

- Used to grant *User Rights Management* privileges to its members.
- Used to control share-level and file-level access to file and folder resources that the SVM owns.

- **Local domain**

A domain that has local scope, which is bounded by the SVM. The local domain's name is the CIFS server name. Local users and groups are contained within the local domain.

- **Security identifier (SID)**

A SID is a variable-length numeric value that identifies Windows-style security principals. For example, a typical SID takes the following form: S-1-5-21-3139654847-1303905135-2517279418-123456.

- **NTLM authentication**

A Microsoft Windows security method used to authenticate users on a CIFS server.

- **Cluster replicated database (RDB)**

A replicated database with an instance on each node in a cluster. Local user and group objects are stored in the RDB.

## Reasons for creating local users and local groups

There are several reasons for creating local users and local groups on your storage virtual machine (SVM). For example, you can access an SMB server by using a local user account if the domain controllers (DCs) are unavailable, you might want to use local groups to assign privileges, or your SMB server is in a workgroup.

You can create one or more local user accounts for the following reasons:

- Your SMB server is in a workgroup, and domain users are not available.

Local users are required in workgroup configurations.

- You want the ability to authenticate and log in to the SMB server if the domain controllers are unavailable.

Local users can authenticate with the SMB server by using NTLM authentication when the domain controller is down, or when network problems prevent your SMB server from contacting the domain controller.

- You want to assign *User Rights Management* privileges to a local user.

*User Rights Management* is the ability for an SMB server administrator to control what rights the users and groups have on the SVM. You can assign privileges to a user by assigning the privileges to the user's account, or by making the user a member of a local group that has those privileges.

You can create one or more local groups for the following reasons:

- Your SMB server is in a workgroup, and domain groups are not available.

Local groups are not required in workgroup configurations, but they can be useful for managing access privileges for local workgroup users.

- You want to control access to file and folder resources by using local groups for share and file-access control.
- You want to create local groups with customized *User Rights Management* privileges.

Some built-in user groups have predefined privileges. To assign a customized set of privileges, you can create a local group and assign the necessary privileges to that group. You can then add local users, domain users, and domain groups to the local group.

## Related information

[How local user authentication works](#)

[List of supported privileges](#)

## How local user authentication works

Before a local user can access data on a CIFS server, the user must create an authenticated session.

Because SMB is session-based, the identity of the user can be determined just once, when the session is first set up. The CIFS server uses NTLM-based authentication when authenticating local users. Both NTLMv1 and NTLMv2 are supported.

ONTAP uses local authentication under three use cases. Each use case depends on whether the domain portion of the user name (with the DOMAIN\user format) matches the CIFS server's local domain name (the CIFS server name):

- The domain portion matches

Users who provide local user credentials when requesting access to data are authenticated locally on the CIFS server.

- The domain portion does not match

ONTAP attempts to use NTLM authentication with a domain controller in the domain to which the CIFS server belongs. If authentication succeeds, the login is complete. If it does not succeed, what happens next depends on why authentication did not succeed.

For example, if the user exists in Active Directory but the password is invalid or expired, ONTAP does not attempt to use the corresponding local user account on the CIFS server. Instead, authentication fails. There are other cases where ONTAP uses the corresponding local account on the CIFS server, if it exists, for authentication—even though the NetBIOS domain names do not match. For example, if a matching domain account exists but it is disabled, ONTAP uses the corresponding local account on the CIFS server for authentication.

- The domain portion is not specified

ONTAP first attempts authentication as a local user. If authentication as a local user fails, then ONTAP authenticates the user with a domain controller in the domain to which the CIFS server belongs.



After local or domain user authentication is completed successfully, ONTAP constructs a complete user access token, which takes into account local group membership and privileges.

For more information about NTLM authentication for local users, see the Microsoft Windows documentation.

### Related information

[Enabling or disabling local user authentication](#)

### How user access tokens are constructed

When a user maps a share, an authenticated SMB session is established and a user access token is constructed that contains information about the user, the user's group membership and cumulative privileges, and the mapped UNIX user.

Unless the functionality is disabled, local user and group information is also added to the user access token. The way access tokens are constructed depends on whether the login is for a local user or an Active Directory domain user:

- Local user login

Although local users can be members of different local groups, local groups cannot be members of other local groups. The local user access token is composed of a union of all privileges assigned to groups to which a particular local user is a member.

- Domain user login

When a domain user logs in, ONTAP obtains a user access token that contains the user SID and SIDs for all the domain groups to which the user is a member. ONTAP uses the union of the domain user access token with the access token provided by local memberships of the user's domain groups (if any), as well as any direct privileges assigned to the domain user or any of its domain group memberships.

For both local and domain user login, the Primary Group RID is also set for the user access token. The default RID is `Domain Users` (RID 513). You cannot change the default.

The Windows-to-UNIX and UNIX-to-Windows name mapping process follows the same rules for both local and domain accounts.



There is no implied, automatic mapping from a UNIX user to a local account. If this is required, an explicit mapping rule must be specified using the existing name mapping commands.

### Guidelines for using SnapMirror on SVMs that contain local groups

You should be aware of the guidelines when you configure SnapMirror on volumes owned by SVMs that contain local groups.

You cannot use local groups in ACEs applied to files, directories, or shares that are replicated by SnapMirror to another SVM. If you use the SnapMirror feature to create a DR mirror to a volume on another SVM and the volume has an ACE for a local group, the ACE is not valid on the mirror. If data is replicated to a different SVM, the data is effectively crossing into a different local domain. The permissions granted to local users and groups are valid only within the scope of the SVM on which they were originally created.

## What happens to local users and groups when deleting CIFS servers

The default set of local users and groups is created when a CIFS server is created, and they are associated with the storage virtual machine (SVM) hosting the CIFS server. SVM administrators can create local users and groups at any time. You need to be aware of what happens to local users and groups when you delete the CIFS server.

Local users and groups are associated with SVMs; therefore, they are not deleted when CIFS servers are deleted due to security considerations. Although local users and groups are not deleted when the CIFS server is deleted, they are hidden. You cannot view or manage local users and groups until you re-create a CIFS server on the SVM.



The CIFS server administrative status does not affect visibility of local users or groups.

## How you can use Microsoft Management Console with local users and groups

You can view information about local users and groups from the Microsoft Management Console. With this release of ONTAP, you cannot perform other management tasks for local users and groups from the Microsoft Management Console.

### Guidelines for reverting

If you plan to revert the cluster to an ONTAP release that does not support local users and groups and local users and groups are being used to manage file access or user rights, you must be aware of certain considerations.

- Due to security reasons, information about configured local users, groups, and privileges are not deleted when ONTAP is reverted to a version that does not support local users and groups functionality.
- Upon a revert to a prior major version of ONTAP, ONTAP does not use local users and groups during authentication and credential creation.
- Local users and groups are not removed from file and folder ACLs.
- File access requests that depend on access being granted because of permissions granted to local users or groups are denied.

To allow access, you must reconfigure file permissions to allow access based on domain objects instead of local user and group objects.

### What local privileges are

#### List of supported privileges

ONTAP has a predefined set of supported privileges. Certain predefined local groups have some of these privileges added to them by default. You can also add or remove privileges from the predefined groups or create new local users or groups and add privileges to the groups that you created or to existing domain users and groups.

The following table lists the supported privileges on the storage virtual machine (SVM) and provides a list of BUILTIN groups with assigned privileges:

Privilege name	Default security setting	Description
SeTcbPrivilege	None	Act as part of the operating system
SeBackupPrivilege	BUILTIN\Administrators, BUILTIN\Backup Operators	Back up files and directories, overriding any ACLs
SeRestorePrivilege	BUILTIN\Administrators, BUILTIN\Backup Operators	Restore files and directories, overriding any ACLs Set any valid user or group SID as the file owner
SeTakeOwnershipPrivilege	BUILTIN\Administrators	Take ownership of files or other objects
SeSecurityPrivilege	BUILTIN\Administrators	Manage auditing This includes viewing, dumping, and clearing the security log.
SeChangeNotifyPrivilege	BUILTIN\Administrators, BUILTIN\Backup Operators, BUILTIN\Power Users, BUILTIN\Users, Everyone	Bypass traverse checking Users with this privilege are not required to have traverse (x) permissions to traverse folders, symlinks, or junctions.

#### Related information

[Managing local privileges](#)

[Configuring bypass traverse checking](#)

#### Assign privileges

You can assign privileges directly to local users or domain users. Alternatively, you can assign users to local groups whose assigned privileges match the capabilities that you want those users to have.

- You can assign a set of privileges to a group that you create.  
You then add a user to the group that has the privileges that you want that user to have.
- You can also assign local users and domain users to predefined groups whose default privileges match the privileges that you want to grant to those users.

#### Related information

[Adding privileges to local or domain users or groups](#)

[Removing privileges from local or domain users or groups](#)

[Resetting privileges for local or domain users and groups](#)

[Configuring bypass traverse checking](#)

## Guidelines for using BUILTIN groups and the local administrator account

There are certain guidelines you should keep in mind when you use BUILTIN groups and the local administrator account. For example, you can rename the local administrator account, but you cannot delete this account.

- The Administrator account can be renamed but cannot be deleted.
- The Administrator account cannot be removed from the BUILTIN\Administrators group.
- BUILTIN groups can be renamed but cannot be deleted.

After the BUILTIN group is renamed, another local object can be created with the well-known name; however, the object is assigned a new RID.

- There is no local Guest account.

### Related information

[Predefined BUILTIN groups and default privileges](#)

### Requirements for local user passwords

By default, local user passwords must meet complexity requirements. The password complexity requirements are similar to the requirements defined in the Microsoft Windows *Local security policy*.

The password must meet the following criteria:

- Must be at least six characters in length
- Must not contain the user account name
- Must contain characters from at least three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Special characters:

~!@#\$%^&\* \_ - + = ` \ | ( ) [ ] ; : " ' < > , . ? /

### Related information

[Enabling or disabling required password complexity for local SMB users](#)

[Displaying information about CIFS server security settings](#)

[Changing local user account passwords](#)

### Predefined BUILTIN groups and default privileges

You can assign membership of a local user or domain user to a predefined set of BUILTIN groups provided by ONTAP. Predefined groups have predefined privileges assigned.

The following table describes the predefined groups:

Predefined BUILTIN group	Default privileges
<p><b>BUILTIN\Administrators</b>RID 544</p> <p>When first created, the local Administrator account, with a RID of 500, is automatically made a member of this group. When the storage virtual machine (SVM) is joined to a domain, the domain\Domain Admins group is added to the group. If the SVM leaves the domain, the domain\Domain Admins group is removed from the group.</p>	<ul style="list-style-type: none"> <li>• SeBackupPrivilege</li> <li>• SeRestorePrivilege</li> <li>• SeSecurityPrivilege</li> <li>• SeTakeOwnershipPrivilege</li> <li>• SeChangeNotifyPrivilege</li> </ul>
<p><b>BUILTIN\Power Users</b>RID 547</p> <p>When first created, this group does not have any members. Members of this group have the following characteristics:</p> <ul style="list-style-type: none"> <li>• Can create and manage local users and groups.</li> <li>• Cannot add themselves or any other object to the BUILTIN\Administrators group.</li> </ul>	<p>SeChangeNotifyPrivilege</p>
<p><b>BUILTIN\Backup Operators</b>RID 551</p> <p>When first created, this group does not have any members. Members of this group can override read and write permissions on files or folders if they are opened with backup intent.</p>	<ul style="list-style-type: none"> <li>• SeBackupPrivilege</li> <li>• SeRestorePrivilege</li> <li>• SeChangeNotifyPrivilege</li> </ul>
<p><b>BUILTIN\Users</b>RID 545</p> <p>When first created, this group does not have any members (besides the implied Authenticated Users special group). When the SVM is joined to a domain, the domain\Domain Users group is added to this group. If the SVM leaves the domain, the domain\Domain Users group is removed from this group.</p>	<p>SeChangeNotifyPrivilege</p>
<p><b>Everyone</b>SID S-1-1-0</p> <p>This group includes all users, including guests (but not anonymous users). This is an implied group with an implied membership.</p>	<p>SeChangeNotifyPrivilege</p>

#### Related information

[Guidelines for using BUILTIN groups and the local administrator account](#)

[List of supported privileges](#)

[Configuring bypass traverse checking](#)

## Enable or disable local users and groups functionality

### Enable or disable local users and groups functionality overview

Before you can use local users and groups for access control of NTFS security-style data, local user and group functionality must be enabled. Additionally, if you want to use local users for SMB authentication, the local user authentication functionality must be enabled.

Local users and groups functionality and local user authentication are enabled by default. If they are not enabled, you must enable them before you can configure and use local users and groups. You can disable local users and groups functionality at any time.

In addition to explicitly disabling local user and group functionality, ONTAP disables local user and group functionality if any node in the cluster is reverted to an ONTAP release that does not support the functionality. Local user and group functionality is not enabled until all nodes in the cluster are running a version of ONTAP that supports it.

### Related information

[Modify local user accounts](#)

[Modify local groups](#)

[Add privileges to local or domain users or groups](#)

## Enable or disable local users and groups

You can enable or disable local users and groups for SMB access on storage virtual machines (SVMs). Local users and groups functionality is enabled by default.

### About this task

You can use local users and groups when configuring SMB share and NTFS file permissions and can optionally use local users for authentication when creating an SMB connection. To use local users for authentication, you must also enable the local users and groups authentication option.

### Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Perform one of the following actions:

If you want local users and groups to be...	Enter the command...
Enabled	<pre>vserver cifs options modify -vserver vserver_name -is-local-users-and -groups-enabled true</pre>

If you want local users and groups to be...	Enter the command...
Disabled	<pre>vserver cifs options modify -vserver vserver_name -is-local-users-and -groups-enabled false</pre>

3. Return to the admin privilege level: `set -privilege admin`

### Example

The following example enables local users and groups functionality on SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

cluster1::*> set -privilege admin
```

### Related information

[Enable or disable local user authentication](#)

[Enable or disable local user accounts](#)

### Enable or disable local user authentication

You can enable or disable local user authentication for SMB access on storage virtual machines (SVMs). The default is to allow local user authentication, which is useful when the SVM cannot contact a domain controller or if you choose not to use domain-level access controls.

### Before you begin

Local users and groups functionality must be enabled on the CIFS server.

### About this task

You can enable or disable local user authentication at any time. If you want to use local users for authentication when creating an SMB connection, you must also enable the CIFS server's local users and groups option.

### Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Perform one of the following actions:

If you want local authentication to be...	Enter the command...
Enabled	<code>vserver cifs options modify -vserver vserver_name -is-local-auth-enabled true</code>
Disabled	<code>vserver cifs options modify -vserver vserver_name -is-local-auth-enabled false</code>

3. Return to the admin privilege level: `set -privilege admin`

### Example

The following example enables local user authentication on SVM vs1:

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth
-enabled true

cluster1::*> set -privilege admin
```

### Related information

[How local user authentication works](#)

[Enabling or disabling local users and groups](#)

### Manage local user accounts

#### Modify local user accounts

You can modify a local user account if you want to change an existing user's full name or description, and if you want to enable or disable the user account. You can also rename a local user account if the user's name is compromised or if a name change is needed for administrative purposes.

If you want to...	Enter the command...
Modify the local user's full name	<code>vserver cifs users-and-groups local-user modify -vserver vserver_name -user -name user_name -full-name text</code> If the full name contains a space, then it must be enclosed within double quotation marks.



If you want to...	Enter the command...
Modify the local user's description	<code>vserver cifs users-and-groups local-user modify -vserver <i>vserver_name</i> -user -name <i>user_name</i> -description <i>text</i></code> If the description contains a space, then it must be enclosed within double quotation marks.
Enable or disable the local user account	<code>vserver cifs users-and-groups local-user modify -vserver <i>vserver_name</i> -user -name <i>user_name</i> -is-account-disabled {true false}</code>
Rename the local user account	<code>vserver cifs users-and-groups local-user rename -vserver <i>vserver_name</i> -user -name <i>user_name</i> -new-user-name <i>new_user_name</i></code> When renaming a local user, the new user name must remain associated with the same CIFS server as the old user name.

### Example

The following example renames the local user “CIFS\_SERVER\sue” to “CIFS\_SERVER\sue\_new” on storage virtual machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

### Enable or disable local user accounts

You enable a local user account if you want the user to be able to access data contained in the storage virtual machine (SVM) over an SMB connection. You can also disable a local user account if you do not want that user to access SVM data over SMB.

#### About this task

You enable a local user by modifying the user account.

#### Step

1. Perform the appropriate action:

If you want to...	Enter the command...
Enable the user account	<code>vserver cifs users-and-groups local-user modify -vserver <i>vserver_name</i> -user-name <i>user_name</i> -is-account-disabled false</code>

If you want to...	Enter the command...
Disable the user account	<pre>vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account -disabled true</pre>

## Change local user account passwords

You can change a local user's account password. This can be useful if the user's password is compromised or if the user has forgotten the password.

### Step

1. Change the password by performing the appropriate action: `vserver cifs users-and-groups local-user set-password -vserver vserver_name -user-name user_name`

### Example

The following example sets the password for the local user "CIFS\_SERVER\sue" associated with storage virtual machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups local-user set-password -user -name CIFS_SERVER\sue -vserver vs1
```

Enter the new password:

Confirm the new password:

### Related information

[Enabling or disabling required password complexity for local SMB users](#)

[Displaying information about CIFS server security settings](#)

### Display information about local users

You can display a list of all local users in a summary form. If you want to determine which account settings are configured for a specific user, you can display detailed account information for that user as well as the account information for multiple users. This information can help you determine if you need to modify a user's settings, and also to troubleshoot authentication or file access issues.

### About this task

Information about a user's password is never displayed.

### Step

1. Perform one of the following actions:

If you want to...	Enter the command...
Display information about all users on the storage virtual machine (SVM)	<code>vserver cifs users-and-groups local-user show -vserver <i>vserver_name</i></code>
Display detailed account information for a user	<code>vserver cifs users-and-groups local-user show -instance -vserver <i>vserver_name</i> -user-name <i>user_name</i></code>

There are other optional parameters that you can choose when you run the command. See the man page for more information.

### Example

The following example displays information about all local users on SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                               Full Name      Description
-----  -
vs1      CIFS_SERVER\Administrator                 James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue                           Sue   Jones
```

### Display information about group memberships for local users

You can display information about which local groups that a local user belongs to. You can use this information to determine what access the user should have to files and folders. This information can be useful in determining what access rights the user should have to files and folders or when troubleshooting file access issues.

#### About this task

You can customize the command to display only the information that you want to see.

#### Step

1. Perform one of the following actions:

If you want to...	Enter the command...
Display local user membership information for a specified local user	<code>vserver cifs users-and-groups local-user show-membership -user-name <i>user_name</i></code>
Display local user membership information for the local group of which this local user is a member	<code>vserver cifs users-and-groups local-user show-membership -membership <i>group_name</i></code>

If you want to...	Enter the command...
Display user membership information for local users that are associated with a specified storage virtual machine (SVM)	<code>vserver cifs users-and-groups local-user show-membership -vserver <i>vserver_name</i></code>
Display detailed information for all local users on a specified SVM	<code>vserver cifs users-and-groups local-user show-membership -instance -vserver <i>vserver_name</i></code>

### Example

The following example displays the membership information for all local users on SVM vs1; user “CIFS\_SERVER\Administrator” is a member of the “BUILTIN\Administrators” group, and “CIFS\_SERVER\sue” is a member of “CIFS\_SERVER\g1” group:

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
Vserver      User Name                Membership
-----
vs1          CIFS_SERVER\Administrator BUILTIN\Administrators
            CIFS_SERVER\sue         CIFS_SERVER\g1
```

### Delete local user accounts

You can delete local user accounts from your storage virtual machine (SVM) if they are no longer needed for local SMB authentication to the CIFS server or for determining access rights to data contained on your SVM.

#### About this task

Keep the following in mind when deleting local users:

- The file system is not altered.  
Windows Security Descriptors on files and directories that refer to this user are not adjusted.
- All references to local users are removed from the membership and privileges databases.
- Standard, well-known users such as Administrator cannot be deleted.

#### Steps

1. Determine the name of the local user account that you want to delete: `vserver cifs users-and-groups local-user show -vserver vserver_name`
2. Delete the local user: `vserver cifs users-and-groups local-user delete -vserver vserver_name -user-name username_name`
3. Verify that the user account is deleted: `vserver cifs users-and-groups local-user show -vserver vserver_name`

## Example

The following example deletes the local user “CIFS\_SERVER\sue” associated with SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                Full Name                Description
-----  -
vs1      CIFS_SERVER\Administrator  James Smith              Built-in administrator
account
vs1      CIFS_SERVER\sue           Sue Jones

cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                Full Name                Description
-----  -
vs1      CIFS_SERVER\Administrator  James Smith              Built-in administrator
account
```

## Manage local groups

### Modify local groups

You can modify existing local groups by changing the description for an existing local group or by renaming the group.

If you want to...	Use the command...
Modify the local group description	<code>vserver cifs users-and-groups local-group modify -vserver <i>vserver_name</i> -group-name <i>group_name</i> -description <i>text</i></code> If the description contains a space, then it must be enclosed within double quotation marks.
Rename the local group	<code>vserver cifs users-and-groups local-group rename -vserver <i>vserver_name</i> -group-name <i>group_name</i> -new-group-name <i>new_group_name</i></code>

### Examples

The following example renames the local group “CIFS\_SERVER\engineering” to “CIFS\_SERVER\engineering\_new”:

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

The following example modifies the description of the local group “CIFS\_SERVER\engineering”:

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

## Display information about local groups

You can display a list of all local groups configured on the cluster or on a specified storage virtual machine (SVM). This information can be useful when troubleshooting file-access issues to data contained on the SVM or user-rights (privilege) issues on the SVM.

### Step

1. Perform one of the following actions:

If you want information about...	Enter the command...
All local groups on the cluster	<code>vserver cifs users-and-groups local-group show</code>
All local groups on the SVM	<code>vserver cifs users-and-groups local-group show -vserver <i>vserver_name</i></code>

There are other optional parameters that you can choose when you run this command. See the man page for more information.

### Example

The following example displays information about all local groups on SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver  Group Name                Description
-----  -
vs1      BUILTIN\Administrators     Built-in Administrators group
vs1      BUILTIN\Backup Operators   Backup Operators group
vs1      BUILTIN\Power Users        Restricted administrative privileges
vs1      BUILTIN\Users              All users
vs1      CIFS_SERVER\engineering
vs1      CIFS_SERVER\sales
```

## Manage local group membership

You can manage local group membership by adding and removing local or domain users, or adding and removing domain groups. This is useful if you want to control access to data based on access controls placed on the group or if you want users to have privileges associated with that group.

### About this task

Guidelines for adding members to a local group:

- You cannot add users to the special *Everyone* group.
- The local group must exist before you can add a user to it.
- The user must exist before you can add the user to a local group.
- You cannot add a local group to another local group.
- To add a domain user or group to a local group, Data ONTAP must be able to resolve the name to a SID.

Guidelines for removing members from a local group:

- You cannot remove members from the special *Everyone* group.
- The group from which you want to remove a member must exist.
- ONTAP must be able to resolve the names of members that you want to remove from the group to a corresponding SID.

### Step

1. Add or remove a member in a group.

If you want to...	Then use the command...
Add a member to a group	<pre>vserver cifs users-and-groups local- group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]</pre> <p>You can specify a comma-delimited list of local users, domain users, or domain groups to add to the specified local group.</p>
Remove a member from a group	<pre>vserver cifs users-and-groups local- group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]</pre> <p>You can specify a comma-delimited list of local users, domain users, or domain groups to remove from the specified local group.</p>

The following example adds a local user “SMB\_SERVER\sue” and a domain group “AD\_DOM\dom\_eng” to the local group “SMB\_SERVER\engineering” on SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

The following example removes the local users “SMB\_SERVER\sue” and “SMB\_SERVER\james” from the local group “SMB\_SERVER\engineering” on SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

## Related information

[Displaying information about members of local groups](#)

### Display information about members of local groups

You can display a list of all members of local groups configured on the cluster or on a specified storage virtual machine (SVM). This information can be useful when troubleshooting file-access issues or user-rights (privilege) issues.

#### Step

1. Perform one of the following actions:

If you want to display information about...	Enter the command...
Members of all local groups on the cluster	<pre>vserver cifs users-and-groups local- group show-members</pre>
Members of all local groups on the SVM	<pre>vserver cifs users-and-groups local- group show-members -vserver vserver_name</pre>

#### Example

The following example displays information about members of all local groups on SVM vs1:



```

cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver   Group Name                               Members
-----
vs1       BUILTIN\Administrators                  CIFS_SERVER\Administrator
                                                AD_DOMAIN\Domain Admins
                                                AD_DOMAIN\dom_grp1
        BUILTIN\Users                        AD_DOMAIN\Domain Users
                                                AD_DOMAIN\dom_usr1
        CIFS_SERVER\engineering              CIFS_SERVER\james

```

## Delete a local group

You can delete a local group from the storage virtual machine (SVM) if it is no longer needed for determining access rights to data associated with that SVM or if it is no longer needed for assigning SVM user rights (privileges) to group members.

### About this task

Keep the following in mind when deleting local groups:

- The file system is not altered.  
Windows Security Descriptors on files and directories that refer to this group are not adjusted.
- If the group does not exist, an error is returned.
- The special *Everyone* group cannot be deleted.
- Built-in groups such as *BUILTIN\Administrators* *BUILTIN\Users* cannot be deleted.

### Steps

1. Determine the name of the local group that you want to delete by displaying the list of local groups on the SVM: `vserver cifs users-and-groups local-group show -vserver vserver_name`
2. Delete the local group: `vserver cifs users-and-groups local-group delete -vserver vserver_name -group-name group_name`
3. Verify that the group is deleted: `vserver cifs users-and-groups local-user show -vserver vserver_name`

### Example

The following example deletes the local group “CIFS\_SERVER\sales” associated with SVM vs1:

```

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver      Group Name          Description
-----
vs1          BUILTIN\Administrators  Built-in Administrators group
vs1          BUILTIN\Backup Operators Backup Operators group
vs1          BUILTIN\Power Users     Restricted administrative
privileges
vs1          BUILTIN\Users           All users
vs1          CIFS_SERVER\engineering
vs1          CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1
-group-name CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver      Group Name          Description
-----
vs1          BUILTIN\Administrators  Built-in Administrators group
vs1          BUILTIN\Backup Operators Backup Operators group
vs1          BUILTIN\Power Users     Restricted administrative
privileges
vs1          BUILTIN\Users           All users
vs1          CIFS_SERVER\engineering

```

### Update domain user and group names in local databases

You can add domain users and groups to a CIFS server's local groups. These domain objects are registered in local databases on the cluster. If a domain object is renamed, the local databases must be manually updated.

#### About this task

You must specify the name of the storage virtual machine (SVM) on which you want to update domain names.

#### Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Perform the appropriate action:

If you want to update domain users and groups and...	Use this command...
Display domain users and groups that successfully updated and that failed to update	<code>vserver cifs users-and-groups update-names -vserver vserver_name</code>

If you want to update domain users and groups and...	Use this command...
Display domain users and groups that successfully updated	<code>vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only false</code>
Display only the domain users and groups that fail to update	<code>vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only true</code>
Suppress all status information about updates	<code>vserver cifs users-and-groups update-names -vserver vserver_name -suppress -all-output true</code>

3. Return to the admin privilege level: `set -privilege admin`

### Example

The following example updates the names of domain users and groups associated with storage virtual machine (SVM, formerly known as Vserver) vs1. For the last update, there is a dependent chain of names that needs to be updated:

```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs users-and-groups update-names -vserver vs1

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654321-12345
Domain:           EXAMPLE1
Out-of-date Name: dom_user1
Updated Name:     dom_user2
Status:           Successfully updated

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654322-23456
Domain:           EXAMPLE2
Out-of-date Name: dom_user1
Updated Name:     dom_user2
Status:           Successfully updated

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654321-123456
Domain:           EXAMPLE1
Out-of-date Name: dom_user3
Updated Name:     dom_user4
Status:           Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                  to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                  to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                  to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                  to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin

```

## Manage local privileges

## Add privileges to local or domain users or groups

You can manage user rights for local or domain users or groups by adding privileges. The added privileges override the default privileges assigned to any of these objects. This provides enhanced security by allowing you to customize what privileges a user or group has.

### Before you begin

The local or domain user or group to which privileges will be added must already exist.

### About this task

Adding a privilege to an object overrides the default privileges for that user or group. Adding a privilege does not remove previously added privileges.

You must keep the following in mind when adding privileges to local or domain users or groups:

- You can add one or more privileges.
- When adding privileges to a domain user or group, ONTAP might validate the domain user or group by contacting the domain controller.

The command might fail if ONTAP is unable to contact the domain controller.

### Steps

1. Add one or more privileges to a local or domain user or group: `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or-group-name name -privileges _privilege_[,...]`
2. Verify that the desired privileges are applied to the object: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

### Example

The following example adds the privileges “SeTcbPrivilege” and “SeTakeOwnershipPrivilege” to the user “CIFS\_SERVER\sue” on storage virtual machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          CIFS_SERVER\sue         SeTcbPrivilege
                                     SeTakeOwnershipPrivilege
```

## Remove privileges from local or domain users or groups

You can manage user rights for local or domain users or groups by removing privileges. This provides enhanced security by allowing you to customize the maximum privileges

that users and groups have.

### Before you begin

The local or domain user or group from which privileges will be removed must already exist.

### About this task

You must keep the following in mind when removing privileges from local or domain users or groups:

- You can remove one or more privileges.
- When removing privileges from a domain user or group, ONTAP might validate the domain user or group by contacting the domain controller.

The command might fail if ONTAP is unable to contact the domain controller.

### Steps

1. Remove one or more privileges from a local or domain user or group: `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or-group-name _name_ -privileges _privilege_[,...]`
2. Verify that the desired privileges have been removed from the object: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

### Example

The following example removes the privileges “SeTcbPrivilege” and “SeTakeOwnershipPrivilege” from the user “CIFS\_SERVER\sue” on storage virtual machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name    Privileges
-----
vs1        CIFS_SERVER\sue      SeTcbPrivilege
                               SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name    Privileges
-----
vs1        CIFS_SERVER\sue      -
```

### Reset privileges for local or domain users and groups

You can reset privileges for local or domain users and groups. This can be useful when you have made modifications to privileges for a local or domain user or group and those modifications are no longer wanted or needed.

### About this task

Resetting privileges for a local or domain user or group removes any privilege entries for that object.

## Steps

1. Reset the privileges on a local or domain user or group: `vserver cifs users-and-groups privilege reset-privilege -vserver vserver_name -user-or-group-name name`
2. Verify that the privileges are reset on the object: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

## Examples

The following example resets the privileges on the user “CIFS\_SERVER\sue” on storage virtual machine (SVM, formerly known as Vserver) vs1. By default, normal users do not have privileges associated with their accounts:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name      Privileges
-----
vs1       CIFS_SERVER\sue        SeTcbPrivilege
                               SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

The following example resets the privileges for the group “BUILTIN\Administrators”, effectively removing the privilege entry:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name      Privileges
-----
vs1       BUILTIN\Administrators  SeRestorePrivilege
                               SeSecurityPrivilege
                               SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

## Display information about privilege overrides

You can display information about custom privileges assigned to domain or local user accounts or groups. This information helps you determine whether the desired user rights

are applied.

### Step

1. Perform one of the following actions:

If you want to display information about...	Enter this command...
Custom privileges for all domain and local users and groups on the storage virtual machine (SVM)	<code>vserver cifs users-and-groups privilege show -vserver <i>vserver_name</i></code>
Custom privileges for a specific domain or local user and group on the SVM	<code>vserver cifs users-and-groups privilege show -vserver <i>vserver_name</i> -user-or-group-name <i>name</i></code>

There are other optional parameters that you can choose when you run this command. See the man page for more information.

### Example

The following command displays all privileges explicitly associated with local or domain users and groups for SVM vs1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          BUILTIN\Administrators  SeTakeOwnershipPrivilege
              SeRestorePrivilege
vs1          CIFS_SERVER\sue         SeTcbPrivilege
              SeTakeOwnershipPrivilege
```

## Configure bypass traverse checking

### Configure bypass traverse checking overview

Bypass traverse checking is a user right (also known as a *privilege*) that determines whether a user can traverse all the directories in the path to a file even if the user does not have permissions on the traversed directory. You should understand what happens when allowing or disallowing bypass traverse checking, and how to configure bypass traverse checking for users on storage virtual machines (SVMs).

### What happens when allowing or disallowing bypass traverse checking

- If allowed, when a user attempts to access a file, ONTAP does not check the traverse permission for the intermediate directories when determining whether to grant or deny access to the file.
- If disallowed, ONTAP checks the traverse (execute) permission for all directories in the path to the file.

If any of the intermediate directories do not have the "X" (traverse permission), ONTAP denies access to the file.



## Configure bypass traverse checking

You can configure bypass traverse checking by using the ONTAP CLI or by configuring Active Directory group policies with this user right.

The `SeChangeNotifyPrivilege` privilege controls whether users are allowed to bypass traverse checking.

- Adding it to local SMB users or groups on the SVM or to domain users or groups allows bypass traverse checking.
- Removing it from local SMB users or groups on the SVM or from domain users or groups disallows bypass traverse checking.

By default, the following BUILTIN groups on the SVM have the right to bypass traverse checking:

- `BUILTIN\Administrators`
- `BUILTIN\Power Users`
- `BUILTIN\Backup Operators`
- `BUILTIN\Users`
- `Everyone`

If you do not want to allow members of one of these groups to bypass traverse checking, you must remove this privilege from the group.

You must keep the following in mind when configuring bypass traverse checking for local SMB users and groups on the SVM by using the CLI:

- If you want to allow members of a custom local or domain group to bypass traverse checking, you must add the `SeChangeNotifyPrivilege` privilege to that group.
- If you want to allow an individual local or domain user to bypass traverse checking and that user is not a member of a group with that privilege, you can add the `SeChangeNotifyPrivilege` privilege to that user account.
- You can disable bypass traverse checking for local or domain users or groups by removing the `SeChangeNotifyPrivilege` privilege at any time.



To disable bypass travers checking for specified local or domain users or groups, you must also remove the `SeChangeNotifyPrivilege` privilege from the `Everyone` group.

### Related information

[Allow users or groups to bypass directory traverse checking](#)

[Disallow users or groups from bypassing directory traverse checking](#)

[Configure character mapping for SMB file name translation on volumes](#)

[Create SMB share access control lists](#)

[Secure file access by using Storage-Level Access Guard](#)

[List of supported privileges](#)

## [Add privileges to local or domain users or groups](#)

### Allow users or groups to bypass directory traverse checking

If you want a user to be able to traverse all the directories in the path to a file even if the user does not have permissions on a traversed directory, you can add the `SeChangeNotifyPrivilege` privilege to local SMB users or groups on storage virtual machines (SVMs). By default, users are able to bypass directory traverse checking.

#### Before you begin

- A SMB server must exist on the SVM.
- The local users and groups SMB server option must be enabled.
- The local or domain user or group to which the `SeChangeNotifyPrivilege` privilege will be added must already exist.

#### About this task

When adding privileges to a domain user or group, ONTAP might validate the domain user or group by contacting the domain controller. The command might fail if ONTAP cannot contact the domain controller.

#### Steps

1. Enable bypass traverse checking by adding the `SeChangeNotifyPrivilege` privilege to a local or domain user or group: `vserver cifs users-and-groups privilege add-privilege -vserver vserver_name -user-or-group-name name -privileges SeChangeNotifyPrivilege`

The value for the `-user-or-group-name` parameter is a local user or group, or a domain user or group.

2. Verify that the specified user or group has bypass traverse checking enabled: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

#### Example

The following command enables users that belong to the “EXAMPLE\eng” group to bypass directory traverse checking by adding the `SeChangeNotifyPrivilege` privilege to the group:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          EXAMPLE\eng              SeChangeNotifyPrivilege
```

#### Related information

[Disallowing users or groups from bypassing directory traverse checking](#)

### Disallow users or groups from bypassing directory traverse checking

If you do not want a user to traverse all the directories in the path to a file because the user does not have permissions on the traversed directory, you can remove the

SeChangeNotifyPrivilege privilege from local SMB users or groups on storage virtual machines (SVMs).

### Before you begin

The local or domain user or group from which privileges will be removed must already exist.

### About this task

When removing privileges from a domain user or group, ONTAP might validate the domain user or group by contacting the domain controller. The command might fail if ONTAP cannot contact the domain controller.

### Steps

1. Disallow bypass traverse checking: `vserver cifs users-and-groups privilege remove-privilege -vserver vserver_name -user-or-group-name name -privileges SeChangeNotifyPrivilege`

The command removes the SeChangeNotifyPrivilege privilege from the local or domain user or group that you specify with the value for the `-user-or-group-name name` parameter.

2. Verify that the specified user or group has bypass traverse checking disabled: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

### Example

The following command disallows users that belong to the “EXAMPLE\eng” group from bypassing directory traverse checking:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          EXAMPLE\eng              SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          EXAMPLE\eng              -
```

### Related information

[Allowing users or groups to bypass directory traverse checking](#)

### Display information about file security and audit policies

[Display information about file security and audit policies overview](#)

You can display information about file security on files and directories contained within volumes on storage virtual machines (SVMs). You can display information about audit

policies on FlexVol volumes. If configured, you can display information about Storage-Level Access Guard and Dynamic Access Control security settings on FlexVol volumes.

### **Displaying information about file security**

You can display information about file security applied to data contained within volumes and qtrees (for FlexVol volumes) with the following security styles:

- NTFS
- UNIX
- Mixed

### **Displaying information about audit policies**

You can display information about audit policies for auditing access events on FlexVol volumes over the following NAS protocols:

- SMB (all versions)
- NFSv4.x

### **Displaying information about Storage-Level Access Guard (SLAG) security**

Storage-Level Access Guard security can be applied on FlexVol volumes and qtree objects with the following security styles:

- NTFS
- Mixed
- UNIX (if a CIFS server is configured on the SVM that contains the volume)

### **Displaying information about Dynamic Access Control (DAC) security**

Dynamic Access Control security can be applied on an object within a FlexVol volume with the following security styles:

- NTFS
- Mixed (if the object has NTFS effective security)

### **Related information**

[Securing file access by using Storage-Level Access Guard](#)

[Displaying information about Storage-Level Access Guard](#)

### **Display information about file security on NTFS security-style volumes**

You can display information about file and directory security on NTFS security-style volumes, including what the security style and effective security styles are, what permissions are applied, and information about DOS attributes. You can use the results to validate your security configuration or to troubleshoot file access issues.

### **About this task**

You must supply the name of the storage virtual machine (SVM) and the path to the data whose file or folder security information you want to display. You can display the output in summary form or as a detailed list.

- Because NTFS security-style volumes and qtrees use only NTFS file permissions and Windows users and groups when determining file access rights, UNIX-related output fields contain display-only UNIX file permission information.
- ACL output is displayed for file and folders with NTFS security.
- Because Storage-Level Access Guard security can be configured on the volume root or qtree, output for a volume or qtree path where Storage-Level Access Guard is configured might display both regular file ACLs and Storage-Level Access Guard ACLs.
- The output also displays information about Dynamic Access Control ACEs if Dynamic Access Control is configured for the given file or directory path.

### Step

1. Display file and directory security settings with the desired level of detail:

If you want to display information...	Enter the following command...
In summary form	<pre>vserver security file-directory show -vserver vserver_name -path path</pre>
With expanded detail	<pre>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</pre>

### Examples

The following example displays the security information about the path `/vol14` in SVM `vs1`:

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4
```

```
                Vserver: vs1
                File Path: /vol4
File Inode Number: 64
    Security Style: ntfs
    Effective Style: ntfs
    DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
    Unix User Id: 0
    Unix Group Id: 0
    Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
                ACLs: NTFS Security Descriptor
                Control:0x8004
                Owner: BUILTIN\Administrators
                Group: BUILTIN\Administrators
                DACL - ACEs
                ALLOW-Everyone-0x1f01ff
                ALLOW-Everyone-0x10000000-
```

OI|CI|IO

The following example displays the security information with expanded masks about the path /data/engineering in SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
/data/engineering -expand-mask true
```

```
                Vserver: vs1
                File Path: /data/engineering
File Inode Number: 5544
    Security Style: ntfs
    Effective Style: ntfs
    DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
    ...0 .... .... = Offline
    .... ..0. .... = Sparse
    .... .... 0... = Normal
    .... .... ..0. = Archive
    .... .... ...1 = Directory
    .... .... .... .0.. = System
    .... .... .... ..0. = Hidden
    .... .... .... ...0 = Read Only
```

```

    Unix User Id: 0
    Unix Group Id: 0
    Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
    ACLs: NTFS Security Descriptor
    Control:0x8004

```

```

    1... .. = Self Relative
    .0.. .. = RM Control Valid
    ..0. .. = SACL Protected
    ...0 .. = DACL Protected
    .... 0... .. = SACL Inherited
    .... .0.. .. = DACL Inherited
    .... ..0. .. = SACL Inherit Required
    .... ...0 .. = DACL Inherit Required
    .... .... .0. .... = SACL Defaulted
    .... .... ...0 .... = SACL Present
    .... .... .... 0... = DACL Defaulted
    .... .... .... .1.. = DACL Present
    .... .... .... ..0. = Group Defaulted
    .... .... .... ...0 = Owner Defaulted

```

```

Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
DACL - ACEs

```

```

ALLOW-Everyone-0x1f01ff

```

```

0... .. =
Generic Read
.0.. .. =
Generic Write
..0. .. =
Generic Execute
...0 .. =
Generic All
.... .0 .. =
System Security
.... .... 1 .. =
Synchronize
.... .... .... 1... .. =
Write Owner
.... .... .... .1.. .. =
Write DAC
.... .... .... ..1. .... =
Read Control
.... .... .... ...1 .. =
Delete

```

```

.....1..... =
Write Attributes
.....1..... =
Read Attributes
.....1..... =
Delete Child
.....1..... =
Execute
.....1..... =
Write EA
.....1..... =
Read EA
.....1..... =
Append
.....1..... =
Write
.....1..... =
Read
.....1..... =

ALLOW-Everyone-0x10000000-OI|CI|IO
0..... =
Generic Read
.0..... =
Generic Write
..0..... =
Generic Execute
...1..... =
Generic All
.....0..... =
System Security
.....0..... =
Synchronize
.....0..... =
Write Owner
.....0..... =
Write DAC
.....0..... =
Read Control
.....0..... =
Delete
.....0..... =
Write Attributes
.....0..... =
Read Attributes
.....0..... =
Delete Child
.....0..... =

```



```
Execute .....0. .... =
Write EA .....0 ..... =
Read EA ..... 0... =
Append ..... .0.. =
Write ..... ..0. =
Read ..... ..0 =
```

The following example displays security information, including Storage-Level Access Guard security information, for the volume with the path /datavol1 in SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1
```

```

    Vserver: vs1
    File Path: /datavol1
File Inode Number: 77
    Security Style: ntfs
    Effective Style: ntfs
    DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
    Unix User Id: 0
    Unix Group Id: 0
    Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
    ACLs: NTFS Security Descriptor
        Control:0x8004
        Owner: BUILTIN\Administrators
        Group: BUILTIN\Administrators
        DACL - ACEs
            ALLOW-Everyone-0x1f01ff
            ALLOW-Everyone-0x10000000-OI|CI|IO

Storage-Level Access Guard security
SACL (Applies to Directories):
    AUDIT-EXAMPLE\Domain Users-0x120089-FA
    AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Directories):
    ALLOW-EXAMPLE\Domain Users-0x120089
    ALLOW-EXAMPLE\engineering-0x1f01ff
    ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
SACL (Applies to Files):
    AUDIT-EXAMPLE\Domain Users-0x120089-FA
    AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Files):
    ALLOW-EXAMPLE\Domain Users-0x120089
    ALLOW-EXAMPLE\engineering-0x1f01ff
    ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

## Related information

[Displaying information about file security on mixed security-style volumes](#)

[Displaying information about file security on UNIX security-style volumes](#)

## Display information about file security on mixed security-style volumes

You can display information about file and directory security on mixed security-style volumes, including what the security style and effective security styles are, what permissions are applied, and information about UNIX owners and groups. You can use the results to validate your security configuration or to troubleshoot file access issues.

### About this task

You must supply the name of the storage virtual machine (SVM) and the path to the data whose file or folder security information you want to display. You can display the output in summary form or as a detailed list.

- Mixed security-style volumes and qtrees can contain some files and folders that use UNIX file permissions, either mode bits or NFSv4 ACLs, and some files and directories that use NTFS file permissions.
- The top level of a mixed security-style volume can have either UNIX or NTFS effective security.
- ACL output is displayed only for file and folders with NTFS or NFSv4 security.

This field is empty for files and directories using UNIX security that have only mode bit permissions applied (no NFSv4 ACLs).

- The owner and group output fields in the ACL output apply only in the case of NTFS security descriptors.
- Because Storage-Level Access Guard security can be configured on a mixed security-style volume or qtree even if the effective security style of the volume root or qtree is UNIX, output for a volume or qtree path where Storage-Level Access Guard is configured might display both UNIX file permissions and Storage-Level Access Guard ACLs.
- If the path entered in the command is to data with NTFS effective security, the output also displays information about Dynamic Access Control ACEs if Dynamic Access Control is configured for the given file or directory path.

### Step

1. Display file and directory security settings with the desired level of detail:

If you want to display information...	Enter the following command...
In summary form	<pre>vserver security file-directory show -vserver vserver_name -path path</pre>
With expanded detail	<pre>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</pre>

### Examples

The following example displays the security information about the path `/projects` in SVM `vs1` in expanded-mask form. This mixed security-style path has UNIX effective security.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true
```

```
        Vserver: vs1
        File Path: /projects
File Inode Number: 78
        Security Style: mixed
        Effective Style: unix
        DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
    ...0 .... .... .... = Offline
    .... ..0. .... .... = Sparse
    .... .... 0... .... = Normal
    .... .... ..0. .... = Archive
    .... .... ...1 .... = Directory
    .... .... .... .0.. = System
    .... .... .... ..0. = Hidden
    .... .... .... ...0 = Read Only
        Unix User Id: 0
        Unix Group Id: 1
        Unix Mode Bits: 700
Unix Mode Bits in Text: rwx-----
        ACLs: -
```

The following example displays the security information about the path /data in SVM vs1. This mixed security-style path has an NTFS effective security.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data
```

```
          Vserver: vs1
          File Path: /data
    File Inode Number: 544
      Security Style: mixed
    Effective Style: ntfs
      DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
          ACLs: NTFS Security Descriptor
                Control:0x8004
                Owner: BUILTIN\Administrators
                Group: BUILTIN\Administrators
                DACL - ACEs
                    ALLOW-Everyone-0x1f01ff
                    ALLOW-Everyone-0x10000000-
```

OI|CI|IO

The following example displays the security information about the volume at the path /datavol5 in SVM vs1. The top level of this mixed security-style volume has UNIX effective security. The volume has Storage-Level Access Guard security.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /datavol5
```

```
      Vserver: vs1
      File Path: /datavol5
File Inode Number: 3374
      Security Style: mixed
      Effective Style: unix
      DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 755
Unix Mode Bits in Text: rwxr-xr-x
      ACLs: Storage-Level Access Guard security
      SACL (Applies to Directories):
          AUDIT-EXAMPLE\Domain Users-0x120089-FA
          AUDIT-EXAMPLE\engineering-0x1f01ff-SA
          AUDIT-EXAMPLE\market-0x1f01ff-SA
      DACL (Applies to Directories):
          ALLOW-BUILTIN\Administrators-0x1f01ff
          ALLOW-CREATOR OWNER-0x1f01ff
          ALLOW-EXAMPLE\Domain Users-0x120089
          ALLOW-EXAMPLE\engineering-0x1f01ff
          ALLOW-EXAMPLE\market-0x1f01ff
      SACL (Applies to Files):
          AUDIT-EXAMPLE\Domain Users-0x120089-FA
          AUDIT-EXAMPLE\engineering-0x1f01ff-SA
          AUDIT-EXAMPLE\market-0x1f01ff-SA
      DACL (Applies to Files):
          ALLOW-BUILTIN\Administrators-0x1f01ff
          ALLOW-CREATOR OWNER-0x1f01ff
          ALLOW-EXAMPLE\Domain Users-0x120089
          ALLOW-EXAMPLE\engineering-0x1f01ff
          ALLOW-EXAMPLE\market-0x1f01ff
```

### Related information

[Displaying information about file security on NTFS security-style volumes](#)

[Displaying information about file security on UNIX security-style volumes](#)

**Display information about file security on UNIX security-style volumes**

You can display information about file and directory security on UNIX security-style volumes, including what the security styles and effective security styles are, what permissions are applied, and information about UNIX owners and groups. You can use

the results to validate your security configuration or to troubleshoot file access issues.

### About this task

You must supply the name of the storage virtual machine (SVM) and the path to the data whose file or directory security information you want to display. You can display the output in summary form or as a detailed list.

- UNIX security-style volumes and qtrees use only UNIX file permissions, either mode bits or NFSv4 ACLs when determining file access rights.
- ACL output is displayed only for file and folders with NFSv4 security.

This field is empty for files and directories using UNIX security that have only mode bit permissions applied (no NFSv4 ACLs).

- The owner and group output fields in the ACL output does not apply in the case of NFSv4 security descriptors.

They are only meaningful for NTFS security descriptors.

- Because Storage-Level Access Guard security is supported on a UNIX volume or qtree if a CIFS server is configured on the SVM, the output might contain information about Storage-Level Access Guard security applied to the volume or qtree specified in the `-path` parameter.

### Step

1. Display file and directory security settings with the desired level of detail:

If you want to display information...	Enter the following command...
In summary form	<pre>vserver security file-directory show -vserver <i>vserver_name</i> -path <i>path</i></pre>
With expanded detail	<pre>vserver security file-directory show -vserver <i>vserver_name</i> -path <i>path</i> -expand-mask true</pre>

### Examples

The following example displays the security information about the path `/home` in SVM `vs1`:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
```

```
          Vserver: vs1
          File Path: /home
    File Inode Number: 9590
          Security Style: unix
          Effective Style: unix
          DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
          Unix User Id: 0
          Unix Group Id: 1
          Unix Mode Bits: 700
    Unix Mode Bits in Text: rwx-----
          ACLs: -
```

The following example displays the security information about the path /home in SVM vs1 in expanded-mask form:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true
```

```
          Vserver: vs1
          File Path: /home
    File Inode Number: 9590
          Security Style: unix
          Effective Style: unix
          DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
    ...0 .... .... .... = Offline
    .... ..0. .... .... = Sparse
    .... .... 0... .... = Normal
    .... .... ..0. .... = Archive
    .... .... ...1 .... = Directory
    .... .... .... .0.. = System
    .... .... .... ..0. = Hidden
    .... .... .... ...0 = Read Only
          Unix User Id: 0
          Unix Group Id: 1
          Unix Mode Bits: 700
    Unix Mode Bits in Text: rwx-----
          ACLs: -
```



## Related information

[Displaying information about file security on NTFS security-style volumes](#)

[Displaying information about file security on mixed security-style volumes](#)

### Display information about NTFS audit policies on FlexVol volumes using the CLI

You can display information about NTFS audit policies on FlexVol volumes, including what the security styles and effective security styles are, what permissions are applied, and information about system access control lists. You can use the results to validate your security configuration or to troubleshoot auditing issues.

### About this task

You must provide the name of the storage virtual machine (SVM) and the path to the files or folders whose audit information you want to display. You can display the output in summary form or as a detailed list.

- NTFS security-style volumes and qtrees use only NTFS system access control lists (SACLs) for audit policies.
- Files and folders in a mixed security-style volume with NTFS effective security can have NTFS audit policies applied to them.

Mixed security-style volumes and qtrees can contain some files and directories that use UNIX file permissions, either mode bits or NFSv4 ACLs, and some files and directories that use NTFS file permissions.

- The top level of a mixed security-style volume can have either UNIX or NTFS effective security and might or might not contain NTFS SACLs.
- Because Storage-Level Access Guard security can be configured on a mixed security-style volume or qtree even if the effective security style of the volume root or qtree is UNIX, the output for a volume or qtree path where Storage-Level Access Guard is configured might display both regular file and folder NFSv4 SACLs and Storage-Level Access Guard NTFS SACLs.
- If the path that is entered in the command is to data with NTFS effective security, the output also displays information about Dynamic Access Control ACEs if Dynamic Access Control is configured for the given file or directory path.
- When displaying security information about files and folders with NTFS effective security, UNIX-related output fields contain display-only UNIX file permission information.

NTFS security-style files and folders use only NTFS file permissions and Windows users and groups when determining file access rights.

- ACL output is displayed only for files and folders with NTFS or NFSv4 security.

This field is empty for files and folders using UNIX security that have only mode bit permissions applied (no NFSv4 ACLs).

- The owner and group output fields in the ACL output apply only in the case of NTFS security descriptors.

## Step

1. Display file and directory audit policy settings with the desired level of detail:

If you want to display information...	Enter the following command...
In summary form	<code>vserver security file-directory show -vserver vserver_name -path path</code>
As a detailed list	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

## Examples

The following example displays the audit policy information for the path `/corp` in SVM `vs1`. The path has NTFS effective security. The NTFS security descriptor contains both a SUCCESS and a SUCCESS/FAIL SACL entry.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
      Vserver: vs1
      File Path: /corp
      File Inode Number: 357
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
      Control:0x8014
      Owner:DOMAIN\Administrator
      Group:BUILTIN\Administrators
      SACL - ACEs
          ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
          SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
      DACL - ACEs
          ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
          ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
          ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

The following example displays the audit policy information for the path `/datavol1` in SVM `vs1`. The path contains both regular file and folder SACLs and Storage-Level Access Guard SACLs.

```

cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

        Vserver: vs1
        File Path: /datavol1
        File Inode Number: 77
        Security Style: ntfs
        Effective Style: ntfs
        DOS Attributes: 10
        DOS Attributes in Text: ----D---
        Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 777
        Unix Mode Bits in Text: rwxrwxrwx
        ACLs: NTFS Security Descriptor
              Control:0xaa14
              Owner: BUILTIN\Administrators
              Group: BUILTIN\Administrators
              SACL - ACEs
                AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
              DACL - ACEs
                ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

        Storage-Level Access Guard security
        SACL (Applies to Directories):
          AUDIT-EXAMPLE\Domain Users-0x120089-FA
          AUDIT-EXAMPLE\engineering-0x1f01ff-SA
        DACL (Applies to Directories):
          ALLOW-EXAMPLE\Domain Users-0x120089
          ALLOW-EXAMPLE\engineering-0x1f01ff
          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
        SACL (Applies to Files):
          AUDIT-EXAMPLE\Domain Users-0x120089-FA
          AUDIT-EXAMPLE\engineering-0x1f01ff-SA
        DACL (Applies to Files):
          ALLOW-EXAMPLE\Domain Users-0x120089
          ALLOW-EXAMPLE\engineering-0x1f01ff
          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

#### Display information about NFSv4 audit policies on FlexVol volumes using the CLI

You can display information about NFSv4 audit policies on FlexVol volumes using the ONTAP CLI, including what the security styles and effective security styles are, what

permissions are applied, and information about system access control lists (SACLs). You can use the results to validate your security configuration or to troubleshoot auditing issues.

### About this task

You must supply the name of the storage virtual machine (SVM) and the path to the files or directories whose audit information you want to display. You can display the output in summary form or as a detailed list.

- UNIX security-style volumes and qtrees use only NFSv4 SACLs for audit policies.
- Files and directories in a mixed security-style volume that are of UNIX security style can have NFSv4 audit policies applied to them.

Mixed security-style volumes and qtrees can contain some files and directories that use UNIX file permissions, either mode bits or NFSv4 ACLs, and some files and directories that use NTFS file permissions.

- The top level of a mixed security-style volume can have either UNIX or NTFS effective security and might or might not contain NFSv4 SACLs.
- ACL output is displayed only for file and folders with NTFS or NFSv4 security.

This field is empty for files and folders using UNIX security that have only mode bit permissions applied (no NFSv4 ACLs).

- The owner and group output fields in the ACL output apply only in the case of NTFS security descriptors.
- Because Storage-Level Access Guard security can be configured on a mixed security-style volume or qtree even if the effective security style of the volume root or qtree is UNIX, output for a volume or qtree path where Storage-Level Access Guard is configured might display both regular NFSv4 file and directory SACLs and Storage-Level Access Guard NTFS SACLs.
- Because Storage-Level Access Guard security is supported on a UNIX volume or qtree if a CIFS server is configured on the SVM, the output might contain information about Storage-Level Access Guard security applied to the volume or qtree specified in the `-path` parameter.

### Steps

1. Display file and directory security settings with the desired level of detail:

If you want to display information...	Enter the following command...
In summary form	<pre>vserver security file-directory show -vserver vserver_name -path path</pre>
With expanded detail	<pre>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</pre>

### Examples

The following example displays the security information about the path `/lab` in SVM `vs1`. This UNIX security-style path has an NFSv4 SACL.

```

cluster::> vserver security file-directory show -vserver vs1 -path /lab

      Vserver: vs1
      File Path: /lab
File Inode Number: 288
      Security Style: unix
      Effective Style: unix
      DOS Attributes: 11
DOS Attributes in Text: ----D--R
Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 0
Unix Mode Bits in Text: -----
      ACLs: NFSV4 Security Descriptor
      Control:0x8014
      SACL - ACEs
              SUCCESSFUL-S-1-520-0-0xf01ff-SA
              FAILED-S-1-520-0-0xf01ff-FA
      DACL - ACEs
              ALLOW-S-1-520-1-0xf01ff

```

#### Ways to display information about file security and audit policies

You can use the wildcard character (\*) to display information about file security and audit policies of all files and directories under a given path or a root volume.

The wildcard character () can be used as the last subcomponent of a given directory path below which you want to display information of all files and directories. If you want to display information of a particular file or directory named as "", then you need to provide the complete path inside double quotes ("").

#### Example

The following command with the wildcard character displays the information about all files and directories below the path /1/ of SVM vs1:

```

cluster::> vserver security file-directory show -vserver vs1 -path /1/*

      Vserver: vs1
      File Path: /1/1
      Security Style: mixed
      Effective Style: ntfs
      DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8514
            Owner: BUILTIN\Administrators
            Group: BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

      Vserver: vs1
      File Path: /1/1/abc
      Security Style: mixed
      Effective Style: ntfs
      DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8404
            Owner: BUILTIN\Administrators
            Group: BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

```

The following command displays the information of a file named as "\*" under the path /vol1/a of SVM vs1. The path is enclosed within double quotes (" ").

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/voll/a/*"
```

```
        Vserver: vs1
        File Path: "/voll/a/*"
        Security Style: mixed
        Effective Style: unix
        DOS Attributes: 10
        DOS Attributes in Text: ----D---
        Expanded Dos Attributes: -
            Unix User Id: 1002
            Unix Group Id: 65533
            Unix Mode Bits: 755
        Unix Mode Bits in Text: rwxr-xr-x
            ACLs: NFSV4 Security Descriptor
                Control:0x8014
                SACL - ACEs
                    AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                DACL - ACEs
                    ALLOW-EVERYONE@-0x1f00a9-FI|DI
                    ALLOW-OWNER@-0x1f01ff-FI|DI
                    ALLOW-GROUP@-0x1200a9-IG
```

## Manage NTFS file security, NTFS audit policies, and Storage-Level Access Guard on SVMs using the CLI

### Manage NTFS file security, NTFS audit policies, and Storage-Level Access Guard on SVMs using the CLI overview

You can manage NTFS file security, NTFS audit policies, and Storage-Level Access Guard on storage virtual machines (SVMs) by using the CLI.

You can manage NTFS file security and audit policies from SMB clients or by using the CLI. However, using the CLI to configure file security and audit policies removes the need to use a remote client to manage file security. Using the CLI can significantly reduce the time it takes to apply security on many files and folders using a single command.

You can configure Storage-Level Access Guard, which is another layer of security applied by ONTAP to SVM volumes. Storage-Level Access Guard applies to accesses from all NAS protocols to the storage object to which Storage-Level Access Guard is applied.

Storage-Level Access Guard can be configured and managed only from the ONTAP CLI. You cannot manage Storage-Level Access Guard settings from SMB clients. Moreover, if you view the security settings on a file or directory from an NFS or SMB client, you will not see the Storage-Level Access Guard security. Storage-Level Access Guard security cannot be revoked from a client, even by a system (Windows or UNIX) administrator. Therefore, Storage-Level Access Guard provides an extra layer of security for data access that is independently set and managed by the storage administrator.



Even though only NTFS access permissions are supported for Storage-Level Access Guard, ONTAP can perform security checks for access over NFS to data on volumes where Storage-Level Access Guard is applied if the UNIX user maps to a Windows user on the SVM that owns the volume.

## NTFS security-style volumes

All files and folders contained within NTFS security-style volumes and qtrees have NTFS effective security. You can use the `vserver security file-directory` command family to implement the following types of security on NTFS security-style volumes:

- File permissions and audit policies to files and folders contained in the volume
- Storage-Level Access Guard security on volumes

## Mixed security-style volumes

Mixed security-style volumes and qtrees can contain some files and folders that have UNIX effective security and use UNIX file permissions, either mode bits or NFSv4.x ACLs and NFSv4.x audit policies, and some files and folders that have NTFS effective security and use NTFS file permissions and audit policies. You can use the `vserver security file-directory` command family to apply the following types of security to mixed security-style data:

- File permissions and audit policies to files and folders with NTFS effective security-style in the mixed volume or qtree
- Storage-Level Access Guard to volumes with either NTFS and UNIX effective security-style

## UNIX security-style volumes

UNIX security-style volumes and qtrees contain files and folders that have UNIX effective security (either mode bits or NFSv4.x ACLs). You must keep the following in mind if you want to use the `vserver security file-directory` command family to implement security on UNIX security-style volumes:

- The `vserver security file-directory` command family cannot be used to manage UNIX file security and audit policies on UNIX security-style volumes and qtrees.
- You can use the `vserver security file-directory` command family to configure Storage-Level Access Guard on UNIX security-style volumes, provided the SVM with the target volume contains a CIFS server.

## Related information

[Display information about file security and audit policies](#)

[Configure and apply file security on NTFS files and folders using the CLI](#)

[Configure and apply audit policies to NTFS files and folders using the CLI](#)

[Secure file access by using Storage-Level Access Guard](#)

## Use cases for using the CLI to set file and folder security

Because you can apply and manage file and folder security locally without involvement from a remote client, you can significantly reduce the time it takes to set bulk security on a large number of files or folders.



You can benefit from using the CLI to set file and folder security in the following use cases:

- Storage of files in large enterprise environments, such as file storage in home directories
- Migration of data
- Change of Windows domain
- Standardization of file security and audit policies across NTFS file systems

#### Limits when using the CLI to set file and folder security

You need to be aware of certain limits when using the CLI to set file and folder security.

- The `vserver security file-directory` command family does not support setting NFSv4 ACLs.

You can only apply NTFS security descriptors to NTFS files and folders.

#### How security descriptors are used to apply file and folder security

Security descriptors contain the access control lists that determine what actions a user can perform on files and folders, and what is audited when a user accesses files and folders.

- **Permissions**

Permissions are allowed or denied by an object's owner and determine what actions an object (users, groups, or computer objects) can perform on specified files or folders.

- **Security descriptors**

Security descriptors are data structures that contain security information that define permissions associated with a file or folder.

- **Access control lists (ACLs)**

Access control lists are the lists contained within a security descriptor that contain information on what actions users, groups, or computer objects can perform on the file or folder to which the security descriptor is applied. The security descriptor can contain the following two types of ACLs:

- Discretionary access control lists (DACLS)
- System access control lists (SACLs)

- **Discretionary access control lists (DACLS)**

DACLS contain the list of SIDS for the users, groups, and computer objects who are allowed or denied access to perform actions on files or folders. DACLS contain zero or more access control entries (ACEs).

- **System access control lists (SACLs)**

SACLs contain the list of SIDS for the users, groups, and computer objects for which successful or failed auditing events are logged. SACLs contain zero or more access control entries (ACEs).

- **Access Control Entries (ACEs)**

ACEs are individual entries in either DACLS or SACLs:

- A DACL access control entry specifies the access rights that are allowed or denied for particular users, groups, or computer objects.
- A SACL access control entry specifies the success or failure events to log when auditing specified actions performed by particular users, groups, or computer objects.

- **Permission inheritance**

Permission inheritance describes how permissions defined in security descriptors are propagated to an object from a parent object. Only inheritable permissions are inherited by child objects. When setting permissions on the parent object, you can decide whether folders, sub-folders, and files can inherit them with “Apply to `this-folder`, `sub-folders`, and `files`”.

## **Related information**

[Configure and apply file security on NTFS files and folders using the CLI](#)

[SMB and NFS auditing and security tracing](#)

[Configuring and applying audit policies to NTFS files and folders using the CLI](#)

### **Guidelines for applying file-directory policies that use local users or groups on the SVM disaster recovery destination**

There are certain guidelines that you must keep in mind before applying file-directory policies on the storage virtual machine (SVM) disaster recovery destination in an ID discard configuration if your file-directory policy configuration uses local users or groups in either the security descriptor or the DACL or SACL entries.

You can configure a disaster recovery configuration for an SVM where the source SVM on the source cluster replicates the data and configuration from the source SVM to a destination SVM on a destination cluster.

You can set up one of two types of SVM disaster recovery:

- Identity preserved

With this configuration, the identity of the SVM and the CIFS server is preserved.

- Identity discarded

With this configuration, the identity of the SVM and the CIFS server is not preserved. In this scenario, the name of the SVM and the CIFS server on the destination SVM is different from the SVM and the CIFS server name on the source SVM.

### **Guidelines for identity discarded configurations**

In an identity discarded configuration, for an SVM source that contains local user, group, and privilege configurations, the name of the local domain (local CIFS server name) must be changed to match the CIFS server name on the SVM destination. For example, if the source SVM name is “vs1” and CIFS server name is “CIFS1”, and the destination SVM name is “vs1\_dst” and the CIFS server name is “CIFS1\_DST”, then the local domain name for a local user named “CIFS1\user1” is automatically changed to “CIFS1\_DST\user1” on the destination SVM:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst
```

Vserver	User Name	Full Name	Description
vs1	CIFS1\Administrator		Built-in administrator account
vs1	CIFS1\user1	-	-

```
cluster1dst::> vserver cifs users-and-groups local-user show -vserver vs1_dst
```

Vserver	User Name	Full Name	Description
vs1_dst	CIFS1_DST\Administrator		Built-in administrator account
vs1_dst	CIFS1_DST\user1	-	-

Even though local user and group names are automatically changed in the local user and group databases, local users or group names are not automatically changed in file-directory policy configurations (policies configured on the CLI using the `vserver security file-directory` command family).

For example, for “vs1”, if you have configured a DACL entry where the `-account` parameter is set to “CIFS1\user1”, the setting is not automatically changed on the destination SVM to reflect the destination’s CIFS server name.

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1
```

```
Vserver: vs1
```

```
NTFS Security Descriptor Name: sd1
```

Account Name	Access Type	Access Rights	Apply To
CIFS1\user1	allow	full-control	this-folder

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1_dst
```

```
Vserver: vs1_dst
```

```
NTFS Security Descriptor Name: sd1
```

Account Name	Access Type	Access Rights	Apply To
**CIFS1**\user1		allow full-control	this-folder

You must use the `vserver security file-directory modify` commands to manually change the CIFS server name to the destination CIFS server name.

### **File-directory policy configuration components that contain account parameters**

There are three file-directory policy configuration components that can use parameter settings that can contain local users or groups:

- Security descriptor

You can optionally specify the owner of the security descriptor and the primary group of the owner of the security descriptor. If the security descriptor uses a local user or group for the owner and primary group entries, you must modify the security descriptor to use the destination SVM in the account name. You can use the `vserver security file-directory ntfs modify` command to make any necessary changes to the account names.

- DACL entries

Each DACL entry must be associated with an account. You must modify any DACLs that use local user or group accounts to use the destination SVM name. Because you cannot modify the account name for existing DACL entries, you must remove any DACL entries with local users or groups from the security descriptors, create new DACL entries with the corrected destination account names, and associate these new DACL entries with the appropriate security descriptors.

- SACL entries

Each SACL entry must be associated with an account. You must modify any SACLs that use local user or group accounts to use the destination SVM name. Because you cannot modify the account name for existing SACL entries, you must remove any SACL entries with local users or groups from the security descriptors, create new SACL entries with the corrected destination account names, and associate these new SACL entries with the appropriate security descriptors.

You must make any necessary changes to local users or groups used in the file-directory policy configuration before applying the policy; otherwise, the apply job fails.

### **Configure and apply file security on NTFS files and folders using the CLI**

#### **Create an NTFS security descriptor**

Creating an NTFS security descriptor (file security policy) is the first step in configuring and applying NTFS access control lists (ACLs) to files and folders residing within storage virtual machines (SVMs). You can associate the security descriptor to the file or folder path in a policy task.

#### **About this task**

You can create NTFS security descriptors for files and folders residing within NTFS security-style volumes, or for files and folders residing on mixed security-style volumes.

By default, when a security descriptor is created, four discretionary access control list (DACL) access control entries (ACEs) are added to that security descriptor. The four default ACEs are as follows:

Object	Access type	Access rights	Where to apply the permissions
BUILTIN\Administrators	Allow	Full Control	this-folder, sub-folders, files
BUILTIN\Users	Allow	Full Control	this-folder, sub-folders, files
CREATOR OWNER	Allow	Full Control	this-folder, sub-folders, files
NT AUTHORITY\SYSTEM	Allow	Full Control	this-folder, sub-folders, files

You can customize the security descriptor configuration by using the following optional parameters:

- Owner of the security descriptor
- Primary group of the owner
- Raw control flags

The value for any optional parameter is ignored for Storage-Level Access Guard. See the man pages for more information.

### Add NTFS DACL access control entries to the NTFS security descriptor

Adding DACL (discretionary access control list) access control entries (ACEs) to the NTFS security descriptor is the second step in configuring and applying NTFS ACLs to a file or folder. Each entry identifies which object is allowed or denied access, and defines what the object can or cannot do to the files or folders defined in the ACE.

#### About this task

You can add one or more ACEs to the security descriptor's DACL.

If the security descriptor contains a DACL that has existing ACEs, the command adds the new ACE to the DACL. If the security descriptor does not contain a DACL, the command creates the DACL and adds the new ACE to it.

You can optionally customize DACL entries by specifying what rights you want to allow or deny for the account specified in the `-account` parameter. There are three mutually exclusive methods for specifying rights:

- Rights
- Advanced rights
- Raw rights (advanced-privilege)



If you do not specify rights for the DACL entry, the default is to set the rights to `Full Control`.

You can optionally customize DACL entries by specifying how to apply inheritance.

The value for any optional parameter is ignored for Storage-Level Access Guard. See the man pages for more information.

### Steps

1. Add a DACL entry to a security descriptor: `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SIDoptional_parameters`

```
vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny
-account domain\joe -rights full-control -apply-to this-folder -vserver vs1
```

2. Verify that the DACL entry is correct: `vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

```
vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
-access-type deny -account domain\joe
```

```
Vserver: vs1
Security Descriptor Name: sd1
    Allow or Deny: deny
    Account Name or SID: DOMAIN\joe
    Access Rights: full-control
Advanced Access Rights: -
    Apply To: this-folder
    Access Rights: full-control
```

### Create security policies

Creating a file security policy for SVMs is the third step in configuring and applying ACLs to a file or folder. A policy acts as a container for various tasks, where each task is a single entry that can be applied to files or folders. You can add tasks to the security policy later.

#### About this task

The tasks that you add to a security policy contain associations between the NTFS security descriptor and the file or folder paths. Therefore, you should associate the security policy with each SVM (containing NTFS security-style volumes or mixed security-style volumes).

### Steps

1. Create a security policy: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory policy create -policy-name policy1 -vserver
vs1
```

2. Verify the security policy: `vserver security file-directory policy show`

```

vserver security file-directory policy show
  Vserver          Policy Name
  -----          -
      vs1          policy1

```

### Add a task to the security policy

Creating and adding a policy task to a security policy is the fourth step in configuring and applying ACLs to files or folders in SVMs. When you create the policy task, you associate the task with a security policy. You can add one or more task entries to a security policy.

#### About this task

The security policy is a container for a task. A task refers to a single operation that can be done by a security policy to files or folders with NTFS or mixed security (or to a volume object if configuring Storage-Level Access Guard).

There are two types of tasks:

- File and directory tasks

Used to specify tasks that apply security descriptors to specified files and folders. ACLs applied through file and directory tasks can be managed with SMB clients or the ONTAP CLI.

- Storage-Level Access Guard tasks

Used to specify tasks that apply Storage-Level Access Guard security descriptors to a specified volume. ACLs applied through Storage-Level Access Guard tasks can be managed only through the ONTAP CLI.

A task contains definitions for the security configuration of a file (or folder) or set of files (or folders). Every task in a policy is uniquely identified by the path. There can be only one task per path within a single policy. A policy cannot have duplicate task entries.

Guidelines for adding a task to a policy:

- There can be a maximum of 10,000 tasks entries per policy.
- A policy can contain one or more tasks.

Even though a policy can contain more than one task, you cannot configure a policy to contain both file-directory and Storage-Level Access Guard tasks. A policy must contain either all Storage-Level Access Guard tasks or all file-directory tasks.

- Storage-Level Access Guard is used to restrict permissions.

It will never give extra access permissions.

When adding tasks to security policies, you must specify the following four required parameters:

- SVM name
- Policy name

- Path
- Security descriptor to associate with the path

You can customize the security descriptor configuration by using the following optional parameters:

- Security type
- Propagation mode
- Index position
- Access control type

The value for any optional parameter is ignored for Storage-Level Access Guard. See the man pages for more information.

### Steps

1. Add a task with an associated security descriptor to the security policy: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

`file-directory` is the default value for the `-access-control` parameter. Specifying the access control type when configuring file and directory access tasks is optional.

```
vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
```

2. Verify the policy task configuration: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

```
vserver security file-directory policy task show
```

```
Vserver: vs1
Policy: policy1

Index      File/Folder      Access          Security        NTFS           NTFS
Security
          Path           Control        Type           Mode
Descriptor Name
-----
-----
1          /home/dir1      file-directory  ntfs           propagate      sd2
```

### Apply security policies

Applying a file security policy to SVMs is the last step in creating and applying NTFS ACLs to files or folders.

### About this task



You can apply security settings defined in the security policy to NTFS files and folders residing within FlexVol volumes (NTFS or mixed security style).

### Step

1. Apply a security policy: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

The policy apply job is scheduled and the Job ID is returned.

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id 53322" command to view the status of the operation
```

### Monitor the security policy job

When applying the security policy to storage virtual machines (SVMs), you can monitor the progress of the task by monitoring the security policy job. This is helpful if you want to ascertain that the application of the security policy succeeded. This is also helpful if you have a long-running job where you are applying bulk security to a large number of files and folders.

#### About this task

To display detailed information about a security policy job, you should use the `-instance` parameter.

### Step

1. Monitor the security policy job: `vserver security file-directory job show -vserver vserver_name`

```
vserver security file-directory job show -vserver vs1
```

```
Job ID Name                Vserver  Node      State
-----
53322  Fsecurity Apply          vs1      node1     Success
      Description: File Directory Security Apply Job
```

### Verify the applied file security

You can verify the file security settings to confirm that the files or folders on the storage virtual machine (SVM) to which you applied the security policy have the desired settings.

#### About this task

You must supply the name of the SVM that contains the data and the path to the file and folders on which you want to verify security settings. You can use the optional `-expand-mask` parameter to display detailed information about the security settings.

## Step

1. Display file and folder security settings: `vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]`

```
vserver security file-directory show -vserver vs1 -path /data/engineering
-expand-mask true
```

```
Vserver: vs1
      File Path: /data/engineering
File Inode Number: 5544
      Security Style: ntfs
Effective Style: ntfs
      DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
...0 .... = Offline
.... ..0. .... = Sparse
.... .... 0... .... = Normal
.... .... ..0. .... = Archive
.... .... ...1 .... = Directory
.... .... .... .0.. = System
.... .... .... ..0. = Hidden
.... .... .... ...0 = Read Only
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
Control:0x8004

1... .... = Self Relative
.0.. .... = RM Control Valid
..0. .... = SACL Protected
...0 .... = DACL Protected
.... 0... = SACL Inherited
.... .0.. = DACL Inherited
.... ..0. = SACL Inherit Required
.... ...0 = DACL Inherit Required
.... .... ..0. = SACL Defaulted
.... .... ...0 = SACL Present
.... .... .... 0... = DACL Defaulted
.... .... .... .1.. = DACL Present
.... .... .... ..0. = Group Defaulted
.... .... .... ...0 = Owner Defaulted

Owner: BUILTIN\Administrators
```

Group: BUILTIN\Administrators

DACL - ACEs

ALLOW-Everyone-0x1f01ff

	0...	.....	.....	.....	.....	.....	.....	.....	.....	=
Generic Read										
	.0..	.....	.....	.....	.....	.....	.....	.....	.....	=
Generic Write										
	..0.	.....	.....	.....	.....	.....	.....	.....	.....	=
Generic Execute										
	...0	.....	.....	.....	.....	.....	.....	.....	.....	=
Generic All										
	.....	...0	.....	.....	.....	.....	.....	.....	.....	=
System Security										
	.....	.....	...1	.....	.....	.....	.....	.....	.....	=
Synchronize										
	.....	.....	.....	1...	.....	.....	.....	.....	.....	=
Write Owner										
	.....	.....	.....	.1..	.....	.....	.....	.....	.....	=
Write DAC										
	.....	.....	.....	..1.	.....	.....	.....	.....	.....	=
Read Control										
	.....	.....	.....	...1	.....	.....	.....	.....	.....	=
Delete										
	.....	.....	.....	.....	.....	...1	.....	.....	.....	=
Write Attributes										
	.....	.....	.....	.....	.....	.....	1...	.....	.....	=
Read Attributes										
	.....	.....	.....	.....	.....	.....	..1..	.....	.....	=
Delete Child										
	.....	.....	.....	.....	.....	.....	..1.	.....	.....	=
Execute										
	.....	.....	.....	.....	.....	.....	...1	.....	.....	=
Write EA										
	.....	.....	.....	.....	.....	.....	.....	1...	.....	=
Read EA										
	.....	.....	.....	.....	.....	.....	.....	..1..	.....	=
Append										
	.....	.....	.....	.....	.....	.....	.....	..1.	.....	=
Write										
	.....	.....	.....	.....	.....	.....	.....	...1	.....	=
Read										

ALLOW-Everyone-0x10000000-OI|CI|IO

	0...	.....	.....	.....	.....	.....	.....	.....	.....	=
Generic Read										
	.0..	.....	.....	.....	.....	.....	.....	.....	.....	=

```

Generic Write           ..0.  ....  .....  .....  .....  .....  .....  .....  .....  =
Generic Execute        ...1  ....  .....  .....  .....  .....  .....  .....  .....  =
Generic All            .....  ...0  ....  .....  .....  .....  .....  .....  .....  =
System Security        .....  .....  ...0  .....  .....  .....  .....  .....  .....  =
Synchronize            .....  .....  .....  0...  .....  .....  .....  .....  .....  =
Write Owner            .....  .....  .....  .0...  .....  .....  .....  .....  .....  =
Write DAC              .....  .....  .....  ..0...  .....  .....  .....  .....  .....  =
Read Control           .....  .....  .....  ...0...  .....  .....  .....  .....  .....  =
Delete                 .....  .....  .....  .....  .....  .....  .....  ...0...  .....  =
Write Attributes       .....  .....  .....  .....  .....  .....  .....  0...  .....  =
Read Attributes        .....  .....  .....  .....  .....  .....  .....  .0...  .....  =
Delete Child           .....  .....  .....  .....  .....  .....  .....  ..0...  .....  =
Execute                .....  .....  .....  .....  .....  .....  .....  ...0...  .....  =
Write EA               .....  .....  .....  .....  .....  .....  .....  .....  0...  .....  =
Read EA                .....  .....  .....  .....  .....  .....  .....  .....  .0...  .....  =
Append                 .....  .....  .....  .....  .....  .....  .....  .....  ..0...  .....  =
Write                  .....  .....  .....  .....  .....  .....  .....  .....  ...0...  .....  =
Read                   .....  .....  .....  .....  .....  .....  .....  .....  ...0...  .....  =

```

**Configure and apply audit policies to NTFS files and folders using the CLI overview**

There are several steps you must perform to apply audit policies to NTFS files and folders when using the ONTAP CLI. First, you create an NTFS security descriptor and add SACLs to the security descriptor. Next you create a security policy and add policy tasks. You then apply the security policy to a storage virtual machine (SVM).

**About this task**

After applying the security policy, you can monitor the security policy job and then verify the settings for the applied audit policy.



When an audit policy and associated SACLs are applied, any existing DACLs are overwritten. You should review existing security policies before creating and applying new ones.

### Related information

[Securing file access by using Storage-Level Access Guard](#)

[Limits when using the CLI to set file and folder security](#)

[How security descriptors are used to apply file and folder security](#)

[SMB and NFS auditing and security tracing](#)

[Configure and apply file security on NTFS files and folders using the CLI](#)

### Create an NTFS security descriptor

Creating an NTFS security descriptor audit policy is the first step in configuring and applying NTFS access control lists (ACLs) to files and folders residing within SVMs. You will associate the security descriptor to the file or folder path in a policy task.

#### About this task

You can create NTFS security descriptors for files and folders residing within NTFS security-style volumes, or for files and folders residing on mixed security-style volumes.

By default, when a security descriptor is created, four discretionary access control list (DACL) access control entries (ACEs) are added to that security descriptor. The four default ACEs are as follows:

Object	Access type	Access rights	Where to apply the permissions
BUILTIN\Administrators	Allow	Full Control	this-folder, sub-folders, files
BUILTIN\Users	Allow	Full Control	this-folder, sub-folders, files
CREATOR OWNER	Allow	Full Control	this-folder, sub-folders, files
NT AUTHORITY\SYSTEM	Allow	Full Control	this-folder, sub-folders, files

You can customize the security descriptor configuration by using the following optional parameters:

- Owner of the security descriptor
- Primary group of the owner
- Raw control flags

The value for any optional parameter is ignored for Storage-Level Access Guard. See the man pages for more information.

## Steps

1. If you want to use the advanced parameters, set the privilege level to advanced: `set -privilege advanced`
2. Create a security descriptor: `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_name optional_parameters`  
  
`vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe`
3. Verify that the security descriptor configuration is correct: `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

```
vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
```

```
          Vserver: vs1
          Security Descriptor Name: sd1
          Owner of the Security Descriptor: DOMAIN\joe
```

4. If you are in the advanced privilege level, return to the admin privilege level: `set -privilege admin`

## Add NTFS SACL access control entries to the NTFS security descriptor

Adding SACL (system access control list) access control entries (ACEs) to the NTFS security descriptor is the second step in creating NTFS audit policies for files or folders in SVMs. Each entry identifies the user or group that you want to audit. The SACL entry defines whether you want to audit successful or failed access attempts.

### About this task

You can add one or more ACEs to the security descriptor's SACL.

If the security descriptor contains a SACL that has existing ACEs, the command adds the new ACE to the SACL. If the security descriptor does not contain a SACL, the command creates the SACL and adds the new ACE to it.

You can configure SACL entries by specifying what rights you want to audit for success or failure events for the account specified in the `-account` parameter. There are three mutually exclusive methods for specifying rights:

- Rights
- Advanced rights
- Raw rights (advanced-privilege)



If you do not specify rights for the SACL entry, the default setting is `Full Control`.

You can optionally customize SACL entries by specifying how to apply inheritance with the `apply to` parameter. If you do not specify this parameter, the default is to apply this SACL entry to this folder, subfolders,

and files.

### Steps

1. Add a SACL entry to a security descriptor: `vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDoptional_parameters`

```
vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type failure -account domain\joe -rights full-control -apply-to this-folder -vserver vs1
```

2. Verify that the SACL entry is correct: `vserver security file-directory ntfs sacl show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

```
vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1 -access-type deny -account domain\joe
```

```
Vserver: vs1
Security Descriptor Name: sd1
Access type for Specified Access Rights: failure
Account Name or SID: DOMAIN\joe
Access Rights: full-control
Advanced Access Rights: -
Apply To: this-folder
Access Rights: full-control
```

### Create security policies

Creating an audit policy for storage virtual machines (SVMs) is the third step in configuring and applying ACLs to a file or folder. A policy acts as a container for various tasks, where each task is a single entry that can be applied to files or folders. You can add tasks to the security policy later.

#### About this task

The tasks that you add to a security policy contain associations between the NTFS security descriptor and the file or folder paths. Therefore, you should associate the security policy with each storage virtual machine (SVM) (containing NTFS security-style volumes or mixed security-style volumes).

### Steps

1. Create a security policy: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory policy create -policy-name policy1 -vserver vs1
```

2. Verify the security policy: `vserver security file-directory policy show`

```

vserver security file-directory policy show
  Vserver          Policy Name
  -----          -
      vs1          policy1

```

### Add a task to the security policy

Creating and adding a policy task to a security policy is the fourth step in configuring and applying ACLs to files or folders in SVMs. When you create the policy task, you associate the task with a security policy. You can add one or more task entries to a security policy.

#### About this task

The security policy is a container for a task. A task refers to a single operation that can be done by a security policy to files or folders with NTFS or mixed security (or to a volume object if configuring Storage-Level Access Guard).

There are two types of tasks:

- File and directory tasks

Used to specify tasks that apply security descriptors to specified files and folders. ACLs applied through file and directory tasks can be managed with SMB clients or the ONTAP CLI.

- Storage-Level Access Guard tasks

Used to specify tasks that apply Storage-Level Access Guard security descriptors to a specified volume. ACLs applied through Storage-Level Access Guard tasks can be managed only through the ONTAP CLI.

A task contains definitions for the security configuration of a file (or folder) or set of files (or folders). Every task in a policy is uniquely identified by the path. There can be only one task per path within a single policy. A policy cannot have duplicate task entries.

Guidelines for adding a task to a policy:

- There can be a maximum of 10,000 tasks entries per policy.
- A policy can contain one or more tasks.

Even though a policy can contain more than one task, you cannot configure a policy to contain both file-directory and Storage-Level Access Guard tasks. A policy must contain either all Storage-Level Access Guard tasks or all file-directory tasks.

- Storage-Level Access Guard is used to restrict permissions.

It will never give extra access permissions.

You can customize the security descriptor configuration by using the following optional parameters:

- Security type
- Propagation mode



- Index position
- Access control type

The value for any optional parameter is ignored for Storage-Level Access Guard. See the man pages for more information.

### Steps

1. Add a task with an associated security descriptor to the security policy: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

`file-directory` is the default value for the `-access-control` parameter. Specifying the access control type when configuring file and directory access tasks is optional.

```
vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
```

2. Verify the policy task configuration: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

```
vserver security file-directory policy task show
```

```
Vserver: vs1
Policy: policy1

Index      File/Folder      Access      Security      NTFS      NTFS
Security
          Path          Control      Type          Mode
Descriptor Name
-----  -
-----
1         /home/dir1      file-directory  ntfs          propagate  sd2
```

### Apply security policies

Applying an audit policy to SVMs is the last step in creating and applying NTFS ACLs to files or folders.

#### About this task

You can apply security settings defined in the security policy to NTFS files and folders residing within FlexVol volumes (NTFS or mixed security style).

#### Step

1. Apply a security policy: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

The policy apply job is scheduled and the Job ID is returned.

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id 53322" command to view the status of the operation
```

### Monitor the security policy job

When applying the security policy to storage virtual machines (SVMs), you can monitor the progress of the task by monitoring the security policy job. This is helpful if you want to ascertain that the application of the security policy succeeded. This is also helpful if you have a long-running job where you are applying bulk security to a large number of files and folders.

#### About this task

To display detailed information about a security policy job, you should use the `-instance` parameter.

#### Step

1. Monitor the security policy job: `vserver security file-directory job show -vserver vserver_name`

```
vserver security file-directory job show -vserver vs1
```

Job ID	Name	Vserver	Node	State
53322	Fsecurity Apply	vs1	node1	Success
Description: File Directory Security Apply Job				

### Verify the applied audit policy

You can verify the audit policy to confirm that the files or folders on the storage virtual machine (SVM) to which you applied the security policy have the desired audit security settings.

#### About this task

You use the `vserver security file-directory show` command to display audit policy information. You must supply the name of the SVM that contains the data and the path to the data whose file or folder audit policy information you want to display.

#### Step

1. Display audit policy settings: `vserver security file-directory show -vserver vserver_name -path path`

#### Example

The following command displays the audit policy information applied to the path `/corp` in SVM `vs1`. The path has both a SUCCESS and a SUCCESS/FAIL SACL entry applied to it:

```

cluster::> vserver security file-directory show -vserver vs1 -path /corp

        Vserver: vs1
        File Path: /corp
        Security Style: ntfs
        Effective Style: ntfs
        DOS Attributes: 10
        DOS Attributes in Text: ----D---
        Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 777
        Unix Mode Bits in Text: rwxrwxrwx
        ACLs: NTFS Security Descriptor
              Control:0x8014
              Owner:DOMAIN\Administrator
              Group:BUILTIN\Administrators
              SACL - ACEs
                ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
              DACL - ACEs
                ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI

```

### Considerations when managing security policy jobs

If a security policy job exists, under certain circumstances, you cannot modify that security policy or the tasks assigned to that policy. You should understand under what conditions you can or cannot modify security policies so that any attempts that you make to modify the policy are successful. Modifications to the policy include adding, removing, or modifying tasks assigned to the policy and deleting or modifying the policy.

You cannot modify a security policy or a task assigned to that policy if a job exists for that policy and that job is in the following states:

- The job is running or in progress.
- The job is paused.
- The job is resumed and is in the running state.
- If the job is waiting to failover to another node.

Under the following circumstances, if a job exists for a security policy, you can successfully modify that security policy or a task assigned to that policy:

- The policy job is stopped.

- The policy job has successfully finished.

#### Commands for managing NTFS security descriptors

There are specific ONTAP commands for managing security descriptors. You can create, modify, delete, and display information about security descriptors.

If you want to...	Use this command...
Create NTFS security descriptors	<code>vserver security file-directory ntfs create</code>
Modify existing NTFS security descriptors	<code>vserver security file-directory ntfs modify</code>
Display information about existing NTFS security descriptors	<code>vserver security file-directory ntfs show</code>
Delete NTFS security descriptors	<code>vserver security file-directory ntfs delete</code>

See the man pages for the `vserver security file-directory ntfs` commands for more information.

#### Commands for managing NTFS DACL access control entries

There are specific ONTAP commands for managing DACL access control entries (ACEs). You can add ACEs to NTFS DACLs at any time. You can also manage existing NTFS DACLs by modifying, deleting, and displaying information about ACEs in DACLs.

If you want to...	Use this command...
Create ACEs and add them to NTFS DACLs	<code>vserver security file-directory ntfs dacl add</code>
Modify existing ACEs in NTFS DACLs	<code>vserver security file-directory ntfs dacl modify</code>
Display information about existing ACEs in NTFS DACLs	<code>vserver security file-directory ntfs dacl show</code>
Remove existing ACEs from NTFS DACLs	<code>vserver security file-directory ntfs dacl remove</code>

See the man pages for the `vserver security file-directory ntfs dacl` commands for more information.

### Commands for managing NTFS SACL access control entries

There are specific ONTAP commands for managing SACL access control entries (ACEs). You can add ACEs to NTFS SACLs at any time. You can also manage existing NTFS SACLs by modifying, deleting, and displaying information about ACEs in SACLs.

If you want to...	Use this command...
Create ACEs and add them to NTFS SACLs	<code>vserver security file-directory ntfs sacl add</code>
Modify existing ACEs in NTFS SACLs	<code>vserver security file-directory ntfs sacl modify</code>
Display information about existing ACEs in NTFS SACLs	<code>vserver security file-directory ntfs sacl show</code>
Remove existing ACEs from NTFS SACLs	<code>vserver security file-directory ntfs sacl remove</code>

See the man pages for the `vserver security file-directory ntfs sacl` commands for more information.

### Commands for managing security policies

There are specific ONTAP commands for managing security policies. You can display information about policies and you can delete policies. You cannot modify a security policy.

If you want to...	Use this command...
Create security policies	<code>vserver security file-directory policy create</code>
Display information about security policies	<code>vserver security file-directory policy show</code>
Delete security policies	<code>vserver security file-directory policy delete</code>

See the man pages for the `vserver security file-directory policy` commands for more information.

### Commands for managing security policy tasks

There are ONTAP commands for adding, modifying, removing, and displaying information about security policy tasks.

If you want to...	Use this command...
Add security policy tasks	<code>vserver security file-directory policy task add</code>
Modify security policy tasks	<code>vserver security file-directory policy task modify</code>
Display information about security policy tasks	<code>vserver security file-directory policy task show</code>
Remove security policy tasks	<code>vserver security file-directory policy task remove</code>

See the man pages for the `vserver security file-directory policy task` commands for more information.

#### Commands for managing security policy jobs

There are ONTAP commands for pausing, resuming, stopping, and displaying information about security policy jobs.

If you want to...	Use this command...
Pause security policy jobs	<code>vserver security file-directory job pause -vserver vserver_name -id integer</code>
Resume security policy jobs	<code>vserver security file-directory job resume -vserver vserver_name -id integer</code>
Display information about security policy jobs	<code>vserver security file-directory job show -vserver vserver_name</code> You can determine the job ID of a job using this command.
Stop security policy jobs	<code>vserver security file-directory job stop -vserver vserver_name -id integer</code>

See the man pages for the `vserver security file-directory job` commands for more information.

#### Configure the metadata cache for SMB shares

##### How SMB metadata caching works

Metadata caching enables file attribute caching on SMB 1.0 clients to provide faster access to file and folder attributes. You can enable or disable attribute caching on a per-share basis. You can also configure the time-to-live for cached entries if metadata caching is enabled. Configuring metadata caching is not necessary if clients are

## connecting to shares over SMB 2.x or SMB 3.0.

When enabled, the SMB metadata cache stores path and file attribute data for a limited amount of time. This can improve SMB performance for SMB 1.0 clients with common workloads.

For certain tasks, SMB creates a significant amount of traffic that can include multiple identical queries for path and file metadata. You can reduce the number of redundant queries and improve performance for SMB 1.0 clients by using SMB metadata caching to fetch information from the cache instead.



While unlikely, it is possible that the metadata cache might serve stale information to SMB 1.0 clients. If your environment cannot afford this risk, you should not enable this feature.

### Enable the SMB metadata cache

You can improve SMB performance for SMB 1.0 clients by enabling the SMB metadata cache. By default, SMB metadata caching is disabled.

#### Step

1. Perform the desired action:

If you want to...	Enter the command...
Enable SMB metadata caching when you create a share	<pre>vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties attributecache</pre>
Enable SMB metadata caching on an existing share	<pre>vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties attributecache</pre>

### Related information

[Configuring the lifetime of SMB metadata cache entries](#)

[Adding or removing share properties on an existing SMB share](#)

### Configure the lifetime of SMB metadata cache entries

You can configure the lifetime of SMB metadata cache entries to optimize the SMB metadata cache performance in your environment. The default is 10 seconds.

#### Before you begin

You must have enabled the SMB metadata cache feature. If SMB metadata caching is not enabled, the SMB cache TTL setting is not used.

#### Step

1. Perform the desired action:

If you want to configure the lifetime of SMB metadata cache entries when you...	Enter the command...
Create a share	<pre>vserver cifs share -create -vserver vserver_name -share-name share_name -path path -attribute-cache-ttl [integerh][integerm][integers]</pre>
Modify an existing share	<pre>vserver cifs share -modify -vserver vserver_name -share-name share_name -attribute-cache-ttl [integerh][integerm][integers]</pre>

You can specify additional share configuration options and properties when you create or modify shares. See the man pages for more information.

## Manage file locks

### About file locking between protocols

File locking is a method used by client applications to prevent a user from accessing a file previously opened by another user. How ONTAP locks files depends on the protocol of the client.

If the client is an NFS client, locks are advisory; if the client is an SMB client, locks are mandatory.

Because of differences between the NFS and SMB file locks, an NFS client might fail to access a file previously opened by an SMB application.

The following occurs when an NFS client attempts to access a file locked by an SMB application:

- In mixed or NTFS volumes, file manipulation operations such as `rm`, `rmdir`, and `mv` can cause the NFS application to fail.
- NFS read and write operations are denied by SMB deny-read and deny-write open modes, respectively.
- NFS write operations fail when the written range of the file is locked with an exclusive SMB bytelock.

In UNIX security-style volumes, NFS unlink and rename operations ignore SMB lock state and allow access to the file. All other NFS operations on UNIX security-style volumes honor SMB lock state.

### How ONTAP treats read-only bits

The read-only bit is set on a file-by-file basis to reflect whether a file is writable (disabled) or read-only (enabled).

SMB clients that use Windows can set a per-file read-only bit. NFS clients do not set a per-file read-only bit because NFS clients do not have any protocol operations that use a per-file read-only bit.

ONTAP can set a read-only bit on a file when an SMB client that uses Windows creates that file. ONTAP can also set a read-only bit when a file is shared between NFS clients and SMB clients. Some software, when used by NFS clients and SMB clients, requires the read-only bit to be enabled.



For ONTAP to keep the appropriate read and write permissions on a file shared between NFS clients and SMB clients, it treats the read-only bit according to the following rules:

- NFS treats any file with the read-only bit enabled as if it has no write permission bits enabled.
- If an NFS client disables all write permission bits and at least one of those bits had previously been enabled, ONTAP enables the read-only bit for that file.
- If an NFS client enables any write permission bit, ONTAP disables the read-only bit for that file.
- If the read-only bit for a file is enabled and an NFS client attempts to discover permissions for the file, the permission bits for the file are not sent to the NFS client; instead, ONTAP sends the permission bits to the NFS client with the write permission bits masked.
- If the read-only bit for a file is enabled and an SMB client disables the read-only bit, ONTAP enables the owner's write permission bit for the file.
- Files with the read-only bit enabled are writable only by root.



Changes to file permissions take effect immediately on SMB clients, but might not take effect immediately on NFS clients if the NFS client enables attribute caching.

#### How ONTAP differs from Windows on handling locks on share path components

Unlike Windows, ONTAP does not lock each component of the path to an open file while the file is open. This behavior also affects SMB share paths.

Because ONTAP does not lock each component of the path, it is possible to rename a path component above the open file or share, which can cause problems for certain applications, or can cause the share path in the SMB configuration to be invalid. This can cause the share to be inaccessible.

To avoid issues caused by renaming path components, you can apply security settings that prevent users or applications from renaming critical directories.

#### Display information about locks

You can display information about the current file locks, including what types of locks are held and what the lock state is, details about byte-range locks, sharelock modes, delegation locks, and opportunistic locks, and whether locks are opened with durable or persistent handles.

#### About this task

The client IP address cannot be displayed for locks established through NFSv4 or NFSv4.1.

By default, the command displays information about all locks. You can use command parameters to display information about locks for a specific storage virtual machine (SVM) or to filter the command's output by other criteria.

The `vserver locks show` command displays information about four types of locks:

- Byte-range locks, which lock only a portion of a file.
- Share locks, which lock open files.
- Opportunistic locks, which control client-side caching over SMB.
- Delegations, which control client-side caching over NFSv4.x.

By specifying optional parameters, you can determine important information about each lock type. See the man page for the command for more information.

## Step

1. Display information about locks by using the `vserver locks show` command.

## Examples

The following example displays summary information for an NFSv4 lock on a file with the path `/vol1/file1`. The sharelock access mode is `write-deny_none`, and the lock was granted with write delegation:

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path          LIF          Protocol  Lock Type  Client
-----
-----
vol1    /vol1/file1           lif1         nfsv4     share-level -
                Sharelock Mode: write-deny_none
                delegation -
                Delegation Type: write
```

The following example displays detailed oplock and sharelock information about the SMB lock on a file with the path `/data2/data2_2/intro.pptx`. A durable handle is granted on the file with a share lock access mode of `write-deny_none` to a client with an IP address of 10.3.1.3. A lease oplock is granted with a batch oplock level:

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                Vserver: vs1
                Volume: data2_2
Logical Interface: lif2
                Object Path: /data2/data2_2/intro.pptx
                Lock UUID: 553cf484-7030-4998-88d3-1125adbbba0b7
                Lock Protocol: cifs
                Lock Type: share-level
Node Holding Lock State: node3
                Lock State: granted
Bytelock Starting Offset: -
Number of Bytes Locked: -
Bytelock is Mandatory: -
Bytelock is Exclusive: -
Bytelock is Superlock: -
                Bytelock is Soft: -
                Oplock Level: -
Shared Lock Access Mode: write-deny_none
                Shared Lock is Soft: false
```

```

    Delegation Type: -
      Client Address: 10.3.1.3
        SMB Open Type: durable
      SMB Connect State: connected
SMB Expiration Time (Secs): -
      SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

      Vserver: vs1
        Volume: data2_2
    Logical Interface: lif2
      Object Path: /data2/data2_2/test.pptx
      Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
      Lock Protocol: cifs
      Lock Type: op-lock
    Node Holding Lock State: node3
      Lock State: granted
    Bytelock Starting Offset: -
      Number of Bytes Locked: -
      Bytelock is Mandatory: -
      Bytelock is Exclusive: -
      Bytelock is Superlock: -
      Bytelock is Soft: -
      Oplock Level: batch
    Shared Lock Access Mode: -
      Shared Lock is Soft: -
      Delegation Type: -
      Client Address: 10.3.1.3
      SMB Open Type: -
      SMB Connect State: connected
SMB Expiration Time (Secs): -
      SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

```

## Break locks

When file locks are preventing client access to files, you can display information about currently held locks, and then break specific locks. Examples of scenarios in which you might need to break locks include debugging applications.

### About this task

The `vserver locks break` command is available only at the advanced privilege level and higher. The man page for the command contains detailed information.

### Steps

1. To find the information you need to break a lock, use the `vserver locks show` command.

The man page for the command contains detailed information.

2. Set the privilege level to advanced: `set -privilege advanced`
3. Perform one of the following actions:

If you want to break a lock by specifying...	Enter the command...
The SVM name, volume name, LIF name, and file path	<code>vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif</code>
The lock ID	<code>vserver locks break -lockid UUID</code>

4. Return to the admin privilege level: `set -privilege admin`

## Monitor SMB activity

### Display SMB session information

You can display information about established SMB sessions, including the SMB connection and session ID and the IP address of the workstation using the session. You can display information about the session's SMB protocol version and continuously available protection level, which helps you identify whether the session supports nondisruptive operations.

### About this task

You can display information for all of the sessions on your SVM in summary form. However, in many cases, the amount of output that is returned is large. You can customize what information is displayed in the output by specifying optional parameters:

- You can use the optional `-fields` parameter to display output about the fields you choose.

You can enter `-fields ?` to determine what fields you can use.


- You can use the `-instance` parameter to display detailed information about established SMB sessions.
- You can use the `-fields` parameter or the `-instance` parameter either alone or in combination with other optional parameters.

### Step

1. Perform one of the following actions:

If you want to display SMB session information...	Enter the following command...
For all sessions on the SVM in summary form	<code>vserver cifs session show -vserver vserver_name</code>

If you want to display SMB session information...	Enter the following command...
On a specified connection ID	<pre>vserver cifs session show -vserver vserver_name -connection-id integer</pre>
From a specified workstation IP address	<pre>vserver cifs session show -vserver vserver_name -address workstation_IP_address</pre>
On a specified LIF IP address	<pre>vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address</pre>
On a specified node	<pre>vserver cifs session show -vserver vserver_name -node {node_name local}</pre>
From a specified Windows user	<pre>vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name</pre>
With a specified authentication mechanism	<pre>vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1 NTLMv2 Kerberos Anonymous}</pre>
With a specified protocol version	<pre>vserver cifs session show -vserver vserver_name -protocol-version {SMB1 SMB2 SMB2_1 SMB3 SMB3_1}</pre> <div data-bbox="873 1318 928 1373" style="float: left; margin-right: 10px;">  </div> <div data-bbox="987 1226 1458 1465"> <p>Continuously available protection and SMB Multichannel are available only on SMB 3.0 and later sessions. To view their status on all qualifying sessions, you should specify this parameter with the value set to SMB3 or later.</p> </div>

If you want to display SMB session information...	Enter the following command...
With a specified level of continuously available protection	<pre>vserver cifs session show -vserver vserver_name -continuously-available {No Yes Partial}</pre> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>If the continuously available status is <b>Partial</b>, this means that the session contains at least one open continuously available file, but the session has some files that are not open with continuously available protection. You can use the <code>vserver cifs sessions file show</code> command to determine which files on the established session are not open with continuously available protection.</p> </div>
With a specified SMB signing session status	<pre>vserver cifs session show -vserver vserver_name -is-session-signed {true false}</pre>

## Examples

The following command displays session information for the sessions on SVM vs1 established from a workstation with IP address 10.1.1.1:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session
ID       ID       Workstation      Windows User      Open      Idle
-----  -
3151272279,
3151272280,
3151272281  1       10.1.1.1        DOMAIN\joe        2         23s
```

The following command displays detailed session information for sessions with continuously available protection on SVM vs1. The connection was made by using the domain account.

```
cluster1::> vserver cifs session show -instance -continuously-available  
Yes
```

```
        Node: nodel  
        Vserver: vs1  
        Session ID: 1  
        Connection ID: 3151274158  
Incoming Data LIF IP Address: 10.2.1.1  
        Workstation IP address: 10.1.1.2  
Authentication Mechanism: Kerberos  
        Windows User: DOMAIN\SERVER1$\br/>        UNIX User: pcuser  
        Open Shares: 1  
        Open Files: 1  
        Open Other: 0  
        Connected Time: 10m 43s  
        Idle Time: 1m 19s  
        Protocol Version: SMB3  
Continuously Available: Yes  
        Is Session Signed: false  
        User Authenticated as: domain-user  
        NetBIOS Name: -  
        SMB Encryption Status: Unencrypted
```

The following command displays session information on a session using SMB 3.0 and SMB Multichannel on SVM vs1. In the example, the user connected to this share from an SMB 3.0 capable client by using the LIF IP address; therefore, the authentication mechanism defaulted to NTLMv2. The connection must be made by using Kerberos authentication to connect with continuously available protection.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

      Node: nodel
      Vserver: vs1
      Session ID: 1
      **Connection IDs: 3151272607,31512726078,3151272609
      Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
      Authentication Mechanism: NTLMv2
      Windows User: DOMAIN\administrator
      UNIX User: pcuser
      Open Shares: 1
      Open Files: 0
      Open Other: 0
      Connected Time: 6m 22s
      Idle Time: 5m 42s
      Protocol Version: SMB3
      Continuously Available: No
      Is Session Signed: false
      User Authenticated as: domain-user
      NetBIOS Name: -
      SMB Encryption Status: Unencrypted
```

## Related information

[Displaying information about open SMB files](#)

### Display information about open SMB files

You can display information about open SMB files, including the SMB connection and session ID, the hosting volume, the share name, and the share path. You can display information about a file's continuously available protection level, which is helpful in determining whether an open file is in a state that supports nondisruptive operations.

### About this task

You can display information about open files on an established SMB session. The displayed information is useful when you need to determine SMB session information for particular files within an SMB session.

For example, if you have an SMB session where some of the open files are open with continuously available protection and some are not open with continuously available protection (the value for the `-continuously-available` field in `vserver cifs session show` command output is `Partial`), you can determine which files are not continuously available by using this command.

You can display information for all open files on established SMB sessions on storage virtual machines (SVMs) in summary form by using the `vserver cifs session file show` command without any optional parameters.



However, in many cases, the amount of output returned is large. You can customize what information is displayed in the output by specifying optional parameters. This can be helpful when you want to view information for only a small subset of open files.

- You can use the optional `-fields` parameter to display output on the fields you choose.

You can use this parameter either alone or in combination with other optional parameters.



- You can use the `-instance` parameter to display detailed information about open SMB files.

You can use this parameter either alone or in combination with other optional parameters.

## Step

1. Perform one of the following actions:

If you want to display open SMB files...	Enter the following command...
On the SVM in summary form	<pre>vserver cifs session file show -vserver vserver_name</pre>
On a specified node	<pre>vserver cifs session file show -vserver vserver_name -node {node_name local}</pre>
On a specified file ID	<pre>vserver cifs session file show -vserver vserver_name -file-id integer</pre>
On a specified SMB connection ID	<pre>vserver cifs session file show -vserver vserver_name -connection-id integer</pre>
On a specified SMB session ID	<pre>vserver cifs session file show -vserver vserver_name -session-id integer</pre>
On the specified hosting aggregate	<pre>vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name</pre>
On the specified volume	<pre>vserver cifs session file show -vserver vserver_name -hosting-volume volume_name</pre>
On the specified SMB share	<pre>vserver cifs session file show -vserver vserver_name -share share_name</pre>

If you want to display open SMB files...	Enter the following command...
On the specified SMB path	<pre>vserver cifs session file show -vserver vserver_name -path path</pre>
With the specified level of continuously available protection	<pre>vserver cifs session file show -vserver vserver_name -continuously -available {No Yes}</pre> <div data-bbox="873 541 928 604" style="float: left; margin-right: 10px;">  </div> <div data-bbox="987 436 1448 709" style="border-left: 1px solid #ccc; padding-left: 10px;"> <p>If the continuously available status is No, this means that these open files are not capable of nondisruptively recovering from takeover and giveback. They also cannot recover from general aggregate relocation between partners in a high-availability relationship.</p> </div>
With the specified reconnected state	<pre>vserver cifs session file show -vserver vserver_name -reconnected {No Yes}</pre> <div data-bbox="873 1066 928 1129" style="float: left; margin-right: 10px;">  </div> <div data-bbox="987 926 1458 1262" style="border-left: 1px solid #ccc; padding-left: 10px;"> <p>If the reconnected state is No, the open file is not reconnected after a disconnection event. This can mean that the file was never disconnected, or that the file was disconnected and is not successfully reconnected. If the reconnected state is Yes, this means that the open file is successfully reconnected after a disconnection event.</p> </div>

There are additional optional parameters that you can use to refine the output results. See the man page for more information.

### Examples

The following example displays information about open files on SVM vs1:

```

cluster1::> vserver cifs session file show -vserver vs1
Node:          node1
Vserver:      vs1
Connection:   3151274158
Session:      1
File          File          Open Hosting          Continuously
ID            Type            Mode Volume           Share                Available
-----
41           Regular        r    data                data                 Yes
Path: \mytest.rtf

```

The following example displays detailed information about open SMB files with file ID 82 on SVM vs1:

```

cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                Node: node1
                Vserver: vs1
                File ID: 82
                Connection ID: 104617
                Session ID: 1
                File Type: Regular
                Open Mode: rw
Aggregate Hosting File: aggr1
  Volume Hosting File: data1
                CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
                Share Mode: rw
                Range Locks: 1
Continuously Available: Yes
                Reconnected: No

```

## Related information

[Displaying SMB session information](#)

### Determine which statistics objects and counters are available

Before you can obtain information about CIFS, SMB, auditing, and BranchCache hash statistics and monitor performance, you must know which objects and counters are available from which you can obtain data.

### Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Perform one of the following actions:

If you want to determine...	Enter...
Which objects are available	<code>statistics catalog object show</code>
Specific objects that are available	<code>statistics catalog object show object object_name</code>
Which counters are available	<code>statistics catalog counter show object object_name</code>

See the man pages for more information about which objects and counters are available.

- Return to the admin privilege level: `set -privilege admin`

### Examples

The following command displays descriptions of selected statistic objects related to CIFS and SMB access in the cluster as seen at the advanced privilege level:

```
cluster1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.

```
Do you want to continue? {y|n}: y
```

```
cluster1::*> statistics catalog object show -object audit
audit_ng          CM object for exporting audit_ng
performance counters
```

```
cluster1::*> statistics catalog object show -object cifs
cifs              The CIFS object reports activity of the
                  Common Internet File System protocol
                  ...
```

```
cluster1::*> statistics catalog object show -object nblade_cifs
nblade_cifs      The Common Internet File System (CIFS)
                  protocol is an implementation of the
Server
                  ...
```

```
cluster1::*> statistics catalog object show -object smb1
smb1              These counters report activity from the
SMB               revision of the protocol. For information
                  ...
```

```
cluster1::*> statistics catalog object show -object smb2
smb2              These counters report activity from the
                  SMB2/SMB3 revision of the protocol. For
                  ...
```

```
cluster1::*> statistics catalog object show -object hashd
hashd            The hashd object provides counters to
measure          the performance of the BranchCache hash
daemon.
```

```
cluster1::*> set -privilege admin
```

The following command displays information about some of the counters for the `cifs` object as seen at the advanced privilege level:



This example does not display all of the available counters for the `cifs` object; output is truncated.

```
cluster1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.

```
Do you want to continue? {y|n}: y
```

```
cluster1::*> statistics catalog counter show -object cifs
```

```
Object: cifs
```

Counter	Description
active_searches	Number of active searches over SMB and SMB2
auth_reject_too_many	Authentication refused after too many requests were made in rapid succession
avg_directory_depth	Average number of directories crossed by SMB and SMB2 path-based commands
...	...

```
cluster2::> statistics start -object client -sample-id
```

```
Object: client
```

Counter	Value
cifs_ops	0
cifs_read_ops	0
cifs_read_recv_ops	0
cifs_read_recv_size	0B
cifs_read_size	0B
cifs_write_ops	0
cifs_write_recv_ops	0
cifs_write_recv_size	0B
cifs_write_size	0B
instance_name	vserver_1:10.72.205.179
instance_uuid	2:10.72.205.179
local_ops	0
mount_ops	0

```
[...]
```

## Related information

[Displaying statistics](#)

## Display statistics

You can display various statistics, including statistics about CIFS and SMB, auditing, and BranchCache hashes, to monitor performance and diagnose issues.

### Before you begin

You must have collected data samples by using the `statistics start` and `statistics stop` commands before you can display information about objects.

### Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Perform one of the following actions:

If you want to display statistics for...	Enter...
All versions of SMB	<code>statistics show -object cifs</code>
SMB 1.0	<code>statistics show -object smb1</code>
SMB 2.x and SMB 3.0	<code>statistics show -object smb2</code>
CIFS subsystem of the node	<code>statistics show -object nblade_cifs</code>
Multiprotocol audit	<code>statistics show -object audit_ng</code>
BranchCache hash service	<code>statistics show -object hashd</code>
Dynamic DNS	<code>statistics show -object ddns_update</code>

See the man page for each command for more information.

3. Return to the admin privilege level: `set -privilege admin`

### Related information

[Determining which statistics objects and counters are available](#)

[Monitoring SMB signed session statistics](#)

[Displaying BranchCache statistics](#)

[Using statistics to monitor automatic node referral activity](#)

[SMB configuration for Microsoft Hyper-V and SQL Server](#)

[Performance monitoring setup](#)

## Deploy SMB client-based services

### Use offline files to allow caching of files for offline use

#### Use offline files to allow caching of files for offline use overview

ONTAP supports the Microsoft Offline Files feature, or *client-side caching*, which allows files to be cached on the local host for offline use. Users can use the offline files functionality to continue working on files even when they are disconnected from the network.

You can specify whether Windows user documents and programs are automatically cached on a share or whether the files must be manually selected for caching. Manual caching is enabled by default for new shares. The files that are made available offline are synchronized to the Windows client's local disk. Synchronization occurs when network connectivity to a specific storage system share is restored.

Because offline files and folders retain the same access permissions as the version of the files and folders saved on the CIFS server, the user must have sufficient permissions on the files and folders saved on the CIFS server to perform actions on the offline files and folders.

When the user and someone else on the network make changes to the same file, the user can save the local version of the file to the network, keep the other version, or save both. If the user keeps both versions, a new file with the local user's changes is saved locally and the cached file is overwritten with changes from the version of the file saved on the CIFS server.

You can configure offline files on a share-by-share basis by using share configuration settings. You can choose one of the four offline folder configurations when you create or modify shares:

- No caching

Disables client-side caching for the share. Files and folders are not automatically cached locally on clients and users cannot choose to cache files or folders locally.

- Manual caching

Enables manual selection of files to be cached on the share. This is the default setting. By default, no files or folders are cached on the local client. Users can choose which files and folders they want to cache locally for offline use.

- Automatic document caching

Enables user documents to be automatically cached on the share. Only files and folders that are accessed are cached locally.

- Automatic program caching

Enables programs and user documents to be automatically cached on the share. Only files, folders, and programs that are accessed are cached locally. Additionally, this setting allows the client to run locally cached executables even when connected to the network.

For more information about configuring offline files on Windows servers and clients, consult the Microsoft TechNet Library.

### Related information



[Using roaming profiles to store user profiles centrally on a CIFS server associated with the SVM](#)

[Using folder redirection to store data on a CIFS server](#)

[Using BranchCache to cache SMB share content at a branch office](#)

[Microsoft TechNet Library: technet.microsoft.com/en-us/library/](http://technet.microsoft.com/en-us/library/)

### **Requirements for using offline files**

Before you can use the Microsoft Offline Files feature with your CIFS server, you need to know which versions of ONTAP and SMB and which Windows clients support the feature.

### **ONTAP version requirements**

ONTAP releases support offline files.

### **SMB protocol version requirements**

For storage virtual machine (SVM), ONTAP supports offline files on all versions of SMB.

### **Windows client requirements**

The Windows client must support the offline files.

For the latest information about which Windows clients supports the Offline Files feature, see the Interoperability Matrix.

[mysupport.netapp.com/matrix](http://mysupport.netapp.com/matrix)

### **Guidelines for deploying offline files**

There are some important guidelines you need to understand when you deploy offline files on home directory shares that have the `showsnapshot` share property set on home directories.

If the `showsnapshot` share property is set on a home directory share that has offline files configured, Windows clients cache all of the Snapshot copies under the `~snapshot` folder in the user's home directory.

Windows clients cache all of the Snapshot copies under the home directory if one of more of the following is true:

- The user makes the home directory available offline from the client.

The contents of the `~snapshot` folder in the home directory is included and made available offline.

- The user configures folder redirection to redirect a folder such as `My Documents` to the root of a home directory residing on the CIFS server share.

Some Windows clients might automatically make the redirected folder available offline. If the folder is redirected to the root of the home directory, the `~snapshot` folder is included in the cached offline content.



Offline file deployments where the `~snapshot` folder is included in offline files should be avoided. The Snapshot copies in the `~snapshot` folder contain all data on the volume at the point at which ONTAP created the Snapshot copy. Therefore, creating an offline copy of the `~snapshot` folder consumes significant local storage on the client, consumes network bandwidth during offline files synchronization, and increases the time it takes to synchronize offline files.

### Configure offline files support on SMB shares using the CLI

You can configure offline files support using the ONTAP CLI by specifying one of the four offline files setting when you create SMB shares or at any time by modifying existing SMB shares. Manual offline files support is the default setting.

#### About this task

When configuring offline files support, you can choose one of the following four offline files settings:

Setting	Description
<code>none</code>	Disallows Windows clients from caching any files on this share.
<code>manual</code>	Allows users on Windows clients to manually select files to be cached.
<code>documents</code>	Allows Windows clients to cache user documents that are used by the user for offline access.
<code>programs</code>	Allows Windows clients to cache programs that are used by the user for offline access. Clients can use the cached program files in offline mode even if the share is available.

You can choose only one offline file setting. If you modify an offline files setting on an existing SMB share, the new offline files setting replaces the original setting. Other existing SMB share configuration settings and share properties are not removed or replaced. They remain in effect until they are explicitly removed or changed.

#### Steps

1. Perform the appropriate action:

If you want to configure offline files on...	Enter the command...
A new SMB share	<pre>vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none manual documents programs}</pre>

If you want to configure offline files on...	Enter the command...
An existing SMB share	<pre>vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none manual documents programs}</pre>

2. Verify that the SMB share configuration is correct: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

### Example

The following command creates an SMB share named “data1” with offline files set to documents:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -comment "Offline files" -offline-files documents
```

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance
```

```

                Vserver: vs1
                Share: data1
    CIFS Server NetBIOS Name: VS1
                Path: /data1
    Share Properties: oplocks
                    browsable
                    changenotify
    Symlink Properties: enable
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
                Share Comment: Offline files
                Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                Volume Name: -
                Offline Files: documents
    Vscan File-Operations Profile: standard
    Maximum Tree Connections on Share: 4294967295
    UNIX Group for File Create: -
```

The following command modifies an existing SMB share named “data1” by changing the offline files setting to manual and adding values for the file and directory mode creation mask:

```

cluster1::> vserver cifs share modify -vserver vs1 -share-name data1
-offline-files manual -file-umask 644 -dir-umask 777

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                Vserver: vs1
                Share: data1
CIFS Server NetBIOS Name: VS1
                Path: /data1
                Share Properties: oplocks
                                browsable
                                changenotify
                Symlink Properties: enable
                File Mode Creation Mask: 644
Directory Mode Creation Mask: 777
                Share Comment: Offline files
                Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
                UNIX Group for File Create: -

```

## Related information

[Adding or removing share properties on an existing SMB share](#)

### Configure offline files support on SMB shares by using the Computer Management MMC

If you want to permit users to cache files locally for offline use, you can configure offline files support by using the Computer Management MMC (Microsoft Management Console).

#### Steps

1. To open the MMC on your Windows server, in Windows Explorer, right-click the icon for the local computer, and then select **Manage**.
2. On the left panel, select **Computer Management**.
3. Select **Action > Connect to another computer**.

The Select Computer dialog box appears.

4. Type the name of the CIFS server or click **Browse** to locate the CIFS server.

If the name of CIFS server is the same as the storage virtual machine (SVM) host name, type the SVM name. If the CIFS server name is different from the SVM host name, type the name of the CIFS server.

5. Click **OK**.
6. In the console tree, click **System Tools > Shared Folders**.
7. Click **Shares**.
8. In the results pane, right-click the share.
9. Click **Properties**.

Properties for the share you selected are displayed.

10. In the **General** tab, click **Offline Settings**.

The Offline Settings dialog box appears.

11. Configure the offline availability options as appropriate.
12. Click **OK**.

## **Use roaming profiles to store user profiles centrally on a SMB server associated with the SVM**

### **Use roaming profiles to store user profiles centrally on a SMB server associated with the SVM overview**

ONTAP supports storing Windows roaming profiles on a CIFS server associated with the storage virtual machine (SVM). Configuring user roaming profiles provides advantages to the user such as automatic resource availability regardless of where the user logs in. Roaming profiles also simplify the administration and management of user profiles.

Roaming user profiles have the following advantages:

- Automatic resource availability

A user's unique profile is automatically available when that user logs in to any computer on the network that is running Windows 8, Windows 7, Windows 2000, or Windows XP. Users do not need to create a profile on each computer they use on a network.

- Simplified computer replacement

Because all of the user's profile information is maintained separately on the network, a user's profile can be easily downloaded onto a new, replacement computer. When the user logs in to the new computer for the first time, the server copy of the user's profile is copied to the new computer.

### **Related information**

[Using offline files to allow caching of files for offline use](#)

[Using folder redirection to store data on a CIFS server](#)

### **Requirements for using roaming profiles**

Before you can use Microsoft's roaming profiles with your CIFS server, you need to know which versions of ONTAP and SMB and which Windows clients support the feature.

## ONTAP version requirements

ONTAP support roaming profiles.

## SMB protocol version requirements

For storage virtual machine (SVM), ONTAP supports roaming profiles on all versions of SMB.

## Windows client requirements

Before a user can use the roaming profiles, the Windows client must support the feature.

For the latest information about which Windows clients support roaming profiles, see the Interoperability Matrix.

[NetApp Interoperability Matrix Tool](#)

## Configure roaming profiles

If you want to automatically make a user's profile available when that user logs on to any computer on the network, you can configure roaming profiles through the Active Directory Users and Computers MMC snap-in. If you are configuring roaming profiles on Windows Server 2012, you can use the Active Directory Administration Center.

### Steps

1. On the Windows server, open the Active Directory Users and Computers MMC (or the Active Directory Administration Center on Windows 2012 and later servers).
2. Locate the user for which you want to configure a roaming profile.
3. Right-click the user and click **Properties**.
4. On the **Profile** tab, enter the profile path to the share where you want to store the user's roaming profile, followed by %username%.

For example, a profile path might be the following: `\\vs1.example.com\profiles\%username%`. The first time a user logs in, %username% is replaced with the user's name.



In the path `\\vs1.example.com\profiles\%username%`, `profiles` is the share name of a share on storage virtual machine (SVM) vs1 that has Full Control rights for Everyone.

5. Click **OK**.

## Use folder redirection to store data on a SMB server

### Use folder redirection to store data on a SMB server overview

ONTAP supports Microsoft folder redirection, which enables users or administrators to redirect the path of a local folder to a location on the CIFS server. It appears as if redirected folders are stored on the local Windows client, even though the data is stored on an SMB share.

Folder redirection is intended mostly for organizations that have already deployed home directories, and that want to maintain compatibility with their existing home directory environment.

- Documents, Desktop, and Start Menu are examples of folders that you can redirect.
- Users can redirect folders from their Windows client.
- Administrators can centrally configure and manage folder redirection by configuring GPOs in Active Directory.
- If administrators have configured roaming profiles, folder redirection enables administrators to divide user data from profile data.
- Administrators can use folder redirection and offline files together to redirect data storage for local folders to the CIFS server, while allowing users to cache the content locally.

## Related information

[Using offline files to allow caching of files for offline use](#)

[Using roaming profiles to store user profiles centrally on a CIFS server associated with the SVM](#)

## Requirements for using folder redirection

Before you can use Microsoft's folder redirection with your CIFS server, you need to know which versions of ONTAP and SMB and which Windows clients support the feature.

### ONTAP version requirements

ONTAP support Microsoft folder redirection.

### SMB protocol version requirements

For storage virtual machine (SVM), ONTAP supports Microsoft's folder redirection on all versions of SMB.

### Windows client requirements

Before a user can use Microsoft's folder redirection, the Windows client must support the feature.

For the latest information about which Windows clients support folder redirection, see the Interoperability Matrix.

[mysupport.netapp.com/matrix](https://mysupport.netapp.com/matrix)

## Configure folder redirection

You can configure folder redirection using the Windows Properties window. The advantage to using this method is that the Windows user can configure folder redirection without assistance from the SVM administrator.

### Steps

1. In Windows Explorer, right-click the folder that you want to redirect to a network share.
2. Click **Properties**.

Properties for the share you selected are displayed.

3. In the **Shortcut** tab, click **Target** and specify the path to the network location where you want to redirect the selected folder.

For example, if you want to redirect a folder to the `data` folder in a home directory that is mapped to `Q:\`, specify `Q:\data` as the target.

#### 4. Click **OK**.

For more information about configuring offline folders, consult the Microsoft TechNet Library.

### Related information

Microsoft TechNet Library: [technet.microsoft.com/en-us/library/](http://technet.microsoft.com/en-us/library/)

### Access the `~snapshot` directory from Windows clients using SMB 2.x

The method that you use to access the `~snapshot` directory from Windows clients using SMB 2.x differs from the method used for SMB 1.0. You need to understand how to access the `~snapshot` directory when using SMB 2.x connections to successfully access data stored in Snapshot copies.

The SVM administrator controls whether users on Windows clients can view and access the `~snapshot` directory on a share by enabling or disabling the `showsnapshot` share property using commands from the `vserver cifs share properties families`.

When the `showsnapshot` share property is disabled, a user on a Windows client using SMB 2.x cannot view the `~snapshot` directory and cannot access Snapshot copies within the `~snapshot` directory, even when manually entering the path to the `~snapshot` directory or to specific Snapshot copies within the directory.

When the `showsnapshot` share property is enabled, a user on a Windows client using SMB 2.x still cannot view the `~snapshot` directory either at the root of the share or within any junction or directory below the root of the share. However, after connecting to a share, the user can access the hidden `~snapshot` directory by manually appending `\~snapshot` to the end of the share path. The hidden `~snapshot` directory is accessible from two entry points:

- At the root of the share
- At every junction point in the share space

The hidden `~snapshot` directory is not accessible from non-junction subdirectories within the share.

### Example

With the configuration shown in the following example, a user on a Windows client with an SMB 2.x connection to the “eng” share can access the `~snapshot` directory by manually appending `\~snapshot` to the share path at the root of the share and at every junction point in the path. The hidden `~snapshot` directory is accessible from the following three paths:

- `\\vs1\eng\~snapshot`
- `\\vs1\eng\projects1\~snapshot`
- `\\vs1\eng\projects2\~snapshot`



```

cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume          junction-path
-----
vs1      vs1_root             /
vs1      vs1_vol1             /eng
vs1      vs1_vol2             /eng/projects1
vs1      vs1_vol3             /eng/projects2

cluster1::> vserver cifs share show
Vserver  Share  Path      Properties      Comment  ACL
-----
vs1      eng    /eng      oplocks         -        Everyone / Full Control
          chngenotify
          browsable
          showsnapshot

```

## Recover files and folders using Previous Versions

### Recover files and folders using previous versions overview

The ability to use Microsoft Previous Versions is applicable to file systems that support Snapshot copies in some form and have them enabled. Snapshot technology is an integral part of ONTAP. Users can recover files and folders from Snapshot copies from their Windows client by using the Microsoft Previous Versions feature.

Previous Versions functionality provides a method for users to browse through the Snapshot copies or to restore data from a Snapshot copy without a storage administrator's intervention. Previous Versions is not configurable. It is always enabled. If the storage administrator has made Snapshot copies available on a share, then the user can use Previous Versions to perform the following tasks:

- Recover files that were accidentally deleted.
- Recover from accidentally overwriting a file.
- Compare versions of file while working.

The data stored in Snapshot copies is read-only. Users must save a copy of a file to another location to make any changes to the file. Snapshot copies are periodically deleted; therefore, users need to create copies of files contained in Previous Versions if they want to indefinitely retain a previous version of a file.

### Requirements for using Microsoft Previous Versions

Before you can use Previous Versions with your CIFS server, you need to know which versions of ONTAP and SMB, and which Windows clients, support it. You also need to know about the Snapshot copy setting requirement.

### ONTAP version requirements

Supports Previous Versions.

## SMB protocol version requirements

For storage virtual machine (SVM), ONTAP supports Previous Versions on all versions of SMB.

## Windows client requirements

Before a user can use Previous Versions to access data in Snapshot copies, the Windows client must support the feature.

For the latest information about which Windows clients support Previous Versions, see the Interoperability Matrix.

[NetApp Interoperability Matrix Tool](#)

## Requirements for Snapshot copy settings

To use Previous Versions to access data in Snapshot copies, an enabled Snapshot policy must be associated to the volume containing the data, clients must be able to access to the Snapshot data, and Snapshot copies must exist.

### Use the Previous Versions tab to view and manage Snapshot copy data

Users on Windows client machines can use the Previous Versions tab on the Windows Properties window to restore data stored in Snapshot copies without needing to involve the storage virtual machine (SVM) administrator.

### About this task

You can only use the Previous Versions tab to view and manage data in Snapshot copies of data stored on the SVM if the administrator has enabled Snapshot copies on the volume containing the share, and if the administrator configures the share to show Snapshot copies.

### Steps

1. In Windows Explorer, display the contents of the mapped drive of the data stored on the CIFS server.
2. Right-click the file or folder in the mapped network drive whose Snapshot copies you want to view or manage.
3. Click **Properties**.

Properties for the file or folder you selected are displayed.

4. Click the **Previous Versions** tab.

A list of available Snapshot copies of the selected file or folder is displayed in the Folder versions: box. The listed Snapshot copies are identified by the Snapshot copy name prefix and the creation timestamp.

5. In the **Folder versions:** box, right-click the copy of the file or folder that you want to manage.
6. Perform the appropriate action:

If you want to...	Do the following...
View data from that Snapshot copy	Click <b>Open</b> .

If you want to...	Do the following...
Create a copy of data from that Snapshot copy	Click <b>Copy</b> .

Data in Snapshot copies is read-only. If you want to make modifications to files and folders listed in the Previous Versions tab, you must save a copy of the files and folders that you want to modify to a writable location and make modifications to the copies.

7. After you finish managing Snapshot data, close the **Properties** dialog box by clicking **OK**.

For more information about using the Previous Versions tab to view and manage Snapshot data, consult the Microsoft TechNet Library.

### Related information

[Microsoft TechNet Library: technet.microsoft.com/en-us/library/](http://technet.microsoft.com/en-us/library/)

#### Determine whether Snapshot copies are available for Previous Versions use

You can view Snapshot copies from the Previous Versions tab only if an enabled Snapshot policy is applied to the volume containing the share, and if the volume configuration allows access to Snapshot copies. Determining Snapshot copy availability is helpful when assisting a user with Previous Versions access.

#### Steps

1. Determine whether the volume on which the share data resides has automatic Snapshot copies enabled and whether clients have access to Snapshot directories: `volume show -vserver vservice-name -volume volume-name -fields vservice, volume, snapdir-access, snapshot-policy, snapshot-count`

The output displays what Snapshot policy is associated with the volume, whether client Snapshot directory access is enabled, and the number of available Snapshot copies.

2. Determine whether the associated Snapshot policy is enabled: `volume snapshot policy show -policy policy-name`
3. List the available Snapshot copies: `volume snapshot show -volume volume_name`

For more information about configuring and managing Snapshot policies and Snapshot schedules, see [Data Protection](#).

#### Example

The following example displays information about Snapshot policies associated with the volume named "data1" that contains the shared data and available Snapshot copies on "data1".

```

cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver  volume snapdir-access snapshot-policy snapshot-count
-----
vs1      data1  true          default      10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1

                Number of Is
Policy Name      Schedules Enabled Comment
-----
default          3 true      Default policy with hourly, daily &
weekly schedules.
  Schedule      Count      Prefix      SnapMirror Label
-----
  hourly        6         hourly      -
  daily         2         daily       daily
  weekly        2         weekly      weekly

cluster1::> volume snapshot show -volume data1

                ---Blocks---
Vserver  Volume  Snapshot              State      Size  Total%  Used%
-----
vs1      data1
        weekly.2012-12-16_0015  valid      408KB    0%     1%
        daily.2012-12-22_0010  valid      420KB    0%     1%
        daily.2012-12-23_0010  valid      192KB    0%     0%
        weekly.2012-12-23_0015  valid      360KB    0%     1%
        hourly.2012-12-23_1405  valid      196KB    0%     0%
        hourly.2012-12-23_1505  valid      196KB    0%     0%
        hourly.2012-12-23_1605  valid      212KB    0%     0%
        hourly.2012-12-23_1705  valid      136KB    0%     0%
        hourly.2012-12-23_1805  valid      200KB    0%     0%
        hourly.2012-12-23_1905  valid      184KB    0%     0%

```

## Related information

[Creating a Snapshot configuration to enable Previous Versions access](#)

## Data protection

### Create a Snapshot configuration to enable Previous Versions access

The Previous Versions functionality is always available, provided that client access to Snapshot copies is enabled and provided that Snapshot copies exist. If your Snapshot copy configuration does not meet these requirements, you can create a Snapshot copy configuration that does.

## Steps

1. If the volume containing the share to which you want to allow Previous Versions access does not have an associated Snapshot policy, associate a Snapshot policy to the volume and enable it by using the `volume modify` command.

For more information about using the `volume modify` command, see the man pages.

2. Enable access to the Snapshot copies by using the `volume modify` command to set the `-snap-dir` option to `true`.

For more information about using the `volume modify` command, see the man pages.

3. Verify that Snapshot policies are enabled and that access to Snapshot directories is enabled by using the `volume show` and `volume snapshot policy show` commands.

For more information about using the `volume show` and `volume snapshot policy show` commands, see the man pages.

For more information about configuring and managing Snapshot policies and Snapshot schedules, see [Data Protection](#).

## Related information

[Data protection](#)

### Guidelines for restoring directories that contain junctions

There are certain guidelines you should keep in mind when using Previous Versions to restore folders that contain junction points.

When using Previous Versions to restore folders that have child folders that are junction points, the restore can fail with an `Access Denied` error.

You can determine whether the folder that you are attempting to restore contains a junction by using the `vol show` command with the `-parent` option. You can also use the `vserver security trace` commands to create detailed logs about file and folder access issues.

## Related information

[Creating and managing data volumes in NAS namespaces](#)

## Deploy SMB server-based services

### Manage home directories

#### How ONTAP enables dynamic home directories

ONTAP home directories enable you to configure an SMB share that maps to different directories based on the user that connects to it and a set of variables. Instead of creating separate shares for each user, you can configure one share with a few home directory parameters to define a user's relationship between an entry point (the share) and the home directory (a directory on the SVM).

A user who is logged in as a guest user does not have a home directory and cannot access other users' home directories. There are four variables that determine how a user is mapped to a directory:

- **Share name**

This is the name of the share that you create to which the user connects. You must set the home directory property for this share.

The share name can use the following dynamic names:

- %w (the user's Windows user name)
- %d (the user's Windows domain name)
- %u (the user's mapped UNIX user name)

To make the share name unique across all home directories, the share name must contain either the %w or the %u variable. The share name can contain both the %d and the %w variable (for example, %d/%w), or the share name can contain a static portion and a variable portion (for example, home\_%w).

- **Share path**

This is the relative path, which is defined by the share and is therefore associated with one of the share names, that is appended to each search path to generate the user's entire home directory path from the root of the SVM. It can be static (for example, home), dynamic (for example, %w), or a combination of the two (for example, eng/%w).

- **Search paths**

This is the set of absolute paths from the root of the SVM that you specify that directs the ONTAP search for home directories. You can specify one or more search paths by using the `vserver cifs home-directory search-path add` command. If you specify multiple search paths, ONTAP tries them in the order specified until it finds a valid path.

- **Directory**

This is the user's home directory that you create for the user. The directory name is usually the user's name. You must create the home directory in one of the directories that are defined by the search paths.

As an example, consider the following setup:

- User: John Smith
- User domain: acme
- User name: jsmith
- SVM name: vs1
- Home directory share name #1: home\_%w - share path: %w
- Home directory share name #2: %w - share path: %d/%w
- Search path #1: /vol0home/home
- Search path #2: /vol1home/home
- Search path #3: /vol2home/home
- Home directory: /vol1home/home/jsmith

Scenario 1: The user connects to `\\vs1\home_jsmith`. This matches the first home directory share name and generates the relative path `jsmith`. ONTAP now searches for a directory named `jsmith` by checking each search path in order:

- `/vol0home/home/jsmith` does not exist; moving on to search path #2.
- `/vol1home/home/jsmith` does exist; therefore, search path #3 is not checked; the user is now connected to his home directory.

Scenario 2: The user connects to `\\vs1\jsmith`. This matches the second home directory share name and generates the relative path `acme/jsmith`. ONTAP now searches for a directory named `acme/jsmith` by checking each search path in order:

- `/vol0home/home/acme/jsmith` does not exist; moving on to search path #2.
- `/vol1home/home/acme/jsmith` does not exist; moving on to search path #3.
- `/vol2home/home/acme/jsmith` does not exist; the home directory does not exist; therefore, the connection fails.

## Home directory shares

### Add a home directory share

If you want to use the SMB home directory feature, you must add at least one share with the home directory property included in the share properties.

#### About this task

You can create a home directory share at the time you create the share by using the `vserver cifs share create` command, or you can change an existing share into a home directory share at any time by using the `vserver cifs share modify` command.

To create a home directory share, you must include the `homedirectory` value in the `-share-properties` option when you create or modify a share. You can specify the share name and share path using variables that are dynamically expanded when users connect to their home directories. Available variables that you can use in the path are `%w`, `%d`, and `%u`, corresponding to the Windows user name, domain, and mapped UNIX user name, respectively.

#### Steps

1. Add a home directory share:

```
vserver cifs share create -vserver vserver_name -share-name share_name -path  
path -share-properties homedirectory[,...]
```

`-vserver vserver` specifies the CIFS-enabled storage virtual machine (SVM) on which to add the search path.

`-share-name share-name` specifies the home directory share name.

In addition to containing one of the required variables, if the share name contains one of the literal strings `%w`, `%u`, or `%d`, you must precede the literal string with a `%` (percent) character to prevent ONTAP from treating the literal string as a variable (for example, `%%w`).

- The share name must contain either the `%w` or the `%u` variable.

- The share name can additionally contain the %d variable (for example, %d/%w) or a static portion in the share name (for example, home1\_%w).
- If the share is used by administrators to connect to other users' home directories or to permit users to connect to other users' home directories, the dynamic share name pattern must be preceded by a tilde (~).

The `vserver cifs home-directory modify` is used to enable this access by setting the `-is-home-dirs-access-for-admin-enabled` option to `true`) or by setting the advanced option `-is-home-dirs-access-for-public-enabled` to `true`.

`-path path` specifies the relative path to the home directory.

`-share-properties homedirectory[,...]` specifies the share properties for that share. You must specify the `homedirectory` value. You can specify additional share properties using a comma delimited list.

1. Verify that you successfully added the home directory share by using the `vserver cifs share show` command.

### Example

The following command creates a home directory share named %w. The `oplocks`, `browsable`, and `changenotify` share properties are set in addition to setting the `homedirectory` share property.



This example does not display output for all of the shares on the SVM. Output is truncated.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name %w -path %w
-share-properties oplocks,browsable,changenotify,homedirectory

vs1::> vserver cifs share show -vserver vs1
Vserver      Share      Path      Properties      Comment      ACL
-----
vs1          %w         %w         oplocks         -            Everyone / Full
Control
                                     browsable
                                     changenotify
                                     homedirectory
```

### Related information

[Adding a home directory search path](#)

[Requirements and guidelines for using automatic node referrals](#)

[Managing accessibility to users' home directories](#)

### Home directory shares require unique user names

Be careful to assign unique user names when creating home directory shares using the %w (Windows user name) or %u (UNIX user name) variables to generate shares dynamically. The share name is mapped to your user name.



Two problems can occur when a static share's name and a user's name are the same:

- When the user lists the shares on a cluster using the `net view` command, two shares with the same user name are displayed.
- When the user connects to that share name, the user is always connected to the static share and cannot access the home directory share with the same name.

For example, there is a share named “administrator” and you have an “administrator” Windows user name. If you create a home directory share and connect to that share, you get connected to the “administrator” static share, not to your “administrator” home directory share.

You can resolve the issue with duplicate share names by following any of these steps:

- Renaming the static share so that it no longer conflicts with the user's home directory share.
- Giving the user a new user name so that it no longer conflicts with the static share name.
- Creating a CIFS home directory share with a static name such as “home” instead of using the `%w` parameter to avoid conflicts with the share names.

### **What happens to static home directory share names after upgrading**

Home directory share names must contain either the `%w` or the `%u` dynamic variable. You should be aware of what happens to existing static home directory share names after upgrading to a version of ONTAP with the new requirement.

If your home directory configuration contains static share names and you upgrade to ONTAP, the static home directory share names are not changed and are still valid. However, you cannot create any new home directory shares that do not contain either the `%w` or `%u` variable.

Requiring that one of these variables is included in the user's home directory share name ensures that every share name is unique across the home directory configuration. If desired, you can change the static home directory share names to names that contain either the `%w` or `%u` variable.

### **Add a home directory search path**

If you want to use ONTAP SMB home directories, you must add at least one home directory search path.

#### **About this task**

You can add a home directory search path by using the `vserver cifs home-directory search-path add` command.

The `vserver cifs home-directory search-path add` command checks the path specified in the `-path` option during command execution. If the specified path does not exist, the command generates a message prompting for whether you want to continue. You choose `y` or `n`. If you choose `y` to continue, ONTAP creates the search path. However, you must create the directory structure before you can use the search path in the home directory configuration. If you choose not to continue, the command fails; the search path is not created. You can then create the path directory structure and rerun the `vserver cifs home-directory search-path add` command.

#### **Steps**

1. Add a home directory search path: `vserver cifs home-directory search-path add -vserver`

```
vserver -path path
```

2. Verify that you successfully added the search path using the `vserver cifs home-directory search-path show` command.

### Example

The following example adds the path `/home1` to the home directory configuration on SVM `vs1`.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

vs1::> vserver cifs home-directory search-path show
Vserver      Position Path
-----
vs1          1      /home1
```

The following example attempts to add the path `/home2` to the home directory configuration on SVM `vs1`. The path does not exist. The choice is made to not continue.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home2
Warning: The specified path "/home2" does not exist in the namespace
        belonging to Vserver "vs1".
Do you want to continue? {y|n}: n
```

### Related information

[Adding a home directory share](#)

#### Create a home directory configuration using the `%w` and `%d` variables

You can create a home directory configuration using the `%w` and `%d` variables. Users can then connect to their home share using dynamically created shares.

### Steps

1. Create a qtree to contain user's home directories: `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Verify that the qtree is using the correct security style: `volume qtree show`
3. If the qtree is not using the desired security style, change the security style using the `volume qtree security` command.
4. Add a home directory share: `vserver cifs share create -vserver vserver -share-name %w -path %d/%w -share-properties homedirectory\[,...\]`

`-vserver vserver` specifies the CIFS-enabled storage virtual machine (SVM) on which to add the search path.

`-share-name %w` specifies the home directory share name. ONTAP dynamically creates the share name

as each user connects to their home directory. The share name will be of the form *windows\_user\_name*.

`-path %d/%w` specifies the relative path to the home directory. The relative path is dynamically created as each user connects to their home directory and will be of the form *domain/windows\_user\_name*.

`-share-properties homedirectory[,...]+` specifies the share properties for that share. You must specify the *homedirectory* value. You can specify additional share properties using a comma delimited list.

5. Verify that the share has the desired configuration using the `vserver cifs share show` command.
6. Add a home directory search path: `vserver cifs home-directory search-path add -vserver vserver -path path`

`-vserver vserver-name` specifies the CIFS-enabled SVM on which to add the search path.

`-path path` specifies the absolute directory path to the search path.

7. Verify that you successfully added the search path using the `vserver cifs home-directory search-path show` command.
8. For users with a home directory, create a corresponding directory in the qtree or volume designated to contain home directories.

For example, if you created a qtree with the path of `/vol/vol1/users` and the user name whose directory you want to create is `mydomain\user1`, you would create a directory with the following path: `/vol/vol1/users/mydomain/user1`.

If you created a volume named "home1" mounted at `/home1`, you would create a directory with the following path: `/home1/mydomain/user1`.

9. Verify that a user can successfully connect to the home share either by mapping a drive or connecting using the UNC path.

For example, if user `mydomain\user1` wants to connect to the directory created in Step 8 that is located on SVM `vs1`, `user1` would connect using the UNC path `\\vs1\user1`.

## Example

The commands in the following example create a home directory configuration with the following settings:

- The share name is `%w`.
- The relative home directory path is `%d/%w`.
- The search path that is used to contain the home directories, `/home1`, is a volume configured with NTFS security style.
- The configuration is created on SVM `vs1`.

You can use this type of home directory configuration when users access their home directories from Windows hosts. You can also use this type of configuration when users access their home directories from Windows and UNIX hosts and the file system administrator uses Windows-based users and groups to control access to the file system.

```
cluster::> vsriver cifs share create -vsriver vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changenotify,homedirectory
```

```
cluster::> vsriver cifs share show -vsriver vs1 -share-name %w
```

```
                Vserver: vs1
                Share: %w
CIFS Server NetBIOS Name: VS1
                Path: %d/%w
    Share Properties: oplocks
                    browsable
                    changenotify
                    homedirectory
    Symlink Properties: enable
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
        Share Comment: -
            Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
        Volume Name: -
        Offline Files: manual
    Vscan File-Operations Profile: standard
```

```
cluster::> vsriver cifs home-directory search-path add -vsriver vs1 -path
/home1
```

```
cluster::> vsriver cifs home-directory search-path show
```

```
Vsriver      Position Path
-----
vs1          1          /home1
```

## Related information

[Configuring home directories using the %u variable](#)

[Additional home directory configurations](#)

[Displaying information about an SMB user's home directory path](#)

### Configure home directories using the %u variable

You can create a home directory configuration where you designate the share name using the %w variable but you use the %u variable to designate the relative path to the home directory share. Users can then connect to their home share using dynamically shares created using their Windows user name without being aware of the actual name or path of the home directory.

## Steps

1. Create a qtree to contain user's home directories: `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Verify that the qtree is using the correct security style: `volume qtree show`
3. If the qtree is not using the desired security style, change the security style using the `volume qtree security` command.
4. Add a home directory share: `vserver cifs share create -vserver vserver -share-name %w -path %u -share-properties homedirectory ,...]`

`-vserver vserver` specifies the CIFS-enabled storage virtual machine (SVM) on which to add the search path.

`-share-name %w` specifies the home directory share name. The share name is dynamically created as each user connects to their home directory and is of the form *windows\_user\_name*.



You can also use the `%u` variable for the `-share-name` option. This creates a relative share path that uses the mapped UNIX user name.

`-path %u` specifies the relative path to the home directory. The relative path is created dynamically as each user connects to their home directory and is of the form *mapped\_UNIX\_user\_name*.



The value for this option can contain static elements as well. For example, `eng/%u`.

`-share-properties homedirectory\[ ,... \]` specifies the share properties for that share. You must specify the `homedirectory` value. You can specify additional share properties using a comma delimited list.

5. Verify that the share has the desired configuration using the `vserver cifs share show` command.
6. Add a home directory search path: `vserver cifs home-directory search-path add -vserver vserver -path path`

`-vserver vserver` specifies the CIFS-enabled SVM on which to add the search path.

`-path path` specifies the absolute directory path to the search path.

7. Verify that you successfully added the search path using the `vserver cifs home-directory search-path show` command.
8. If the UNIX user does not exist, create the UNIX user using the `vserver services unix-user create` command.



The UNIX user name to which you map the Windows user name must exist before mapping the user.

9. Create a name mapping for the Windows user to the UNIX user using the following command: `vserver name-mapping create -vserver vserver_name -direction win-unix -priority integer -pattern windows_user_name -replacement unix_user_name`



If name mappings already exist that map Windows users to UNIX users, you do not have to perform the mapping step.

The Windows user name is mapped to the corresponding UNIX user name. When the Windows user connects to their home directory share, they connect to a dynamically created home directory with a share name that corresponds to their Windows user name without being aware that the directory name corresponds to the UNIX user name.

10. For users with a home directory, create a corresponding directory in the qtree or volume designated to contain home directories.

For example, if you created a qtree with the path of `/vol/vol1/users` and the mapped UNIX user name of the user whose directory you want to create is “unixuser1”, you would create a directory with the following path: `/vol/vol1/users/unixuser1`.

If you created a volume named “home1” mounted at `/home1`, you would create a directory with the following path: `/home1/unixuser1`.

11. Verify that a user can successfully connect to the home share either by mapping a drive or connecting using the UNC path.

For example, if user `mydomain\user1` maps to UNIX user `unixuser1` and wants to connect to the directory created in Step 10 that is located on SVM `vs1`, user1 would connect using the UNC path `\\vs1\user1`.

### Example

The commands in the following example create a home directory configuration with the following settings:

- The share name is `%w`.
- The relative home directory path is `%u`.
- The search path that is used to contain the home directories, `/home1`, is a volume configured with UNIX security style.
- The configuration is created on SVM `vs1`.

You can use this type of home directory configuration when users access their home directories from both Windows hosts or Windows and UNIX hosts and the file system administrator uses UNIX-based users and groups to control access to the file system.

```
cluster::> vsserver cifs share create -vsserver vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory
```

```
cluster::> vsserver cifs share show -vsserver vs1 -share-name %u
```

```
                Vserver: vs1
                Share: %w
CIFS Server NetBIOS Name: VS1
                Path: %u
Share Properties: oplocks
                  browsable
                  changenotify
                  homedirectory
Symlink Properties: enable
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: manual
Vscan File-Operations Profile: standard
```

```
cluster::> vsserver cifs home-directory search-path add -vsserver vs1 -path
/home1
```

```
cluster::> vsserver cifs home-directory search-path show -vsserver vs1
```

```
Vserver      Position Path
-----
vs1          1        /home1
```

```
cluster::> vsserver name-mapping create -vsserver vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1
```

```
cluster::> vsserver name-mapping show -pattern user1
```

```
Vserver      Direction Position
-----
vs1          win-unix  5        Pattern: user1
                    Replacement: unixuser1
```

## Related information

[Creating a home directory configuration using the %w and %d variables](#)

[Additional home directory configurations](#)

[Displaying information about an SMB user's home directory path](#)

## Additional home directory configurations

You can create additional home directory configurations using the %w, %d, and %u variables, which enables you to customize the home directory configuration to meet your needs.

You can create a number of home directory configurations using a combination of variables and static strings in the share names and search paths. The following table provides some examples illustrating how to create different home directory configurations:

Paths created when /vol1/user contains home directories...	Share command...
To create a share path \\vs1\~win_username that directs the user to /vol1/user/win_username	<pre>vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changenotify,homedirectory</pre>
To create a share path \\vs1\win_username that directs the user to /vol1/user/domain/win_username	<pre>vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,homedirectory</pre>
To create a share path \\vs1\win_username that directs the user to /vol1/user/unix_username	<pre>vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changenotify,homedirectory</pre>
To create a share path \\vs1\unix_username that directs the user to /vol1/user/unix_username	<pre>vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changenotify,homedirectory</pre>

## Commands for managing search paths

There are specific ONTAP commands for managing search paths for SMB home directory configurations. For example, there are commands for adding, removing, and displaying information about search paths. There is also a command for changing the search path order.

If you want to...	Use this command...
Add a search path	<pre>vserver cifs home-directory search-path add</pre>
Display search paths	<pre>vserver cifs home-directory search-path show</pre>



If you want to...	Use this command...
Change the search path order	<code>vserver cifs home-directory search-path reorder</code>
Remove a search path	<code>vserver cifs home-directory search-path remove</code>

See the man page for each command for more information.

### Display information about an SMB user's home directory path

You can display an SMB user's home directory path on the storage virtual machine (SVM), which can be used if you have multiple CIFS home directory paths configured and you want to see which path holds the user's home directory.

#### Step

1. Display the home directory path by using the `vserver cifs home-directory show-user` command.

```
vserver cifs home-directory show-user -vserver vs1 -username user1
```

Vserver	User	Home Dir Path
-----	-----	-----
vs1	user1	/home/user1

### Related information

[Managing accessibility to users' home directories](#)

#### Manage accessibility to users' home directories

By default, a user's home directory can be accessed only by that user. For shares where the dynamic name of the share is preceded with a tilde (~), you can enable or disable access to users' home directories by Windows administrators or by any other user (public access).

#### Before you begin

Home directory shares on the storage virtual machine (SVM) must be configured with dynamic share names that are preceded with a tilde (~). The following cases illustrate share naming requirements:

Home directory share name	Example of command to connect to the share
~%d~%w	<code>net use * \\IPAddress\~domain~user/u:credentials</code>
~%w	<code>net use * \\IPAddress\~user/u:credentials</code>

Home directory share name	Example of command to connect to the share
~abc~%w	net use * \\IPAddress\abc~user/u:credentials

## Step

1. Perform the appropriate action:

If you want to enable or disable access to users' home directories to...	Enter the following...
Windows administrators	<pre>vserver cifs home-directory modify -vserver vserver_name -is-home-dirs -access-for-admin-enabled {true false}</pre> <p>The default is true.</p>
Any user (public access)	<ol style="list-style-type: none"> <li>Set the privilege level to advanced:  <pre>set -privilege advanced</pre> </li> <li>Enable or disable access: <pre>vserver cifs home-directory modify -vserver vserver_name -is-home-dirs-access -for-public-enabled {true false}</pre> <p>The default is false.</p> </li> <li>Return to the admin privilege level:  <pre>set -privilege admin</pre> </li> </ol>

The following example enables public access to users' home directories:

```
set -privilege advanced
vserver cifs home-directory modify -vserver vs1 -is-home-dirs-access-for-public
-enabled true
set -privilege admin
```

## Related information

[Displaying information about an SMB user's home directory path](#)

## Configure SMB client access to UNIX symbolic links

**How ONTAP enables you to provide SMB client access to UNIX symbolic links**

A symbolic link is a file that is created in a UNIX environment that contains a reference to another file or directory. If a client accesses a symbolic link, the client is redirected to the target file or directory to which the symbolic link refers. ONTAP supports relative and absolute symbolic links, including widelinks (absolute links with targets outside the local file system).

ONTAP provides SMB clients the ability to follow UNIX symbolic links that are configured on the SVM. This feature is optional, and you can configure it on a per-share basis, using the `-symlink-properties` option of the `vserver cifs share create` command, with one of the following settings:

- Enabled with read/write access
- Enabled with read-only access
- Disabled by hiding symbolic links from SMB clients
- Disabled with no access to symbolic links from SMB clients

If you enable symbolic links on a share, relative symbolic links work without further configuration.

If you enable symbolic links on a share, absolute symbolic links do not work right away. You must first create a mapping between the UNIX path of the symbolic link to the destination SMB path. When creating absolute symbolic link mappings, you can specify whether it is a local link or a *widelink*; widelinks can be links to file systems on other storage devices or links to file systems hosted in separate SVMs on the same ONTAP system. When you create a widelink, it must include the information for the client to follow; that is, you create a reparse point for the client to discover the directory junction point. If you create an absolute symbolic link to a file or directory outside of the local share but set the locality to local, ONTAP disallows access to the target.



If a client attempts to delete a local symbolic link (absolute or relative), only the symbolic link is deleted, not the target file or directory. However, if a client attempts to delete a widelink, it might delete the actual target file or directory to which the widelink refers. ONTAP does not have control over this because the client can explicitly open the target file or directory outside the SVM and delete it.

#### • Reparse points and ONTAP file system services

A *reparse point* is an NTFS file system object that can be optionally stored on volumes along with a file. Reparse points provide SMB clients the ability to receive enhanced or extended file system services when working with NTFS style volumes. Reparse points consist of standard tags that identify the type of reparse point, and the content of the reparse point that can be retrieved by SMB clients for further processing by the client. Of the object types available for extended file system functionality, ONTAP implements support for NTFS symbolic links and directory junction points using reparse point tags. SMB clients that cannot understand the contents of a reparse point simply ignore it and don't provide the extended file system service that the reparse point might enable.

#### • Directory junction points and ONTAP support for symbolic links

Directory junction points are locations within a file system directory structure that can refer to alternate locations where files are stored, either on a different path (symbolic links) or a separate storage device (widelinks). ONTAP SMB servers expose directory junction points to Windows clients as reparse points, allowing capable clients to obtain reparse point contents from ONTAP when a directory junction point is traversed. They can thereby navigate and connect to different paths or storage devices as though they were part of the same file system.


#### • Enabling widelink support using reparse point options

The `-is-use-junctions-as-reparse-points-enabled` option is enabled by default in ONTAP 9. Not all SMB clients support widelinks, so the option to enable the information is configurable on a per-protocol version basis, allowing administrators to accommodate both supported and non-supported SMB clients. In ONTAP 9.2 and later releases, you must enable the option `-widelink-as-reparse-point-versions` for each client protocol that accesses the share using widelinks; the default is SMB1. In earlier releases, only widelinks accessed using the default SMB1 were reported, and systems using SMB2 or SMB3 were unable to access the widelinks.

For more information, see the Microsoft NTFS documentation.

### Limits when configuring UNIX symbolic links for SMB access

You need to be aware of certain limits when configuring UNIX symbolic links for SMB access.

Limit	Description
45	<p>Maximum length of the CIFS server name that you can specify when using an FQDN for the CIFS server name.</p> <p> You can alternatively specify the CIFS server name as a NetBIOS name, which is limited to 15 characters.</p>
80	<p>Maximum length of the share name.</p>
256	<p>Maximum length of the UNIX path that you can specify when creating a symbolic link or when modifying an existing symbolic link's UNIX path. The UNIX path must start with a "/" (slash) and end with a "/". Both the beginning and ending slashes count as part of the 256-character limit.</p>
256	<p>Maximum length of the CIFS path that you can specify when creating a symbolic link or when modifying an existing symbolic link's CIFS path. The CIFS path must start with a "/" (slash) and end with a "/". Both the beginning and ending slashes count as part of the 256-character limit.</p>

#### Related information

[Creating symbolic link mappings for SMB shares](#)

#### Control automatic DFS advertisements in ONTAP with a CIFS server option

A CIFS server option controls how DFS capabilities are advertised to SMB clients when connecting to shares. Because ONTAP uses DFS referrals when clients access symbolic links over SMB, you should be aware of what the impact is when disabling or enabling this option.

A CIFS server option determines whether the CIFS servers automatically advertise that they are DFS capable to SMB clients. By default, this option is enabled and the CIFS server always advertises that it is DFS capable to SMB clients (even when connecting to shares where access to symbolic links is disabled). If you want the CIFS server to advertise that it is DFS capable to clients only when they are connecting to shares where access to symbolic links is enabled, you can disable this option.

You should be aware of what happens when this option is disabled:

- The share configurations for symbolic links is unchanged.
- If the share parameter is set to allow symbolic link access (either read-write access or read-only access), the CIFS server advertises DFS capabilities to clients connecting to that share.

Client connections and access to symbolic links continue without interruption.

- If the share parameter is set to not allow symbolic link access (either by disabling access or if the value for the share parameter is null), the CIFS server does not advertise DFS capabilities to clients connecting to that share.

Because clients have cached information that the CIFS server is DFS capable and it is no longer advertising that it is, clients that are connected to shares where symbolic link access is disabled might not be able to access these shares after the CIFS server option is disabled. After the option is disabled, you might need to reboot clients that are connected to these shares, thus clearing the cached information.

These changes do not apply to SMB 1.0 connections.

### Configure UNIX symbolic link support on SMB shares

You can configure UNIX symbolic link support on SMB shares by specifying a symbolic link share-property setting when you create SMB shares or at any time by modifying existing SMB shares. UNIX symbolic link support is enabled by default. You can also disable UNIX symbolic link support on a share.

#### About this task

When configuring UNIX symbolic link support for SMB shares, you can choose one of the following settings:

Setting	Description
<code>enable</code> (DEPRECATED*)	Specifies that symbolic links are enabled for read-write access.
<code>read_only</code> (DEPRECATED*)	Specifies that symlinks are enabled for read-only access. This setting does not apply to widelinks. Widelink access is always read-write.
<code>hide</code> (DEPRECATED*)	Specifies that SMB clients are prevented from seeing symlinks.
<code>no-strict-security</code>	Specifies that clients follow symlinks outside of share boundaries.
<code>symlinks</code>	Specifies that symlinks are enabled locally for read-write access. The DFS advertisements are not generated even if the CIFS option <code>is-advertise-dfs-enabled</code> is set to <code>true</code> . This is the default setting.

Setting	Description
<code>symlinks-and-widelinks</code>	Specifies that both local symlinks and widelinks for read-write access. The DFS advertisements are generated for both local symlink and widelinks even if the CIFS option <code>is-advertise-dfs-enabled</code> is set to <code>false</code> .
<code>disable</code>	Specifies that symlinks and widelinks are disabled. The DFS advertisements are not generated even if the CIFS option <code>is-advertise-dfs-enabled</code> is set to <code>true</code> .
<code>""</code> (null, not set)	Disables symbolic links on the share.
<code>-</code> (not set)	Disables symbolic links on the share.



\*The *enable*, *hide*, and *read-only* parameters are deprecated and may be removed in a future release of ONTAP.

## Steps

1. Configure or disable symbolic link support:

If it is...	Enter...
A new SMB share	<pre>vserver cifs share create -vserver vserver_name -share-name share_name -path path -symlink-properties {enable hide read-only "" -  symlinks symlinks-and- widelinks disable},...</pre>
An existing SMB share	<pre>vserver cifs share modify -vserver vserver_name -share-name share_name -symlink-properties {enable hide read- only "" - symlinks symlinks-and- widelinks disable},...</pre>

2. Verify that the SMB share configuration is correct: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

## Example

The following command creates an SMB share named “data1” with the UNIX symbolic link configuration set to `enable`:

```

cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -symlink-properties enable

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                Vserver: vs1
                Share: data1
CIFS Server NetBIOS Name: VS1
                Path: /data1
                Share Properties: oplocks
                                browsable
                                changenotify
                Symlink Properties: enable
                File Mode Creation Mask: -
                Directory Mode Creation Mask: -
                Share Comment: -
                Share ACL: Everyone / Full Control
                File Attribute Cache Lifetime: -
                Volume Name: -
                Offline Files: manual
                Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
                UNIX Group for File Create: -

```

## Related information

[Creating symbolic link mappings for SMB shares](#)

### Create symbolic link mappings for SMB shares

You can create mappings of UNIX symbolic links for SMB shares. You can either create a relative symbolic link, which refers to the file or folder relative to its parent folder, or you can create an absolute symbolic link, which refers to the file or folder using an absolute path.

#### About this task

Widelinks are not accessible from Mac OS X clients if you use SMB 2.x. When a user attempts to connect to a share using widelinks from a Mac OS X client, the attempt fails. However, you can use widelinks with Mac OS X clients if you use SMB 1.

#### Steps

1. To create symbolic link mappings for SMB shares: `vserver cifs symlink create -vserver virtual_server_name -unix-path path -share-name share_name -cifs-path path [-cifs-server server_name] [-locality {local|free|widelink}] [-home-directory {true|false}]`  
  
`-vserver virtual_server_name` specifies the storage virtual machine (SVM) name.

`-unix-path path` specifies the UNIX path. The UNIX path must begin with a slash (/) and must end with a slash (/).

`-share-name share_name` specifies the name of the SMB share to map.

`-cifs-path path` specifies the CIFS path. The CIFS path must begin with a slash (/) and must end with a slash (/).

`-cifs-server server_name` specifies the CIFS server name. The CIFS server name can be specified as a DNS name (for example, `mynetwork.cifs.server.com`), IP address, or NetBIOS name. The NetBIOS name can be determined by using the `vserver cifs show` command. If this optional parameter is not specified, the default value is the NetBIOS name of the local CIFS server.

`-locality {local|free|widelink}` specifies whether to create a local link, a free link or a wide symbolic link. A local symbolic link maps to the local SMB share. A free symbolic link can map anywhere on the local SMB server. A wide symbolic link maps to any SMB share on the network. If you do not specify this optional parameter, the default value is `local`.

`-home-directory {true|false}` specifies whether the target share is a home directory. Even though this parameter is optional, you must set this parameter to `true` when the target share is configured as a home directory. The default is `false`.

## Example

The following command creates a symbolic link mapping on the SVM named `vs1`. It has the UNIX path `/src/`, the SMB share name "SOURCE", the CIFS path `/mycompany/source/`, and the CIFS server IP address `123.123.123.123`, and it is a `widelink`.

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /src/
-share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server
123.123.123.123 -locality widelink
```

## Related information

[Configuring UNIX symbolic link support on SMB shares](#)

## Commands for managing symbolic link mappings

There are specific ONTAP commands for managing symbolic link mappings.

If you want to...	Use this command...
Create a symbolic link mapping	<code>vserver cifs symlink create</code>
Display information about symbolic link mappings	<code>vserver cifs symlink show</code>
Modify a symbolic link mapping	<code>vserver cifs symlink modify</code>
Delete a symbolic link mapping	<code>vserver cifs symlink delete</code>



See the man page for each command for more information.

## **Use BranchCache to cache SMB share content at a branch office**

### **Use BranchCache to cache SMB share content at a branch office overview**

BranchCache was developed by Microsoft to enable caching of content on computers local to requesting clients. ONTAP implementation of BranchCache can reduce wide-area network (WAN) utilization and provide improved access response time when users in a branch office access content stored on storage virtual machines (SVMs) using SMB.

If you configure BranchCache, Windows BranchCache clients first retrieve content from the SVM and then cache the content on a computer within the branch office. If another BranchCache-enabled client in the branch office requests the same content, the SVM first authenticates and authorizes the requesting user. The SVM then determines whether the cached content is still up-to-date and, if it is, sends the client metadata about the cached content. The client then uses the metadata to retrieve content directly from the locally based cache.

### **Related information**

[Using offline files to allow caching of files for offline use](#)

### **Requirements and guidelines**

#### **BranchCache version support**

You should be aware of which BranchCache versions ONTAP supports.

ONTAP supports BranchCache 1 and the enhanced BranchCache 2:

- When you configure BranchCache on the SMB server for the storage virtual machine (SVM), you can enable BranchCache 1, BranchCache 2, or all versions.

By default, all versions are enabled.

- If you enable only BranchCache 2, the remote office Windows client machines must support BranchCache 2.

Only SMB 3.0 or later clients support BranchCache 2.

For more information about BranchCache versions, see the Microsoft TechNet Library.

### **Related information**

[Microsoft TechNet Library: technet.microsoft.com/en-us/library/](http://technet.microsoft.com/en-us/library/)

#### **Network protocol support requirements**

You must be aware of the network protocol requirements for implementing ONTAP BranchCache.

You can implement the ONTAP BranchCache feature over IPv4 and IPv6 networks using SMB 2.1 or later.

All CIFS servers and branch office machines participating in the BranchCache implementation must have the SMB 2.1 or later protocol enabled. SMB 2.1 has protocol extensions that allow a client to participate in a BranchCache environment. This is the minimum SMB protocol version that offers BranchCache support. SMB

2.1 supports version BranchCache version 1.

If you want to use BranchCache version 2, SMB 3.0 is the minimum supported version. All CIFS servers and branch office machines participating in a BranchCache 2 implementation must have SMB 3.0 or later enabled.

If you have remote offices where some of the clients support only SMB 2.1 and some of the clients support SMB 3.0, you can implement a BranchCache configuration on the CIFS server that provides caching support over both BranchCache 1 and BranchCache 2.



Even though the Microsoft BranchCache feature supports using both the HTTP/HTTPS and SMB protocols as file access protocols, ONTAP BranchCache only supports the use of SMB.

## **ONTAP and Windows hosts version requirements**

ONTAP and branch office Windows hosts must meet certain version requirements before you can configure BranchCache.

Before configuring BranchCache, you must ensure that the version of ONTAP on the cluster and participating branch office clients support SMB 2.1 or later and support the BranchCache feature. If you configure Hosted Cache mode, you must also ensure that you use a supported host for the cache server.

BranchCache 1 is supported on the following ONTAP versions and Windows hosts:

- Content server: storage virtual machine (SVM) with ONTAP
- Cache server: Windows Server 2008 R2 or Windows Server 2012 or later
- Peer or client: Windows 7 Enterprise, Windows 7 Ultimate, Windows 8, Windows Server 2008 R2 or Windows Server 2012 or later

BranchCache 2 is supported on the following ONTAP versions and Windows hosts:

- Content server: SVM with ONTAP
- Cache server: Windows Server 2012 or later
- Peer or client: Windows 8 or Windows Server 2012 or later

For the latest information about which Windows clients support BranchCache, see the Interoperability Matrix.

[mysupport.netapp.com/matrix](https://mysupport.netapp.com/matrix)

## **Reasons ONTAP invalidates BranchCache hashes**

Understanding the reasons why ONTAP invalidates hashes can be helpful as you plan your BranchCache configuration. It can help you decide which operating mode you should configure and can help you choose on which shares to enable BranchCache.

ONTAP must manage BranchCache hashes to ensure that hashes are valid. If a hash is not valid, ONTAP invalidates the hash and computes a new hash the next time that content is requested, assuming that BranchCache is still enabled.

ONTAP invalidates hashes for the following reasons:

- The server key is modified.

If the server key is modified, ONTAP invalidates all hashes in the hash store.

- A hash is flushed from the cache because the BranchCache hash store maximum size has been reached.

This is a tunable parameter and can be modified to meet your business requirements.

- A file is modified either through SMB or NFS access.
- A file for which there are computed hashes is restored using the `snap restore` command.
- A volume that contains SMB shares that are BranchCache-enabled is restored using the `snap restore` command.

## Guidelines for choosing the hash store location

When configuring BranchCache, you choose where to store hashes and what size the hash store should be. Understanding the guidelines when choosing the hash store location and size can help you plan your BranchCache configuration on a CIFS-enabled SVM.

- You should locate the hash store on a volume where atime updates are permitted.

The access time on a hash file is used to keep frequently accessed files in the hash store. If atime updates are disabled, the creation time is used for this purpose. It is preferable to use atime to track frequently used files.

- You cannot store hashes on read-only file systems such as SnapMirror destinations and SnapLock volumes.
- If the maximum size of the hash store is reached, older hashes are flushed to make room for new hashes.

You can increase the maximum size of the hash store to reduce the amount of hashes that are flushed from the cache.

- If the volume on which you store hashes is unavailable or full, or if there is an issue with intra-cluster communication where the BranchCache service cannot retrieve hash information, BranchCache services are not available.

The volume might be unavailable because it is offline or because the storage administrator specified a new location for the hash store.

This does not cause issues with file access. If access to the hash store is impeded, ONTAP returns a Microsoft-defined error to the client, which causes the client to request the file using the normal SMB read request.

## Related information

[Configure BranchCache on the SMB server](#)

[Modify the BranchCache configuration](#)

## BranchCache recommendations

Before you configure BranchCache, there are certain recommendations you should keep in mind when deciding on which SMB shares you want to enable BranchCache caching.

You should keep the following recommendations in mind when deciding on which operating mode to use and on which SMB shares to enable BranchCache:

- The benefits of BranchCache are reduced when the data to be remotely cached changes frequently.
- BranchCache services are beneficial for shares containing file content that is reused by multiple remote office clients or by file content that is repeatedly accessed by a single remote user.
- Consider enabling caching for read-only content such as data in Snapshot copies and SnapMirror destinations.

## **Configure BranchCache**

### **Configure BranchCache overview**

You configure BranchCache on your SMB server using ONTAP commands. To implement BranchCache, you must also configure your clients, and optionally your hosted cache servers at the branch offices where you want to cache content.

If you configure BranchCache to enable caching on a share-by-share basis, you must enable BranchCache on the SMB shares for which you want to provide BranchCache caching services.

### **Requirements for configuring BranchCache**

After meeting some prerequisites, you can set up BranchCache.

The following requirements must be met before configuring BranchCache on the CIFS server for your SVM:

- ONTAP must be installed on all nodes in the cluster.
- CIFS must be licensed and a CIFS server must be configured.
- IPv4 or IPv6 network connectivity must be configured.
- For BranchCache 1, SMB 2.1 or later must be enabled.
- For BranchCache 2, SMB 3.0 must be enabled and the remote Windows clients must support BranchCache 2.

### **Configure BranchCache on the SMB server**

You can configure BranchCache to provide BranchCache services on a per-share basis. Alternatively, you can configure BranchCache to automatically enable caching on all SMB shares.

#### **About this task**

You can configure BranchCache on SVMs.

- You can create an all-shares BranchCache configuration if you want to offer caching services for all content contained within all SMB shares on the CIFS server.
- You can create a per-share BranchCache configuration if you want to offer caching services for content contained within selected SMB shares on the CIFS server.

You must specify the following parameters when configuring BranchCache:

Required parameters	Description
<i>SVM name</i>	BranchCache is configured on a per SVM basis. You must specify on which CIFS-enabled SVM you want to configure the BranchCache service.
<i>Path to hash store</i>	<p>BranchCache hashes are stored in regular files on the SVM volume. You must specify the path to an existing directory where you want ONTAP to store the hash data. The BranchCache hash path must be read-writable. Read-only paths, such as Snapshot directories are not allowed. You can store hash data in a volume that contains other data or you can create a separate volume to store hash data.</p> <p>If the SVM is an SVM disaster recovery source, the hash path cannot be on the root volume. This is because the root volume is not replicated to the disaster recovery destination.</p> <p>The hash path can contain blanks and any valid file name characters.</p>

You can optionally specify the following parameters:

Optional parameters	Description
<i>Supported Versions</i>	ONTAP support BranchCache 1 and 2. You can enable version 1, version 2, or both versions. The default is to enable both versions.
<i>Maximum size of hash store</i>	<p>You can specify the size to use for the hash data store. If the hash data exceeds this value, ONTAP deletes older hashes to make room for newer hashes. The default size for the hash store is 1 GB.</p> <p>BranchCache performs more efficiently if hashes are not discarded in an overly aggressive manner. If you determine that hashes are discarded frequently because the hash store is full, you can increase the hash store size by modifying the BranchCache configuration.</p>

Optional parameters	Description
<i>Server key</i>	You can specify a server key that the BranchCache service uses to prevent clients from impersonating the BranchCache server. If you do not specify a server key, one is randomly generated when you create the BranchCache configuration. You can set the server key to a specific value so that if multiple servers are providing BranchCache data for the same files, clients can use hashes from any server using that same server key. If the server key contains any spaces, you must enclose the server key in quotation marks.
<i>Operating mode</i>	<p>The default is to enable BranchCache on a per-share basis.</p> <ul style="list-style-type: none"> <li>• To create a BranchCache configuration where you enable BranchCache on a per-share basis, you can either not specify this optional parameter or you can specify <code>per-share</code>.</li> <li>• To automatically enable BranchCache on all shares, you must set the operating mode to <code>all-shares</code>.</li> </ul>

## Steps

1. Enable SMB 2.1 and 3.0 as needed:

- a. Set the privilege level to advanced: `set -privilege advanced`
- b. Check the configured SVM SMB settings to determine whether all needed versions of SMB are enabled: `vserver cifs options show -vserver vserver_name`
- c. If necessary, enable SMB 2.1: `vserver cifs options modify -vserver vserver_name -smb2-enabled true`

The command enables both SMB 2.0 and SMB 2.1.

- d. If necessary, enable SMB 3.0: `vserver cifs options modify -vserver vserver_name -smb3-enabled true`
- e. Return to the admin privilege level: `set -privilege admin`

2. Configure BranchCache: `vserver cifs branchcache create -vserver vserver_name -hash -store-path path [-hash-store-max-size {integer[KB|MB|GB|TB|PB]}] [-versions {v1-enable|v2-enable|enable-all}] [-server-key text] -operating-mode {per-share|all-shares}`

The specified hash storage path must exist and must reside on a volume managed by the SVM. The path must also be located on a read-writable volume. The command fails if the path is read-only or does not exist.

If you want to use the same server key for additional SVM BranchCache configurations, record the value you enter for the server key. The server key does not appear when you display information about the BranchCache configuration.

3. Verify that the BranchCache configuration is correct: `vserver cifs branchcache show -vserver vserver_name`

### Examples

The following commands verify that both SMB 2.1 and 3.0 are enabled and configure BranchCache to automatically enable caching on all SMB shares on SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
-----
vs1      true      true

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
Supported BranchCache Versions: enable_all
                                Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: all_shares
```

The following commands verify that both SMB 2.1 and 3.0 are enabled, configure BranchCache to enable caching on a per-share basis on SVM vs1, and verify the BranchCache configuration:

```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vsserver cifs options show -vsserver vs1 -fields smb2-
enabled,smb3-enabled
vsserver smb2-enabled smb3-enabled
-----
vs1      true      true

cluster1::*> set -privilege admin

cluster1::> vsserver cifs branchcache create -vsserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key"

cluster1::> vsserver cifs branchcache show -vsserver vs1

                                Vserver: vs1
Supported BranchCache Versions: enable_all
                                Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: per_share

```

## Related information

[Requirements and guidelines: BranchCache version support](#)

[Where to find information about configuring BranchCache at the remote office](#)

[Create a BranchCache-enabled SMB share](#)

[Enable BranchCache on an existing SMB share](#)

[Modify the BranchCache configuration](#)

[Disable BranchCache on SMB shares overview](#)

[Delete the BranchCache configuration on SVMs](#)

## Where to find information about configuring BranchCache at the remote office

After configuring BranchCache on the SMB server, you must install and configure BranchCache on client computers and, optionally, on caching servers at your remote office. Microsoft provides instructions for configuring BranchCache at the remote office.

Instructions for configuring branch office clients and, optionally, caching servers to use BranchCache are on



the Microsoft BranchCache web site.

[Microsoft BranchCache Docs: What's New](#)

## Configure BranchCache-enabled SMB shares

### Configure BranchCache-enabled SMB shares overview

After you configure BranchCache on the SMB server and at the branch office, you can enable BranchCache on SMB shares that contain content that you want to allow clients at branch offices to cache.

BranchCache caching can be enabled on all SMB shares on the SMB server or on a share-by-share basis.

- If you enable BranchCache on a share-by-share basis, you can enable BranchCache as you create the share or by modifying existing shares.

If you enable caching on an existing SMB share, ONTAP begins computing hashes and sending metadata to clients requesting content as soon as you enable BranchCache on that share.

- Any clients that have an existing SMB connection to a share do not get BranchCache support if BranchCache is subsequently enabled on that share.

ONTAP advertises BranchCache support for a share at the time the SMB session is set up. Clients that already have established sessions when BranchCache is enabled need to disconnect and reconnect to use cached content for this share.



If BranchCache on a SMB share is subsequently disabled, ONTAP stops sending metadata to the requesting client. A client that needs data retrieves it directly from the content server (SMB server).

### Create a BranchCache-enabled SMB share

You can enable BranchCache on an SMB share when you create the share by setting the `branchcache` share property.

#### About this task

- If BranchCache is enabled on the SMB share, the share must have the offline files configuration set to manual caching.

This is the default setting when you create a share.

- You can also specify additional optional share parameters when you create the BranchCache-enabled share.
- You can set the `branchcache` property on a share even if BranchCache is not configured and enabled on the storage virtual machine (SVM).

However, if you want the share to offer cached content, you must configure and enable BranchCache on the SVM.

- Since there are no default share properties applied to the share when you use the `-share-properties` parameter, you must specify all other share properties that you want applied to the share in addition to the

branchcache share property by using a comma-delimited list.

- For more information, see the man page for the `vserver cifs share create` command.

## Step

1. Create a BranchCache-enabled SMB share:

```
vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties branchcache[,...]
```

2. Verify that the BranchCache share property is set on the SMB share by using the `vserver cifs share show` command.

## Example

The following command creates a BranchCache-enabled SMB share named “data” with a path of `/data` on SVM vs1. By default, the offline files setting is set to manual:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data -path /data -share-properties branchcache,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name data
          Vserver: vs1
          Share: data
CIFS Server NetBIOS Name: VS1
          Path: /data
    Share Properties: branchcache
                    oplocks
                    browsable
                    changenotify
    Symlink Properties: enable
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
          Share Comment: -
          Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
          Volume Name: data
          Offline Files: manual
    Vscan File-Operations Profile: standard
```

## Related information

[Disabling BranchCache on a single SMB share](#)

## Enable BranchCache on an existing SMB share

You can enable BranchCache on an existing SMB share by adding the `branchcache` share property to the existing list of share properties.

## About this task

- If BranchCache is enabled on the SMB share, the share must have the offline files configuration set to

manual caching.

If the existing share's offline files setting is not set to manual caching, you must configure it by modifying the share.

- You can set the `branchcache` property on a share even if BranchCache is not configured and enabled on the storage virtual machine (SVM).

However, if you want the share to offer cached content, you must configure and enable BranchCache on the SVM.

- When you add the `branchcache` share property to the share, existing share settings and share properties are preserved.

The BranchCache share property is added to the existing list of share properties. For more information about using the `vserver cifs share properties add` command, see the man pages.

### Steps

1. If necessary, configure the offline files share setting for manual caching:
  - a. Determine what the offline files share setting is by using the `vserver cifs share show` command.
  - b. If the offline files share setting is not set to manual, change it to the required value: `vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files manual`
2. Enable BranchCache on an existing SMB share: `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties branchcache`
3. Verify that the BranchCache share property is set on the SMB share: `vserver cifs share show -vserver vserver_name -share-name share_name`

### Example

The following command enables BranchCache on an existing SMB share named "data2" with a path of /data2 on SVM vs1:

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2
```

```
          Vserver: vs1
          Share: data2
CIFS Server NetBIOS Name: VS1
          Path: /data2
    Share Properties: oplocks
                    browsable
                    changenotify
                    showsnapshot
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
          Share Comment: -
          Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
          Volume Name: -
          Offline Files: manual
Vscan File-Operations Profile: standard
```

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
data2 -share-properties branchcache
```

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2
```

```
          Vserver: vs1
          Share: data2
CIFS Server NetBIOS Name: VS1
          Path: /data2
    Share Properties: oplocks
                    browsable
                    showsnapshot
                    changenotify
                    branchcache
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
          Share Comment: -
          Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
          Volume Name: -
          Offline Files: manual
Vscan File-Operations Profile: standard
```

## Related information

[Adding or removing share properties on an existing SMB share](#)

[Disabling BranchCache on a single SMB share](#)

**Manage and monitor the BranchCache configuration**


### **Modify BranchCache configurations**

You can modify the configuration of the BranchCache service on SVMs, including changing the hash store directory path, the hash store maximum directory size, the operating mode, and which BranchCache versions are supported. You can also increase the size of the volume that contains the hash store.

#### **Steps**

1. Perform the appropriate action:

<b>If you want to...</b>	<b>Enter the following...</b>
Modify the hash store directory size	<pre>vserver cifs branchcache modify -vserver vserver_name -hash-store-max -size {integer[KB MB GB TB PB]}</pre>
Increase the size of the volume that contains the hash store	<pre>volume size -vserver vserver_name -volume volume_name -new-size new_size[k m g t]</pre> <p>If the volume containing the hash store fills up, you might be able to increase the size of the volume. You can specify the new volume size as a number followed by a unit designation.</p> <p>See <a href="#">Logical storage management</a> for more information about increasing volume size.</p>

If you want to...	Enter the following...
Modify the hash store directory path	<pre>vserver cifs branchcache modify -vserver vserver_name -hash-store-path path -flush-hashes {true false}</pre> <p>If the SVM is an SVM disaster recovery source, the hash path cannot be on the root volume. This is because the root volume is not replicated to the disaster recovery destination.</p> <p>The BranchCache hash path can contain blanks and any valid file name characters.</p> <p>If you modify the hash path, <code>-flush-hashes</code> is a required parameter that specifies whether you want ONTAP to flush the hashes from the original hash store location. You can set the following values for the <code>-flush-hashes</code> parameter:</p> <ul style="list-style-type: none"> <li>• If you specify <code>true</code>, ONTAP deletes the hashes in the original location and creates new hashes in the new location as new requests are made by BranchCache-enabled clients.</li> <li>• If you specify <code>false</code>, the hashes are not flushed.</li> </ul> <p>In this case, you can choose to reuse the existing hashes later by changing the hash store path back to the original location.</p>
Change the operating mode	<pre>vserver cifs branchcache modify -vserver vserver_name -operating-mode {per-share all-shares disable}</pre> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> You should be aware of the following when modifying the operating mode:</p> <ul style="list-style-type: none"> <li>- ONTAP advertises BranchCache support for a share when the SMB session is set up.</li> <li>- Clients that already have established sessions when BranchCache is enabled need to disconnect and reconnect to use cached content for this share.</li> </ul> </div>
Change the BranchCache version support	<pre>vserver cifs branchcache modify -vserver vserver_name -versions {v1- enable v2-enable enable-all}</pre>

2. Verify the configuration changes by using the `vserver cifs branchcache show` command.

## Related information

[Logical Storage Management Guide](#)

## Display information about BranchCache configurations

You can display information about BranchCache configurations on storage virtual machines (SVMs), which can be used when verifying a configuration or when determining current settings before modifying a configuration.

### Step

1. Perform one of the following actions:

If you want to display...	Enter this command...
Summary information about BranchCache configurations on all SVMs	<code>vserver cifs branchcache show</code>
Detailed information about the configuration on a specific SVM	<code>vserver cifs branchcache show -vserver <i>vserver_name</i></code>

### Example

The following example displays information about the BranchCache configuration on SVM vs1:

```
cluster1::> vserver cifs branchcache show -vserver vs1

                Vserver: vs1
Supported BranchCache Versions: enable_all
                Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: per_share
```

## Change the BranchCache server key

You can change the BranchCache server key by modifying the BranchCache configuration on the storage virtual machine (SVM) and specifying a different server key.

### About this task

You can set the server key to a specific value so that if multiple servers are providing BranchCache data for the same files, clients can use hashes from any server using that same server key.

When you change the server key, you must also flush the hash cache. After flushing the hashes, ONTAP creates new hashes as new requests are made by BranchCache-enabled clients.

### Steps

1. Change the server key by using the following command: `vserver cifs branchcache modify -vserver vserver_name -server-key text -flush-hashes true`

When configuring a new server key, you must also specify `-flush-hashes` and set the value to `true`.

2. Verify that the BranchCache configuration is correct by using the `vserver cifs branchcache show` command.

### Example

The following example sets a new server key that contains spaces and flushes the hash cache on SVM vs1:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new
vserver secret" -flush-hashes true

cluster1::> vserver cifs branchcache show -vserver vs1

                Vserver: vs1
Supported BranchCache Versions: enable_all
                Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: per_share
```

### Related information

[Reasons ONTAP invalidates BranchCache hashes](#)

### Pre-compute BranchCache hashes on specified paths

You can configure the BranchCache service to pre-compute hashes for a single file, for a directory, or for all files in a directory structure. This can be helpful if you want to compute hashes on data in a BranchCache-enabled share during off, non-peak hours.

#### About this task

If you want to collect a data sample before you display hash statistics, you must use the `statistics start` and optional `statistics stop` commands.

- You must specify the storage virtual machine (SVM) and path on which you want to pre-compute hashes.
- You must also specify whether you want hashes computed recursively.
- If you want hashes computed recursively, the BranchCache service traverses the entire directory tree under the specified path, and computes hashes for each eligible object.

### Steps

1. Pre-compute hashes as desired:

If you want to pre-compute hashes on...	Enter the command...
A single file or directory	<pre>vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse false</pre>



If you want to pre-compute hashes on...	Enter the command...
Recursively on all files in a directory structure	<pre>vserver cifs branchcache hash-create -vserver vserver_name -path absolute_path -recurse true</pre>

2. Verify that hashes are being computed by using the `statistics` command:

- a. Display statistics for the `hashd` object on the desired SVM instance: `statistics show -object hashd -instance vserver_name`
- b. Verify that the number of hashes created is increasing by repeating the command.

### Examples

The following example creates hashes on the path `/data` and on all contained files and subdirectories on SVM vs1:

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data
-recurse true
```

```
cluster1::> statistics show -object hashd -instance vs1
```

```
Object: hashd
```

```
Instance: vs1
```

```
Start-time: 9/6/2012 19:09:54
```

```
End-time: 9/6/2012 19:11:15
```

```
Cluster: cluster1
```

Counter	Value
-----	-----
branchcache_hash_created	85
branchcache_hash_files_replaced	0
branchcache_hash_rejected	0
branchcache_hash_store_bytes	0
branchcache_hash_store_size	0
instance_name	vs1
node_name	node1
node_uuid	11111111-1111-1111-1111-111111111111
process_name	-

```
cluster1::> statistics show -object hashd -instance vs1
```

```
Object: hashd
```

```
Instance: vs1
```

```
Start-time: 9/6/2012 19:09:54
```

```
End-time: 9/6/2012 19:11:15
```

```
Cluster: cluster1
```

Counter	Value
-----	-----
branchcache_hash_created	92
branchcache_hash_files_replaced	0
branchcache_hash_rejected	0
branchcache_hash_store_bytes	0
branchcache_hash_store_size	0
instance_name	vs1
node_name	node1
node_uuid	11111111-1111-1111-1111-111111111111
process_name	-

## Related information

[Performance monitoring setup](#)

## Flush hashes from the SVM BranchCache hash store

You can flush all cached hashes from the BranchCache hash store on the storage virtual machine (SVM). This can be useful if you have changed the branch office BranchCache configuration. For example, if you recently reconfigured the caching mode from distributed caching to hosted caching mode, you would want to flush the hash store.

### About this task

After flushing the hashes, ONTAP creates new hashes as new requests are made by BranchCache-enabled clients.

### Step

1. Flush the hashes from the BranchCache hash store: `vserver cifs branchcache hash-flush -vserver vserver_name`

```
vserver cifs branchcache hash-flush -vserver vs1
```

## Display BranchCache statistics

You can display BranchCache statistics to, among other things, identify how well caching is performing, determine whether your configuration is providing cached content to clients, and determine whether hash files were deleted to make room for more recent hash data.

### About this task

The `hashd` statistic object contains counters that provide statistical information about BranchCache hashes. The `cifs` statistic object contains counters that provide statistical information about BranchCache-related activity. You can collect and display information about these objects at the advanced-privilege level.

### Steps

1. Set the privilege level to advanced: `set -privilege advanced`

```
cluster1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them  
only when directed to do so by support personnel.
```

```
Do you want to continue? {y|n}: y
```

2. Display the BranchCache-related counters by using the `statistics catalog counter show` command.

For more information about statistics counters, see the man page for this command.

```
cluster1::*> statistics catalog counter show -object hashd
```

```
Object: hashd
```

```
Counter
```

```
Description
```

```

-----
branchcache_hash_created      Number of times a request to generate
                               BranchCache hash for a file succeeded.
branchcache_hash_files_replaced
                               Number of times a BranchCache hash file
was
                               deleted to make room for more recent
hash
                               data. This happens if the hash store
size is
                               exceeded.
branchcache_hash_rejected     Number of times a request to generate
                               BranchCache hash data failed.
branchcache_hash_store_bytes  Total number of bytes used to store hash
data.
branchcache_hash_store_size  Total space used to store BranchCache
hash
                               data for the Vserver.
instance_name                 Instance Name
instance_uuid                 Instance UUID
node_name                     System node name
node_uuid                     System node id
9 entries were displayed.

```

```
cluster1::*> statistics catalog counter show -object cifs
```

```
Object: cifs
```

Counter	Description
active_searches	Number of active searches over SMB and SMB2
auth_reject_too_many	Authentication refused after too many requests were made in rapid succession
avg_directory_depth	Average number of directories crossed by SMB and SMB2 path-based commands
avg_junction_depth	Average number of junctions crossed by SMB and SMB2 path-based commands
branchcache_hash_fetch_fail	Total number of times a request to fetch hash data failed. These are failures when attempting to read existing hash data.

```

It
data
branchcache_hash_fetch_ok
hash
branchcache_hash_sent_bytes
branchcache_missing_hash_bytes
to be
that
.....Output truncated.....

```

does not include attempts to fetch hash data that has not yet been generated.

Total number of times a request to fetch hash data succeeded.

Total number of bytes sent to clients requesting hashes.

Total number of bytes of data that had to be read by the client because the hash for that content was not available on the server.

3. Collect BranchCache-related statistics by using the `statistics start` and `statistics stop` commands.

```

cluster1::*> statistics start -object cifs -vserver vs1 -sample-id 11
Statistics collection is being started for Sample-id: 11

cluster1::*> statistics stop -sample-id 11
Statistics collection is being stopped for Sample-id: 11

```

4. Display the collected BranchCache statistics by using the `statistics show` command.

```
cluster1::*> statistics show -object cifs -counter  
branchcache_hash_sent_bytes -sample-id 11
```

```
Object: cifs  
Instance: vs1  
Start-time: 12/26/2012 19:50:24  
End-time: 12/26/2012 19:51:01  
Cluster: cluster1
```

Counter	Value
branchcache_hash_sent_bytes	0
branchcache_hash_sent_bytes	0
branchcache_hash_sent_bytes	0
branchcache_hash_sent_bytes	0

```
cluster1::*> statistics show -object cifs -counter  
branchcache_missing_hash_bytes -sample-id 11
```

```
Object: cifs  
Instance: vs1  
Start-time: 12/26/2012 19:50:24  
End-time: 12/26/2012 19:51:01  
Cluster: cluster1
```

Counter	Value
branchcache_missing_hash_bytes	0
branchcache_missing_hash_bytes	0
branchcache_missing_hash_bytes	0
branchcache_missing_hash_bytes	0

5. Return to the admin privilege level: `set -privilege admin`

```
cluster1::*> set -privilege admin
```

## Related information

[Displaying statistics](#)

[Performance monitoring setup](#)

## Support for BranchCache Group Policy Objects

ONTAP BranchCache provides support for BranchCache Group Policy Objects (GPOs),

which allow centralized management for certain BranchCache configuration parameters. There are two GPOs used for BranchCache, the Hash Publication for BranchCache GPO and the Hash Version Support for BranchCache GPO.

- **Hash Publication for BranchCache GPO**

The Hash Publication for BranchCache GPO corresponds to the `-operating-mode` parameter. When GPO updates occur, this value is applied to storage virtual machine (SVM) objects contained within the organizational unit (OU) to which the group policy applies.

- **Hash Version Support for BranchCache GPO**

The Hash Version Support for BranchCache GPO corresponds to the `-versions` parameter. When GPO updates occur, this value is applied to SVM objects contained within the organizational unit to which the group policy applies.

## Related information

[Applying Group Policy Objects to CIFS servers](#)

## Display information about BranchCache Group Policy Objects

You can display information about the CIFS server's Group Policy Object (GPO) configuration to determine whether BranchCache GPOs are defined for the domain to which the CIFS server belongs and, if so, what the allowed settings are. You can also determine whether BranchCache GPO settings are applied to the CIFS server.

### About this task

Even though a GPO setting is defined within the domain to which the CIFS server belongs, it is not necessarily applied to the organizational unit (OU) containing the CIFS-enabled storage virtual machine (SVM). Applied GPO settings are the subset of all defined GPOs that are applied to the CIFS-enabled SVM. BranchCache settings applied through GPOs override settings applied through the CLI.

### Steps

1. Display the defined BranchCache GPO setting for the Active Directory domain by using the `vserver cifs group-policy show-defined` command.



This example does not display all of the available output fields for the command. Output is truncated.

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1
```

```
Vserver: vs1
```

```
-----  
      GPO Name: Default Domain Policy  
      Level: Domain  
      Status: enabled  
Advanced Audit Settings:  
  Object Access:  
    Central Access Policy Staging: failure  
Registry Settings:  
  Refresh Time Interval: 22  
  Refresh Random Offset: 8  
  Hash Publication Mode for BranchCache: per-share  
  Hash Version Support for BranchCache: version1  
[...]  
  
      GPO Name: Resultant Set of Policy  
      Status: enabled  
Advanced Audit Settings:  
  Object Access:  
    Central Access Policy Staging: failure  
Registry Settings:  
  Refresh Time Interval: 22  
  Refresh Random Offset: 8  
  Hash Publication for Mode BranchCache: per-share  
  Hash Version Support for BranchCache: version1  
[...]
```

2. Display the BranchCache GPO setting applied to the CIFS server by using the `vserver cifs group-policy show-applied` command. ``



This example does not display all of the available output fields for the command. Output is truncated.



```
cluster1::> vserver cifs group-policy show-applied -vserver vs1
```

```
Vserver: vs1
```

```
-----
```

```
  GPO Name: Default Domain Policy
```

```
    Level: Domain
```

```
    Status: enabled
```

```
Advanced Audit Settings:
```

```
  Object Access:
```

```
    Central Access Policy Staging: failure
```

```
Registry Settings:
```

```
  Refresh Time Interval: 22
```

```
  Refresh Random Offset: 8
```

```
  Hash Publication Mode for BranchCache: per-share
```

```
  Hash Version Support for BranchCache: version1
```

```
[...]
```

```
  GPO Name: Resultant Set of Policy
```

```
    Level: RSOP
```

```
Advanced Audit Settings:
```

```
  Object Access:
```

```
    Central Access Policy Staging: failure
```

```
Registry Settings:
```

```
  Refresh Time Interval: 22
```

```
  Refresh Random Offset: 8
```

```
  Hash Publication Mode for BranchCache: per-share
```

```
  Hash Version Support for BranchCache: version1
```

```
[...]
```

## Related information

[Enabling or disabling GPO support on a CIFS server](#)

### Disable BranchCache on SMB shares

### Disable BranchCache on SMB shares overview

If you do not want to provide BranchCache caching services on certain SMB shares but you might want to provide caching services on those shares later, you can disable BranchCache on a share-by-share basis. If you have BranchCache configured to offer caching on all shares but you want to temporarily disable all caching services, you can modify the BranchCache configuration to stop automatic caching on all shares.

If BranchCache on an SMB share is subsequently disabled after first being enabled, ONTAP stops sending metadata to the requesting client. A client that needs data retrieves it directly from the content server (CIFS server on the storage virtual machine (SVM)).

## Related information

[Configuring BranchCache-enabled SMB shares](#)

### Disable BranchCache on a single SMB share

If you do not want to offer caching services on certain shares that previously offered cached content, you can disable BranchCache on an existing SMB share.

#### Step

1. Enter the following command: `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties branchcache`

The BranchCache share property is removed. Other applied share properties remain in effect.

#### Example

The following command disables BranchCache on an existing SMB share named “data2”:

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2
```

```
        Vserver: vs1
        Share: data2
CIFS Server NetBIOS Name: VS1
        Path: /data2
    Share Properties: oplocks
                    browsable
                    changenotify
                    attributecache
                    branchcache
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
        Share Comment: -
            Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
        Volume Name: -
        Offline Files: manual
Vscan File-Operations Profile: standard
```

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
data2 -share-properties branchcache
```

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2
```

```
        Vserver: vs1
        Share: data2
CIFS Server NetBIOS Name: VS1
        Path: /data2
    Share Properties: oplocks
                    browsable
                    changenotify
                    attributecache
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
        Share Comment: -
            Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
        Volume Name: -
        Offline Files: manual
Vscan File-Operations Profile: standard
```

## Stop automatic caching on all SMB shares

If your BranchCache configuration automatically enables caching on all SMB shares on each storage virtual machine (SVM), you can modify the BranchCache configuration to stop automatically caching content for all SMB shares.

### About this task

To stop automatic caching on all SMB shares, you change the BranchCache operating mode to per-share caching.

### Steps

1. Configure BranchCache to stop automatic caching on all SMB shares: `vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
2. Verify that the BranchCache configuration is correct: `vserver cifs branchcache show -vserver vserver_name`

### Example

The following command changes the BranchCache configuration on storage virtual machine (SVM, formerly known as Vserver) vs1 to stop automatic caching on all SMB shares:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
per-share

cluster1::> vserver cifs branchcache show -vserver vs1

                Vserver: vs1
Supported BranchCache Versions: enable_all
                Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: per_share
```

## Disable or enable BranchCache on the SVM

### What happens when you disable or reenables BranchCache on the CIFS server

If you previously configured BranchCache but do not want the branch office clients to use cached content, you can disable caching on the CIFS server. You must be aware of what happens when you disable BranchCache.

When you disable BranchCache, ONTAP no longer computes hashes or sends the metadata to the requesting client. However, there is no interruption to file access. Thereafter, when BranchCache-enabled clients request metadata information for content they want to access, ONTAP responds with a Microsoft-defined error, which causes the client to send a second request, requesting the actual content. In response to the request for content, the CIFS server sends the actual content that is stored on the storage virtual machine (SVM).

After BranchCache is disabled on the CIFS server, SMB shares do not advertise BranchCache capabilities. To access data on new SMB connections, clients make normal read SMB requests.

You can reenable BranchCache on the CIFS server at any time.

- Because the hash store is not deleted when you disable BranchCache, ONTAP can use the stored hashes when replying to hash requests after you reenable BranchCache, provided that the requested hash is still valid.
- Any clients that have made SMB connections to BranchCache-enabled shares during the time when BranchCache was disabled do not get BranchCache support if BranchCache is subsequently reenabled.

This is because ONTAP advertises BranchCache support for a share at the time the SMB session is set up. Clients that established sessions to BranchCache-enabled shares while BranchCache was disabled need to disconnect and reconnect to use cached content for this share.



If you do not want to save the hash store after you disable BranchCache on a CIFS server, you can manually delete it. If you reenable BranchCache, you must ensure that the hash store directory exists. After BranchCache is reenabled, BranchCache-enabled shares advertise BranchCache capabilities. ONTAP creates new hashes as new requests are made by BranchCache-enabled clients.

### Disable or enable BranchCache

You can disable BranchCache on the storage virtual machine (SVM) by changing the BranchCache operating mode to `disabled`. You can enable BranchCache at any time by changing the operating mode to either offer BranchCache services per-share or automatically for all shares.

#### Steps

1. Run the appropriate command:

If you want to...	Then enter the following...
Disable BranchCache	<pre>vserver cifs branchcache modify -vserver vserver_name -operating-mode disable</pre>
Enable BranchCache per share	<pre>vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share</pre>
Enable BranchCache for all shares	<pre>vserver cifs branchcache modify -vserver vserver_name -operating-mode all-shares</pre>

2. Verify that the BranchCache operating mode is configured with the desired setting: 

```
vserver cifs  
branchcache show -vserver vserver_name
```

#### Example

The following example disables BranchCache on SVM vs1:

```

cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
disable

cluster1::> vserver cifs branchcache show -vserver vs1

                Vserver: vs1
Supported BranchCache Versions: enable_all
                Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: disable

```

### Delete the BranchCache configuration on SVMs

#### What happens when you delete the BranchCache configuration

If you previously configured BranchCache but do not want the storage virtual machine (SVM) to continue providing cached content, you can delete the BranchCache configuration on the CIFS server. You must be aware of what happens when you delete the configuration.

When you delete the configuration, ONTAP removes the configuration information for that SVM from the cluster and stops the BranchCache service. You can choose whether ONTAP should delete the hash store on the SVM.

Deleting the BranchCache configuration does not disrupt access by BranchCache-enabled clients. Thereafter, when BranchCache-enabled clients request metadata information on existing SMB connections for content that is already cached, ONTAP responds with a Microsoft defined error, which causes the client to send a second request, requesting the actual content. In response to the request for content, the CIFS server sends the actual content that is stored on the SVM.

After the BranchCache configuration is deleted, SMB shares do not advertise BranchCache capabilities. To access content that has not previously been cached using new SMB connections, clients make normal read SMB requests.

#### Delete the BranchCache configuration

The command you use for deleting the BranchCache service on your storage virtual machine (SVM) differs depending on whether you want to delete or keep existing hashes.

##### Step

1. Run the appropriate command:

If you want to...	Then enter the following...
Delete the BranchCache configuration and delete existing hashes	<pre> vserver cifs branchcache delete -vserver vserver_name -flush-hashes true </pre>

If you want to...	Then enter the following...
Delete the BranchCache configuration but keep existing hashes	<pre>vserver cifs branchcache delete -vserver vserver_name -flush-hashes false</pre>

### Example

The following example deletes the BranchCache configuration on SVM vs1 and deletes all existing hashes:

```
cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes
true
```

### What happens to BranchCache when reverting

It is important to understand what happens when you revert ONTAP to a release that does not support BranchCache.

- When you revert to a version of ONTAP that does not support BranchCache, the SMB shares do not advertise BranchCache capabilities to BranchCache-enabled clients; therefore, the clients do not request hash information.

Instead, they request the actual content using normal SMB read requests. In response to the request for content, the SMB server sends the actual content that is stored on the storage virtual machine (SVM).

- When a node hosting a hash store is reverted to a release that does not support BranchCache, the storage administrator needs to manually revert the BranchCache configuration using a command that is printed out during the revert.

This command deletes the BranchCache configuration and hashes.

After the revert completes, the storage administrator can manually delete the directory that contained the hash store if desired.

### Related information

[Deleting the BranchCache configuration on SVMs](#)

### Improve Microsoft remote copy performance

#### Improve Microsoft remote copy performance overview

Microsoft Offloaded Data Transfer (ODX), also known as *copy offload*, enables direct data transfers within or between compatible storage devices without transferring the data through the host computer.

ONTAP supports ODX for both the SMB and SAN protocols. The source can be either a CIFS server or LUN, and the destination can be either a CIFS server or LUN.

In non-ODX file transfers, the data is read from the source and is transferred across the network to the client computer. The client computer transfers the data back over the network to the destination. In summary, the

client computer reads the data from the source and writes it to the destination. With ODX file transfers, data is copied directly from the source to the destination.

Because ODX offloaded copies are performed directly between the source and destination storage, there are significant performance benefits. The performance benefits realized include faster copy time between source and destination, reduced resource utilization (CPU, memory) on the client, and reduced network I/O bandwidth utilization.

For SMB environments, this functionality is only available when both the client and the storage server support SMB 3.0 and the ODX feature. For SAN environments, this functionality is only available when both the client and the storage server support the ODX feature. Client computers that support ODX and have ODX enabled automatically and transparently use offloaded file transfer when moving or copying files. ODX is used irrespective of whether you drag-and-drop files through Windows Explorer or use command-line file copy commands, or whether a client application initiates file copy requests.

### Related information

[Improving client response time by providing SMB automatic node referrals with Auto Location](#)

[SMB configuration for Microsoft Hyper-V and SQL Server](#)

### How ODX works

ODX copy offload uses a token-based mechanism for reading and writing data within or between ODX-enabled CIFS servers. Instead of routing the data through the host, the CIFS server sends a small token, which represents the data, to the client. The ODX client presents that token to the destination server, which then can transfer the data represented by that token from the source to the destination.

When an ODX client learns that the CIFS server is ODX-capable, it opens the source file and requests a token from the CIFS server. After opening the destination file, the client uses the token to instruct the server to copy the data directly from the source to the destination.



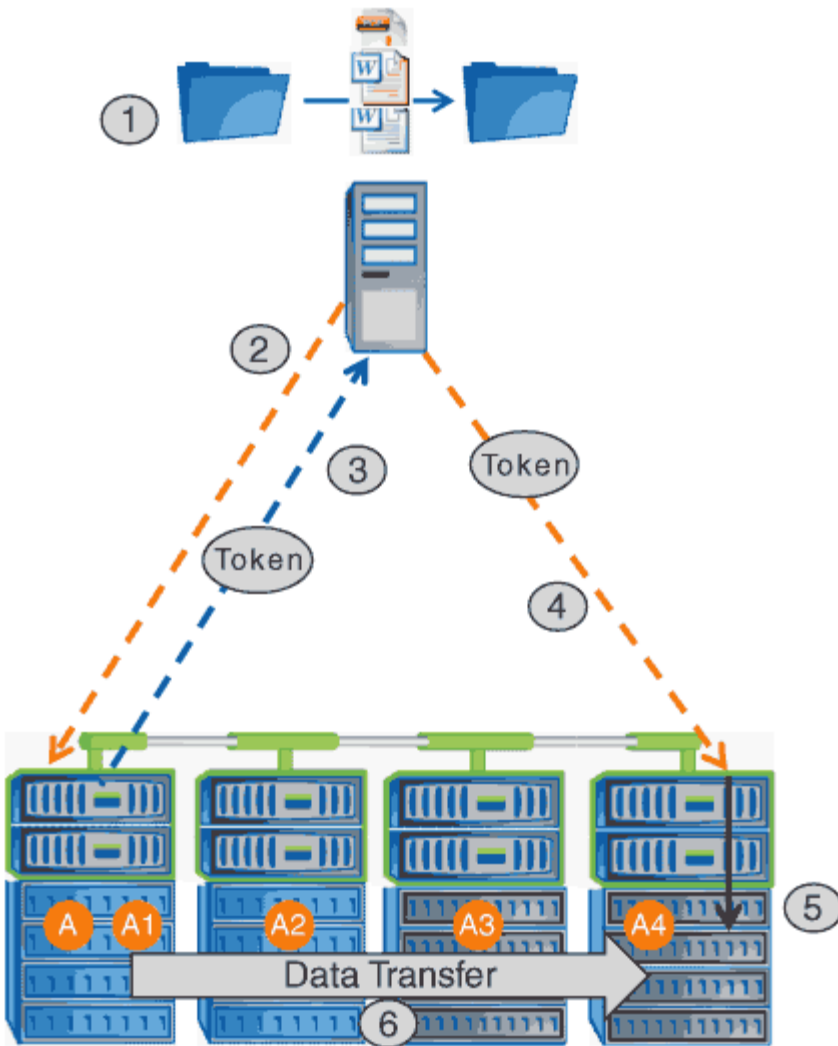
The source and destination can be on the same storage virtual machine (SVM) or on different SVMs, depending on the scope of the copy operation.

The token serves as a point-in-time representation of the data. As an example, when you copy data between storage locations, a token representing a data segment is returned to the requesting client, which the client copies to the destination, thereby removing the need to copy the underlying data through the client.

ONTAP supports tokens that represent 8 MB of data. ODX copies of greater than 8 MB are performed by using multiple tokens, with each token representing 8 MB of data.

The following figure explains the steps that are involved with an ODX copy operation:





1. A user copies or moves a file by using Windows Explorer, a command-line interface, or as part of a virtual machine migration, or an application initiates file copies or moves.
2. The ODX-capable client automatically translates this transfer request into an ODX request.

The ODX request that is sent to the CIFS server contains a request for a token.

3. If ODX is enabled on the CIFS server and the connection is over SMB 3.0, the CIFS server generates a token, which is a logical representation of the data on the source.
4. The client receives a token that represents the data and sends it with the write request to the destination CIFS server.

This is the only data that is copied over the network from the source to the client and then from the client to the destination.

5. The token is delivered to the storage subsystem.
6. The SVM internally performs the copy or move.

If the file that is copied or moved is larger than 8 MB, multiple tokens are needed to perform the copy. Steps 2 through 6 as performed as needed to complete the copy.



If there is a failure with the ODX offloaded copy, the copy or move operation falls back to traditional reads and writes for the copy or move operation. Similarly, if the destination CIFS server does not support ODX or ODX is disabled, the copy or move operation falls back to traditional reads and writes for the copy or move operation.

### Requirements for using ODX

Before you can use ODX for copy offloads with your storage virtual machine (SVM), you need to be aware of certain requirements.

#### ONTAP version requirements

ONTAP releases support ODX for copy offloads.

#### SMB version requirements

- ONTAP supports ODX with SMB 3.0 and later.
- SMB 3.0 must be enabled on the CIFS server before ODX can be enabled:
  - Enabling ODX also enables SMB 3.0, if it is not already enabled.
  - Disabling SMB 3.0 also disables ODX.

#### Windows server and client requirements

Before you can use ODX for copy offloads, the Windows client must support the feature. Support for ODX starts with Windows 2012 Server and Windows 8.

The Interoperability Matrix contains the latest information about supported Windows clients.

[NetApp Interoperability Matrix Tool](#)

#### Volume requirements

- Source volumes must be a minimum of 1.25 GB.
- Deduplication must be enabled on volumes used with copy offload.
- If you use compressed volumes, the compression type must be adaptive and only compression group size 8K is supported.

Secondary compression type is not supported.

#### Guidelines for using ODX

Before you can use ODX for copy offload, you need to be aware of the guidelines. For example, you need to know on which types of volumes you can use ODX and you need to understand the intra-cluster and inter-cluster ODX considerations.

#### Volume guidelines

- You cannot use ODX for copy offload with the following volume configurations:
  - Source volume size is less than 1.25 GB

The volume size must be 1.25 GB or larger to use ODX.

- Read-only volumes

ODX is not used for files and folders residing in load-sharing mirrors or in SnapMirror or SnapVault destination volumes.

- If the source volume is not deduplicated
- ODX copies are supported only for intra-cluster copies.

You cannot use ODX to copy files or folders to a volume in another cluster.

## Other guidelines

- In SMB environments, to use ODX for copy offload, the files must be 256 kb or larger.

Smaller files are transferred using a traditional copy operation.

- ODX copy offload uses deduplication as part of the copy process.

If you do not want deduplication to occur on SVM volumes when copying or moving data, you should disable ODX copy offload on that SVM.

- The application that performs the data transfer must be written to support ODX.

Application operations that support ODX include the following:

- Hyper-V management operations, such as creating and converting virtual hard disks (VHDs), managing Snapshot copies, and copying files between virtual machines
- Windows Explorer operations
- Windows PowerShell copy commands
- Windows command prompt copy commands

Robocopy at the Windows command prompt supports ODX.



The applications must be running on Windows servers or clients that support ODX.

For more information about supported ODX applications on Windows servers and clients, consult the Microsoft TechNet Library.

## Related information

[Microsoft TechNet Library: technet.microsoft.com/en-us/library/](https://technet.microsoft.com/en-us/library/)

## Use cases for ODX

You should be aware of the use cases for using ODX on SVMs so that you can determine under what circumstances ODX provides you with performance benefits.

Windows servers and clients that support ODX use copy offload as the default way of copying data across remote servers. If the Windows server or client does not support ODX or the ODX copy offload fails at any point, the copy or move operation falls back to traditional reads and writes for the copy or move operation.

The following use cases support using ODX copies and moves:

- Intra-volume

The source and destination files or LUNs are within the same volume.

- Inter-volume, same node, same SVM

The source and destination files or LUNs are on different volumes that are located on the same node. The data is owned by the same SVM.

- Inter-volume, different nodes, same SVM

The source and destination files or LUNs are on different volumes that are located on different nodes. The data is owned by the same SVM.

- Inter-SVM, same node

The source and destination file or LUNs are on different volumes that are located on the same node. The data is owned by different SVMs.

- Inter-SVM, different nodes

The source and destination file or LUNs are on different volumes that are located on different nodes. The data is owned by different SVMs.

- Inter-cluster

The source and destination LUNs are on different volumes that are located on different nodes across clusters. This is only supported for SAN and does not work for CIFS.

There are some additional special use cases:

- With the ONTAP ODX implementation, you can use ODX to copy files between SMB shares and FC or iSCSI attached virtual drives.

You can use Windows Explorer, the Windows CLI or PowerShell, Hyper-V, or other applications that support ODX to copy or move files seamlessly using ODX copy offload between SMB shares and connected LUNs, provided that the SMB shares and LUNs are on the same cluster.

- Hyper-V provides some additional use cases for ODX copy offload:

- You can use ODX copy offload pass-through with Hyper-V to copy data within or across virtual hard disk (VHD) files or to copy data between mapped SMB shares and connected iSCSI LUNs within the same cluster.

This allows copies from guest operating systems to pass through to the underlying storage.

- When creating fixed-sized VHDs, ODX is used for initializing the disk with zeros, using a well-known zeroed token.
- ODX copy offload is used for virtual machine storage migration if the source and destination storage is on the same cluster.



To take advantage of the use cases for ODX copy offload pass-through with Hyper-V, the guest operating system must support ODX and the guest operating system's disks must be SCSI disks backed by storage (either SMB or SAN) that supports ODX. IDE disks on the guest operating system do not support ODX pass-through.

### Enable or disable ODX

You can enable or disable ODX on storage virtual machines (SVMs). The default is to enable support for ODX copy offload if SMB 3.0 is also enabled.

#### Before you begin

SMB 3.0 must be enabled.

#### About this task

If you disable SMB 3.0, ONTAP also disables SMB ODX. If you reenable SMB 3.0, you must manually reenable SMB ODX.

#### Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Perform one of the following actions:

If you want ODX copy offload to be...	Enter the command...
Enabled	<code>vserver cifs options modify -vserver vserver_name -copy-offload-enabled true</code>
Disabled	<code>vserver cifs options modify -vserver vserver_name -copy-offload-enabled false</code>

3. Return to the admin privilege level: `set -privilege admin`

#### Example

The following example enables ODX copy offload on SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster1::*> set -privilege admin
```

#### Related information

## Improve client response time by providing SMB automatic node referrals with Auto Location

### Improve client response time by providing SMB automatic node referrals with Auto Location overview

Auto Location uses SMB automatic node referrals to increase SMB client performance on storage virtual machines (SVMs). Automatic node referrals automatically redirect the requesting client to a LIF on the node SVM that is hosting the volume in which the data resides, which can lead to improved client response times.

When an SMB client connects to an SMB share hosted on the SVM, it might connect using a LIF that is on a node that does not own the requested data. The node to which the client is connected accesses data owned by another node by using the cluster network. The client can experience faster response times if the SMB connection uses a LIF located on the node containing the requested data:

- ONTAP provides this functionality by using Microsoft DFS referrals to inform SMB clients that a requested file or folder in the namespace is hosted somewhere else.

A node makes a referral when it determines that there is an SVM LIF on the node containing the data.

- Automatic node referrals are supported for IPv4 and IPv6 LIF IP addresses.
- Referrals are made based on the location of the root of the share through which the client is connected.
- The referral occurs during SMB negotiation.

The referral is made before the connection is established. After ONTAP refers the SMB client to the target node, the connection is made, and the client accesses data through the referred LIF path from that point on. This allows the clients faster access to the data and avoids extra cluster communication.



If a share spans multiple junction points and some of the junctions are to volumes contained on other nodes, data within the share is spread across multiple nodes. Because ONTAP provides referrals that are local to the root of the share, ONTAP must use the cluster network to retrieve the data contained within these non-local volumes. With this type of namespace architecture, automatic node referrals might not provide significant performance benefits.

If the node hosting the data does not have an available LIF, ONTAP establishes the connection using the LIF chosen by the client. After a file is opened by an SMB client, it continues to access the file through the same referred connection.

If, for any reason, the CIFS server cannot make a referral, there is no disruption to SMB service. The SMB connection is established as if automatic node referrals were not enabled.

### Related information

[Improving Microsoft remote copy performance](#)

### Requirements and guidelines for using automatic node referrals

Before you can use SMB automatic node referrals, also known as *autolocation*, you need to be aware of certain requirements, including which versions of ONTAP support the feature. You also need to know about supported SMB protocol versions and certain other

special guidelines.

### **ONTAP version and license requirements**

- All nodes in the cluster must be running a version of ONTAP that supports automatic node referrals.
- Widelinks must be enabled on a SMB share to use autolocation.
- CIFS must be licensed, and an SMB server must exist on the SVMs.

### **SMB protocol version requirements**

- For SVMs, ONTAP supports automatic node referrals on all versions of SMB.

### **SMB client requirements**

All Microsoft clients supported by ONTAP support SMB automatic node referrals.

The Interoperability Matrix contains the latest information about which Windows clients ONTAP supports.

[NetApp Interoperability Matrix Tool](#)

### **Data LIF requirements**

If you want to use a data LIF as a potential referral for SMB clients, you must create data LIFs with both NFS and CIFS enabled.

Automatic node referrals can fail to work if the target node contains data LIFs that are enabled only for the NFS protocol, or enabled only for the SMB protocol.

If this requirement is not met, data access is not affected. The SMB client maps the share using the original LIF that the client used to connect to the SVM.

### **NTLM authentication requirements when making a referred SMB connection**

NTLM authentication must be allowed on the domain containing the CIFS server and on the domains containing clients that want to use automatic node referrals.

When making a referral, the SMB server refers an IP address to the Windows client. Because NTLM authentication is used when making a connection using an IP address, Kerberos authentication is not performed for referred connections.

This happens because the Windows client cannot craft the service principal name used by Kerberos (which is of the form `service/NetBIOS name` and `service/FQDN`), which means that the client cannot request a Kerberos ticket to the service.

### **Guidelines for using automatic node referrals with the home directory feature**

When shares are configured with the home directory share property enabled, there can be one or more home directory search paths configured for a home directory configuration. The search paths can point to volumes contained on each node containing SVM volumes. Clients receive a referral and, if an active, local data LIF is available, connect through a referred LIF that is local to the home user's home directory.

There are guidelines when SMB 1.0 clients access dynamic home directories with automatic node referrals enabled. This is because SMB 1.0 clients require the automatic node referral before they have authenticated, which is before the SMB server has the user's name. However, SMB home directory access works correctly for

SMB 1.0 clients if the following statements are true:

- SMB home directories are configured to use simple names, such as “%w” (Windows user name) or “%u” (mapped UNIX user name), and not domain-name style names, such as “%d\%w” (domain-name\user-name).
- When creating home directory shares, the CIFS home directory shares names are configured with variables (“%w” or “%u”), and not with static names, such as “HOME”.

For SMB 2.x and SMB 3.0 clients, there are no special guidelines when accessing home directories using automatic node referrals.

### **Guidelines for disabling automatic node referrals on CIFS servers with existing referred connections**

If you disable automatic node referrals after the option has been enabled, clients currently connected to a referred LIF keep the referred connection. Because ONTAP uses DFS referrals as the mechanism for SMB automatic node referrals, clients can even reconnect to the referred LIF after you disable the option until the client’s cached DFS referral for the referred connection times out. This is true even in the case of a revert to a version of ONTAP that does not support automatic node referrals. Clients continue to use referrals until the DFS referral times out from the client’s cache.

Autolocation uses SMB automatic node referrals to increase SMB client performance by referring clients to the LIF on the node that owns the data volume of an SVM. When an SMB client connects to an SMB share hosted on an SVM, it might connect using a LIF on a node that does not own the requested data and uses cluster interconnect network to retrieve data. The client can experience faster response times if the SMB connection uses a LIF located on the node containing the requested data.

ONTAP provides this functionality by using Microsoft Distributed File System (DFS) referrals to inform SMB clients that a requested file or folder in the namespace is hosted somewhere else. A node makes a referral when it determines that there is an SVM LIF on the node containing the data. Referrals are made based on the location of the root of the share through which the client is connected.

The referral occurs during SMB negotiation. The referral is made before the connection is established. After ONTAP refers the SMB client to the target node, the connection is made, and the client accesses data through the referred LIF path from that point on. This allows the clients faster access to the data and avoids extra cluster communication.

### **Guidelines for using automatic node referrals with Mac OS clients**

Mac OS X clients do not support SMB automatic node referrals, even though the Mac OS supports Microsoft’s Distributed File System (DFS). Windows clients make a DFS referral request before connecting to an SMB share. ONTAP provides a referral to a data LIF found on the same node that hosts the requested data, which leads to improved client response times. Although the Mac OS supports DFS, Mac OS clients do not behave exactly like Windows clients in this area.

#### **Related information**

[How ONTAP enables dynamic home directories](#)

[Network management](#)

[NetApp Interoperability Matrix Tool](#)

#### **Support for SMB automatic node referrals**

Before you enable SMB automatic node referrals, you should be aware that certain



## ONTAP functionality does not support referrals.

- The following types of volumes do not support SMB automatic node referrals:
  - Read-only members of a load-sharing mirror
  - Destination volume of a data-protection mirror
- Node referrals do not move alongside a LIF move.

If a client is using a referred connection over an SMB 2.x or SMB 3.0 connection and a data LIF moves nondisruptively, the client continues to use the same referred connection, even if the LIF is no longer local to the data.

- Node referrals do not move alongside a volume move.

If a client is using a referred connection over any SMB connection and a volume move occurs, the client continues to use the same referred connection, even if the volume is no longer located on the same node as the data LIF.

### Enable or disable SMB automatic node referrals

You can enable SMB automatic node referrals to increase SMB client access performance. You can disable automatic node referrals if you do not want ONTAP to make referrals to SMB clients.

#### Before you begin

A CIFS server must be configured and running on the storage virtual machine (SVM).

#### About this task

The SMB automatic node referrals functionality is disabled by default. You can enable or disable this functionality on each SVM as required.

This option is available at the advanced privilege level.

#### Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Enable or disable SMB automatic node referrals as required:

If you want SMB automatic node referrals to be...	Enter the following command...
Enabled	<pre>vserver cifs options modify -vserver vserver_name -is-referral-enabled true</pre>
Disabled	<pre>vserver cifs options modify -vserver vserver_name -is-referral-enabled false</pre>

The option setting takes effect for new SMB sessions. Clients with existing connection can utilize node referral only when their existing cache timeout expires.

3. Switch to the admin privilege level: `set -privilege admin`

### Related information

[Available SMB server options](#)

### Use statistics to monitor automatic node referral activity

To determine how many SMB connections are referred, you can monitor automatic node referral activity by using the `statistics` command. By monitoring referrals you can determine the extent to which automatic referrals are locating connections on nodes that host the shares and whether you should redistribute your data LIFs to provide better local access to shares on the CIFS server.

### About this task

The `cifs` object provides several counters at the advanced privilege level that are helpful when monitoring SMB automatic node referrals:

- `node_referral_issued`

Number of clients that have been issued a referral to the share root's node after the client connected using a LIF hosted by a node different from the share root's node.

- `node_referral_local`

Number of clients that connected using a LIF hosted by the same node that hosts the share root. Local access generally provides optimal performance.

- `node_referral_not_possible`

Number of clients that have not been issued a referral to the node hosting the share root after connecting using a LIF hosted by a node different from the share root's node. This is because an active data LIF for the share root's node was not found.

- `node_referral_remote`

Number of clients that connected using a LIF hosted by a node different from the node that hosts the share root. Remote access might result in degraded performance.

You can monitor automatic node referral statistics on your storage virtual machine (SVM) by collecting and viewing data for a specific time period (a sample). You can view data from the sample if you do not stop data collection. Stopping data collection gives you a fixed sample. Not stopping data collection gives you the ability to get updated data that you can use to compare against previous queries. The comparison can help you identify performance trends.



To evaluate and use the information you gather from the `statistics` command, you should understand the distribution of clients in your environments.

### Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. View automatic node referral statistics by using the `statistics` command.

This example views automatic node referral statistics by collecting and viewing data for a sampled time period:

- a. Start the collection: `statistics start -object cifs -instance vs1 -sample-id sample1`

```
Statistics collection is being started for Sample-id: sample1
```

- b. Wait for the desired collection time to elapse.
- c. Stop the collection: `statistics stop -sample-id sample1`

```
Statistics collection is being stopped for Sample-id: sample1
```

- d. View the automatic node referral statistics: `statistics show -sample-id sample1 -counter node`

```
Object: cifs
Instance: vs1
Start-time: 2/4/2013 19:27:02
End-time: 2/4/2013 19:30:11
Cluster: cluster1

      Counter                                          Value
-----
node_name                                           node1
node_referral_issued                                0
node_referral_local                                  1
node_referral_not_possible                           2
node_referral_remote                                 2
...

node_name                                           node2
node_referral_issued                                2
node_referral_local                                  1
node_referral_not_possible                           0
node_referral_remote                                 2
...
```

Output displays counters for all nodes participating in SVM vs1. For clarity, only output fields related to automatic node referral statistics are provided in the example.

3. Return to the admin privilege level: `set -privilege admin`

## Related information

[Displaying statistics](#)

## Performance monitoring setup

### Monitor client-side SMB automatic node referral information using a Windows client

To determine what referrals are made from the client's perspective, you can use the Windows `dfsutil.exe` utility.

The Remote Server Administration Tools (RSAT) kit available with Windows 7 and later clients contains the `dfsutil.exe` utility. Using this utility, you can display information about the contents of the referral cache as well as view information about each referral that the client is currently using. You can also use the utility to clear the client's referral cache. For more information, consult the Microsoft TechNet Library.

#### Related information

[Microsoft TechNet Library: technet.microsoft.com/en-us/library/](https://technet.microsoft.com/en-us/library/)

### Provide folder security on shares with access-based enumeration

#### Provide folder security on shares with access-based enumeration overview

When access-based enumeration (ABE) is enabled on an SMB share, users who do not have permission to access a folder or file contained within the share (whether through individual or group permission restrictions) do not see that shared resource displayed in their environment, although the share itself remains visible.

Conventional share properties allow you to specify which users (individually or in groups) have permission to view or modify files or folders contained within the share. However, they do not allow you to control whether folders or files within the share are visible to users who do not have permission to access them. This could pose problems if the names of these folders or files within the share describe sensitive information, such as the names of customers or products under development.

Access-based enumeration (ABE) extends share properties to include the enumeration of files and folders within the share. ABE therefore enables you to filter the display of files and folders within the share based on user access rights. That is, the share itself would be visible to all users, but files and folders within the share could be displayed to or hidden from designated users. In addition to protecting sensitive information in your workplace, ABE enables you to simplify the display of large directory structures for the benefit of users who do not need access to your full range of content. For example, the share itself would be visible to all users, but files and folders within the share could be displayed or hidden.

Learn about [Performance impact when using SMB/CIFS Access Based Enumeration](#).

#### Enable or disable access-based enumeration on SMB shares

You can enable or disable access-based enumeration (ABE) on SMB shares to allow or prevent users from seeing shared resources that they do not have permission to access.

#### About this task

By default, ABE is disabled.

#### Steps

1. Perform one of the following actions:

If you want to...	Enter the command...
Enable ABE on a new share	<pre>vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties access- based-enumeration</pre> <p>You can specify additional optional share settings and additional share properties when you create an SMB share. For more information, see the man page for the <code>vserver cifs share create</code> command.</p>
Enable ABE on an existing share	<pre>vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties access- based-enumeration</pre> <p>Existing share properties are preserved. The ABE share property is added to the existing list of share properties.</p>
Disable ABE on an existing share	<pre>vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties access- based-enumeration</pre> <p>Other share properties are preserved. Only the ABE share property is removed from the list of share properties.</p>

2. Verify that the share configuration is correct by using the `vserver cifs share show` command.

### Examples

The following example creates an ABE SMB share named “sales” with a path of `/sales` on SVM vs1. The share is created with `access-based-enumeration` as a share property:

```

cluster1::> vserver cifs share create -vserver vs1 -share-name sales -path
/sales -share-properties access-based-
enumeration,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name sales

                Vserver: vs1
                Share: sales
CIFS Server NetBIOS Name: VS1
                Path: /sales
                Share Properties: access-based-enumeration
                                oplocks
                                browsable
                                changenotify
                Symlink Properties: enable
                File Mode Creation Mask: -
                Directory Mode Creation Mask: -
                Share Comment: -
                Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

```

The following example adds the `access-based-enumeration` share property to an SMB share named “data2”:

```

cluster1::> vserver cifs share properties add -vserver vs1 -share-name
data2 -share-properties access-based-enumeration

cluster1::> vserver cifs share show -vserver vs1 -share-name data2 -fields
share-name,share-properties
server  share-name share-properties
-----
vs1     data2      oplocks,browsable,changenotify,access-based-enumeration

```

## Related information

[Adding or removing share properties on an existing SMB share](#)

### Enable or disable access-based enumeration from a Windows client

You can enable or disable access-based enumeration (ABE) on SMB shares from a Windows client, which allows you to configure this share setting without needing to connect to the CIFS server.



The `abecmd` utility is not available in new versions of Windows Server and Windows clients. It was released as part of Windows Server 2008. Support ended for Windows Server 2008 on January 14, 2020.

## Steps

1. From a Windows client that supports ABE, enter the following command: `abecmd [/enable | /disable] [/server CIFS_server_name] {/all | share_name}`

For more information about the `abecmd` command, see your Windows client documentation.

## NFS and SMB file and directory naming dependencies

### NFS and SMB file and directory naming dependencies overview

File and directory naming conventions depend on both the network clients' operating systems and the file-sharing protocols, in addition to language settings on the ONTAP cluster and clients.

The operating system and the file-sharing protocols determine the following:

- Characters a file name can use
- Case-sensitivity of a file name

ONTAP supports multi-byte characters in file, directory, and `qtree` names, depending on the ONTAP release.

### Characters a file or directory name can use

If you are accessing a file or directory from clients with different operating systems, you should use characters that are valid in both operating systems.

For example, if you use UNIX to create a file or directory, do not use a colon (:) in the name because the colon is not allowed in MS-DOS file or directory names. Because restrictions on valid characters vary from one operating system to another, see the documentation for your client operating system for more information about prohibited characters.

### Case-sensitivity of file and directory names in a multiprotocol environment

File and directory names are case-sensitive for NFS clients and case-insensitive but case-preserving for SMB clients. You must understand what the implications are in a multiprotocol environment and the actions you might need to take when specifying the path while creating SMB shares and when accessing data within the shares.

If an SMB client creates a directory named `testdir`, both SMB and NFS clients display the file name as `testdir`. However, if an SMB user later tries to create a directory name `TESTDIR`, the name is not allowed because, to the SMB client, that name currently exists. If an NFS user later creates a directory named `TESTDIR`, NFS and SMB clients display the directory name differently, as follows:

- On NFS clients, you see both directory names as they were created, for example `testdir` and `TESTDIR`, because directory names are case-sensitive.

- SMB clients use the 8.3 names to distinguish between the two directories. One directory has the base file name. Additional directories are assigned an 8.3 file name.
  - On SMB clients, you see `testdir` and `TESTDI~1`.
  - ONTAP creates the `TESTDI~1` directory name to differentiate the two directories.

In this case, you must use the 8.3 name when specifying a share path while creating or modifying a share on a storage virtual machine (SVM).

Similarly for files, if an SMB client creates `test.txt`, both SMB and NFS clients display the file name as `test.txt`. However, if an SMB user later tries to create `Test.txt`, the name is not allowed because, to the SMB client, that name currently exists. If an NFS user later creates a file named `Test.txt`, NFS and SMB clients display the file name differently, as follows:

- On NFS clients, you see both file names as they were created, `test.txt` and `Test.txt`, because file names are case-sensitive.
- SMB clients use the 8.3 names to distinguish between the two files. One file has the base file name. Additional files are assigned an 8.3 file name.
  - On SMB clients, you see `test.txt` and `TEST~1.TXT`.
  - ONTAP creates the `TEST~1.TXT` file name to differentiate the two files.



If you have enabled or modified character mapping using the Vserver CIFS character-mapping commands, a normally case-insensitive Windows lookup becomes case-sensitive.

### How ONTAP creates file and directory names

ONTAP creates and maintains two names for files or directories in any directory that has access from an SMB client: the original long name and a name in 8.3 format.

For file or directory names that exceed the eight character name or the three character extension limit (for files), ONTAP generates an 8.3-format name as follows:

- It truncates the original file or directory name to six characters, if the name exceeds six characters.
- It appends a tilde (~) and a number, one through five, to file or directory names that are no longer unique after being truncated.

If it runs out of numbers because there are more than five similar names, it creates a unique name that bears no relation to the original name.

- In the case of files, it truncates the file name extension to three characters.

For example, if an NFS client creates a file named `specifications.html`, the 8.3 format file name created by ONTAP is `specif~1.htm`. If this name already exists, ONTAP uses a different number at the end of the file name. For example, if an NFS client then creates another file named `specifications_new.html`, the 8.3 format of `specifications_new.html` is `specif~2.htm`.

### How ONTAP handles multi-byte file, directory, and qtree names

Beginning with ONTAP 9.5, support for 4-byte UTF-8 encoded names enables the creation and display of file, directory, and tree names that include Unicode supplementary



characters outside the Basic Multilingual Plane (BMP). In earlier releases, these supplementary characters did not display correctly in multiprotocol environments.

To enable support for 4-byte UTF-8 encoded names, a new *utf8mb4* language code is available for the `vserver` and `volume` command families.

- You must create a new volume in one of the following ways:
- Setting the volume `-language` option explicitly: `volume create -language utf8mb4 {...}`
- Inheriting the volume `-language` option from an SVM that has been created with or modified for the option: `vserver [create|modify] -language utf8mb4 {...}` `volume create {...}`
- You cannot modify existing volumes for *utf8mb4* support; you must create a new *utf8mb4*-ready volume, and then migrate the data using client-based copy tools.

You can update SVMs for *utf8mb4* support, but existing volumes retain their original language codes.



LUN names with 4-byte UTF-8 characters are not currently supported.

- Unicode character data is typically represented in Windows file systems applications using the 16-bit Unicode Transformation Format (UTF-16) and in NFS file systems using the 8-bit Unicode Transformation Format (UTF-8).

In releases prior to ONTAP 9.5, names including UTF-16 supplementary characters that were created by Windows clients were correctly displayed to other Windows clients but were not translated correctly to UTF-8 for NFS clients. Similarly, names with UTF-8 supplementary characters by created NFS clients were not translated correctly to UTF-16 for Windows clients.

- When you create file names on systems running ONTAP 9.4 or earlier that contain valid or invalid supplementary characters, ONTAP rejects the file name and returns an invalid file name error.

To avoid this issue, use only BMP characters in file names and avoid using supplementary characters, or upgrade to ONTAP 9.5 or later.

Beginning with ONTAP 9, Unicode characters are allowed in `qtree` names.

- You can use either the `volume qtree` command family or System Manager to set or modify `qtree` names.
- `qtree` names can include multi-byte characters in Unicode format, such as Japanese and Chinese characters.
- In releases before ONTAP 9.5, only BMP characters (that is, those that could be represented in 3 bytes) were supported.



In releases before ONTAP 9.5, the junction-path of the `qtree`'s parent volume can contain `qtree` and directory names with Unicode characters. The `volume show` command displays these names correctly when the parent volume has a UTF-8 language setting. However, if the parent volume language is not one of the UTF-8 language settings, some parts of the junction-path are displayed using a numeric NFS alternate name.

- In 9.5 and later releases, 4-byte characters are supported in `qtree` names, provided that the `qtree` is in a volume enabled for *utf8mb4*.

## Configure character mapping for SMB file name translation on volumes

NFS clients can create file names that contain characters that are not valid for SMB clients and certain Windows applications. You can configure character mapping for file name translation on volumes to allow SMB clients to access files with NFS names that would otherwise not be valid.

### About this task

When files created by NFS clients are accessed by SMB clients, ONTAP looks at the name of the file. If the name is not a valid SMB file name (for example, if it has an embedded colon ":" character), ONTAP returns the 8.3 file name that is maintained for each file. However, this causes problems for applications that encode important information into long file names.

Therefore, if you are sharing a file between clients on different operating systems, you should use characters in the file names that are valid in both operating systems.

However, if you have NFS clients that create file names containing characters that are not valid file names for SMB clients, you can define a map that converts the invalid NFS characters into Unicode characters that both SMB and certain Windows applications accept. For example, this functionality supports the CATIA MCAD and Mathematica applications as well as other applications that have this requirement.

You can configure character mapping on a volume-by-volume basis.

You must keep the following in mind when configuring character mapping on a volume:

- Character mapping is not applied across junction points.

You must explicitly configure character mapping for each junction volume.

- You must make sure that the Unicode characters that are used to represent invalid or illegal characters are characters that do not normally appear in file names; otherwise, unwanted mappings occur.

For example, if you try to map a colon (:) to a hyphen (-) but the hyphen (-) was used in the file name correctly, a Windows client trying to access a file named "a-b" would have its request mapped to the NFS name of "a:b" (not the desired outcome).

- After applying character mapping, if the mapping still contains an invalid Windows character, ONTAP falls back to Windows 8.3 file names.
- In FPolicy notifications, NAS audit logs, and security trace messages, the mapped file names are shown.
- When a SnapMirror relation of type DP is created, the source volume's character mapping is not replicated on the destination DP volume.
- Case sensitivity: Because the mapped Windows names turn into NFS names, the lookup of the names follows NFS semantics. That includes the fact that NFS lookups are case-sensitive. This means that the applications accessing mapped shares must not rely on Windows case-insensitive behavior. However, the 8.3 name is available, and that is case-insensitive.
- Partial or invalid mappings: After mapping a name to return to clients doing directory enumeration ("dir"), the resulting Unicode name is checked for Windows validity. If that name still has invalid characters in it, or if it is otherwise invalid for Windows (e.g. it ends in "." or blank) the 8.3 name is returned instead of the invalid name.

### Step

1. Configure character mapping: +

```
vserver cifs character-mapping create -vserver vserver_name -volume volume_name
-mapping mapping_text, ... +
```

The mapping consists of a list of source-target character pairs separated by “:”. The characters are Unicode characters entered using hexadecimal digits. For example: 3C:E03C. +

The first value of each `mapping_text` pair that is separated by a colon is the hexadecimal value of the NFS character you want to translate, and the second value is the Unicode value that SMB uses. The mapping pairs must be unique (a one-to-one mapping should exist).

- Source mapping +

The following table shows the permissible Unicode character set for source mapping:

+

Unicode character	Printed character	Description
0x01-0x19	Not applicable	Non-printing control characters
0x5C		Backslash
0x3A	:	Colon
0x2A	*	Asterisk
0x3F	?	Question mark
0x22	"	Quotation mark
0x3C	<	Less than
0x3E	>	Greater than
0x7C		Vertical line
0xB1	±	Plus-minus sign

- Target mapping

You can specify target characters in the “Private Use Area” of Unicode in the following range: U+E0000... U+F8FF.

### Example

The following command creates a character mapping for a volume named “data” on storage virtual machine (SVM) vs1:

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show
```

```
Vserver          Volume Name  Character Mapping
-----          -
vs1              data        3c:e17c, 3e:f17d, 2a:f745
```

### Related information

[Creating and managing data volumes in NAS namespaces](#)

### Commands for managing character mappings for SMB file name translation

You can manage character mapping by creating, modifying, displaying information about, or deleting file character mappings used for SMB file name translation on FlexVol volumes.

If you want to...	Use this command...
Create new file character mappings	<code>vserver cifs character-mapping create</code>
Display information about file character mappings	<code>vserver cifs character-mapping show</code>
Modify existing file character mappings	<code>vserver cifs character-mapping modify</code>
Delete file character mappings	<code>vserver cifs character-mapping delete</code>

For more information, see the man page for each command.

### Related information

[Configuring character mapping for SMB file name translation on volumes](#)

## SMB configuration for Microsoft Hyper-V and SQL Server

### SMB configuration for Microsoft Hyper-V and SQL Server overview

ONTAP features allow you to enable nondisruptive operations for two Microsoft applications over the SMB protocol: Microsoft Hyper-V and Microsoft SQL Server.

You should use these procedures if you want to implement SMB nondisruptive operations under the following circumstances:

- Basic SMB protocol file access has been configured.
- You want to enable SMB 3.0 or later file shares residing in SVMs to store the following objects:
  - Hyper-V virtual machine files

- SQL Server system databases

### Related information

For additional information about ONTAP technology and interaction with external services, see these Technical Reports (TRs):

[NetApp Technical Report 4172: Microsoft Hyper-V over SMB 3.0 with ONTAP Best Practices](#)

[NetApp Technical Report 4369: Best Practices for Microsoft SQL Server and SnapManager 7.2 for SQL Server with Clustered Data ONTAP](#)

## Configure ONTAP for Microsoft Hyper-V and SQL Server over SMB solutions

You can use continuously available SMB 3.0 and later file shares to store Hyper-V virtual machine files or SQL Server system databases and user databases on volumes residing in SVMs, while at the same time providing nondisruptive operations (NDOs) for both planned and unplanned events.

### Microsoft Hyper-V over SMB

To create a Hyper-V over SMB solution, you must first configure ONTAP to provide storage services for Microsoft Hyper-V servers. Additionally, you must also configure Microsoft clusters (if using a clustered configuration), Hyper-V servers, continuously available SMB 3.0 connections to the shares hosted by the CIFS server, and, optionally, backup services to protect the virtual machine files that are stored on SVM volumes.



The Hyper-V servers must be configured on Windows 2012 Server or later. Both stand-alone and clustered Hyper-V server configurations are supported.

- For information about creating Microsoft clusters and Hyper-V servers, see the Microsoft web site.
- SnapManager for Hyper-V is a host-based application that facilitates rapid, Snapshot copy-based backup services, designed to integrate with Hyper-V over SMB configurations.

For information about using SnapManager with Hyper-V over SMB configurations, see *SnapManager for Hyper-V Installation and Administration Guide*.

### Microsoft SQL Server over SMB

To create a SQL Server over SMB solution, you must first configure ONTAP to provide storage services for the Microsoft SQL Server application. Additionally, you must also configure Microsoft clusters (if using a clustered configuration). You would then install and configure SQL Server on the Windows servers and create continuously available SMB 3.0 connections to the shares hosted by the CIFS server. You can optionally configure backup services to protect the database files that are stored on SVM volumes.



SQL Server must be installed and configured on Windows 2012 Server or later. Both stand-alone and clustered configurations are supported.

- For information about creating Microsoft clusters and installing and configuring SQL Server, see the Microsoft web site.
- SnapCenter Plug-in for Microsoft SQL Server is a host-based application that facilitates rapid, Snapshot copy-based backup services, designed to integrate with SQL Server over SMB configurations.

For information about using SnapCenter Plug-in for Microsoft SQL Server, see the [SnapCenter Plug-in for Microsoft SQL Server](#) document.

## Nondisruptive operations for Hyper-V and SQL Server over SMB

### What nondisruptive operations for Hyper-V and SQL Server over SMB means

Nondisruptive operations for Hyper-V and SQL Server over SMB refers to the combination of capabilities that enable the application servers and the contained virtual machines or databases to remain online and to provide continuous availability during many administrative tasks. This includes both planned and unplanned downtime of the storage infrastructure.

Supported nondisruptive operations for application servers over SMB include the following:

- Planned takeover and giveback
- Unplanned takeover
- Upgrade
- Planned aggregate relocation (ARL)
- LIF migration and failover
- Planned volume move

### Protocols that enable nondisruptive operations over SMB

Along with the release of SMB 3.0, Microsoft has released new protocols to provide the capabilities necessary to support nondisruptive operations for Hyper-V and SQL Server over SMB.

ONTAP uses these protocols when providing nondisruptive operations for application servers over SMB:

- SMB 3.0
- Witness

### Key concepts about nondisruptive operations for Hyper-V and SQL Server over SMB

There are certain concepts about nondisruptive operations (NDOs) that you should understand before you configure your Hyper-V or SQL Server over SMB solution.

- **Continuously available share**

An SMB 3.0 share that has the continuously available share property set. Clients connecting through continuously available shares can survive disruptive events such as takeover, giveback, and aggregate relocation.

- **Node**

A single controller that is a member of a cluster. To distinguish between the two nodes in an SFO pair, one node is sometimes called the *local node* and the other node is sometimes called the *partner node* or *remote node*. The primary owner of the storage is the local node. The secondary owner, which takes control of the storage when the primary owner fails, is the partner node. Each node is the primary owner of its storage and secondary owner for its partner's storage.

- **Nondisruptive aggregate relocation**

The ability to move an aggregate between partner nodes within an SFO pair in a cluster without interrupting client applications.

- **Nondisruptive failover**

See *Takeover*.

- **Nondisruptive LIF migration**

The ability to perform a LIF migration without interrupting client applications that are connected to the cluster through that LIF. For SMB connections, this is only possible for clients that connect using SMB 2.0 or later.

- **Nondisruptive operations**

The ability to perform major ONTAP management and upgrade operations as well as withstand node failures without interrupting client applications. This term refers to the collection of nondisruptive takeover, nondisruptive upgrade, and nondisruptive migration capabilities as a whole.

- **Nondisruptive upgrade**

The ability to upgrade node hardware or software without application interruption.

- **Nondisruptive volume move**

The ability to move a volume freely throughout the cluster without interrupting any applications that are using the volume. For SMB connections, all versions of SMB support nondisruptive volume moves.

- **Persistent handles**

A property of SMB 3.0 that allows continuously available connections to transparently reconnect to the CIFS server in the event of a disconnection. Similar to durable handles, persistent handles are maintained by the CIFS server for a period of time after communication to the connecting client is lost. However, persistent handles have more resilience than durable handles. In addition to giving the client a chance to reclaim the handle within a 60-second window after reconnecting, the CIFS server denies access to any other clients requesting access to the file during that 60-second window.

Information about persistent handles is mirrored on the SFO partner's persistent storage, which allows clients with disconnected persistent handles to reclaim the durable handles after an event where the SFO partner takes ownership of the node's storage. In addition to providing nondisruptive operations in the event of LIF moves (which durable handles support), persistent handles provide nondisruptive operations for takeover, giveback, and aggregate relocation.

- **SFO giveback**

Returning aggregates to their home locations when recovering from a takeover event.

- **SFO pair**

A pair of nodes whose controllers are configured to serve data for each other if one of the two nodes stops functioning. Depending on the system model, both controllers can be in a single chassis, or the controllers can be in separate chassis. Known as an HA pair in a two-node cluster.

- **Takeover**

The process by which the partner takes control of the storage when the primary owner of that storage fails. In the context of SFO, failover and takeover are synonymous.

### **How SMB 3.0 functionality supports nondisruptive operations over SMB shares**

SMB 3.0 provides crucial functionality that enables support for nondisruptive operations for Hyper-V and SQL Server over SMB shares. This includes the `continuously-available` share property and a type of file handle known as a *persistent handle* that allow SMB clients to reclaim file open state and transparently reestablish SMB connections.

Persistent handles can be granted to SMB 3.0 capable clients that connect to a share with the `continuously available` share property set. If the SMB session is disconnected, the CIFS server retains information about persistent handle state. The CIFS server blocks other client requests during the 60-second period in which the client is allowed to reconnect, thus allowing the client with the persistent handle to reclaim the handle after a network disconnection. Clients with persistent handles can reconnect by using one of the data LIFs on the storage virtual machine (SVM), either by reconnecting through the same LIF or through a different LIF.

Aggregate relocation, takeover, and giveback all occur between SFO pairs. To seamlessly manage the disconnection and reconnection of sessions with files that have persistent handles, the partner node maintains a copy of all persistent handle lock information. Whether the event is planned or unplanned, the SFO partner can nondisruptively manage the persistent handle reconnects. With this new functionality, SMB 3.0 connections to the CIFS server can transparently and nondisruptively fail over to another data LIF assigned to the SVM in what traditionally has been disruptive events.

Although the use of persistent handles allows the CIFS server to transparently fail over SMB 3.0 connections, if a failure causes the Hyper-V application to fail over to another node in the Windows Server cluster, the client has no way to reclaim the file handles of these disconnected handles. In this scenario, file handles in the disconnected state can potentially block access of the Hyper-V application if it is restarted on a different node. "Failover Clustering" is a part of SMB 3.0 that addresses this scenario by providing a mechanism to invalidate stale, conflicting handles. Using this mechanism, a Hyper-V cluster can recover quickly when Hyper-V cluster nodes fail.

### **What the Witness protocol does to enhance transparent failover**

The Witness protocol provides enhanced client failover capabilities for SMB 3.0 continuously available shares (CA shares). Witness facilitates faster failover because it bypass the LIF failover recovery period. It notifies applications servers when a node is unavailable without needing to wait for the SMB 3.0 connection to time out.

The failover is seamless, with applications running on the client not being aware that a failover occurred. If Witness is not available, failover operations still occur successfully, but failover without Witness is less efficient.

Witness enhanced failover is possible when the following requirements are met:

- It can only be used with SMB 3.0-capable CIFS servers that have SMB 3.0 enabled.
- The shares must use SMB 3.0 with the `continuous availability` share property set.
- The SFO partner of the node to which the application servers are connected must have at least one operational data LIF assigned to the storage virtual machine (SVM) hosting data for the application servers.





The Witness protocol operates between SFO pairs. Because LIFs can migrate to any node within the cluster, any node might need to be the witness for its SFO partner. The Witness protocol cannot provide rapid failover of SMB connections on a given node if the SVM hosting data for the application servers does not have an active data LIF on the partner node. Therefore, every node in the cluster must have at least one data LIF for each SVM hosting one of these configurations.

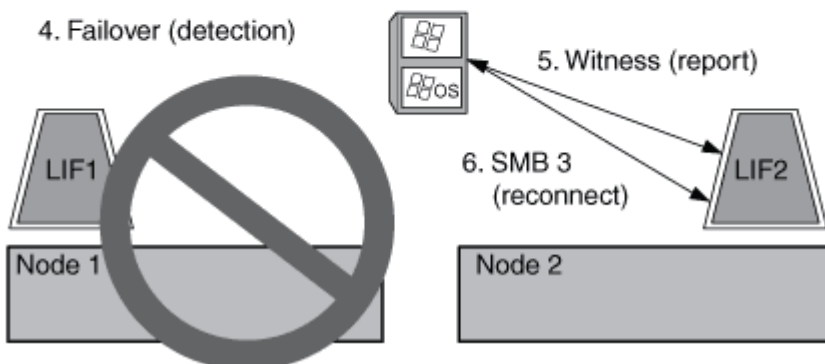
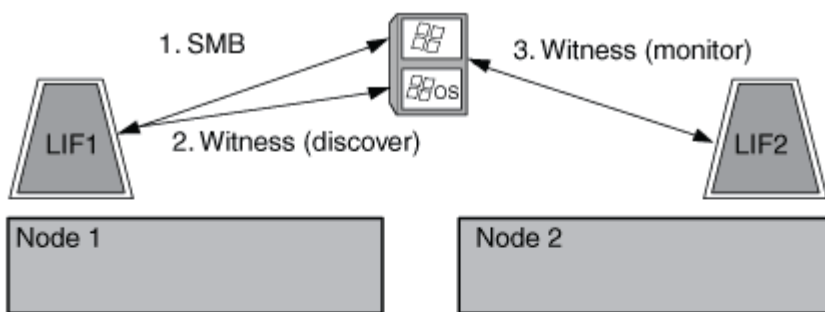
- The application servers must connect to the CIFS server by using the CIFS server name that is stored in DNS instead of by using individual LIF IP addresses.

### How the Witness protocol works

ONTAP implements the Witness protocol by using a node's SFO partner as the witness. In the event of a failure, the partner quickly detects the failure and notifies the SMB client.

The Witness protocol provides enhanced failover using the following process:

1. When the application server establishes a continuously available SMB connection to Node1, the CIFS server informs the application server that Witness is available.
2. The application server requests the IP addresses of the Witness server from Node1 and receives a list of Node2 (the SFO partner) data LIF IP addresses assigned to the storage virtual machine (SVM).
3. The application server chooses one of the IP addresses, creates a Witness connection to Node2, and registers to be notified if the continuously available connection on Node1 must move.
4. If a failover event occurs on Node1, Witness facilitates failover events, but is not involved with giveback.
5. Witness detects the failover event and notifies the application server through the Witness connection that the SMB connection must move to Node2.
6. The application server moves the SMB session to Node2 and recovers the connection without interruption to client access.



## Share-based backups with Remote VSS

### Share-based backups with Remote VSS overview

You can use Remote VSS to perform share-based backups of Hyper-V virtual machine files that are stored on a CIFS server.

Microsoft Remote VSS (Volume Shadow Copy Services) is an extension of the existing Microsoft VSS infrastructure. Previously, VSS could be used for backup services only for data stored on local disk. This limited the use of VSS to applications that store data either on a local disk or on SAN-based storage. With Remote VSS, Microsoft has extended the VSS infrastructure to support the shadow copying of SMB shares. Server applications such as Hyper-V are now storing VHD files on SMB file shares. With these new extensions, it is possible to take application consistent shadow copies for virtual machines that store data and configuration files on shares.

### Remote VSS concepts

You should be aware of certain concepts that are required to understand how Remote VSS (Volume Shadow Copy Service) is used by backup services with Hyper-V over SMB configurations.

- **VSS (Volume Shadow Copy Service)**

A Microsoft technology that is used to take backup copies or snapshots of data on a specific volume at a specific point in time. VSS coordinates among data servers, backup applications, and storage management software to support the creation and management of consistent backups.

- **Remote VSS (Remote Volume Shadow Copy Service)**

A Microsoft technology that is used to take share-based backup copies of data that is in a data-consistent state at a specific point in time where the data is accessed over SMB 3.0 shares. Also known as *Volume Shadow Copy Service*.

- **Shadow copy**

A duplicate set of data contained in the share at a well-defined instant in time. Shadow copies are used to create consistent point-in-time backups of data, allowing the system or applications to continue updating data on the original volumes.

- **Shadow copy set**

A collection of one or more shadow copies, with each shadow copy corresponding to one share. The shadow copies within a shadow copy set represent all the shares that must be backed up in the same operation. The VSS client on the VSS-enabled application identifies which shadow copies to include in the set.

- **Shadow copy set automatic recovery**

The part of the backup process for remote VSS-enabled backup applications where the replica directory containing the shadow copies is made point-in-time consistent. At the start of the backup, the VSS client on the application triggers the application to take software checkpoints on the data scheduled for backup (the virtual machine files in the case of Hyper-V). The VSS client then allows the applications to continue. After the shadow copy set is created, Remote VSS makes the shadow copy set writeable and exposes the writeable copy to the applications. The application prepares the shadow copy set for backup by performing

an automatic recovery using the software checkpoint taken earlier. Automatic recovery brings the shadow copies into a consistent state by unrolling the changes made to the files and directories since the checkpoint was created. Automatic recovery is an optional step for VSS-enabled backups.

- **Shadow copy ID**

A GUID that uniquely identifies a shadow copy.

- **Shadow copy set ID**

A GUID that uniquely identifies a collection of shadow copy IDs to the same server.

- **SnapManager for Hyper-V**

The software that automates and simplifies backup-and-restore operations for Microsoft Windows Server 2012 Hyper-V. SnapManager for Hyper-V uses Remote VSS with automatic recovery to back up Hyper-V files over SMB shares.

### **Related information**

[Key concepts about nondisruptive operations for Hyper-V and SQL Server over SMB](#)

[Share-based backups with Remote VSS](#)

### **Example of a directory structure used by Remote VSS**

Remote VSS traverses the directory structure that stores Hyper-V virtual machine files as it creates shadow copies. It is important to understand what an appropriate directory structure is, so that you can successfully create backups of virtual machine files.

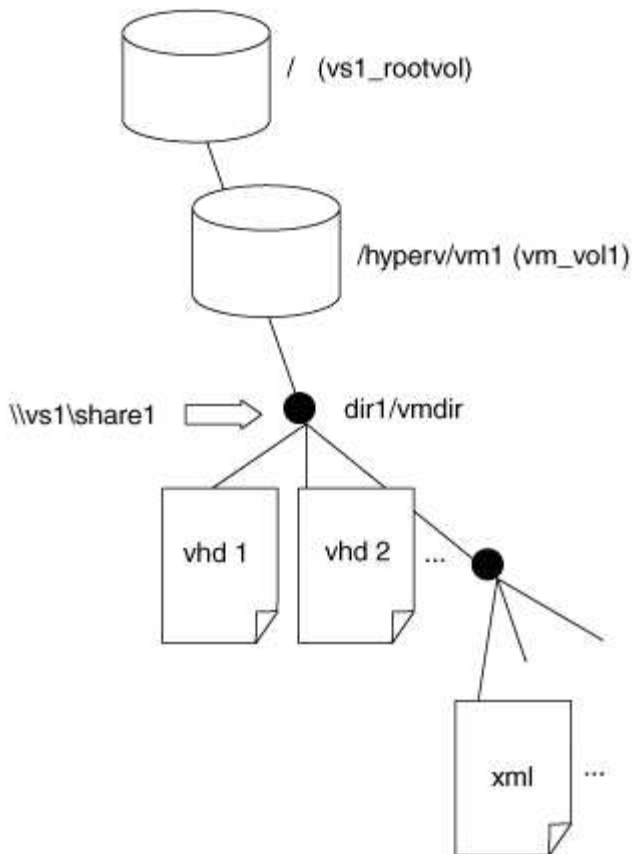
A supported directory structure for the successful creation of shadow copies conforms to the following requirements:

- Only directories and regular files are present within the directory structure that is used to store virtual machine files.

The directory structure does not contain junctions, links, or non-regular files.

- All files for a virtual machine reside within a single share.
- The directory structure that is used to store virtual machine files does not exceed the configured depth of the shadow copy directory.
- The root directory of the share contains only virtual machine files or directories.

In the following illustration, the volume named `vm_vol1` is created with a junction point at `/hyperv/vm1` on storage virtual machine (SVM) `vs1`. Subdirectories to contain the virtual machine files are created under the junction point. The virtual machine files of the Hyper-V server are accessed over `share1` that has the path `/hyperv/vm1/dir1/vmdir`. The shadow copy service creates shadow copies of all the virtual machine files that are contained within the directory structure under `share1` (up to the configured depth of the shadow copy directory).



### How SnapManager for Hyper-V manages Remote VSS-based backups for Hyper-V over SMB

You can use SnapManager for Hyper-V to manage Remote VSS-based backup services. There are benefits to using SnapManager for Hyper-V managed backup service to create space efficient backup sets.

Optimizations to SnapManager for Hyper-V managed backups include the following:

- SnapDrive integration with ONTAP provides performance optimization when discovering SMB share location.

ONTAP provides SnapDrive with the name of the volume where the share resides.

- SnapManager for Hyper-V specifies the list of virtual machine files in the SMB shares that the shadow copy service needs to copy.

By providing a targeted list of virtual machine files, the shadow copy service does not need to create shadow copies of all the files in the share.

- The storage virtual machine (SVM) retains the Snapshot copies for SnapManager for Hyper-V to use for restores.

There is no backup phase. The backup is the space-efficient Snapshot copy.

SnapManager for Hyper-V provides backup and restore capabilities for HyperV over SMB using the following process:

1. Preparing for the shadow copy operation

The SnapManager for Hyper-V application's VSS client sets up the shadow copy set. The VSS client gathers information about what shares to include in the shadow copy set and provides this information to ONTAP. A set might contain one or more shadow copies, and one shadow copy corresponds to one share.

## 2. Creating the shadow copy set (if automatic-recovery is used)

For every share included in the shadow copy set, ONTAP creates a shadow copy and makes the shadow copy writable.

## 3. Exposing the shadow copy set

After ONTAP creates the shadow copies, they are exposed to SnapManager for Hyper-V so that the application's VSS writers can perform automatic recovery.

## 4. Automatically recovering the shadow copy set

During the shadow copy set creation, there is a period of time when active changes are occurring to the files included in the backup set. The application's VSS writers must update the shadow copies to make sure that they are in a completely consistent state prior to backup.



The way that automatic recovery is done is application specific. Remote VSS is not involved in this phase.

## 5. Completing and cleaning up the shadow copy set

The VSS client notifies ONTAP after it completes automatic recovery. The shadow copy set is made read-only and then is ready for backup. When using SnapManager for Hyper-V for backup, the files in a Snapshot copy become the backup; therefore, for the backup phase, a Snapshot copy is created for every volume containing shares in the backup set. After the backup is complete, the shadow copy set is removed from the CIFS server.

## How ODX copy offload is used with Hyper-V and SQL Server over SMB shares

Offloaded Data Transfer (ODX), also known as *copy offload*, enables direct data transfers within or between compatible storage devices without transferring the data through the host computer. ONTAP ODX copy offload provides you with performance benefits when performing copy operations on your application server over SMB installation.

In non-ODX file transfers, the data is read from the source CIFS server and is transferred across the network to the client computer. The client computer transfers the data back over the network to the destination CIFS server. In summary, the client computer reads the data from the source and writes it to the destination. With ODX file transfers, data is copied directly from the source to the destination.

Because ODX offloaded copies are performed directly between the source and destination storage, there are significant performance benefits. The performance benefits realized include faster copy time between source and destination, reduced resource utilization (CPU, memory) on the client, and reduced network I/O bandwidth utilization.

This functionality is available on Windows Server 2012 servers. ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0 continuously available connections.

The following use cases support using ODX copies and moves:

- Intra-volume

The source and destination files or LUNs are within the same volume.

- Inter-volume, same node, same storage virtual machine (SVM)

The source and destination files or LUNs are on different volumes that are located on the same node. The data is owned by the same SVM.

- Inter-volume, different nodes, same SVM

The source and destination files or LUNs are on different volumes that are located on different nodes. The data is owned by the same SVM.

- Inter-SVM, same node

The source and destination file or LUNs are on different volumes that are located on the same node. The data is owned by different SVMs.

- Inter-SVM, different nodes

The source and destination file or LUNs are on different volumes that are located on different nodes. The data is owned by different SVMs.

Specific use cases for ODX copy offload with Hyper-V solutions include the following:

- You can use ODX copy offload pass-through with Hyper-V to copy data within or across virtual hard disk (VHD) files or to copy data between mapped SMB shares and connected iSCSI LUNs within the same cluster.

This allows copies from guest operating systems to pass through to the underlying storage.

- When creating fixed-sized VHDs, ODX is used for initializing the disk with zeros, using a well-known zeroed token.
- ODX copy offload is used for virtual machine storage migration if the source and destination storage is on the same cluster.



To take advantage of the use cases for ODX copy offload pass-through with Hyper-V, the guest operating system must support ODX and the guest operating system's disks must be SCSI disks backed by storage (either SMB or SAN) that supports ODX. IDE disks on the guest operating system do not support ODX pass-through.

Specific use cases for ODX copy offload with SQL Server solutions include the following:

- You can use ODX copy offload to export and import SQL Server databases between mapped SMB shares or between SMB shares and connected iSCSI LUNs within the same cluster.
- ODX copy offload is used for database exports and imports if the source and destination storage is on the same cluster.

## Configuration requirements and considerations

## ONTAP and licensing requirements

You need to be aware of certain ONTAP and licensing requirements when creating SQL Server or Hyper-V over SMB solutions for nondisruptive operations on SVMs.

### ONTAP version requirements

- Hyper-V over SMB

ONTAP supports nondisruptive operations over SMB shares for Hyper-V running on Windows 2012 or later.

- SQL Server over SMB

ONTAP supports nondisruptive operations over SMB shares for SQL Server 2012 or later running on Windows 2012 or later.

For the latest information about supported versions of ONTAP, Windows Server, and SQL Server for nondisruptive operations over SMB shares, see the Interoperability Matrix.

[NetApp Interoperability Matrix Tool](#)

### Licensing requirements

The following licenses are required:

- CIFS
- FlexClone (for Hyper-V over SMB only)

This license is required if Remote VSS is used for backups. The shadow copy service uses FlexClone to create point-in-time copies of files that are then used when creating a backup.

A FlexClone license is optional if you use a backup method that does not use Remote VSS.

### Network and data LIF requirements

You need to be aware of certain network and data LIF requirements when creating SQL Server or Hyper-V over SMB configurations for nondisruptive operations).

#### Network protocol requirements

- IPv4 and IPv6 networks are supported.
- SMB 3.0 or later is required.

SMB 3.0 provides the functionality needed to create the continuously available SMB connections necessary to offer nondisruptive operations.

- DNS servers must contain entries that map the CIFS server name to the IP addresses assigned to the data LIFs on the storage virtual machine (SVM).

The Hyper-V or SQL Server application servers typically make multiple connections over multiple data LIFs when accessing virtual machine or database files. For proper functionality, the application servers must make these multiple SMB connections by using the CIFS server name instead of making multiple

connections to multiple unique IP addresses.

Witness also requires the use of the CIFS server's DNS name instead of individual LIF IP addresses.

Beginning with ONTAP 9.4, you can improve throughput and fault tolerance for Hyper-V and SQL server over SMB configurations by enabling SMB Multichannel. To do so, you must have multiple 1G, 10G, or larger NICs deployed on the cluster and clients.

#### **Data LIF requirements**

- The SVM hosting the application server over SMB solution must have at least one operational data LIF on every node in the cluster.

SVM data LIFs can fail over to other data ports within the cluster, including nodes that are not currently hosting data accessed by the application servers. Additionally, because the Witness node is always the SFO partner of a node to which the application server is connected, every node in the cluster is a potential Witness node.

- Data LIFs must not be configured to automatically revert.

After a takeover or giveback event, you should manually revert the data LIFs to their home ports.

- All data LIF IP addresses must have an entry in DNS and all entries must resolve to the CIFS server name.

The application servers must connect to SMB shares by using the CIFS server name. You must not configure the application servers to make connections by using the LIF IP addresses.

- If the CIFS server name is different from the SVM name, the DNS entries must resolve to the CIFS server name.

#### **SMB server and volume requirements for Hyper-V over SMB**

You need to be aware of certain SMB server and volume requirements when creating Hyper-V over SMB configurations for nondisruptive operations.

#### **SMB server requirements**

- SMB 3.0 must be enabled.

This is enabled by default.

- The default UNIX user CIFS server option must be configured with a valid UNIX user account.

The application servers use the machine account when creating an SMB connection. Because all SMB access requires that the Windows user successfully map to a UNIX user account or to the default UNIX user account, ONTAP must be able to map the application server's machine account to the default UNIX user account.

- Automatic node referrals must be disabled (this functionality is disabled by default).

If you want to use automatic node referrals for access to data other than Hyper-V machine files, you must create a separate SVM for that data.

- Both Kerberos and NTLM authentication must be allowed in the domain to which the SMB server belongs.



ONTAP does not advertise the Kerberos service for Remote VSS; therefore, the domain should be set to permit NTLM.

- Shadow copy functionality must be enabled.

This functionality is enabled by default.

- The Windows domain account that the shadow copy service uses when creating shadow copies must be a member of the SMB server local BUILTIN\Administrators or BUILTIN\Backup Operators group.

### Volume requirements

- Volumes used to store virtual machine files must be created as NTFS security-style volumes.

To provide NDOs for application servers using continuously available SMB connections, the volume containing the share must be an NTFS volume. Moreover, it must always have been an NTFS volume. You cannot change a mixed security-style volume or UNIX security-style volume to an NTFS security-style volume and directly use it for NDOs over SMB shares. If you change a mixed security-style volume to an NTFS security style volume and intend to use it for NDOs over SMB shares, you must manually place an ACL at the top of the volume and propagate that ACL to all contained files and folders. Otherwise, virtual machine migrations or database file exports and imports where files are moved to another volume can fail if either the source or the destination volumes were initially created as mixed or UNIX security-style volumes and later changed to NTFS security style.

- For shadow copy operations to succeed, you must have enough available space on the volume.

The available space must be at least as large as the combined space used by all files, directories, and subdirectories contained within the shares included in the shadow copy backup set. This requirement only applies to shadow copies with auto-recovery.

### Related information

Microsoft TechNet Library: [technet.microsoft.com/en-us/library/](https://technet.microsoft.com/en-us/library/)

### SMB server and volume requirements for SQL Server over SMB

You need to be aware of certain SMB server and volume requirements when creating SQL Server over SMB configurations for nondisruptive operations.

#### SMB server requirements

- SMB 3.0 must be enabled.

This is enabled by default.

- The default UNIX user CIFS server option must be configured with a valid UNIX user account.

The application servers use the machine account when creating an SMB connection. Because all SMB access requires that the Windows user successfully map to a UNIX user account or to the default UNIX user account, ONTAP must be able to map the application server's machine account to the default UNIX user account.

Additionally, SQL Server uses a domain user as the SQL Server service account. The service account must also map to the default UNIX user.

- Automatic node referrals must be disabled (this functionality is disabled by default).

If you want to use automatic node referrals for access to data other than SQL server database files, you must create a separate SVM for that data.

- The Windows user account used for installing SQL Server on ONTAP must be assigned the SeSecurityPrivilege privilege.

This privilege is assigned to the SMB server local BUILTIN\Administrators group.

### Volume requirements

- Volumes used to store virtual machine files must be created as NTFS security-style volumes.

To provide NDOs for application servers using continuously available SMB connections, the volume containing the share must be an NTFS volume. Moreover, it must always have been an NTFS volume. You cannot change a mixed security-style volume or UNIX security-style volume to an NTFS security-style volume and directly use it for NDOs over SMB shares. If you change a mixed security-style volume to an NTFS security style volume and intend to use it for NDOs over SMB shares, you must manually place an ACL at the top of the volume and propagate that ACL to all contained files and folders. Otherwise, virtual machine migrations or database file exports and imports where files are moved to another volume can fail if either the source or the destination volumes were initially created as mixed or UNIX security-style volumes and later changed to NTFS security style.

- Although the volume containing the database files can contain junctions, SQL Server does not cross junctions when creating the database directory structure.
- For SnapCenter Plug-in for Microsoft SQL Server backup operations to succeed, you must have enough available space on the volume.

The volume on which the SQL Server database files reside must be large enough to hold the database directory structure and all contained files residing within the share.

### Related information

[Microsoft TechNet Library: technet.microsoft.com/en-us/library/](https://technet.microsoft.com/en-us/library/)

### Continuously available share requirements and considerations for Hyper-V over SMB

You need to be aware of certain requirements and considerations when configuring continuously available shares for Hyper-V over SMB configurations that support nondisruptive operations.

#### Share requirements

- Shares used by the application servers must be configured with the continuously available property set.

Application servers that connect to continuously available shares receive persistent handles that allow them to reconnect nondisruptively to SMB shares and reclaim file locks after disruptive events, such as takeover, giveback, and aggregate relocation.

- If you want to use Remote VSS-enabled backup services, you cannot put Hyper-V files into shares that contain junctions.

In the auto-recovery case, the shadow copy creation fails if a junction is encountered while traversing the

share. In the non auto-recovery case, the shadow copy creation does not fail, but the junction does not point to anything.

- If you want to use Remote VSS-enabled backup services with auto-recovery, you cannot put Hyper-V files into shares that contain the following:
  - Symlinks, hardlinks, or widelinks
  - Non-regular files

The shadow copy creation fails if there are any links or non-regular files in the share to shadow copy. This requirement only applies to shadow copies with auto-recovery.

- For shadow copy operations to succeed, you must have enough available space on the volume (for Hyper-V over SMB only).

The available space must be at least as large as the combined space used by all files, directories, and subdirectories contained within the shares included in the shadow copy backup set. This requirement only applies to shadow copies with auto-recovery.

- The following share properties must not be set on continuously available shares used by the application servers:
  - Home directory
  - Attribute caching
  - BranchCache

### Considerations

- Quotas are supported on continuously available shares.
- The following functionality is not supported for Hyper-V over SMB configurations:
  - Auditing
  - FPolicy
- Virus scanning is not performed on SMB shares with the `continuously-availability` parameter set to `Yes`.

### Continuously available share requirements and considerations for SQL Server over SMB

You need to be aware of certain requirements and considerations when configuring continuously available shares for SQL Server over SMB configurations that support nondisruptive operations.

#### Share requirements

- Volumes used to store virtual machine files must be created as NTFS security-style volumes.

To provide nondisruptive operations for application servers using continuously available SMB connections, the volume containing the share must be an NTFS volume. Moreover, it must always have been an NTFS volume. You cannot change a mixed security-style volume or UNIX security-style volume to an NTFS security-style volume and directly use it for nondisruptive operations over SMB shares. If you change a mixed security-style volume to an NTFS security style volume and intend to use it for nondisruptive operations over SMB shares, you must manually place an ACL at the top of the volume and propagate that ACL to all contained files and folders. Otherwise, virtual machine migrations or database file exports and

imports where files are moved to another volume can fail if either the source or the destination volumes were initially created as mixed or UNIX security-style volumes and later changed to NTFS security style.

- Shares used by the application servers must be configured with the continuously available property set.

Application servers that connect to continuously available shares receive persistent handles that allow them to reconnect nondisruptively to SMB shares and reclaim file locks after disruptive events, such as takeover, giveback, and aggregate relocation.

- Although the volume containing the database files can contain junctions, SQL Server does not cross junctions when creating the database directory structure.
- For SnapCenter Plug-in for Microsoft SQL Server operations to succeed, you must have enough available space on the volume.

The volume on which the SQL Server database files reside must be large enough to hold the database directory structure and all contained files residing within the share.

- The following share properties must not be set on continuously available shares used by the application servers:
  - Home directory
  - Attribute caching
  - BranchCache

#### Share considerations

- Quotas are supported on continuously available shares.
- The following functionality is not supported for SQL Server over SMB configurations:
  - Auditing
  - FPolicy
- Virus scanning is not performed on SMB shares with the `continuously-availability` share property set.

#### Remote VSS considerations for Hyper-V over SMB configurations

You need to be aware of certain considerations when using Remote VSS-enabled backup solutions for Hyper-V over SMB configurations.

#### General Remote VSS considerations

- A maximum of 64 shares can be configured per Microsoft application server.

The shadow copy operation fails if there are more than 64 shares in a shadow copy set. This is a Microsoft requirement.

- Only one active shadow copy set per CIFS server is allowed.

A shadow copy operation will fail if there is an ongoing shadow copy operation on the same CIFS server. This is a Microsoft requirement.

- No junctions are allowed within the directory structure on which Remote VSS creates a shadow copy.

- In the automatic recovery case, the shadow copy creation will fail if a junction is encountered while traversing the share.
- In the nonautomatic recovery case, the shadow copy creation does not fail, but the junction does not point to anything.

#### **Remote VSS considerations that apply only for shadow copies with automatic recovery**

Certain limits apply only for shadow copies with automatic recovery.

- A maximum directory depth of five subdirectories is allowed for shadow copy creation.

This is the directory depth over which the shadow copy service creates a shadow copy backup set. Shadow copy creation fails if directories containing virtual machine files are nested deeper than five levels. This is intended to limit the directory traversal when cloning the share. The maximum directory depth can be changed by using a CIFS server option.

- Amount of available space on the volume must be adequate.

The available space must be at least as large as the combined space used by all files, directories, and subdirectories contained within the shares included in the shadow copy backup set.

- No links or non-regular files are allowed within the directory structure on which Remote VSS creates a shadow copy.

The shadow copy creation fails if there are any links or non-regular files in the share to the shadow copy. The clone process does not support them.

- No NFSv4 ACLs are allowed on directories.

Although shadow copy creation retains NFSv4 ACLs on files, the NFSv4 ACLs on directories are lost.

- A maximum of 60 seconds is allowed to create a shadow copy set.

Microsoft specifications allow a maximum of 60 seconds to create the shadow copy set. If the VSS client cannot create the shadow copy set within this time, the shadow copy operation fails; therefore, this limits the number of files in a shadow copy set. The actual number of files or virtual machines that can be included in a backup set varies; that number is dependent on many factors, and must be determined for each customer environment.

#### **ODX copy offload requirements for SQL Server and Hyper-V over SMB**

ODX copy offload must be enabled if you want to migrate virtual machine files or export and import database files directly from source to the destination storage location without sending data through the application servers. There are certain requirements that you must understand about using ODX copy offload with SQL Server and Hyper-V over SMB solutions.

Using ODX copy offload provides a significant performance benefit. This CIFS server option is enabled by default.

- SMB 3.0 must be enabled to use ODX copy offload.
- Source volumes must be a minimum of 1.25 GB.

- Deduplication must be enabled on volumes used with copy offload.
- If you use compressed volumes, the compression type must be adaptive and only compression group size 8K is supported.

Secondary compression type is not supported

- To use ODX copy offload to migrate Hyper-V guests within and between disks, the Hyper-V servers must be configured to use SCSI disks.

The default is to configure IDE disks, but ODX copy offload does not work when guests are migrated if disks are created using IDE disks.

## Recommendations for SQL Server and Hyper-V over SMB configurations

To be sure that your SQL Server and Hyper-V over SMB configurations are robust and operational, you need to be familiar with recommended best practices when configuring the solutions.

### General recommendations

- Separate application server files from general user data.

If possible, devote an entire storage virtual machine (SVM) and its storage for the application server's data.

- For best performance, do not enable SMB signing on SVMs that are used to store the application server's data.
- For best performance and improved fault tolerance, enable SMB Multichannel to provide multiple connections between ONTAP and clients in a single SMB session.
- Do not create continuously available shares on any shares other than those used in the Hyper-V or SQL Server over SMB configuration.
- Disable change notify on shares used for continuous availability.
- Do not perform a volume move at the same time as aggregate relocation (ARL) because ARL has phases that pause some operations.
- For Hyper-V over SMB solutions, use in-guest iSCSI drives when creating clustered virtual machines. Shared .VHDX files are not supported for Hyper-V over SMB in ONTAP SMB shares.

## Plan the Hyper-V or SQL Server over SMB configuration

### Complete the volume configuration worksheet

The worksheet provides an easy way to record the values that you need when creating volumes for SQL Server and Hyper-V over SMB configurations.

For each volume, you must specify the following information:

- storage virtual machine (SVM) name

The SVM name is the same for all volumes.

- Volume name

- Aggregate name

You can create volumes on aggregates located on any node in the cluster.

- Size
- Junction path

You should keep the following in mind when creating volumes used to store application server data:

- If the root volume does not have NTFS security style, you must specify the security style as NTFS when you create the volume.

By default, volumes inherit the security style of the SVM root volume.

- Volumes should be configured with the default volume space guarantee.
- You can optionally configure the autosize space management setting.
- You should set the option that determines the Snapshot copy space reserve to 0.
- The Snapshot policy applied to the volume must be disabled.

If the SVM Snapshot policy is disabled, then you do not need to specify a Snapshot policy for the volumes. The volumes inherit the Snapshot policy for the SVM. If the Snapshot policy for the SVM is not disabled and is configured to create Snapshot copies, you must specify a Snapshot policy at the volume level, and that policy must be disabled. Shadow copy service-enabled backups and SQL Server backups manage Snapshot copy creation and deletion.

- You cannot configure load-sharing mirrors for the volumes.

Junction paths on which you plan to create shares that the application servers use should be chosen so that there are no junctioned volumes below the share entry point.

For example, if you want to store virtual machine files on four volumes named “vol1”, “vol2”, “vol3”, and “vol4”, you can create the namespace shown in the example. You can then create shares for the application servers at the following paths: /data1/vol1, /data1/vol2, /data2/vol3, and /data2/vol4.

Vserver	Volume	Junction Active	Junction Path	Junction Path Source
vs1	data1	true	/data1	RW_volume
vs1	vol1	true	/data1/vol1	RW_volume
vs1	vol2	true	/data1/vol2	RW_volume
vs1	data2	true	/data2	RW_volume
vs1	vol3	true	/data2/vol3	RW_volume
vs1	vol4	true	/data2/vol4	RW_volume

Types of information	Values
<i>Volume 1: Volume name, aggregate, size, junction path</i>	

<b>Types of information</b>	<b>Values</b>
<i>Volume 2: Volume name, aggregate, size, junction path</i>	
<i>Volume 3: Volume name, aggregate, size, junction path</i>	
<i>Volume 4: Volume name, aggregate, size, junction path</i>	
<i>Volume 5: Volume name, aggregate, size, junction path</i>	
<i>Volume 6: Volume name, aggregate, size, junction path</i>	
<i>Additional volumes: Volume name, aggregate, size, junction path</i>	

### **Complete the SMB share configuration worksheet**

Use this worksheet to record the values that you need when creating continuously available SMB shares for SQL Server and Hyper-V over SMB configurations.

#### **Information about SMB shares properties and configuration settings**

For each share, you must specify the following information:

- storage virtual machine (SVM) name

The SVM name is the same for all shares

- Share name
- Path
- Share properties

You must configure the following two share properties:

- oplocks
- continuously-available

The following share properties must not be set:

- homedirectory attributecache
- branchcache
- access-based-enumeration





With change notify disabled, Windows 2012 Server does not refresh the Explorer window, which causes an inconsistent view of directory contents.

- Symlinks must be disabled (the value for the `-symlink-properties` parameter must be null [""]).

### Information about share paths

If you are using Remote VSS to back up Hyper-V files, the choice of share paths to use when making SMB connections from the Hyper-V servers to the storage locations where the virtual machine files are stored is important. Although shares can be created at any point in the namespace, paths for shares that the Hyper-V servers use should not contain junctioned volumes. Shadow copy operations cannot be performed on share paths that contain junction points.

SQL Server cannot cross junctions when creating the database directory structure. You should not create share paths for SQL server that contain junction points.

For example, given the namespace shown, if you want to store virtual machine files or database files on volumes “vol1”, “vol2”, “vol3”, and “vol4”, you should create shares for the application servers at the following paths: `/data1/vol1`, `/data1/vol2`, `/data2/vol3`, and `/data2/vol4`.

Vserver	Volume	Junction Active	Junction Path	Junction Path Source
vs1	data1	true	/data1	RW_volume
vs1	vol1	true	/data1/vol1	RW_volume
vs1	vol2	true	/data1/vol2	RW_volume
vs1	data2	true	/data2	RW_volume
vs1	vol3	true	/data2/vol3	RW_volume
vs1	vol4	true	/data2/vol4	RW_volume



Although you can create shares on the `/data1` and `/data2` paths for administrative management, you must not configure the application servers to use those shares to store data.

### Planning worksheet

Types of information	Values
<i>Volume 1: SMB share name and path</i>	
<i>Volume 2: SMB share name and path</i>	
<i>Volume 3: SMB share name and path</i>	
<i>Volume 4: SMB share name and path</i>	
<i>Volume 5: SMB share name and path</i>	

Types of information	Values
<i>Volume 6: SMB share name and path</i>	
<i>Volume 7: SMB share name and path</i>	
<i>Additional volumes: SMB share names and paths</i>	

## Create ONTAP configurations for nondisruptive operations with Hyper-V and SQL Server over SMB

### Create ONTAP configurations for nondisruptive operations with Hyper-V and SQL Server over SMB overview

There are several ONTAP configuration steps you must perform to prepare for Hyper-V and SQL Server installations that provides nondisruptive operations over SMB.

Before you create the ONTAP configuration for nondisruptive operations with Hyper-V and SQL Server over SMB, the following tasks must be completed:

- Time services must be set up on the cluster.
- Networking must be set up for the SVM.
- The SVM must be created.
- Data LIF interfaces must be configured on the SVM.
- DNS must be configured on the SVM.
- Desired names services must be set up for the SVM.
- The SMB server must be created.

#### Related information

[Plan the Hyper-V or SQL Server over SMB configuration](#)

[Configuration requirements and considerations](#)

### Verify that both Kerberos and NTLMv2 authentication are permitted (Hyper-V over SMB shares)

Nondisruptive operations for Hyper-V over SMB require that the CIFS server on a data SVM and the Hyper-V server permit both Kerberos and NTLMv2 authentication. You must verify settings on both the CIFS server and the Hyper-V servers that control what authentication methods are permitted.

#### About this task

Kerberos authentication is required when making a continuously available share connection. Part of the Remote VSS process uses NTLMv2 authentication. Therefore, connections using both authentication methods must be supported for Hyper-V over SMB configurations.

The following settings must be configured to allow both Kerberos and NTLMv2 authentication:

- Export policies for SMB must be disabled on the storage virtual machine (SVM).

Both Kerberos and NTLMv2 authentication are always enabled on SVMs, but export policies can be used to restrict access based on authentication method.

Export policies for SMB are optional and are disabled by default. If export policies are disabled, both Kerberos and NTLMv2 authentication are allowed on a CIFS server by default.

- The domain to which the CIFS server and Hyper-V servers belong must permit both Kerberos and NTLMv2 authentication.

Kerberos authentication is enabled by default on Active Directory domains. However, NTLMv2 authentication can be disallowed, either using Security Policy settings or Group Policies.

### Steps

1. Perform the following to verify that export policies are disabled on the SVM:

- a. Set the privilege level to advanced:

```
set -privilege advanced
```

- b. Verify that the `-is-exportpolicy-enabled` CIFS server option is set to `false`:

```
vserver cifs options show -vserver vserver_name -fields vserver,is-exportpolicy-enabled
```

- c. Return to the admin privilege level:

```
set -privilege admin
```

2. If export policies for SMB are not disabled, disable them:

```
vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled false
```

3. Verify that both NTLMv2 and Kerberos authentication are allowed in the domain.

For information about determining what authentication methods are allowed in the domain, see the Microsoft TechNet Library.

4. If the domain does not permit NTLMv2 authentication, enable NTLMv2 authentication by using one of the methods described in Microsoft documentation.

### Example

The following commands verify that export policies for SMB are disabled on SVM vs1:

```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vservers cifs options show -vservers vs1 -fields vservers,is-
exportpolicy-enabled

vservers  is-exportpolicy-enabled
-----  -----
vs1       false

cluster1::*> set -privilege admin

```

### Verify that domain accounts map to the default UNIX user

Hyper-V and SQL Server use domain accounts to create SMB connections to continuously available shares. To successfully create the connection, the computer account must successfully map to a UNIX user. The most convenient way to accomplish this is to map the computer account to the default UNIX user.

#### About this task

Hyper-V and SQL Server use the domain computer accounts to create SMB connections. In addition, SQL Server uses a domain user account as the service account that also makes SMB connections.

When you create a storage virtual machine (SVM), ONTAP automatically creates the default user named “pcuser” (with a UID of 65534) and the group named “pcuser” (with a GID of 65534), and adds the default user to the “pcuser” group. If you are configuring a Hyper-V over SMB solution on an SVM that existed prior to upgrading the cluster to Data ONTAP 8.2, the default user and group might not exist. If they do not, you must create them before configuring the CIFS server’s default UNIX user.

#### Steps

1. Determine whether there is a default UNIX user:

```
vservers cifs options show -vservers vservers_name
```

2. If the default user option is not set, determine whether there is a UNIX user that can be designated as the default UNIX user:

```
vservers services unix-user show -vservers vservers_name
```

3. If the default user option is not set and there is not a UNIX user that can be designated as the default UNIX user, create the default UNIX user and the default group, and add the default user to the group.

Generally, the default user is given the user name “pcuser” and must be assigned the UID of 65534. The default group is generally given the group name “pcuser”. The GID assigned to the group must be 65534.

- a. Create the default group:

+

```
vserver services unix-group create -vserver vserver_name -name pcuser -id 65534
```

- b. Create the default user and add the default user to the default group:

+

```
vserver services unix-user create -vserver vserver_name -user pcuser -id 65534 -primary-gid 65534
```

- c. Verify that the default user and default group are configured correctly:

+

```
vserver services unix-user show -vserver vserver_name
```

+

```
vserver services unix-group show -vserver vserver_name -members
```

4. If the CIFS server's default user is not configured, perform the following:

- a. Configure the default user:

```
vserver cifs options modify -vserver *vserver_name -default-unix-user pcuser*
```

- b. Verify that the default UNIX user is configured correctly:

```
vserver cifs options show -vserver vserver_name
```

5. To verify that the application server's computer account correctly maps to the default user, map a drive to a share residing on the SVM and confirm the Windows user to UNIX user mapping by using the `vserver cifs session show` command.

For more information about using this command, see the man pages.

### Example

The following commands determine that the CIFS server's default user is not set, but determines that the "pcuser" user and "pcuser" group exist. The "pcuser" user is assigned as the CIFS server's default user on SVM vs1.

```
cluster1::> vserver cifs options show

Vserver: vs1

Client Session Timeout : 900
Default Unix Group      : -
Default Unix User       : -
Guest Unix User         : -
Read Grants Exec        : disabled
Read Only Delete        : disabled
WINS Servers            : -

cluster1::> vserver services unix-user show
      User           User   Group   Full
```

```

Vserver      Name                ID      ID      Name
-----
vs1          nobody             65535   65535   -
vs1          pcuser             65534   65534   -
vs1          root               0       1       -

cluster1::> vserver services unix-group show -members
Vserver      Name                ID
vs1          daemon              1
      Users: -
vs1          nobody             65535
      Users: -
vs1          pcuser             65534
      Users: -
vs1          root               0
      Users: -

cluster1::> vserver cifs options modify -vserver vs1 -default-unix-user
pcuser

cluster1::> vserver cifs options show

Vserver: vs1

Client Session Timeout : 900
Default Unix Group      : -
Default Unix User       : pcuser
Guest Unix User         : -
Read Grants Exec        : disabled
Read Only Delete        : disabled
WINS Servers            : -

```

### Verify that the security style of the SVM root volume is set to NTFS

To ensure that nondisruptive operations for Hyper-V and SQL Server over SMB are successful, volumes must be created with NTFS security style. Since the root volume's security style is applied by default to volumes created on the storage virtual machine (SVM), the security style of the root volume should be set to NTFS.

#### About this task

- You can specify the root volume security style at the time you create the SVM.
- If the SVM is not created with the root volume set to NTFS security style, you can change the security style later by using the `volume modify` command.

#### Steps

1. Determine the current security style of the SVM root volume:

```
volume show -vserver vserver_name -fields vserver,volume,security-style
```

2. If the root volume is not an NTFS security-style volume, change the security style to NTFS:

```
volume modify -vserver vserver_name -volume root_volume_name -security-style ntfs
```

3. Verify that the SVM root volume is set to NTFS security style:

```
volume show -vserver vserver_name -fields vserver,volume,security-style
```

### Example

The following commands verify that the root volume security style is NTFS on SVM vs1:

```
cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume      security-style
-----  -
vs1      vs1_root     unix

cluster1::> volume modify -vserver vs1 -volume vs1_root -security-style
ntfs

cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume      security-style
-----  -
vs1      vs1_root     ntfs
```

### Verify that required CIFS server options are configured

You must verify that the required CIFS server options are enabled and configured according to requirements for nondisruptive operations for Hyper-V and SQL Server over SMB.

#### About this task

- SMB 2.x and SMB 3.0 must be enabled.
- ODX copy offload must be enabled to use performance enhancing copy offload.
- VSS Shadow Copy services must be enabled if the Hyper-V over SMB solution uses Remote VSS-enabled backup services (Hyper-V only).

#### Steps

1. Verify that the required CIFS server options are enabled on the storage virtual machine (SVM):
  - a. Set the privilege level to advanced:

```
set -privilege advanced
```

- b. Enter the following command:

```
vserver cifs options show -vserver vserver_name
```

The following options should be set to `true`:

- `-smb2-enabled`
- `-smb3-enabled`
- `-copy-offload-enabled`
- `-shadowcopy-enabled` (Hyper-V only)

2. If any of the options are not set to `true`, perform the following:

- a. Set them to `true` by using the `vserver cifs options modify` command.
- b. Verify that the options are set to `true` by using the `vserver cifs options show` command.

3. Return to the admin privilege level:

```
set -privilege admin
```

### Example

The following commands verify that the required options for the Hyper-V over SMB configuration are enabled on SVM vs1. In the example, ODX copy offload must be enabled to meet the option requirements.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled,copy-offload-enabled,shadowcopy-enabled
vserver smb2-enabled smb3-enabled copy-offload-enabled shadowcopy-enabled
-----
vs1      true          true          false         true

cluster-1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster-1::*> vserver cifs options show -vserver vs1 -fields copy-offload-
enabled
vserver  copy-offload-enabled
-----
vs1      true

cluster1::*> set -privilege admin
```

### Configure SMB Multichannel for performance and redundancy

Beginning with ONTAP 9.4, you can configure SMB Multichannel to provide multiple



connections between ONTAP and clients in a single SMB session. Doing so improves throughput and fault tolerance for Hyper-V and SQL server over SMB configurations.

### What you'll need

You can use SMB Multichannel functionality only when clients negotiate at SMB 3.0 or later versions. SMB 3.0 and later is enabled on the ONTAP SMB server by default.

### About this task

SMB clients automatically detect and use multiple network connections if a proper configuration is identified on the ONTAP cluster.

The number of simultaneous connections in an SMB session depends on the NICs you have deployed:

- **1G NICs on client and ONTAP cluster**

The client establishes one connection per NIC and binds the session to all connections.

- **10G and larger capacity NICs on client and ONTAP cluster**

The client establishes up to four connections per NIC and binds the session to all connections. The client can establish connections on multiple 10G and larger capacity NICs.

You can also modify the following parameters (advanced privilege):

- **-max-connections-per-session**

The maximum number of connections allowed per Multichannel session. The default is 32 connections.

If you want to enable more connections than the default, you must make comparable adjustments to the client configuration, which also has a default of 32 connections.

- **-max-lifs-per-session**

The maximum number of network interfaces advertised per Multichannel session. The default is 256 network interfaces.

### Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Enable SMB Multichannel on the SMB server:

```
vserver cifs options modify -vserver vserver_name -is-multichannel-enabled true
```

3. Verify that ONTAP is reporting SMB Multichannel sessions:

```
vserver cifs session show options
```

4. Return to the admin privilege level:

```
set -privilege admin
```

## Example

The following example displays information about all SMB sessions, showing multiple connections for a single session:

```
cluster1::> vserver cifs session show
Node:      node1
Vserver:   vs1
Connection Session                               Open
Idle
IDs        ID      Workstation      Windows User      Files
Time
-----
-----
138683,
138684,
138685     1      10.1.1.1        DOMAIN\
4s                                                Administrator      0
```

The following example displays detailed information about an SMB session with session-id 1:

```
cluster1::> vserver cifs session show -session-id 1 -instance
Vserver: vs1
Node: node1
Session ID: 1
Connection IDs: 138683,138684,138685
Connection Count: 3
Incoming Data LIF IP Address: 192.1.1.1
Workstation IP Address: 10.1.1.1
Authentication Mechanism: NTLMv1
User Authenticated as: domain-user
Windows User: DOMAIN\administrator
UNIX User: root
Open Shares: 2
Open Files: 5
Open Other: 0
Connected Time: 5s
Idle Time: 5s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
NetBIOS Name: -
```

## Create NTFS data volumes

You must create NTFS data volumes on the storage virtual machine (SVM) before you can configure continuously available shares for use with Hyper-V or SQL Server over SMB application servers. Use the volume configuration worksheet to create your data volumes.

### About this task

There are optional parameters that you can use to customize a data volume. For more information about customizing volumes, see the xref:./smb-hyper-v-sql/Logical storage management.

As you create your data volumes, you should not create junction points within a volume that contains the following:

- Hyper-V files for which ONTAP makes shadow copies
- SQL Server database files that are backed up using SQL Server



If you inadvertently create a volume that uses mixed or UNIX security style, you cannot change the volume to an NTFS security style volume and then directly use it to create continuously available shares for nondisruptive operations. Nondisruptive operations for Hyper-V and SQL Server over SMB do not work correctly unless the volumes used in the configuration are created as NTFS security-style volumes. You must either delete the volume and re-create the volume with NTFS security style, or you can map the volume on a Windows host and apply an ACL at the top of the volume and propagate the ACL to all files and folders in the volume.

### Steps

1. Create the data volume by entering the appropriate command:

If you want to create a volume in an SVM where the root volume security style is...	Enter the command...
NTFS	<pre>volume create -vserver <i>vserver_name</i> -volume <i>volume_name</i> -aggregate <i>aggregate_name</i> -size integer[KB MB GB TB PB] -junction-path <i>path</i></pre>
Not NTFS	<pre>volume create -vserver <i>vserver_name</i> -volume <i>volume_name</i> -aggregate <i>aggregate_name</i> -size integer[KB MB GB TB PB] - security-style ntfs -junction-path <i>path</i></pre>

2. Verify that the volume configuration is correct:

```
volume show -vserver vserver_name -volume volume_name
```

## Create continuously available SMB shares

After you create your data volumes, you can create the continuously available shares that the application servers use to access Hyper-V virtual machine and configuration files and

SQL Server database files. You should use the share configuration worksheet as you create the SMB shares.

### Steps

1. Display information about the existing data volumes and their junction paths:

```
volume show -vserver vserver_name -junction
```

2. Create a continuously available SMB share:

```
vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties oplocks,continuously-available -symlink "" [-comment text]
```

- You can optionally add a comment to the share configuration.
  - By default, the offline files share property is configured on the share and is set to manual.
  - ONTAP creates the share with the Windows default share permission of Everyone / Full Control.
3. Repeat the previous step for all shares in the share configuration worksheet.
  4. Verify that your configuration is correct by using the `vserver cifs share show` command.
  5. Configure NTFS file permissions on the continuously available shares by mapping a drive to each share, and configuring file permissions by using the **Windows Properties** window.

### Example

The following commands create a continuously available share named “data2” on storage virtual machine (SVM, formerly known as Vserver) vs1. Symlinks are disabled by setting the `-symlink` parameter to “”:

```

cluster1::> volume show -vserver vs1 -junction

```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1	data	true	/data	RW_volume
vs1	data1	true	/data/data1	RW_volume
vs1	data2	true	/data/data2	RW_volume
vs1	vs1_root	-	/	-

```

cluster1::> vserver cifs share create -vserver vs1 -share-name data2 -path
/data/data2 -share-properties oplocks,continuously-available -symlink ""

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

```

```

Vserver: vs1
Share: data2
CIFS Server NetBIOS Name: VS1
Path: /data/data2
Share Properties: oplocks
continuously-available
Symlink Properties: -
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: manual
Vscan File-Operations Profile: standard

```

### Add the SeSecurityPrivilege privilege to the user account (for SQL Server of SMB shares)

The domain user account used for installing the SQL server must be assigned the “SeSecurityPrivilege” privilege to perform certain actions on the CIFS server that require privileges not assigned by default to domain users.

#### What you’ll need

The domain account used for installing the SQL Server must already exist.

#### About this task

When adding the privilege to the SQL Server installer’s account, ONTAP might validate the account by contacting the domain controller. The command might fail if ONTAP cannot contact the domain controller.

#### Steps

1. Add the “SeSecurityPrivilege” privilege:

```
vserver cifs users-and-groups privilege add-privilege -vserver vserver_name -user-or-group-name account_name -privileges SeSecurityPrivilege
```

The value for the `-user-or-group-name` parameter is the name of the domain user account used for installing the SQL Server.

2. Verify that the privilege is applied to the account:

```
vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name account_name
```

### Example

The following command adds the “SeSecurityPrivilege” privilege to the SQL Server installer’s account in the EXAMPLE domain for storage virtual machine (SVM) vs1:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver vs1 -user-or-group-name EXAMPLE\SQLinstaller -privileges SeSecurityPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name          Privileges
-----
vs1          EXAMPLE\SQLinstaller        SeSecurityPrivilege
```

### Configure the VSS shadow copy directory depth (for Hyper-V over SMB shares)

Optionally, you can configure the maximum depth of directories within SMB shares on which to create shadow copies. This parameter is useful if you want to manually control the maximum level of subdirectories on which ONTAP should create shadow copies.

#### What you’ll need

The VSS shadow copy feature must be enabled.

#### About this task

The default is to create shadow copies for a maximum of five subdirectories. If the value is set to 0, ONTAP creates shadow copies for all subdirectories.



Although you can specify that the shadow copy set directory depth include more than five subdirectories or all subdirectories, there is a Microsoft requirement that shadow copy set creation must be completed within 60 seconds. Shadow copy set creation fails if it cannot be completed within this time. The shadow copy directory depth you choose must not cause the creation time to exceed the time limit.

#### Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Set the VSS shadow copy directory depth to the desired level:

```
vserver cifs options modify -vserver vserver_name -shadowcopy-dir-depth integer
```

```
vserver cifs options modify -vserver vs1 -shadowcopy-dir-depth 6
```

3. Return to the admin privilege level:

```
set -privilege admin
```

## Manage Hyper-V and SQL Server over SMB configurations

### Configure existing shares for continuous availability

You can modify existing shares to become continuously available shares that the Hyper-V and SQL Server application servers use to nondisruptively access Hyper-V virtual machine and configuration files and SQL Server database files.

#### About this task

You cannot use an existing share as a continuously available share for nondisruptive operations with application servers over SMB if the share has the following characteristics:

- If the `homedirectory` share property is set on that share
- If the share contains enabled symlinks or widelinks
- If the share contains junctioned volumes below the root of the share

You must verify that the two following share parameters are set correctly:

- The `-offline-files` parameter is set to either `manual` (the default) or `none`.
- Symlinks must be disabled.

The following share properties must be configured:

- `continuously-available`
- `oplocks`

The following share properties must not be set. If they are present in the list of current share properties, they need to be removed from the continuously available share:

- `attributecache`
- `branchcache`

#### Steps

1. Display the current share parameter settings and the current list of configured share properties:

```
vserver cifs share show -vserver vserver_name -share-name share_name
```

2. If necessary, modify the share parameters to disable symlinks and set offline files to manual by using the

`vserver cifs share properties modify` command.

You can disable symlinks by setting the value of the `-symlink` parameter to `""`.

- You can disable symlinks by setting the value of the `-symlink` parameter to `""`.
- You can set the `-offline-files` parameter to the correct setting by specifying `manual`.

3. Add the `continuously-available` share property, and, if needed, the `oplocks` share property:

```
vserver cifs share properties add -vserver vserver_name -share-name share_name
-share-properties continuously-available[,oplock]
```

If the `oplocks` share property is not already set, you must add it along with the `continuously-available` share property.

4. Remove any share properties that are not supported on continuously available shares:

```
vserver cifs share properties remove -vserver vserver_name -share-name
share_name -share-properties properties[,...]
```

You can remove one or more share properties by specifying the share properties with a comma-delimited list.

5. Verify that the `-symlink` and `-offline-files` parameters are set correctly:

```
vserver cifs share show -vserver vserver_name -share-name share_name -fields
symlink-properties,offline-files
```

6. Verify that the list of configured share properties is correct:

```
vserver cifs shares properties show -vserver vserver_name -share-name
share_name
```

## Examples

The following example shows how to configure an existing share named “share1” on storage virtual machine (SVM) vs1 for NDOs with an application server over SMB:

- Symlinks are disabled on the share by setting the `-symlink` parameter to `""`.
- The `-offline-file` parameter is modified and set to `manual`.
- The `continuously-available` share property is added to the share.
- The `oplocks` share property is already in the list of share properties; therefore, it does not need to be added.
- The `attributecache` share property is removed from the share.
- The `browsable` share property is optional for a continuously available share used for NDOs with application servers over SMB and is retained as one of the share properties.



```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1
```

```
          Vserver: vs1
          Share: share1
CIFS Server NetBIOS Name: vs1
          Path: /data
    Share Properties: oplocks
                    browsable
                    attributecache
    Symlink Properties: enable
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
    Share Comment: -
          Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
          Volume Name: data
          Offline Files: documents
Vscan File-Operations Profile: standard
```

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name share1
-offline-file manual -symlink ""
```

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties continuously-available
```

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share1 -share-properties attributecache
```

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1
-fields symlink-properties,offline-files
vserver  share-name symlink-properties offline-files
```

```
-----
vs1      share1  -                manual
```

```
cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1
```

```
          Vserver: vs1
          Share: share1
Share Properties: oplocks
                    browsable
                    continuously-available
```

## Enable or disable VSS shadow copies for Hyper-V over SMB backups

If you use a VSS-aware backup application to back up Hyper-V virtual machine files stored on SMB shares, VSS shadow copy must be enabled. You can disable the VSS shadow copy if you do not use VSS-aware backup applications. The default is to enable the VSS shadow copy.

### About this task

You can enable or disable VSS shadow copies at any time.

### Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Perform one of the following actions:

If you want VSS shadow copies to be...	Enter the command...
Enabled	<pre>vserver cifs options modify -vserver vserver_name -shadowcopy-enabled true</pre>
Disabled	<pre>vserver cifs options modify -vserver vserver_name -shadowcopy-enabled false</pre>

3. Return to the admin privilege level:

```
set -privilege admin
```

### Example

The following commands enable VSS shadow copies on SVM vs1:

```
cluster1::> set -privilege advanced  
Warning: These advanced commands are potentially dangerous; use them  
only when directed to do so by technical support personnel.  
Do you wish to continue? (y or n): y  
  
cluster1::*> vserver cifs options modify -vserver vs1 -shadowcopy-enabled  
true  
  
cluster1::*> set -privilege admin
```

## Use statistics to monitor Hyper-V and SQL Server over SMB activity

### Determine which statistics objects and counters are available

Before you can obtain information about CIFS, SMB, auditing, and BranchCache hash

statistics and monitor performance, you must know which objects and counters are available from which you can obtain data.

### Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Perform one of the following actions:

<b>If you want to determine...</b>	<b>Enter...</b>
Which objects are available	<b>statistics catalog object show</b>
Specific objects that are available	<b>statistics catalog object show object object_name</b>
Which counters are available	<b>statistics catalog counter show object object_name</b>

See the man pages for more information about which objects and counters are available.

3. Return to the admin privilege level:

```
set -privilege admin
```

### Examples

The following command displays descriptions of selected statistic objects related to CIFS and SMB access in the cluster as seen at the advanced privilege level:

```
cluster1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.

```
Do you want to continue? {y|n}: y
```

```
cluster1::*> statistics catalog object show -object audit
audit_ng          CM object for exporting audit_ng
performance counters
```

```
cluster1::*> statistics catalog object show -object cifs
cifs              The CIFS object reports activity of the
                  Common Internet File System protocol
                  ...
```

```
cluster1::*> statistics catalog object show -object nblade_cifs
nblade_cifs      The Common Internet File System (CIFS)
                  protocol is an implementation of the
Server
                  ...
```

```
cluster1::*> statistics catalog object show -object smb1
smb1             These counters report activity from the
SMB              revision of the protocol. For information
                  ...
```

```
cluster1::*> statistics catalog object show -object smb2
smb2            These counters report activity from the
                  SMB2/SMB3 revision of the protocol. For
                  ...
```

```
cluster1::*> statistics catalog object show -object hashd
hashd           The hashd object provides counters to
measure        the performance of the BranchCache hash
daemon.
```

```
cluster1::*> set -privilege admin
```

The following command displays information about some of the counters for the `cifs` object as seen at the advanced privilege level:



This example does not display all of the available counters for the `cifs` object; output is truncated.

```
cluster1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.

```
Do you want to continue? {y|n}: y
```

```
cluster1::*> statistics catalog counter show -object cifs
```

```
Object: cifs
```

Counter	Description
active_searches	Number of active searches over SMB and SMB2
auth_reject_too_many	Authentication refused after too many requests were made in rapid succession
avg_directory_depth	Average number of directories crossed by SMB and SMB2 path-based commands
...	...

```
cluster2::> statistics start -object client -sample-id
```

```
Object: client
```

Counter	Value
cifs_ops	0
cifs_read_ops	0
cifs_read_recv_ops	0
cifs_read_recv_size	0B
cifs_read_size	0B
cifs_write_ops	0
cifs_write_recv_ops	0
cifs_write_recv_size	0B
cifs_write_size	0B
instance_name	vserver_1:10.72.205.179
instance_uuid	2:10.72.205.179
local_ops	0
mount_ops	0

```
[...]
```

## Display SMB statistics

You can display various SMB statistics to monitor performance and diagnose issues.

## Steps

1. Use the `statistics start` and optional `statistics stop` commands to collect a data sample.

For more information about these commands, see the [System Administration Reference](#).

2. Perform one of the following actions:

If you want to display statistics for...	Enter the following command...
All versions of SMB	<code>statistics show -object cifs</code>
SMB 1.0	<code>statistics show -object smb1</code>
SMB 2.x and SMB 3.0	<code>statistics show -object smb2</code>
CIFS subsystem of the node	<code>statistics show -object nblade_cifs</code>

See the man page for more information.

## Verify that the configuration is capable of nondisruptive operations

### Use health monitoring to determine whether nondisruptive operation status is healthy

Health monitoring provides information about system health status across the cluster. The health monitor monitors Hyper-V and SQL Server over SMB configurations to ensure nondisruptive operations (NDOs) for the application servers. If the status is degraded, you can view details about the problem, including the probable cause and recommended recovery actions.

There are several health monitors. ONTAP monitors both overall system health and health for individual health monitors. The node connectivity health monitor contains the CIFS-NDO subsystem. The monitor has a set of health policies that trigger alerts if certain physical conditions can lead to disruption, and if a disruptive condition exists, generates alerts and provides information about corrective actions. For NDO over SMB configurations, alerts are generated for the two following conditions:

Alert ID	Severity	Condition
<code>HaNotReadyCifsNdo_Alert</code>	Major	One or more files hosted by a volume in an aggregate on the node have been opened through a continuously available SMB share with the promise of persistence in the event of a failure; however, the HA relationship with the partner is either not configured or not healthy.

Alert ID	Severity	Condition
NoStandbyLifCifsNdo_Alert	Minor	The storage virtual machine (SVM) is actively serving data over SMB through a node, and there are SMB files opened persistently over continuously available shares; however, its partner node is not exposing any active data LIFs for the SVM.

### Display nondisruptive operation status by using system health monitoring

You can use the `system health` commands to display information about the overall system health of the cluster and the health of the CIFS-NDO subsystem, to respond to alerts, to configure future alerts, and to display information about how health monitoring is configured.

#### Steps

1. Monitor health status by performing the appropriate action:

If you want to display...	Enter the command...
The health status of the system, which reflects the overall status of individual health monitors	<code>system health status show</code>
Information about the health status of the CIFS-NDO subsystem	<code>system health subsystem show -subsystem CIFS-NDO -instance</code>

2. Display information about how CIFS-NDO alert monitoring is configured by performing the appropriate actions:

If you want to display information about...	Enter the command...
The configuration and status of the health monitor for the CIFS-NDO subsystem, such as nodes monitored, initialization state, and status	<code>system health config show -subsystem CIFS-NDO</code>
The CIFS-NDO alerts that a health monitor can potentially generate	<code>system health alert definition show -subsystem CIFS-NDO</code>
CIFS-NDO health monitor policies, which determine when alerts are raised	<code>system health policy definition show -monitor node-connect</code>



Use the `-instance` parameter to display detailed information.

#### Examples

The following output shows information about the overall health status of the cluster and the CIFS-NDO subsystem:

```
cluster1::> system health status show
Status
-----
ok

cluster1::> system health subsystem show -instance -subsystem CIFS-NDO

                Subsystem: CIFS-NDO
                  Health: ok
    Initialization State: initialized
Number of Outstanding Alerts: 0
Number of Suppressed Alerts: 0
                  Node: node2
Subsystem Refresh Interval: 5m
```

The following output shows detailed information about the configuration and status of the health monitor of the CIFS-NDO subsystem:



```

cluster1::> system health config show -subsystem CIFS-NDO -instance

                Node: node1
                Monitor: node-connect
                Subsystem: SAS-connect, HA-health, CIFS-NDO
                Health: ok
                Monitor Version: 2.0
                Policy File Version: 1.0
                Context: node_context
                Aggregator: system-connect
                Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

                Node: node2
                Monitor: node-connect
                Subsystem: SAS-connect, HA-health, CIFS-NDO
                Health: ok
                Monitor Version: 2.0
                Policy File Version: 1.0
                Context: node_context
                Aggregator: system-connect
                Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

```

### Verify the continuously available SMB share configuration

To support nondisruptive operations, Hyper-V and SQL Server SMB shares must be configured as continuously available shares. Additionally, there are certain other share settings that you must check. You should verify that the shares are properly configured to provide seamless nondisruptive operations for the application servers if there are planned or unplanned disruptive events.

#### About this task

You must verify that the two following share parameters are set correctly:

- The `-offline-files` parameter is set to either `manual` (the default) or `none`.
- Symlinks must be disabled.

For proper nondisruptive operations, the following share properties must be set:

- `continuously-available`
- `oplocks`

The following share properties must not be set:

- `homedirectory`
- `attributecache`
- `branchcache`
- `access-based-enumeration`

### Steps

1. Verify that the offline files are set to `manual` or `disabled` and that symlinks are disabled:

```
vserver cifs shares show -vserver vserver_name
```

2. Verify that the SMB shares are configured for continuous availability:

```
vserver cifs shares properties show -vserver vserver_name
```

### Examples

The following example displays the share setting for a share named “share1” on storage virtual machine (SVM, formerly known as Vserver) `vs1`. Offline files are set to `manual` and symlinks are disabled (designated by a hyphen in the `Symlink Properties` field output):

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1
          Vserver: vs1
          Share: share1
CIFS Server NetBIOS Name: VS1
          Path: /data/share1
    Share Properties: oplocks
                    continuously-available
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
          Share Comment: -
          Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
          Volume Name: -
          Offline Files: manual
    Vscan File-Operations Profile: standard
```

The following example displays the share properties for a share named “share1” on SVM vs1:

```
cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1
Vserver      Share      Properties
-----      -
vs1          share1     oplocks
              continuously-available
```

### Verify LIF status

Even if you configure storage virtual machines (SVMs) with Hyper-V and SQL Server over SMB configurations to have LIFs on each node in a cluster, during day-to-day operations, some LIFs might move to ports on another node. You must verify LIF status and take any necessary corrective actions.

### About this task

To provide seamless, nondisruptive operation support, each node in a cluster must have at least one LIF for the SVM, and all the LIFs must be associated with a home port. If some of the configured LIFs are not currently associated with their home port, you must fix any port issues and then revert the LIFs to their home port.

### Steps

1. Display information about configured LIFs for the SVM:

```
network interface show -vserver vserver_name
```

In this example, “lif1” is not located on the home port.

```
network interface show -vserver vs1
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
vs1	lif1	up/up	10.0.0.128/24	node2	e0d	false
	lif2	up/up	10.0.0.129/24	node2	e0d	true

2. If some of the LIFs are not on their home ports, perform the following steps:
  - a. For each LIF, determine what the LIF's home port is:

```
network interface show -vserver vserver_name -lif lif_name -fields home-node,home-port
```

```
network interface show -vserver vs1 -lif lif1 -fields home-node,home-port
```

```
vserver lif  home-node  home-port
-----
vs1      lif1  node1      e0d
```

- b. For each LIF, determine whether the LIF's home port is up:

```
network port show -node node_name -port port -fields port,link
```

```
network port show -node node1 -port e0d -fields port,link
```

```
node      port link
-----
node1     e0d  up
```

In this example, "lif1" should be migrated back to its home port, node1:e0d.

3. If any of the home port network interfaces to which the LIFs should be associated are not in the up state, resolve the problem so that these interfaces are up.
4. If needed, revert the LIFs to their home ports:

```
network interface revert -vserver vserver_name -lif lif_name
```

```
network interface revert -vserver vs1 -lif lif1
```

5. Verify that each node in the cluster has an active LIF for the SVM:

```
network interface show -vserver vserver_name
```

```
network interface show -vserver vs1
```

```

      Logical   Status   Network   Current   Current Is
Vserver Interface Admin/Oper Address/Mask Node       Port
Home
-----
----
vs1
      lif1      up/up    10.0.0.128/24  node1     e0d
true
      lif2      up/up    10.0.0.129/24  node2     e0d
true
```

## Determine whether SMB sessions are continuously available

### Display SMB session information

You can display information about established SMB sessions, including the SMB connection and session ID and the IP address of the workstation using the session. You can display information about the session's SMB protocol version and continuously available protection level, which helps you to identify whether the session supports nondisruptive operations.

### About this task

You can display information for all of the sessions on your SVM in summary form. However, in many cases, the amount of output that is returned is large. You can customize what information is displayed in the output by specifying optional parameters:

- You can use the optional `-fields` parameter to display output about the fields you choose.


You can enter `-fields ?` to determine what fields you can use.


- You can use the `-instance` parameter to display detailed information about established SMB sessions.
- You can use the `-fields` parameter or the `-instance` parameter either alone or in combination with other optional parameters.

### Steps

1. Perform one of the following actions:

If you want to display SMB session information...	Enter the following command...
For all sessions on the SVM in summary form	<code>vserver cifs session show -vserver vserver_name</code>
On a specified connection ID	<code>vserver cifs session show -vserver vserver_name -connection-id integer</code>
From a specified workstation IP address	<code>vserver cifs session show -vserver vserver_name -address workstation_IP_address</code>
On a specified LIF IP address	<code>vserver cifs session show -vserver vserver_name -lif -address LIF_IP_address</code>
On a specified node	<code>vserver cifs session show -vserver vserver_name -node {node_name local}</code>

<p><b>If you want to display SMB session information...</b></p>	<p><b>Enter the following command...</b></p>
<p>From a specified Windows user</p>	<pre><b>vserver cifs session show -vserver vserver_name -windows -user user_name</b></pre> <p>The format for <code>user_name</code> is <code>[domain]\user</code>.</p>
<p>With a specified authentication mechanism</p>	<pre><b>vserver cifs session show -vserver vserver_name -auth -mechanism authentication_mechanism</b></pre> <p>The value for <code>-auth-mechanism</code> can be one of the following:</p> <ul style="list-style-type: none"> <li>• NTLMv1</li> <li>• NTLMv2</li> <li>• Kerberos</li> <li>• Anonymous</li> </ul>
<p>With a specified protocol version</p>	<pre><b>vserver cifs session show -vserver vserver_name -protocol -version protocol_version</b></pre> <p>The value for <code>-protocol-version</code> can be one of the following:</p> <ul style="list-style-type: none"> <li>• SMB1</li> <li>• SMB2</li> <li>• SMB2_1</li> <li>• SMB3</li> <li>• SMB3_1</li> </ul> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  <p>Continuously available protection and SMB Multichannel are available only on SMB 3.0 and later sessions. To view their status on all qualifying sessions, you should specify this parameter with the value set to <code>SMB3</code> or later.</p> </div>

<b>If you want to display SMB session information...</b>	<b>Enter the following command...</b>
With a specified level of continuously available protection	<pre><b>vserver cifs session show -vserver vserver_name -continuously-available continuously_available_protection_level</b></pre> <p>The value for <code>-continuously-available</code> can be one of the following:</p> <ul style="list-style-type: none"> <li>• No</li> <li>• Yes</li> <li>• Partial</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>If the continuously available status is <code>Partial</code>, this means that the session contains at least one open continuously available file, but the session has some files that are not open with continuously available protection. You can use the <code>vserver cifs sessions file show</code> command to determine which files on the established session are not open with continuously available protection.</p> </div>
With a specified SMB signing session status	<pre><b>vserver cifs session show -vserver vserver_name -is-session-signed {true false}</b></pre>

### Examples

The following command displays session information for the sessions on SVM vs1 established from a workstation with IP address 10.1.1.1:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    nodel
Vserver: vs1
Connection Session
ID       ID       Workstation   Windows User   Open   Idle
-----  -
3151272279,
3151272280,
3151272281  1       10.1.1.1     DOMAIN\joe     2     23s
```

The following command displays detailed session information for sessions with continuously available protection on SVM vs1. The connection was made by using the domain account.

```
cluster1::> vserver cifs session show -instance -continuously-available  
Yes
```

```
        Node: nodel  
        Vserver: vs1  
        Session ID: 1  
        Connection ID: 3151274158  
Incoming Data LIF IP Address: 10.2.1.1  
        Workstation IP address: 10.1.1.2  
Authentication Mechanism: Kerberos  
        Windows User: DOMAIN\SERVER1$\br/>        UNIX User: pcuser  
        Open Shares: 1  
        Open Files: 1  
        Open Other: 0  
        Connected Time: 10m 43s  
        Idle Time: 1m 19s  
        Protocol Version: SMB3  
Continuously Available: Yes  
        Is Session Signed: false  
        User Authenticated as: domain-user  
        NetBIOS Name: -  
        SMB Encryption Status: Unencrypted
```

The following command displays session information on a session using SMB 3.0 and SMB Multichannel on SVM vs1. In the example, the user connected to this share from an SMB 3.0 capable client by using the LIF IP address; therefore, the authentication mechanism defaulted to NTLMv2. The connection must be made by using Kerberos authentication to connect with continuously available protection.



```

cluster1::> vserver cifs session show -instance -protocol-version SMB3

                Node: nodel
                Vserver: vs1
                Session ID: 1
                **Connection IDs: 3151272607,31512726078,3151272609
                Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
                Workstation IP address: 10.1.1.3
                Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                UNIX User: pcuser
                Open Shares: 1
                Open Files: 0
                Open Other: 0
                Connected Time: 6m 22s
                Idle Time: 5m 42s
                Protocol Version: SMB3
                Continuously Available: No
                Is Session Signed: false
                User Authenticated as: domain-user
                NetBIOS Name: -
                SMB Encryption Status: Unencrypted

```

### Display information about open SMB files

You can display information about open SMB files, including the SMB connection and session ID, the hosting volume, the share name, and the share path. You can also display information about the continuously available protection level of a file, which is helpful in determining whether an open file is in a state that supports nondisruptive operations.

#### About this task

You can display information about open files on an established SMB session. The displayed information is useful when you need to determine SMB session information for particular files within an SMB session.

For example, if you have an SMB session where some of the open files are open with continuously available protection and some are not open with continuously available protection (the value for the `-continuously-available` field in `vserver cifs session show` command output is `Partial`), you can determine which files are not continuously available by using this command.

You can display information for all open files on established SMB sessions on storage virtual machines (SVMs) in summary form by using the `vserver cifs session file show` command without any optional parameters.

However, in many cases, the amount of output returned is large. You can customize what information is displayed in the output by specifying optional parameters. This can be helpful when you want to view information for only a small subset of open files.

- You can use the optional `-fields` parameter to display output on the fields you choose.

You can use this parameter either alone or in combination with other optional parameters.

- You can use the `-instance` parameter to display detailed information about open SMB files.

You can use this parameter either alone or in combination with other optional parameters.

## Steps

1. Perform one of the following actions:

If you want to display open SMB files...	Enter the following command...
On the SVM in summary form	<code>vserver cifs session file show -vserver vserver_name</code>
On a specified node	<code>vserver cifs session file show -vserver vserver_name -node {node_name local}</code>
On a specified file ID	<code>vserver cifs session file show -vserver vserver_name -file-id integer</code>
On a specified SMB connection ID	<code>vserver cifs session file show -vserver vserver_name -connection-id integer</code>
On a specified SMB session ID	<code>vserver cifs session file show -vserver vserver_name -session-id integer</code>
On the specified hosting aggregate	<code>vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name</code>
On the specified volume	<code>vserver cifs session file show -vserver vserver_name -hosting-volume volume_name</code>
On the specified SMB share	<code>vserver cifs session file show -vserver vserver_name -share share_name</code>
On the specified SMB path	<code>vserver cifs session file show -vserver vserver_name -path path</code>

If you want to display open SMB files...	Enter the following command...
<p>With the specified level of continuously available protection</p>	<pre data-bbox="841 163 1430 300"><b>vserver cifs session file show</b> <b>-vserver vserver_name -continuously</b> <b>-available</b> <b>continuously_available_status</b></pre> <p data-bbox="841 338 1451 405">The value for <code>-continuously-available</code> can be one of the following:</p> <ul data-bbox="865 443 938 527" style="list-style-type: none"> <li>• No</li> <li>• Yes</li> </ul> <div data-bbox="922 701 976 758" style="border: 1px solid black; border-radius: 50%; width: 30px; height: 30px; display: flex; align-items: center; justify-content: center; margin: 10px 0;"> <span data-bbox="938 709 959 737" style="font-size: 12px;">i</span> </div> <p data-bbox="1036 575 1435 884">If the continuously available status is <code>No</code>, this means that these open files are not capable of nondisruptively recovering from takeover and giveback. They also cannot recover from general aggregate relocation between partners in a high-availability relationship.</p>
<p>With the specified reconnected state</p>	<pre data-bbox="841 968 1414 1066"><b>vserver cifs session file show</b> <b>-vserver vserver_name -reconnected</b> <b>reconnected_state</b></pre> <p data-bbox="841 1104 1438 1171">The value for <code>-reconnected</code> can be one of the following:</p> <ul data-bbox="865 1209 938 1293" style="list-style-type: none"> <li>• No</li> <li>• Yes</li> </ul> <div data-bbox="922 1503 976 1560" style="border: 1px solid black; border-radius: 50%; width: 30px; height: 30px; display: flex; align-items: center; justify-content: center; margin: 10px 0;"> <span data-bbox="938 1512 959 1539" style="font-size: 12px;">i</span> </div> <p data-bbox="1036 1346 1455 1717">If the reconnected state is <code>No</code>, the open file is not reconnected after a disconnection event. This can mean that the file was never disconnected, or that the file was disconnected and is not successfully reconnected. If the reconnected state is <code>Yes</code>, this means that the open file is successfully reconnected after a disconnection event.</p>

There are additional optional parameters that you can use to refine the output results. See the man page for more information.

## Examples

The following example displays information about open files on SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:      node1
Vserver:   vs1
Connection: 3151274158
Session:   1
File      File      Open Hosting      Continuously
ID       Type      Mode Volume      Share      Available
-----
41      Regular  r   data      data      Yes
Path:   \mytest.rtf
```

The following example displays detailed information about open SMB files with file ID 82 on SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

Node: node1
Vserver: vs1
File ID: 82
Connection ID: 104617
Session ID: 1
File Type: Regular
Open Mode: rw
Aggregate Hosting File: aggr1
Volume Hosting File: data1
CIFS Share: data1
Path from CIFS Share: windows\win8\test\test.txt
Share Mode: rw
Range Locks: 1
Continuously Available: Yes
Reconnected: No
```

# SAN storage management

## SAN administration

### SAN provisioning

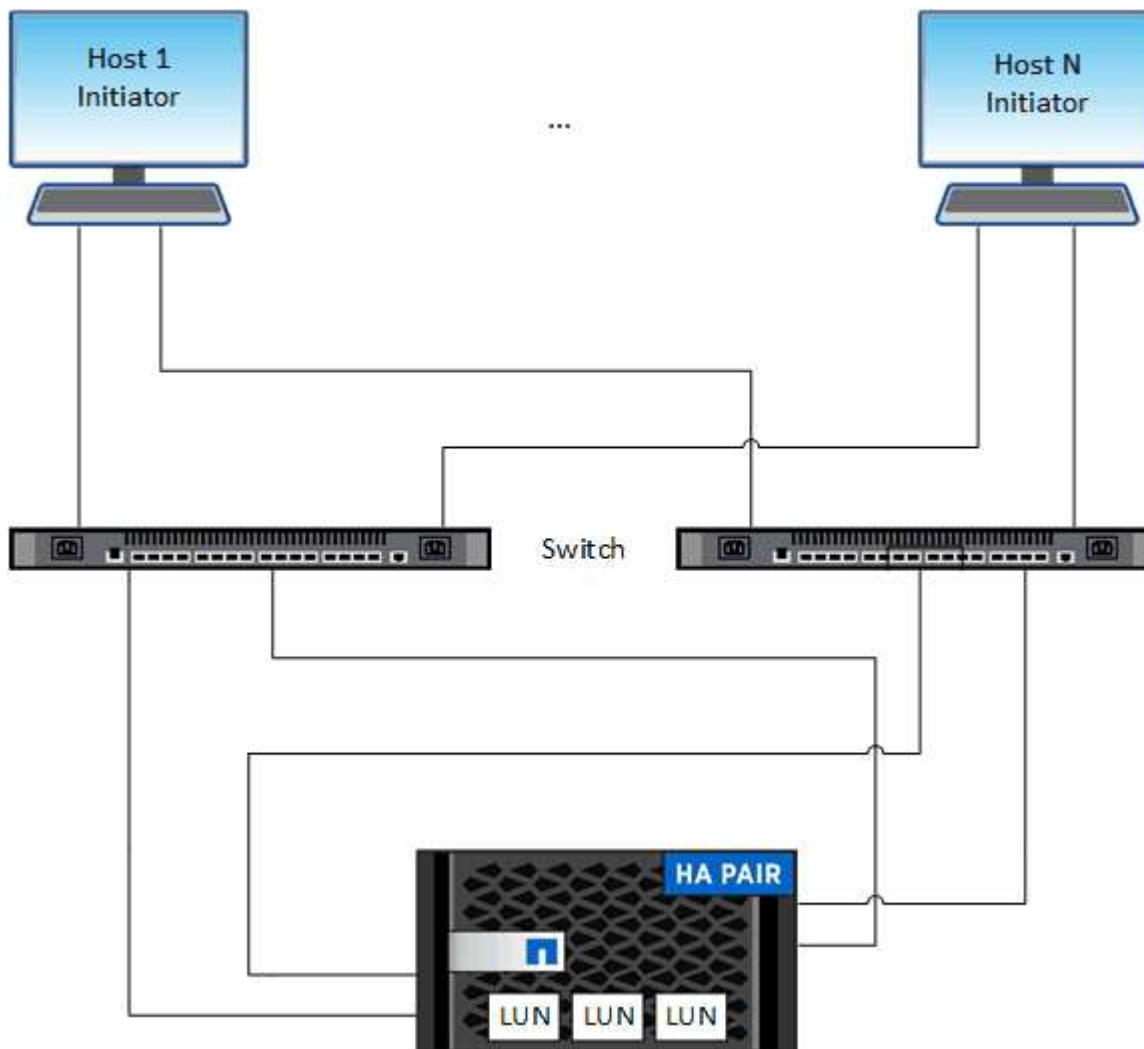
#### SAN management overview

The content in this section shows you how to configure and manage SAN environments with the ONTAP command line interface (CLI) and System Manager in ONTAP 9.7 and later releases.

If you are using the classic System Manager (available only in ONTAP 9.7 and earlier), see these topics:

- [iSCSI protocol](#)
- [FC/FCoE protocol](#)

You can use the iSCSI and FC protocols to provide storage in a SAN environment.



With iSCSI and FC, storage targets are called LUNs (logical units) and are presented to hosts as standard

block devices. You create LUNs and then map them to initiator groups (igroups). Initiator groups are tables of FC host WWPNs and iSCSI host node names and control which initiators have access to which LUNs.

FC targets connect to the network through FC switches and host-side adapters and are identified by world-wide port names (WWPNs). iSCSI targets connect to the network through standard Ethernet network adapters (NICs), TCP offload engine (TOE) cards with software initiators, converged network adapters (CNAs) or dedicated host bus adapters (HBAs) and are identified by iSCSI qualified names (IQNs).

## Configure switches for FCoE

You must configure your switches for FCoE before your FC service can run over the existing Ethernet infrastructure.

### What you'll need

- Your SAN configuration must be supported.

For more information about supported configurations, see the [NetApp Interoperability Matrix Tool](#).

- A Unified Target Adapter (UTA) must be installed on your storage system.

If you are using a UTA2, it must be set to `cna` mode.

- A converged network adapter (CNA) must be installed on your host.

### Steps

1. Use your switch documentation to configure your switches for FCoE.
2. Use the `dcb show` command to verify that the DCB settings for each node in the cluster have been correctly configured.

```
run -node node1 -command dcb show
```

DCB settings are configured on the switch. Consult your switch documentation if the settings are incorrect.

3. Use the `fcp adapter show` command to verify that the FCoE login is working when the FC target port online status is `true`.

```
cluster1::> fcp adapter show -fields node,adapter,status,state,speed,fabric-established,physical-protocol
```

If the FC target port online status is `false`, consult your switch documentation.

### Related information

[NetApp Interoperability Matrix Tool](#)

[NetApp Technical Report 3800: Fibre Channel over Ethernet \(FCoE\) End-to-End Deployment Guide](#)

[Cisco MDS 9000 NX-OS and SAN-OS Software Configuration Guides](#)

[Brocade products](#)

## System Requirements

Setting up LUNs involves creating a LUN, creating an igroup, and mapping the LUN to the igroup. Your system must meet certain prerequisites before you can set up your LUNs.

- The Interoperability Matrix must list your SAN configuration as supported.
- Your SAN environment must meet the SAN host and controller configuration limits specified in [NetApp Hardware Universe](#) for your version of the ONTAP software.
- A supported version of Host Utilities must be installed.

The Host Utilities documentation provides more information.

- You must have SAN LIFs on the LUN owning node and the owning node's HA partner.

### Related information

[NetApp Interoperability Matrix Tool](#)

[ONTAP SAN Host Configuration](#)

[NetApp Technical Report 4017: Fibre Channel SAN Best Practices](#)

## What to know before you create a LUN

### Why actual LUN sizes slightly vary

You should be aware of the following regarding the size of your LUNs.

- When you create a LUN, the actual size of the LUN might vary slightly based on the OS type of the LUN. The LUN OS type cannot be modified after the LUN is created.
- If you create a LUN at the max 16 TB size, be aware that the actual size of the LUN might be slightly less. ONTAP rounds down the limit to be slightly less.
- The metadata for each LUN requires approximately 64 KB of space in the containing aggregate. When you create a LUN, you must ensure that the containing aggregate has enough space for the LUN's metadata. If the aggregate does not contain enough space for the LUN's metadata, some hosts might not be able to access the LUN.

### Guidelines for assigning LUN IDs

Typically, the default LUN ID begins with 0 and is assigned in increments of 1 for each additional mapped LUN. The host associates the LUN ID with the location and path name of the LUN. The range of valid LUN ID numbers depends on the host. For detailed information, see the documentation provided with your Host Utilities.

### Guidelines for mapping LUNs to igroups

- You can map a LUN to only one igroup.
- You can map a LUN to only one specific initiator through the igroup.
- You can add a single initiator to multiple igroups, but the initiator can be mapped to only one LUN.
- You cannot use the same LUN ID for two LUNs mapped to the same igroup.

- You should use the same protocol type for igroups and port sets.

### **Verify and add your protocol FC or iSCSI license**


Before you can enable block access for a storage virtual machine (SVM) with FC or iSCSI, you must have a license.



## Example 1. Steps

### System Manager

Verify and add your FC or iSCSI license with ONTAP System Manager (9.7 and later).

1. In System Manager, click **Cluster > Settings > Licenses**
2. If the license is not listed, click  and enter the license key.
3. Click **Add**.

### CLI

Verify and add your FC or iSCSI license with the ONTAP CLI.

1. Verify that you have a active license for FC or iSCSI.

```
system license show
```

Package	Type	Description	Expiration
Base	site	Cluster Base License	-
NFS	site	NFS License	-
CIFS	site	CIFS License	-
iSCSI	site	iSCSI License	-
FCP	site	FCP License	-

1. If you do not have a active license for FC or iSCSI, add your license code.

```
license add -license-code your_license_code
```

= Provision SAN storage for VMware datastores

```
:toc: macro  
:toclevels: 1  
:hardbreaks:  
:icons: font  
:linkattrs:  
:relative_path: ./  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/
```

This procedure creates new LUNs on an existing storage VM which already has the FC or iSCSI protocol configured.

If you need to create a new storage VM and configure the FC or iSCSI protocol, see [Configure an SVM for FC](#) or [Configure an SVM for iSCSI](#).



Asymmetric logical unit access (ALUA) is always enabled during LUN creation. You cannot change the ALUA setting.

Beginning with ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

When you have completed this procedure, you can manage VMware datastores with Virtual Storage Console (VSC) for VMware vSphere. Beginning with VSC 7.0, VSC is part of the [ONTAP Tools for VMware vSphere virtual appliance](#), which includes VSC, vStorage APIs for Storage Awareness (VASA) Provider, and Storage Replication Adapter (SRA) for VMware vSphere capabilities.

Be sure to check the [NetApp Interoperability Matrix](#) to confirm compatibility between your current ONTAP and VSC releases.

For more information, see [TR-4597: VMware vSphere for ONTAP](#) and the documentation for your VSC release.

## System Manager

Create LUNs to provide storage with System Manager for ONTAP 9.7 or later.

LUNs appear as disks to the ESXi host.

To set up SAN protocol access for ESXi hosts to datastores using System Manager Classic (for ONTAP 9.7 and earlier releases), see the following topics:

- [FC configuration for ESXi using VSC overview](#)
- [iSCSI configuration for ESXi using VSC overview](#)



Asymmetric logical unit access (ALUA) is always enabled during LUN creation. You cannot change the ALUA setting.

## Steps

1. In System Manager, click **Storage > LUNs** and then click **Add**.
2. Enter the required information to create the LUN.
3. You can click **More Options** to do any of the following, depending upon your version of ONTAP.

Option	Available beginning with
<ul style="list-style-type: none"> <li>• Assign QoS policy to LUNs instead of parent volume               <ul style="list-style-type: none"> <li>◦ <b>More Options &gt; Storage and Optimization</b></li> <li>◦ Select <b>Performance Service Level</b>.</li> <li>◦ To apply the QoS policy to individual LUNs instead of the entire volume, select <b>Apply these performance limits enforcements to each LUN</b>.</li> </ul> <p>By default, performance limits are applied at the volume level.</p> </li> </ul>	ONTAP 9.10.1
<ul style="list-style-type: none"> <li>• Create a new initiator group using existing initiator groups               <ul style="list-style-type: none"> <li>◦ <b>More Options &gt; HOST INFORMATION</b></li> <li>◦ Select <b>New initiator group using existing initiator groups</b>.</li> </ul> <p><b>NOTE:</b> The OS type for an igroup containing other igroups cannot be changed after it has been created.</p> </li> </ul>	ONTAP 9.9.1

<ul style="list-style-type: none"> <li>• Add a description to your igroup or host initiator</li> </ul> <p>The description serves as an alias for the igroup or host initiator.</p> <ul style="list-style-type: none"> <li>◦ <b>More Options &gt; HOST INFORMATION</b></li> </ul>	ONTAP 9.9.1
<ul style="list-style-type: none"> <li>• Create your LUN on an existing volume</li> </ul> <p>By default, a new LUN is created in a new volume.</p> <ul style="list-style-type: none"> <li>◦ <b>More Options &gt; Add LUNs</b></li> <li>◦ Select <b>Group related LUNs</b>.</li> </ul>	ONTAP 9.9.1
<ul style="list-style-type: none"> <li>• Disable QoS or choose a custom QoS policy</li> </ul> <ul style="list-style-type: none"> <li>◦ <b>More Options &gt; Storage and Optimization</b></li> <li>◦ Select <b>Performance Service Level</b>.</li> </ul> <p><b>NOTE:</b> In ONTAP 9.9.1 and later, if you select a custom QoS policy, you can also select manual placement on a specified local tier.</p>	ONTAP 9.8

4. For FC, zone your FC switches by WWPN. Use one zone per initiator and include all target ports in each zone.
5. Use Virtual Storage Console (VSC) for VMware vSphere, to discover and initialize the LUN.
6. Verify that the ESXi hosts can write and read data on the LUN.

## CLI

Create LUNs to provide storage with the ONTAP CLI.

1. Use the `system license show` command to verify that you have a license for FC or iSCSI.

```
system license show
```

Package	Type	Description	Expiration
Base	site	Cluster Base License	-
NFS	site	NFS License	-
CIFS	site	CIFS License	-
iSCSI	site	iSCSI License	-
FCP	site	FCP License	-

2. If you do not have a license for FC or iSCSI, use the `license add` command.

```
license add -license-code your_license_code
```

3. Enable your protocol service on the SVM:

**For iSCSI:** `vserver iscsi create -vserver vserver_name -target-alias vserver_name`

**For FC:** `vserver fcp create -vserver vserver_name -status-admin up`

4. Create two LIFs for the SVMs on each node:

```
network interface create -vserver vserver_name -lif lif_name -role data -data
-protocol iscsi|fc -home-node node_name -home-port port_name -address
ip_address -netmask netmask
```

NetApp supports a minimum of one iSCSI or FC LIF per node for each SVM serving data. However, two LIFS per node are required for redundancy.

5. Verify that your LIFs have been created and that their operational status is online:

```
network interface show -vserver vserver_name lif_name
```

6. Create your LUNs:

```
lun create -vserver vserver_name -volume volume_name -lun lun_name -size
lun_size -ostype linux -space-reserve enabled|disabled
```

Your LUN name cannot exceed 255 characters and cannot contain spaces.



The NVFAIL option is automatically enabled when a LUN is created in a volume.

7. Create your igroups:

```
igroup create -vserver vserver_name -igroup igroup_name -protocol
fcp|iscsi|mixed -ostype linux -initiator initiator_name
```

8. Map your LUNs to igroups:

```
lun mapping create -vserver vserver_name -volume volume_name -lun lun_name
-igroup igroup_name
```

9. Verify that your LUNs are configured correctly:

```
lun show -vserver vserver_name
```

10. [Create a port set and bind to an igroup](#) (optional).

11. Follow steps in your host documentation for enabling block access on your specific hosts.

12. Use the Host Utilities to complete the FC or iSCSI mapping and to discover your LUNs on the host.

## Related information

[ONTAP SAN Host Configuration](#)

[SAN Administration overview](#)

[View and manage SAN initiator groups in System Manager](#)

[NetApp Technical Report 4017: Fibre Channel SAN Best Practices](#)

= Provision SAN storage for Linux servers

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

This procedure creates new LUNs on an existing storage VM which already has the FC or iSCSI protocol configured.

If you need to create a new storage VM and configure the FC or iSCSI protocol, see [Configure an SVM for FC](#) or [Configure an SVM for iSCSI](#).

LUNs appear to Linux as SCSI disk devices.



Asymmetric logical unit access (ALUA) is always enabled during LUN creation. You cannot change the ALUA setting.

You must have an FC license and it must be enabled. If the FC license is not enabled, the LIFs and SVMs appear to be online but the operational status is down. The FC service must be enabled for your LIFs and SVMs to be operational. You must use single initiator zoning for all of the FC LIFs in the SVM to host the initiators.

You need to know the initiator identifiers (FC WWPN or iSCSI iqn) for your Linux server.

Beginning with ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

## System Manager

Create LUNs to provide storage for a Linux server using the FC or iSCSI SAN protocol with ONTAP System Manager (9.7 and later).

To complete this task using System Manager Classic (available with 9.7 and earlier) refer to [iSCSI configuration for Red Hat Enterprise Linux](#)

1. On your Linux server, install the [NetApp Linux Host Utilities](#) package.
2. In System Manager, click **Storage > LUNs** and then click **Add**.
3. Enter the required information to create the LUN.
4. You can click **More Options** to do any of the following, depending upon your version of ONTAP.

Option	Available beginning with
<ul style="list-style-type: none"> <li>• Assign QoS policy to LUNs instead of parent volume               <ul style="list-style-type: none"> <li>◦ <b>More Options &gt; Storage and Optimization</b></li> <li>◦ Select <b>Performance Service Level</b>.</li> <li>◦ To apply the QoS policy to individual LUNs instead of the entire volume, select <b>Apply these performance limits enforcements to each LUN</b>.</li> </ul> </li> </ul> <p>By default, performance limits are applied at the volume level.</p>	ONTAP 9.10.1
<ul style="list-style-type: none"> <li>• Create a new initiator group using existing initiator groups               <ul style="list-style-type: none"> <li>◦ <b>More Options &gt; HOST INFORMATION</b></li> <li>◦ Select <b>New initiator group using existing initiator groups</b>.</li> </ul> </li> </ul> <p><b>NOTE:</b> The OS type for an igroup containing other igroups cannot be changed after it has been created.</p>	ONTAP 9.9.1
<ul style="list-style-type: none"> <li>• Add a description to your igroup or host initiator</li> </ul> <p>The description serves as an alias for the igroup or host initiator.</p> <ul style="list-style-type: none"> <li>◦ <b>More Options &gt; HOST INFORMATION</b></li> </ul>	ONTAP 9.9.1
<ul style="list-style-type: none"> <li>• Create your LUN on an existing volume</li> </ul> <p>By default, a new LUN is created in a new volume.</p> <ul style="list-style-type: none"> <li>◦ <b>More Options &gt; Add LUNs</b></li> <li>◦ Select <b>Group related LUNs</b>.</li> </ul>	ONTAP 9.9.1
<ul style="list-style-type: none"> <li>• Disable QoS or choose a custom QoS policy               <ul style="list-style-type: none"> <li>◦ <b>More Options &gt; Storage and Optimization</b></li> <li>◦ Select <b>Performance Service Level</b>.</li> </ul> </li> </ul> <p><b>NOTE:</b> In ONTAP 9.9.1 and later, if you select a custom QoS policy, you can also select manual placement on a specified local tier.</p>	ONTAP 9.8

5. For FC, zone your FC switches by WWPN. Use one zone per initiator and include all target ports in each zone.
6. On your Linux server, discover the new LUNs:

```
/usr/bin/rescan-scsi-bus.sh
```



Optionally partition the LUNs and create file systems.

7. Verify the Linux server can write and read data on the LUN.

## CLI

Create LUNs to provide storage for a Linux server using the FC or iSCSI SAN protocol with ONTAP CLI.

1. Use the `system license show` command to verify that you have a license for FC or iSCSI.

```
system license show
```

Package	Type	Description	Expiration
Base	site	Cluster Base License	-
NFS	site	NFS License	-
CIFS	site	CIFS License	-
iSCSI	site	iSCSI License	-
FCP	site	FCP License	-

2. If you do not have a license for FC or iSCSI, use the `license add` command.

```
license add -license-code your_license_code
```

3. Enable your protocol service on the SVM:

**For iSCSI:** `vserver iscsi create -vserver vserver_name -target-alias vserver_name`

**For FC:** `vserver fcp create -vserver vserver_name -status-admin up`

4. Create two LIFs for the SVMs on each node:

```
network interface create -vserver vserver_name -lif lif_name -role data -data  
-protocol iscsi|fc -home-node node_name -home-port port_name -address  
ip_address -netmask netmask
```

NetApp supports a minimum of one iSCSI or FC LIF per node for each SVM serving data. However, two LIFS per node are required for redundancy.

5. Verify that your LIFs have been created and that their operational status is online:

```
network interface show -vserver vserver_name lif_name
```

6. Create your LUNs:

```
lun create -vserver vserver_name -volume volume_name -lun lun_name -size  
lun_size -ostype linux -space-reserve enabled|disabled
```

Your LUN name cannot exceed 255 characters and cannot contain spaces.



The NVFAIL option is automatically enabled when a LUN is created in a volume.

7. Create your igroups:

```
igroup create -vserver vserver_name -igroup igroup_name -protocol
fc|iscsi|mixed -ostype linux -initiator initiator_name
```

#### 8. Map your LUNs to igroups:

```
lun mapping create -vserver vserver_name -volume volume_name -lun lun_name
-igroup igroup_name
```

#### 9. Verify that your LUNs are configured correctly:

```
lun show -vserver vserver_name
```

#### 10. [Create a port set and bind to an igroup](#) (optional).

11. Follow steps in your host documentation for enabling block access on your specific hosts.

12. Use the Host Utilities to complete the FC or iSCSI mapping and to discover your LUNs on the host.

#### Related information

[SAN Administration overview](#)

[ONTAP SAN Host Configuration](#)

[View and manage SAN initiator groups in System Manager](#)

[NetApp Technical Report 4017: Fibre Channel SAN Best Practices](#)

= Provision SAN storage for Windows servers

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

This procedure creates new LUNs on an existing storage VM which already has the FC or iSCSI protocol configured.

If you need to create a new storage VM and configure the FC or iSCSI protocol, see [Configure an SVM for FC](#) or [Configure an SVM for iSCSI](#).

LUNs appear as disks to the Windows host.



Asymmetric logical unit access (ALUA) is always enabled during LUN creation. You cannot change the ALUA setting.

Beginning with ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

#### System Manager

Create LUNs to provide storage for a Windows server using the FC or iSCSI SAN protocol with ONTAP System Manager (9.7 and later)

To complete this task using System Manager Classic (available with 9.7 and earlier) refer to [iSCSI](#)



**Steps**

1. On your Windows server, install the native DSM for Windows MPIO.
2. In System Manager, click **Storage > LUNs** and then click **Add**.
3. Enter the required information to create the LUN.
4. You can click **More Options** to do any of the following, depending upon your version of ONTAP.

Option	Available beginning with
<ul style="list-style-type: none"> <li>• Assign QoS policy to LUNs instead of parent volume                             <ul style="list-style-type: none"> <li>◦ <b>More Options &gt; Storage and Optimization</b></li> <li>◦ Select <b>Performance Service Level</b>.</li> <li>◦ To apply the QoS policy to individual LUNs instead of the entire volume, select <b>Apply these performance limits enforcements to each LUN</b>.</li> </ul> <p>By default, performance limits are applied at the volume level.</p> </li> </ul>	ONTAP 9.10.1
<ul style="list-style-type: none"> <li>• Create a new initiator group using existing initiator groups                             <ul style="list-style-type: none"> <li>◦ <b>More Options &gt; HOST INFORMATION</b></li> <li>◦ Select <b>New initiator group using existing initiator groups</b>.</li> </ul> <p><b>NOTE:</b> The OS type for an igroup containing other igroups cannot be changed after it has been created.</p> </li> </ul>	ONTAP 9.9.1
<ul style="list-style-type: none"> <li>• Add a description to your igroup or host initiator                             <p>The description serves as an alias for the igroup or host initiator.</p> <ul style="list-style-type: none"> <li>◦ <b>More Options &gt; HOST INFORMATION</b></li> </ul> </li> </ul>	ONTAP 9.9.1
<ul style="list-style-type: none"> <li>• Create your LUN on an existing volume                             <p>By default, a new LUN is created in a new volume.</p> <ul style="list-style-type: none"> <li>◦ <b>More Options &gt; Add LUNs</b></li> <li>◦ Select <b>Group related LUNs</b>.</li> </ul> </li> </ul>	ONTAP 9.9.1
<ul style="list-style-type: none"> <li>• Disable QoS or choose a custom QoS policy                             <ul style="list-style-type: none"> <li>◦ <b>More Options &gt; Storage and Optimization</b></li> <li>◦ Select <b>Performance Service Level</b>.</li> </ul> <p><b>NOTE:</b> In ONTAP 9.9.1 and later, if you select a custom QoS policy, you can also select manual placement on a specified local tier.</p> </li> </ul>	ONTAP 9.8

5. For FC, zone your FC switches by WWPN. Use one zone per initiator and include all target ports in each zone.
6. On your Windows server, discover the new LUN.
7. Initialize the LUN and optionally format it with a file system.
8. Verify the Windows server can write and read data on the LUN.

## CLI

Create LUNs to provide storage for a Windows server using the FC or iSCSI SAN protocol with the ONTAP CLI.

1. Use the `system license show` command to verify that you have a license for FC or iSCSI.

```
system license show
```

Package	Type	Description	Expiration
Base	site	Cluster Base License	-
NFS	site	NFS License	-
CIFS	site	CIFS License	-
iSCSI	site	iSCSI License	-
FCP	site	FCP License	-

2. If you do not have a license for FC or iSCSI, use the `license add` command.

```
license add -license-code your_license_code
```

3. Enable your protocol service on the SVM:

**For iSCSI:** `vserver iscsi create -vserver vserver_name -target-alias vserver_name`

**For FC:** `vserver fcp create -vserver vserver_name -status-admin up`

4. Create two LIFs for the SVMs on each node:

```
network interface create -vserver vserver_name -lif lif_name -role data -data
-protocol iscsi|fc -home-node node_name -home-port port_name -address
ip_address -netmask netmask
```

NetApp supports a minimum of one iSCSI or FC LIF per node for each SVM serving data. However, two LIFS per node are required for redundancy.

5. Verify that your LIFs have been created and that their operational status is online:

```
network interface show -vserver vserver_name lif_name
```

6. Create your LUNs:

```
lun create -vserver vserver_name -volume volume_name -lun lun_name -size
lun_size -ostype linux -space-reserve enabled|disabled
```

Your LUN name cannot exceed 255 characters and cannot contain spaces.



The NVFAIL option is automatically enabled when a LUN is created in a volume.

7. Create your igroups:

```
igroup create -vserver vserver_name -igroup igroup_name -protocol  
fc|iSCSI|mixed -ostype linux -initiator initiator_name
```

8. Map your LUNs to igroups:

```
lun mapping create -vserver vserver_name -volume volume_name -lun lun_name  
-igroup igroup_name
```

9. Verify that your LUNs are configured correctly:

```
lun show -vserver vserver_name
```

10. [Create a port set and bind to an igroup](#) (optional).

11. Follow steps in your host documentation for enabling block access on your specific hosts.

12. Use the Host Utilities to complete the FC or iSCSI mapping and to discover your LUNs on the host.

## Related information

[ONTAP SAN Host Configuration](#)

[SAN Administration overview](#)

[View and manage SAN initiator groups in System Manager](#)

[NetApp Technical Report 4017: Fibre Channel SAN Best Practices](#)

= Provision SAN storage

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

If a procedure for your specific host is not available, you can use these steps to provision storage for any support SAN host.

This procedure creates new LUNs on an existing storage VM which already has the FC or iSCSI protocol configured.

If you need to create a new storage VM and configure the FC or iSCSI protocol, see [Configure an SVM for FC](#) or [Configure an SVM for iSCSI](#).

If the FC license is not enabled, the LIFs and SVMs appear to be online but the operational status is down.

LUNs appear to your host as disk devices.



Asymmetric logical unit access (ALUA) is always enabled during LUN creation. You cannot change the ALUA setting.

You must use single initiator zoning for all of the FC LIFs in the SVM to host the initiators.

Unresolved directive in san-admin/provision-storage.adoc -  
include::\_include/98\_qos\_enabled\_by\_default.adoc[]

## System Manager

Create LUNs to provide storage for a SAN host using the FC or iSCSI protocol with ONTAP System Manager (9.7 and later).

To complete this task using System Manager Classic (available with 9.7 and earlier) refer to [iSCSI configuration for Red Hat Enterprise Linux](#)

## Steps

1. Install the appropriate [SAN host utilities](#) on your host.
2. In System Manager, click **Storage > LUNs** and then click **Add**.
3. Enter the required information to create the LUN.

Unresolved directive in san-admin/provision-storage.adoc -

```
include::_include/san_add_lun_more_options.adoc[]
```

5. For FC, zone your FC switches by WWPN. Use one zone per initiator and include all target ports in each zone.
6. Discover LUNs on your host.
7. Verify that the host can write and read data on the LUN.

## CLI

Create LUNs to provide storage for a SAN host using the FC or iSCSI protocol with the ONTAP CLI.

1. Use the `system license show` command to verify that you have a license for FC or iSCSI.

```
system license show
```

Package	Type	Description	Expiration
Base	site	Cluster Base License	-
NFS	site	NFS License	-
CIFS	site	CIFS License	-
iSCSI	site	iSCSI License	-
FCP	site	FCP License	-

2. If you do not have a license for FC or iSCSI, use the `license add` command.

```
license add -license-code your_license_code
```

3. Enable your protocol service on the SVM:

**For iSCSI:** `vserver iscsi create -vserver vserver_name -target-alias vserver_name`

**For FC:** `vserver fcp create -vserver vserver_name -status-admin up`

4. Create two LIFs for the SVMs on each node:

```
network interface create -vserver vserver_name -lif lif_name -role data -data  
-protocol iscsi|fc -home-node node_name -home-port port_name -address  
ip_address -netmask netmask
```

NetApp supports a minimum of one iSCSI or FC LIF per node for each SVM serving data. However, two LIFS per node are required for redundancy.

5. Verify that your LIFs have been created and that their operational status is online:

```
network interface show -vserver vserver_name lif_name
```

6. Create your LUNs:

```
lun create -vserver vserver_name -volume volume_name -lun lun_name -size  
lun_size -ostype linux -space-reserve enabled|disabled
```

Your LUN name cannot exceed 255 characters and cannot contain spaces.



The NVFAIL option is automatically enabled when a LUN is created in a volume.

7. Create your igroups:

```
igroup create -vserver vserver_name -igroup igroup_name -protocol  
fcp|iscsi|mixed -ostype linux -initiator initiator_name
```

8. Map your LUNs to igroups:

```
lun mapping create -vserver vserver_name -volume volume_name -lun lun_name  
-igroup igroup_name
```

9. Verify that your LUNs are configured correctly:

```
lun show -vserver vserver_name
```

10. [Create a port set and bind to an igroup](#) (optional).

11. Follow steps in your host documentation for enabling block access on your specific hosts.

12. Use the Host Utilities to complete the FC or iSCSI mapping and to discover your LUNs on the host.

## Related information

[SAN Administration overview](#)

[ONTAP SAN Host Configuration](#)

[View and manage SAN initiator groups in System Manager](#)

[NetApp Technical Report 4017: Fibre Channel SAN Best Practices](#)

= NVMe provisioning

= NVMe Overview

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

Beginning with ONTAP 9.4, NVMe/FC is supported on non-MetroCluster AFF configurations. Beginning with ONTAP 9.9.1 NVMe/FC is also supported on all non-MetroCluster All SAN Array (ASA) configurations.

You can use the non-volatile memory express (NVMe) protocol to provide storage in a SAN environment. The NVMe protocol is optimized for performance with solid state storage.

For NVMe, storage targets are called namespaces. An NVMe namespace is a quantity of non-volatile storage that can be formatted into logical blocks and presented to a host as a standard block device. You create namespaces and subsystems, and then map the namespaces to the subsystems, similar to the way LUNs are provisioned and mapped to igroups for FC and iSCSI.

NVMe targets are connected to the network through a standard FC infrastructure using FC switches or a standard TCP infrastructure using Ethernet switches and host-side adapters.

== What NVMe is

The nonvolatile memory express (NVMe) protocol is a transport protocol used for accessing nonvolatile storage media.

NVMe over Fabrics (NVMeoF) is a specification-defined extension to NVMe that enables NVMe-based communication over connections other than PCIe. This interface allows for external storage enclosures to be connected to a server.

NVMe is designed to provide efficient access to storage devices built with non-volatile memory, from flash technology to higher performing, persistent memory technologies. As such, it does not have the same limitations as storage protocols designed for hard disk drives. Flash and solid state devices (SSDs) are a type of non-volatile memory (NVM). NVM is a type of memory that keeps its content during a power outage. NVMe is a way that you can access that memory.

The benefits of NVMe include increased speeds, productivity, throughput, and capacity for data transfer. Specific characteristics include the following:

- NVMe is designed to have up to 64 thousand queues.

Each queue in turn can have up to 64 thousand concurrent commands.

- NVMe is supported by multiple hardware and software vendors
- NVMe is more productive with Flash technologies enabling faster response times

- NVMe allows for multiple data requests for each “request” sent to the SSD.

NVMe takes less time to decode a “request” and does not require thread locking in a multithreaded program.

- NVMe supports functionality that prevents bottlenecks at the CPU level and enables massive scalability as systems expand.

== About NVMe namespaces

An NVMe namespace is a quantity of non-volatile memory (NVM) that can be formatted into logical blocks. Namespaces are used when a storage virtual machine is configured with the NVMe protocol and are the equivalent of LUNs for FC and iSCSI protocols.

One or more namespaces are provisioned and connected to an NVMe host. Each namespace can support various block sizes.

The NVMe protocol provides access to namespaces through multiple controllers. Using NVMe drivers, which are supported on most operating systems, solid state drive (SSD) namespaces appear as standard-block devices on which file systems and applications can be deployed without any modification.

A namespace ID (NSID) is an identifier used by a controller to provide access to a namespace. When setting the NSID for a host or host group, you also configure the accessibility to a volume by a host. A logical block can only be mapped to a single host group at a time, and a given host group does not have any duplicate NSIDs.

== About NVMe subsystems

An NVMe subsystem includes one or more NVMe controllers, namespaces, NVM subsystem ports, an NVM storage medium, and an interface between the controller and the NVM storage medium. When you create an NVMe namespace, by default it is not mapped to a subsystem. You can also choose to map it a new or existing subsystem.

### Related information

- [Provision NVMe storage for SUSE Linux](#)
- [Provision NVMe storage for other hosts](#)
- [Map an NVMe namespace to a subsystem](#)

= NVMe license requirements

:icons: font

:relative\_path: ./nvme/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

Beginning with ONTAP 9.5 a license is required to support NVMe. If NVMe is enabled in ONTAP 9.4, a 90 day grace period is given to acquire the license after upgrading to ONTAP 9.5.

You can enable the license using the following command:

```
system license add -license-code NVMe_license_key
```

= NVMe support and limitations

:icons: font



:relative\_path: ./nvme/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

NVMe support and limitations varies based on your version of ONTAP, your platform and your configuration.

== Namespace limitations and support

To set up the NVMe protocol in your SAN environment, you must configure an SVM for NVMe, create namespaces and subsystems, configure an NVMe/FC LIF, and then map the namespaces to the subsystems. When working with NVMe namespaces you should be aware of the following:

- Beginning with ONTAP 9.10.1, you can [resize a namespace](#). Resizing a namespace is not supported in releases prior to ONTAP 9.10.1.

- Beginning with ONTAP 9.6, namespaces support 512 byte blocks and 4096 byte blocks.

4096 is the default value. 512 should only be used if the host operating system does not support 4096 byte blocks.

- If you lose data in a LUN, it cannot be restored from a namespace, or vice versa.
- The space guarantee for namespaces is the same as the space guarantee of the containing volume.
- Namespaces do not support the following:

- Renaming

You cannot rename a namespace.

- Inter-volume move
- Inter-volume copy

== Protocol support

Protocol	Beginning with ...	Allowed by...
TCP	ONTAP 9.10.1	Default
FCP	ONTAP 9.4	Default

== Platform and configuration support and limitations

Support for NVMe-oF protocol varies by platform and configuration. For details on your specific configuration, see the [NetApp Interoperability Matrix Tool](#).

Beginning with ONATP...	Platforms	Supported configurations
9.9.1	AFF and All SAN Array (ASA) platforms	Non-MetroCluster configurations only
9.4	AFF platforms only	Non-MetroCluster configurations only

= Configure a storage VM for NVMe

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/


If you want to use the NVMe protocol on a node, you must configure your SVM specifically for NVMe.

#### What you'll need

Your FC or Ethernet adapters must support NVMe. Supported adapters are listed in the [NetApp Hardware Universe](#).

## System Manager

Configure an storage VM for NVMe with ONTAP System Manager (9.7 and later).

To configure NVMe on a new storage VM	To configure NVMe on an existing storage VM
<ol style="list-style-type: none"><li>1. In System Manager, click <b>Storage &gt; Storage VMs</b> and then click <b>Add</b>.</li><li>2. Enter a name for the storage VM.</li><li>3. Select <b>NVMe</b> for the <b>Access Protocol</b>.</li><li>4. Click <b>Enable FC</b> and <b>Save</b>.</li></ol>	<ol style="list-style-type: none"><li>1. In System Manager, click <b>Storage &gt; Storage VMs</b>.</li><li>2. Click on the storage VM you want to configure.</li><li>3. Click on the <b>Settings</b> tab, and then click  next to the NVMe protocol.</li><li>4. Click <b>Enable FC</b> and <b>Save</b>.</li></ol>

## CLI

Configure an storage VM for NVMe with the ONTAP CLI.

1. If you do not want to use an existing SVM, create one:

```
vserver create -vserver SVM_name
```

- a. Verify that the SVM is created:

```
vserver show
```

2. Verify that you have NVMe or TCP capable adapters installed in your cluster:

```
For NVMe: network fcp adapter show -data-protocols-supported fc-nvme
```

```
For TCP: network port show
```

3. If you are running ONTAP 9.7 or earlier, remove all protocols from the SVM:

```
vserver remove-protocols -vserver SVM_name -protocols iscsi, fcp, nfs, cifs, ndmp
```

Beginning with ONTAP 9.8, it is not necessary to remove other protocols when adding NVMe.

4. Add the NVMe protocol to the SVM:

```
vserver add-protocols -vserver SVM_name -protocols nvme
```

5. If you are running ONTAP 9.7 or earlier, verify that NVMe is the only protocol allowed on the SVM:

```
vserver show -vserver SVM_name -fields allowed-protocols
```

NVMe should be the only protocol displayed under the `allowed protocols` column.

6. Create the NVMe service:

```
vserver nvme create -vserver SVM_name
```

7. Verify that the NVMe service was created:

```
vserver nvme show -vserver SVM_name
```

The `Administrative Status` of the SVM should be listed as `up`.

8. Create an NVMe/FC LIF:

ONTAP version	Applicable protocols	Command
ONTAP 9.9.1 or earlier	FC	<pre>network interface create -vserver <i>SVM_name</i> -lif lif_name -role data -data -protocol fc-nvme -home -node home_node -home -port home_port</pre>
ONTAP 9.10.1	FC or TCP	<pre>network interface create -vserver <i>SVM_name</i> -lif lif_name -service-policy {default-data-nvme-tcp   default-data-nvme-fc} -home-node home_node -home-port home_port -status admin up -failover-policy disabled -firewall-policy data -auto-revert false -failover-group failover_group -is-dns -update-enabled false</pre>

9. Create an NVMe/FC LIF on the HA partner node:

ONTAP version	Applicable protocols	Command
ONTAP 9.9.1 or earlier	FC	<pre>network interface create -vserver <i>SVM_name</i> -lif lif_name -role data -data -protocol fc-nvme -home -node home_node -home -port home_port</pre>

ONTAP version	Applicable protocols	Command
ONTAP 9.10.1 or later	FC or TCP	<pre>network interface create -vserver SVM_name -lif lif_name -service-policy {default-data-nvme-tcp   default-data-nvme-fc} -home-node home_node -home-port home_port -status admin up -failover-policy disabled -firewall-policy data -auto-revert false -failover-group failover_group -is-dns -update-enabled false</pre>

10. Verify the NVMe/FC LIFs were created:

```
network interface show -vserver SVM_name
```

11. Create volume on the same node as the LIF:

```
vol create -vserver SVM_name -volume vol_name -aggregate aggregate_name -size
volume_size
```

If a warning message is displayed about the auto efficiency policy, it can be safely ignored.

= Provision NVMe storage for SUSE Linux

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

Create namespaces to provide storage for a SUSE Linux server using the NVMe protocol. Namespaces appear to Linux as SCSI disk devices.

This procedure creates new namespaces on an existing storage VM. Your storage VM must be configured for NVMe, and your FC or TCP transport should already be set up.

Beginning with ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

## System Manager

Create namespaces to provide storage using the NVMe protocol with ONTAP System Manager (9.7 and later).

1. In System Manager, click **Storage > NVMe Namespaces** and then click **Add**.

- a. If you need to create a new subsystem, click **More Options**.
  - b. If you are running ONTAP 9.8 or later and you want to disable QoS or choose a custom QoS policy, click **More Options** and then, under **Storage and Optimization** select **Performance Service Level**.
2. Zone your FC switches by WWPN. Use one zone per initiator and include all target ports in each zone.
  3. On your Linux server, discover the new namespaces.
  4. Initialize the namespace and format it with a file system.
  5. Verify the Linux server can write and read data on the namespace.

## CLI

Create namespaces to provide storage using the NVMe protocol with the ONTAP CLI.

This procedure creates an NVMe namespace and subsystem on an existing storage VM which has already been configured for the NVMe protocol, then maps the namespace to the subsystem to allow data access from your host system.

If you need to configure the storage VM for NVMe, see [Configure an SVM for NVMe](#).

### Steps

1. Verify that the SVM is configured for NVMe:

```
vserver show -vserver SVM_name -fields allowed-protocols
```

NVMe should be displayed under the `allowed-protocols` column.

2. Create the NVMe namespace:

```
vserver nvme namespace create -vserver SVM_name -path path -size size_of_namespace -ostype OS_type
```

3. Create the NVMe subsystem:

```
vserver nvme subsystem create -vserver SVM_name -subsystem name_of_subsystem -ostype OS_type
```

The NVMe subsystem name is case sensitive. It must contain 1 to 96 characters. Special characters are allowed.

4. Verify that the subsystem was created:

```
vserver nvme subsystem show -vserver SVM_name
```

The `nvme` subsystem should be displayed under the `Subsystem` column.

5. Obtain the NQN from the host.
6. Add the host NQN to the subsystem:

```
vserver nvme subsystem host add -vserver SVM_name -subsystem subsystem_name -host-nqn Host_NQN:subsystem.subsystem_name
```

7. Map the namespace to the subsystem:

```
vserver nvme subsystem map add -vserver SVM_name -subsystem subsystem_name
-path path
```

A namespace can only be mapped to a single subsystem.

8. Verify that the namespace is mapped to the subsystem:

```
vserver nvme namespace show -vserver SVM_name -instance
```

The subsystem should be listed as the `Attached` subsystem.

```
= Provision NVMe storage
:icons: font
:relative_path: ./san-admin/
:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/
```

If a procedure for your specific host is not available, you can use these steps to create namespaces and provision storage for any NVMe supported host.

Namespaces appear to Linux as SCSI disk devices.

This procedure creates new namespaces on an existing storage VM. Your storage VM must be configured for NVMe, and your FC or TCP transport should already be set up.

```
Unresolved directive in san-admin/create-nvme-namespace-subsystem-task.adoc -
include::_include/98_qos_enabled_by_default.adoc[]
```

## System Manager

Create namespaces to provide storage using the NVMe protocol with ONTAP System Manager (9.7 and later).

1. In System Manager, click **Storage > NVMe Namespaces** and then click **Add**.

If you need to create a new subsystem, click **More Options**.

```
Unresolved directive in san-admin/create-nvme-namespace-subsystem-task.adoc -
include::_include/98_qos_how_to_modify.adoc[]
```

2. Zone your FC switches by WWPN. Use one zone per initiator and include all target ports in each zone.
3. On your host, discover the new namespaces.
4. Initialize the namespace and format it with a file system.
5. Verify that your host can write and read data on the namespace.

## CLI

Create namespaces to provide storage using the NVMe protocol with the ONTAP CLI.

This procedure creates an NVMe namespace and subsystem on an existing storage VM which has already been configured for the NVMe protocol, then maps the namespace to the subsystem to allow data access from your host system.

If you need to configure the storage VM for NVMe, see [Configure an SVM for NVMe](#).

Unresolved directive in san-admin/create-nvme-namespace-subsystem-task.adoc - include::\_include/nvme-provisioning-cli.adoc[]

## About NVMe subsystems

An NVMe subsystem includes one or more controllers, one or more namespaces, one or more non-volatile memory (NVM) subsystem ports (FC-NVMe or RDMA transport ports), an NVM storage medium, and an interface between the controllers and the NVM storage medium. For controller mapping and management, an NVM subsystem maps to a vserver in ONTAP.

An NVMe over Fabric (NVMeoF) subsystem is a separate kernel object that resides in the FreeBSD kernel. The NVMeoF subsystem interfaces with the following components:

- SAN components, such as BCOMKA, FCT, and VDOM
- WAFL
- RAS components, such as CM, ASUP, and EMS

All interfaces with NVMeoF subsystems adhere to the current definitions and patterns found in ONTAP.

## Map an NVMe namespace to a subsystem

This procedure maps an existing NVMe namespace to an existing NVMe subsystem using the ONTAP CLI.

Your namespace and subsystem should already be created. If you need to create a namespace and subsystem, see [Provision NVMe storage](#).

### Steps

1. Obtain the NQN from the host.
2. Add the host NQN to the subsystem:

```
vserver nvme subsystem host add -vserver SVM_name -subsystem subsystem_name
-host-nqn Host_NQN:subsystem.subsystem_name
```

3. Map the namespace to the subsystem:

```
vserver nvme subsystem map add -vserver SVM_name -subsystem subsystem_name
-path path
```

A namespace can only be mapped to a single subsystem.

4. Verify that the namespace is mapped to the subsystem:

```
vserver nvme namespace show -vserver SVM_name -instance
```

The subsystem should be listed as the `Attached` subsystem.

## Manage LUNs

## Edit LUN QoS policy group

Beginning with ONTAP 9.10.1, you can use System Manager to assign or remove Quality of Service (QoS) policies on multiple LUNs at the same time.



If the QoS policy is assigned at the volume level, it must be change at the volume level. You can only edit the QoS policy at the LUN level if it was originally assigned at the LUN level.

### Steps

1. In System Manager, click **Storage > LUNs**.
2. Select the LUN or LUNs you want to edit.

If you are editing more than one LUN at a time, the LUNs must belong to the same Storage Virtual Machine (SVM). If you select LUNs that do not belong to the same SVM, the option to edit the QoS Policy Group is not displayed.

3. Click **More** and select **Edit QoS Policy Group**.

## Convert a LUN into a namespace

Beginning with ONTAP 9.11.1, you can use the ONTAP CLI to in-place convert an existing LUN to an NVMe namespace.

### What you'll need

- Specified LUN should not have any existing maps to an igroup.
- LUN should not be in a MetroCluster configured SVM or in an SM-BC relationship.
- LUN should not be a protocol endpoint or bound to a protocol endpoint.
- LUN should not have non-zero prefix and/or suffix stream.
- LUN should not be part of a snapshot or on the destination side of SnapMirror relationship as a read-only LUN.

### Steps

1. You enter the following command to convert a LUN to an NVMe namespace:

```
vserver nvme namespace convert-from-lun -vserver -lun-path
```

## Take a LUN offline


Beginning with ONTAP 9.10.1 you can use System Manager to take LUNs offline. Prior to ONTAP 9.10.1, you must use the ONTAP CLI to take LUNs offline.



## System Manager

### Steps

1. In System Manager, click **Storage>LUNs**.
2. Take a single LUN or multiple LUNs offline

If you want to...	Do this...
Take a single LUN offline	Next to the LUN name, click  and select <b>Take Offline</b> .
Take multiple LUNs offline	<ol style="list-style-type: none"><li>a. Select the LUNs you want to take offline.</li><li>b. Click <b>More</b> and select <b>Take Offline</b>.</li></ol>

### CLI

You can only take one LUN offline at a time when using the CLI.

### Step

1. Take the LUN offline: `lun offline lun_name -vserver SVM_name`

## Resize a LUN

You can increase or decrease the size of a LUN.



Solaris LUNs cannot be resized.

### Increase the size of a LUN

The size to which you can increase your LUN varies depending upon your version of ONTAP.

ONTAP version	Maximum LUN size
ONTAP 9.8 and later	<ul style="list-style-type: none"><li>• 128 TB for All SAN Arrays (ASAs)</li><li>• 16 TB for non-ASAs</li></ul>
ONTAP 9.5, 9.6, 9.7	16TB
ONTAP 9.4 or earlier	<p>10 times the original LUN size, but not greater than 16TB, which is the maximum LUN size.</p> <p>For example, if you create a 100 GB LUN, you can only grow it to 1,000 GB.</p> <p>The actual maximum size of the LUN might not be exactly 16TB. ONTAP rounds down the limit to be slightly less.</p>


You do not need to take the LUN offline to increase the size. However, after you have increased the size, you must rescan the LUN on the host for the host to recognize the change in size.

See the Command Reference page for the `lun resize` command for more information about resizing a LUN.

## Example 2. Steps

### System Manager

Increase the size of a LUN with ONTAP System Manager (9.7 and later).

1. In System Manager, click **Storage > LUNs**.
2. Click  and select **Edit**.
3. Under **Storage and Optimization** increase the size of the LUN and **Save**.

### CLI

Increase the size of a LUN with the ONTAP CLI.

1. Increase the size of the LUN:

```
lun resize -vserver vserver_name -volume volume_name -lun lun_name -size lun_size
```

2. Verify the increased LUN size:

```
lun show -vserver vserver_name
```

ONTAP operations round down the actual maximum size of the LUN so it is slightly less than the expected value. Also, actual LUN size might vary slightly based on the OS type of the LUN. To obtain the exact resized value, run the following commands in advanced mode:



```
+  
set -unit B
```

```
+  
lun show -fields max-resize-size -volume volume_name -lun lun_name
```

3. Rescan the LUN on the host.
4. Follow your host documentation to make the newly created LUN size visible to the host file system.

## Decrease the size of a LUN

Before you decrease the size of a LUN, the host needs to migrate the blocks containing the LUN data into the boundary of the smaller LUN size. You should use a tool such as SnapDrive for Windows to ensure that the LUN is properly decreased without truncating blocks containing LUN data. Manually decreasing the size of your LUN is not recommended.

After you decrease the size of your LUN, ONTAP automatically notifies the initiator that the LUN size has decreased. However, additional steps might be required on your host for the host to recognize the new LUN size. Check your host documentation for specific information about decreasing the size of the host file

structure.

## Move a LUN

You can move a LUN across volumes within a storage virtual machine (SVM), but you cannot move a LUN across SVMs. LUNs moved across volumes within an SVM are moved immediately and without loss of connectivity.

### What you'll need

If your LUN is using Selective LUN Map (SLM), the SLM reporting nodes must have been modified to include the destination node and its HA partner.

### About this task

Storage efficiency features, such as deduplication, compression, and compaction are not preserved during a LUN move. They must be reapplied after the LUN move is completed.

Data protection through Snapshot copies occurs at the volume level. Therefore, when you move a LUN, it falls under the data protection scheme of the destination volume. If you do not have Snapshot copies established for the destination volume, Snapshot copies of the LUN are not created. Also, all of the Snapshot copies of the LUN stay in the original volume until those Snapshot copies are deleted.

You cannot move a LUN to the following volumes:

- A SnapMirror destination volume
- The SVM root volume

You cannot move the following types of LUNs:

- A LUN that has been created from a file
- A LUN that is in NVFail state
- A LUN that is in a load-sharing relationship
- A protocol-endpoint class LUN



For Solaris `os_type` LUNs that are 1 TB or larger, the host might experience a timeout during the LUN move. For this LUN type, you should unmount the LUN before initiating the move.


### Example 3. Steps

#### System Manager

Move a LUN with ONTAP System Manager (9.7 and later).

Beginning with ONTAP 9.10.1, you can use System Manager to create a new volume when you move a single LUN. In ONTAP 9.8 and 9.9.1, the volume to which you are moving your LUN must exist before you begin the LUN move.

#### Steps

1. In System Manager, click **Storage>LUNs**.
2. Right click the LUN you want to move, then click  and select **Move LUN**.

In ONTAP 9.10.1, select to move the LUN to **An existing volume** or to a **New volume**.

If you select to create a new volume, provide the volume specifications.

3. Click **Move**.

#### CLI

Move a LUN with the ONTAP CLI.

1. Move the LUN:

```
lun move start.
```

During a very brief period, the LUN is visible on both the origin and destination volume. This is expected and is resolved upon completion of the move.

2. Track the status of the move and verify successful completion:

```
lun move show.
```

#### Related information

- [Selective LUN Map](#)
- [Modifying the SLM reporting-nodes list](#)

#### Delete LUNs

You can delete a LUN from a storage virtual machine (SVM) if you no longer need the LUN.

#### What you'll need

The LUN must be unmapped from its igroup before you can delete it.

#### Steps

1. Verify that the application or host is not using the LUN.
2. Unmap the LUN from the igroup:

```
lun mapping delete
```

```
lun mapping delete -vserver vs5 -volume vo5 -lun lun5 -igroup igr5
```

### 3. Delete the LUN:

```
lun delete
```

```
lun delete -vserver vs5 -volume vol5 -lun lun5
```

### 4. Verify that you deleted the LUN:

```
lun show
```

```
lun show -vserver vs5
```

Vserver	Path	State	Mapped	Type	Size
vs5	/vol/vol116/lun8	online	mapped	windows	10.00GB

## What to know before copying LUNs

You should be aware of certain things before copying a LUN.

Cluster administrators can copy a LUN across storage virtual machines (SVMs) within the cluster by using the `lun copy` command. Cluster administrators must establish the storage virtual machine (SVM) peering relationship using the `vserver peer create` command before an inter-SVM LUN copy operation is performed. There must be enough space in the source volume for a SIS clone.

LUNs in Snapshot copies can be used as source LUNs for the `lun copy` command. When you copy a LUN using the `lun copy` command, the LUN copy is immediately available for read and write access. The source LUN is unchanged by creation of a LUN copy. Both the source LUN and the LUN copy exist as unique LUNs with different LUN serial numbers. Changes made to the source LUN are not reflected in the LUN copy, and changes made to the LUN copy are not reflected in the source LUN. The LUN mapping of the source LUN is not copied to the new LUN; the LUN copy must be mapped.

Data protection through Snapshot copies occurs at the volume level. Therefore, if you copy a LUN to a volume different from the volume of the source LUN, the destination LUN falls under the data protection scheme of the destination volume. If you do not have Snapshot copies established for the destination volume, Snapshot copies are not created of the LUN copy.

Copying LUNs is a nondisruptive operation.

You cannot copy the following types of LUNs:

- A LUN that has been created from a file
- A LUN that is in NVFAIL state
- A LUN that is in a load-sharing relationship
- A protocol-endpoint class LUN

## Examine configured and used space of a LUN

Knowing the configured space and actual space used for your LUNs can help you determine the amount of space that can be reclaimed when doing space reclamation, the amount of reserved space that contains data, and the total configured size versus the actual size used for a LUN.

### Step

1. View the configured space versus the actual space used for a LUN:

```
lun show
```

The following example shows the configured space versus the actual space used by the LUNs in the vs3 storage virtual machine (SVM):

```
lun show -vserver vs3 -fields path, size, size-used, space-reserve
```

```
vs3 /vol/vol0/lun1 50.01GB disabled 25.00GB
vs3 /vol/vol0/lun1_backup 50.01GB disabled 32.15GB
vs3 /vol/vol0/lun2 75.00GB disabled 0B
vs3 /vol/vol0/lun0 5.00GB enabled 4.50GB
4 entries were displayed.
```

## Control and monitor I/O performance to LUNs by using Storage QoS

You can control input/output (I/O) performance to LUNs by assigning LUNs to Storage QoS policy groups. You might control I/O performance to ensure that workloads achieve specific performance objectives or to throttle a workload that negatively impacts other workloads.

### About this task

Policy groups enforce a maximum throughput limit (for example, 100 MB/s). You can create a policy group without specifying a maximum throughput, which enables you to monitor performance before you control the workload.

You can also assign storage virtual machines (SVMs) with FlexVol volumes and LUNs to policy groups.

Note the following requirements about assigning a LUN to a policy group:

- The LUN must be contained by the SVM to which the policy group belongs.

You specify the SVM when you create the policy group.

- If you assign a LUN to a policy group, then you cannot assign the LUN's containing volume or SVM to a policy group.

For more information about how to use Storage QoS, see the [System administration reference](#).

## Steps

1. Use the `qos policy-group create` command to create a policy group.
2. Use the `lun create` command or the `lun modify` command with the `-qos-policy-group` parameter to assign a LUN to a policy group.
3. Use the `qos statistics` commands to view performance data.
4. If necessary, use the `qos policy-group modify` command to adjust the policy group's maximum throughput limit.

## Tools available to effectively monitor your LUNs

Tools are available to help you effectively monitor your LUNs and avoid running out of space.

- Active IQ Unified Manager is a free tool that enables you to manage all storage across all clusters in your environment.
- System Manager is a graphical user interface built into ONTAP that enables you to manually manage storage needs at the cluster level.
- OnCommand Insight presents a single view of your storage infrastructure and enables you to set up automatic monitoring, alerts, and reporting when your LUNs, volumes, and aggregates are running out of storage space.

## Capabilities and restrictions of transitioned LUNs

In a SAN environment, a disruption in service is required during the transition of a 7-Mode volume to ONTAP. You need to shut down your hosts to complete the transition. After transition, you must update your host configurations before you can begin serving data in ONTAP.

You need to schedule a maintenance window during which you can shut down your hosts and complete the transition.

LUNs that have been transitioned from Data ONTAP operating in 7-Mode to ONTAP have certain capabilities and restrictions that affect the way the LUNs can be managed.

You can do the following with transitioned LUNs:

- View the LUN using the `lun show` command
- View the inventory of LUNs transitioned from the 7-Mode volume using the `transition 7-mode show` command
- Restore a volume from a 7-Mode Snapshot copy

Restoring the volume transitions all of the LUNs captured in the Snapshot copy

- Restore a single LUN from a 7-Mode Snapshot copy using the `snapshot restore-file` command
- Create a clone of a LUN in a 7-Mode Snapshot copy
- Restore a range of blocks from a LUN captured in a 7-Mode Snapshot copy
- Create a FlexClone of the volume using a 7-Mode Snapshot copy

You cannot do the following with transitioned LUNs:

- Access Snapshot copy-backed LUN clones captured in the volume

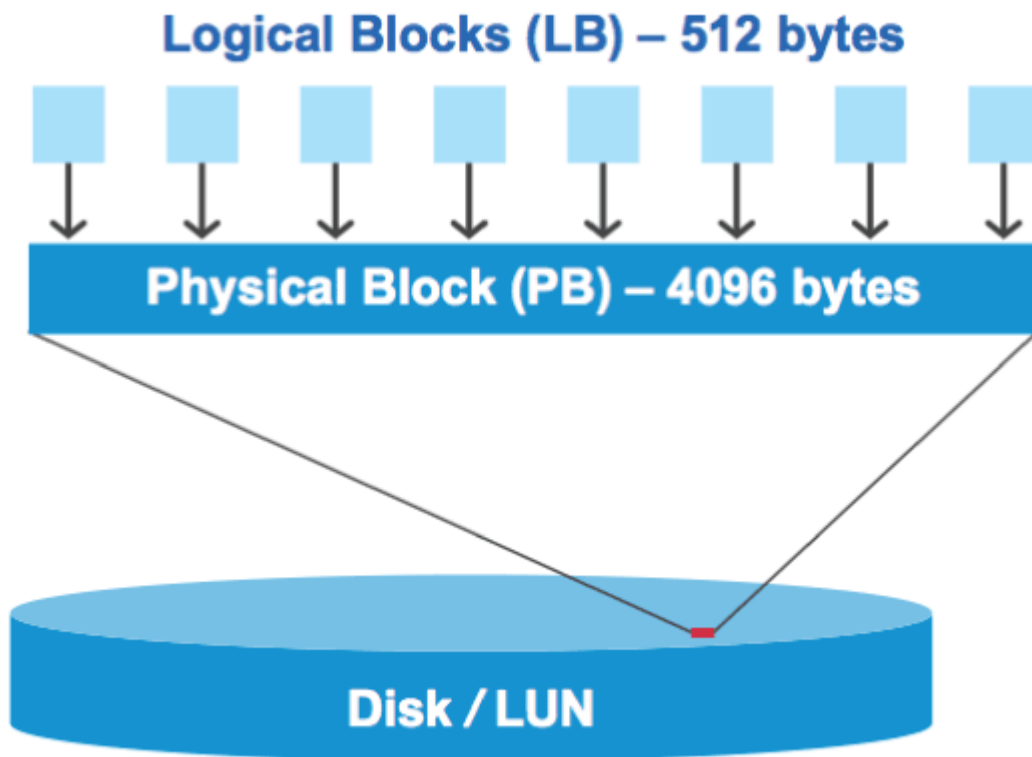
#### Related information

[Copy-based transition](#)

#### I/O misalignments on properly aligned LUNs overview

ONTAP might report I/O misalignments on properly aligned LUNs. In general, these misalignment warnings can be disregarded as long as you are confident that your LUN is properly provisioned and your partitioning table is correct.

LUNs and hard disks both provide storage as blocks. Because the block size for disks on the host is 512 bytes, LUNs present blocks of that size to the host while actually using larger, 4-KB blocks to store data. The 512-byte data block used by the host is referred to as a logical block. The 4-KB data block used by the LUN to store data is referred to as a physical block. This means that there are eight 512-byte logical blocks in each 4-KB physical block.



The host operating system can begin a read or write I/O operation at any logical block. I/O operations are only considered aligned when they begin at the first logical block in the physical block. If an I/O operation begins at a logical block that is not also the start of a physical block, the I/O is considered misaligned. ONTAP automatically detects the misalignment and reports it on the LUN. However, the presence of misaligned I/O does not necessarily mean that the LUN is also misaligned. It is possible for misaligned I/O to be reported on properly aligned LUNs.

If you require further investigation, see the Knowledge Base article [How to identify unaligned IO on LUNs?](#)

For more information about tools for correcting alignment problems, see the following documentation: +



- [Windows Unified Host Utilities 7.1](#)
- [Virtual Storage Console for VMware vSphere Installation and Administration Guide](#)

### Achieve I/O alignment using LUN OS types

To achieve I/O alignment with your OS partitioning scheme, you should use the recommended ONTAP LUN `ostype` value that most closely matches your operating system.

The partition scheme employed by the host operating system is a major contributing factor to I/O misalignments. Some ONTAP LUN `ostype` values use a special offset known as a “prefix” to enable the default partitioning scheme used by the host operating system to be aligned.



In some circumstances, a custom partitioning table might be required to achieve I/O alignment. However, for `ostype` values with a “prefix” value greater than 0, a custom partition might create misaligned I/O.

The LUN `ostype` values in the following table should be used based on your operating system.

LUN <code>ostype</code>	Prefix (bytes)	Prefix (sectors)	Operating system
windows	32,256	63	Windows 2000, 2003 (MBR format)
windows_gpt	17,408	34	Windows 2003 (GPT format)
windows_2008	0	0	Windows 2008 and later
linux	0	0	All Linux distributions
xen	0	0	Citrix XenServer
vmware	0	0	VMware ESX
solaris	1MB	2,048	Solaris
solaris_efi	17,408	34	Solaris
hpux	0	0	HP-UX
aix	0	0	AIX

### Special I/O alignment considerations for Linux

Linux distributions offer a wide variety of ways to use a LUN including as raw devices for databases, various volume managers, and file systems. It is not necessary to create partitions on a LUN when used as a raw device or as physical volume in a logical volume.

For RHEL 5 and earlier and SLES 10 and earlier, if the LUN will be used without a volume manager, you should partition the LUN to have one partition that begins at an aligned offset, which is a sector that is an even multiple of eight logical blocks.

### Special I/O alignment considerations for Solaris LUNs

You need to consider various factors when determining whether you should use the `solaris` ostype or the `solaris_efi` ostype.

See the [Solaris Host Utilities Installation and Administration Guide](#) for detailed information.

### ESX boot LUNs report as misaligned

LUNs used as ESX boot LUNs are typically reported by ONTAP as misaligned. ESX creates multiple partitions on the boot LUN, making it very difficult to align. Misaligned ESX boot LUNs are not typically a performance problem because the total amount of misaligned I/O is small. Assuming that the LUN was correctly provisioned with the VMware `ostype`, no action is needed.

### Related information

[Guest VM file system partition/disk alignment for VMware vSphere, other virtual environments, and NetApp storage systems](#)

### Ways to address issues when LUNs go offline

When no space is available for writes, LUNs go offline to preserve data integrity. LUNs can run out of space and go offline for various reasons, and there are several ways you can address the issue.

If the...	You can...
Aggregate is full	<ul style="list-style-type: none"><li>• Add more disks.</li><li>• Use the <code>volume modify</code> command to shrink a volume that has available space.</li><li>• If you have space-guarantee volumes that have available space, change the volume space guarantee to <code>none</code> with the <code>volume modify</code> command.</li></ul>

If the...	You can...
Volume is full but there is space available in the containing aggregate	<ul style="list-style-type: none"> <li>• For space guarantee volumes, use the <code>volume modify</code> command to increase the size of your volume.</li> <li>• For thinly provisioned volumes, use the <code>volume modify</code> command to increase the maximum size of your volume.</li> </ul> <p>If volume autogrow is not enabled, use <code>volume modify -autogrow-mode</code> to enable it.</p> <ul style="list-style-type: none"> <li>• Delete Snapshot copies manually with the <code>volume snapshot delete</code> command, or use the <code>volume snapshot autodelete modify</code> command to automatically delete Snapshot copies.</li> </ul>

### Related information

[Disk and aggregate management](#)

[Logical storage management](#)

### Troubleshoot iSCSI LUNs not visible on the host

The iSCSI LUNs appear as local disks to the host. If the storage system LUNs are not available as disks on the host, you should verify the configuration settings.

Configuration setting	What to do
Cabling	Verify that the cables between the host and storage system are properly connected.
Network connectivity	<p>Verify that there is TCP/IP connectivity between the host and storage system.</p> <ul style="list-style-type: none"> <li>• From the storage system command line, ping the host interfaces that are being used for iSCSI: <pre>ping -node <i>node_name</i> -destination <i>host_ip_address_for_iSCSI</i></pre> </li> <li>• From the host command line, ping the storage system interfaces that are being used for iSCSI: <pre>ping -node <i>node_name</i> -destination <i>host_ip_address_for_iSCSI</i></pre> </li> </ul>

Configuration setting	What to do
System requirements	Verify that the components of your configuration are qualified. Also, verify that you have the correct host operating system (OS) service pack level, initiator version, ONTAP version, and other system requirements. The Interoperability Matrix contains the most up-to-date system requirements.
Jumbo frames	If you are using jumbo frames in your configuration, verify that jumbo frames are enabled on all devices in the network path: the host Ethernet NIC, the storage system, and any switches.
iSCSI service status	Verify that the iSCSI service is licensed and started on the storage system.
Initiator login	Verify that the initiator is logged in to the storage system. If the <code>iscsi initiator show</code> command output shows no initiators are logged in, check the initiator configuration on the host. Also verify that the storage system is configured as a target of the initiator.
iSCSI node names (IQNs)	Verify that you are using the correct initiator node names in the igroup configuration. On the host, you can use the initiator tools and commands to display the initiator node name. The initiator node names configured in the igroup and on the host must match.
LUN mappings	Verify that the LUNs are mapped to an igroup. On the storage system console, you can use one of the following commands: <ul style="list-style-type: none"> <li>• <code>lun mapping show</code> displays all LUNs and the igroups to which they are mapped.</li> <li>• <code>lun mapping show -igroup</code> displays the LUNs mapped to a specific igroup.</li> </ul>
iSCSI LIFs enable	Verify that the iSCSI logical interfaces are enabled.

## Related information

[NetApp Interoperability Matrix Tool](#)

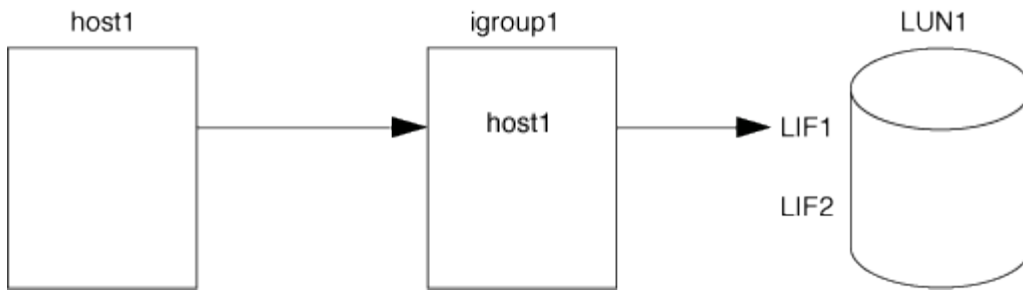
## Manage igroups and portsets

### Ways to limit LUN access with portsets and igroups

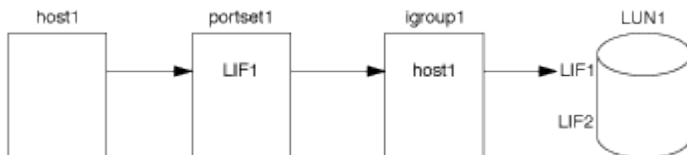
In addition to using Selective LUN Map (SLM), you can limit access to your LUNs through igroups and portsets.

Portsets can be used with SLM to further restrict access of certain targets to certain initiators. When using SLM with portsets, LUNs will be accessible on the set of LIFs in the portset on the node that owns the LUN and on that node's HA partner.

In the following example, initiator1 does not have a portset. Without a portset, initiator1 can access LUN1 through both LIF1 and LIF2.



You can limit access to LUN1 by using a portset. In the following example, initiator1 can access LUN1 only through LIF1. However, initiator1 cannot access LUN1 through LIF2 because LIF2 is not in portset1.



### Related information

- [Selective LUN Map](#)
- [Create a portset and bind to an igroup](#)

### View and manage SAN initiators and igroups

You can use System Manager to view and manage initiator groups (igroups) and initiators.

#### About this task

- The initiator groups identify which hosts are able to access specific LUNs on the storage system.
- After an initiator and initiator groups are created, you can also edit them or delete them.
- To manage SAN initiators groups and initiators, you can perform the following tasks:
  - [View and manage SAN initiator groups](#)
  - [View and manage SAN initiators](#)

#### View and manage SAN initiator groups

You can use System Manager to view a list of initiator groups (igroups). From the list, you can perform additional operations.

#### Steps

1. In System Manager, click **Hosts > SAN Initiator Groups**.

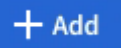
The page displays a list of initiator groups (igroups). If the list is large, you can view additional pages of the list by clicking the page numbers at the lower right corner of the page.

The columns display various information about the igroups. Beginning with 9.11.1, the connection status of the group is also displayed. Hover over status alerts to view details.


2. (Optional): You can perform the following tasks by clicking the icons at the upper right corner of the list:
  - **Search**

- **Download** the list.
- **Show** or **Hide** columns in the list.
- **Filter** the data in the list.

3. You can perform operations from the list:

- Click  to add an igroup.
- Click the igroup name to view the **Overview** page that shows details about the igroup.

On the **Overview** page, you can view the LUNs associated with the igroup, and you can initiate the operations to create LUNs and map the LUNs. Click **All SAN Initiators** to return to the main list.

- Hover over the igroup, then click  next to an igroup name to edit or delete the igroup.
- Hover over the area to the left of the igroup name, then check the check box. If you click **+Add to Initiator Group**, you can add that igroup to another igroup.
- In the **Storage VM** column, click the name of a storage VM to view details about it.

### View and manage SAN initiators

You can use System Manager to view a list of initiators. From the list, you can perform additional operations.

#### Steps

1. In System Manager, click **Hosts > SAN Initiator Groups**.

The page displays a list of initiator groups (igroups).

2. To view initiators, perform the following:

- Click the **FC Initiators** tab to view a list of FC initiators.
- Click the **iSCSI Initiators** tab to view a list of iSCSI initiators.

The columns display various information about the initiators.

Beginning with 9.11.1, the connection status of the initiator is also displayed. Hover over status alerts to view details.

3. (Optional): You can perform the following tasks by clicking the icons at the upper right corner of the list:

- **Search** the list for particular initiators.
- **Download** the list.
- **Show** or **Hide** columns in the list.
- **Filter** the data in the list.

### Create nested igroup

Beginning with ONTAP 9.9.1, you can create an igroup that consists of other existing igroups.

1. In System Manager, click **Host > SAN Initiator Groups**, and then click **Add**.
2. Enter the igroup **Name** and **Description**.

The description serves as the igroup alias.

3. Select the **Storage VM** and **Host Operating System**.



The OS type of a nested igroup cannot be changed after the igroup is created.

4. Under **Initiator Group Members** select **Existing initiator group**.

You can use **Search** to find and select the initiator groups you want to add.

### Map igroups to multiple LUNs

Beginning with ONTAP 9.9.1, you can map igroups to two or more LUNs simultaneously.

1. In System Manager, click **Storage > LUNs**.
2. Select the LUNs you want to map.
3. Click **More**, then click **Map To Initiator Groups**.



The selected igroups are added to the selected LUNs. The pre-existing mappings are not overwritten.

### Create a portsets and bind to an igroup

In addition to using [Selective LUN Map \(SLM\)](#), you can create a portset and bind the portset to an igroup to further limit which LIFs can be used by an initiator to access a LUN.

If you do not bind a portset to an igroup, then all of the initiators in the igroup can access mapped LUNs through all of the LIFs on the node owning the LUN and the owning node's HA partner.

#### What you'll need

You must have at least one LIF and one igroup.

Unless you are using interface groups, two LIFs are recommended for redundancy for both iSCSI and FC. Only one LIF is recommended for interface groups.

#### About this task

It is advantageous to use portsets with SLM when you have more than two LIFs on a node and you want to restrict a certain initiator to a subset of LIFs. Without portsets, all targets on the node will be accessible by all of the initiators with access to the LUN through the node owning the LUN and the owning node's HA partner.

## Example 4. Steps

### System Manager

Beginning with ONTAP 9.10.1, you can use System Manager to create portsets and bind them to igroups.

If you need to create a portset and bind it to an igroup in an ONTAP release earlier than 9.10.1 you must use the ONTAP CLI procedure.

1. In System Manager, click **Network > Overview > Portsets**, and click **Add**.
2. Enter the information for the new portset and click **Add**.
3. Click **Hosts > SAN Initiator Groups**.
4. To bind the portset to a new igroup, click **Add**.

To bind the portset to an existing igroup, select the igroup, click , and then click **Edit Initiator Group**.

### Related information

[View and manage initiators and igroups](#)

### CLI

1. Create a port set containing the appropriate LIFs:

```
portset create -vserver vserver_name -portset portset_name -protocol
protocol -port-name port_name
```

If you are using FC, specify the `protocol` parameter as `fc`. If you are using iSCSI, specify the `protocol` parameter as `iscsi`.

2. Bind the igroup to the port set:

```
lun igroup bind -vserver vserver_name -igroup igroup_name -portset
portset_name
```

3. Verify that your port sets and LIFs are correct:

```
portset show -vserver vserver_name
```

Vserver	Portset	Protocol	Port Names	Igroups
vs3	portset0	iscsi	lif0,lif1	igroup1


## Manage portsets

In addition to [Selective LUN Map \(SLM\)](#), you can use portsets to further limit which LIFs can be used by an initiator to access a LUN.

Beginning with ONTAP 9.10.1, you can use System Manager to change the network interfaces associated with portsets and to delete portsets.



## Change network interfaces associated with a portset

1. In System Manager, click **Network > Overview > Portsets**.
2. Select the portset you want to edit and click , then select **Edit Portset**.

## Delete a portset

1. In System Manager, click **Network > Overview > Portsets**.
2. To delete a single portset, select the portset, click , and then select **Delete Portsets**.

To delete multiple portsets, select the portsets, and click **Delete**.

## Selective LUN Map

### Selective LUN Map overview

Selective LUN Map (SLM) reduces the number of paths from the host to the LUN. With SLM, when a new LUN map is created, the LUN is accessible only through paths on the node owning the LUN and its HA partner.

SLM enables management of a single igroup per host and also supports nondisruptive LUN move operations that do not require portset manipulation or LUN remapping.

Portsets can be used with SLM just as in previous versions of ONTAP to further restrict access of certain targets to certain initiators. When using SLM with portsets, LUNs will be accessible on the set of LIFs in the portset on the node that owns the LUN and on that node's HA partner.

SLM is enabled by default on all new LUN maps.

### Determine whether SLM is enabled on a LUN map

If your environment has a combination of LUNs created in ONTAP and LUNs transitioned from previous versions, you might need to determine whether Selective LUN Map (SLM) is enabled on a specific LUN.

You can use the information displayed in the output of the `lun mapping show -fields reporting-nodes, node` command to determine whether SLM is enabled on your LUN map. If SLM is not enabled, "-" is displayed in the cells under the `reporting-nodes` column of the command output. If SLM is enabled, the list of nodes displayed under the `nodes` column is duplicated in the `reporting-nodes` column.

### Modify the SLM reporting-nodes list

If you are moving a LUN or a volume containing LUNs to another high availability (HA) pair within the same cluster, you should modify the Selective LUN Map (SLM) reporting-nodes list before initiating the move to ensure that active, optimized LUN paths are maintained.

### Steps

1. Add the destination node and its partner node to the reporting-nodes list of the aggregate or volume:

```
lun mapping add-reporting-nodes -vserver vservice_name -path lun_path -igroup
```

```
igroup_name [-destination-aggregate aggregate_name]-destination-volume  
volume_name]
```

If you have a consistent naming convention, you can modify multiple LUN mappings at the same time by using **-igroup** instead of `igroup`.

2. Rescan the host to discover the newly added paths.
3. If your OS requires it, add the new paths to your multipath network I/O (MPIO) configuration.
4. Run the command for the needed move operation and wait for the operation to finish.
5. Verify that I/O is being serviced through the Active/Optimized path:

```
lun mapping show -fields reporting-nodes
```

6. Remove the previous LUN owner and its partner node from the reporting-nodes list:

```
lun mapping remove-reporting-nodes -vserver vserver_name -path lun_path  
-igroup igroup_name -remote-nodes
```

7. Verify that the LUN has been removed from the existing LUN map:

```
lun mapping show -fields reporting-nodes
```

8. Remove any stale device entries for the host OS.
9. Change any multipathing configuration files if required.
10. Rescan the host to verify removal of old paths.  
See your host documentation for specific steps to rescan your hosts.

## Manage iSCSI protocol

### Configure your network for best performance

Ethernet networks vary greatly in performance. You can maximize the performance of the network used for iSCSI by selecting specific configuration values.

#### Steps

1. Connect the host and storage ports to the same network.

It is best to connect to the same switches. Routing should never be used.

2. Select the highest speed ports available, and dedicate them to iSCSI.

10 GbE ports are best. 1 GbE ports are the minimum.

3. Disable Ethernet flow control for all ports.

You should see [Network management](#) for using the CLI to configure Ethernet port flow control.

4. Enable jumbo frames (typically MTU of 9000).

All devices in the data path, including initiators, targets, and switches, must support jumbo frames. Otherwise, enabling jumbo frames actually reduces network performance substantially.

## Configure an SVM for iSCSI

To configure a storage virtual machine (SVM) for iSCSI, you must create LIFs for the SVM and assign the iSCSI protocol to those LIFs.


### About this task

You need a minimum of one iSCSI LIF per node for each SVM serving data with the iSCSI protocol. For redundancy, you should create at least two LIFs per node.

### Example 5. Steps

#### System Manager

Configure an storage VM for iSCSI with ONTAP System Manager (9.7 and later).

To configure iSCSI on a new storage VM	To configure iSCSI on an existing storage VM
<ol style="list-style-type: none"><li>1. In System Manager, click <b>Storage &gt; Storage VMs</b> and then click <b>Add</b>.</li><li>2. Enter a name for the storage VM.</li><li>3. Select <b>iSCSI</b> for the <b>Access Protocol</b>.</li><li>4. Click <b>Enable iSCSI</b> and enter the IP address and subnet mask for the network interface. + Each node should have at least two network interfaces.</li><li>5. Click <b>Save</b>.</li></ol>	<ol style="list-style-type: none"><li>1. In System Manager, click <b>Storage &gt; Storage VMs</b>.</li><li>2. Click on the storage VM you want to configure.</li><li>3. Click on the <b>Settings</b> tab, and then click  next to the iSCSI protocol.</li><li>4. Click <b>Enable iSCSI</b> and enter the IP address and subnet mask for the network interface. + Each node should have at least two network interfaces.</li><li>5. Click <b>Save</b>.</li></ol>

#### CLI

Configure an storage VM for iSCSI with the ONTAP CLI.

1. Enable the SVMs to listen for iSCSI traffic:

```
vserver iscsi create -vserver vserver_name -target-alias vserver_name
```

2. Create a LIF for the SVMs on each node to use for iSCSI:

```
network interface create -vserver vserver_name -lif lif_name -role data  
-data-protocol iscsi -home-node node_name -home-port port_name -address  
ip_address -netmask netmask
```

3. Verify that you set up your LIFs correctly:

```
network interface show -vserver vserver_name
```

4. Verify that iSCSI is up and running and the target IQN for that SVM:

```
vserver iscsi show -vserver vserver_name
```

5. From your host, create iSCSI sessions to your LIFs.

## Related information

[NetApp Technical Report 4080: Best practices for modern SAN](#)

## Define a security policy method for an initiator

You can define a list of initiators and their authentication methods. You can also modify the default authentication method that applies to initiators that do not have a user-defined authentication method.

### About this task

You can generate unique passwords using security policy algorithms in the product or you can manually specify the passwords that you want to use.



Not all initiators support hexadecimal CHAP secret passwords.

### Steps

1. Use the `vserver iscsi security create` command to create a security policy method for an initiator.

```
vserver iscsi security create -vserver vs2 -initiator iqn.1991-05.com.microsoft:host1 -auth-type CHAP -user-name bob1 -outbound-user-name bob2
```

2. Follow the screen commands to add the passwords.

Creates a security policy method for initiator `iqn.1991-05.com.microsoft:host1` with inbound and outbound CHAP user names and passwords.

## Related information

- [How iSCSI authentication works](#)
- [Guidelines for using CHAP authentication](#)
- [What CHAP authentication is](#)

## Delete an iSCSI service for an SVM

You can delete an iSCSI service for a storage virtual machine (SVM) if it is no longer required.

### What you'll need

The administration status of the iSCSI service must be in the “down” state before you can delete an iSCSI service. You can move the administration status to down with the `vserver iscsi modify` command.

### Steps

1. Use the `vserver iscsi modify` command to stop the I/O to the LUN.

```
vserver iscsi modify -vserver vs1 -status-admin down
```

2. Use the `vserver iscsi delete` command to remove the iscsi service from the SVM.

```
vserver iscsi delete -vserver vs_1
```

3. Use the `vserver iscsi show` command to verify that you deleted the iSCSI service from the SVM.

```
vserver iscsi show -vserver vs1
```

### Get more details in iSCSI session error recoveries

Increasing the iSCSI session error recovery level enables you to receive more detailed information about iSCSI error recoveries. Using a higher error recovery level might cause a minor reduction in iSCSI session performance.

#### About this task

By default, ONTAP is configured to use error recovery level 0 for iSCSI sessions. If you are using an initiator that has been qualified for error recovery level 1 or 2, you can choose to increase the error recovery level. The modified session error recovery level affects only the newly created sessions and does not affect existing sessions.

Beginning with ONTAP 9.4, the `max-error-recovery-level` option is not supported in the `iscsi show` and `iscsi modify` commands.

#### Steps

1. Enter advanced mode:

```
set -privilege advanced
```

2. Verify the current setting by using the `iscsi show` command.

```
iscsi show -vserver vs3 -fields max-error-recovery-level
```

```
vserver max-error-recovery-level
-----
vs3      0
```

3. Change the error recovery level by using the `iscsi modify` command.

```
iscsi modify -vserver vs3 -max-error-recovery-level 2
```

### Register the SVM with an iSNS server

You can use the `vserver iscsi isns` command to configure the storage virtual machine (SVM) to register with an iSNS server.

#### About this task

The `vserver iscsi isns create` command configures the SVM to register with the iSNS server. The SVM does not provide commands that enable you to configure or manage the iSNS server. To manage the iSNS server, you can use the server administration tools or the interface provided by the vendor for the iSNS server.

#### Steps

1. On your iSNS server, ensure that your iSNS service is up and available for service.
2. Create the SVM management LIF on a data port:

```
network interface create -vserver SVM_name -lif lif_name -role data -data
-protocol none -home-node home_node_name -home-port home_port -address
IP_address -netmask network_mask
```

3. Create an iSCSI service on your SVM if one does not already exist:

```
vserver iscsi create -vserver SVM_name
```

4. Verify that the iSCSI service was created successfully:

```
iscsi show -vserver SVM_name
```

5. Verify that a default route exists for the SVM:

```
network route show -vserver SVM_name
```

6. If a default route does not exist for the SVM, create a default route:

```
network route create -vserver SVM_name -destination destination -gateway
gateway
```

7. Configure the SVM to register with the iSNS service:

```
vserver iscsi isns create -vserver SVM_name -address IP_address
```

Both IPv4 and IPv6 address families are supported. The address family of the iSNS server must be the same as that of the SVM management LIF.

For example, you cannot connect an SVM management LIF with an IPv4 address to an iSNS server with an IPv6 address.

8. Verify that the iSNS service is running:

```
vserver iscsi isns show -vserver SVM_name
```

9. If the iSNS service is not running, start it:

```
vserver iscsi isns start -vserver SVM_name
```

## Resolve iSCSI error messages on the storage system

There are a number of common iSCSI-related error messages that you can view with the `event log show` command. You need to know what these messages mean and what you can do to resolve the issues they identify.

The following table contains the most common error messages, and instructions for resolving them:

Message	Explanation	What to do
ISCSI: network interface identifier disabled for use; incoming connection discarded	The iSCSI service is not enabled on the interface.	You can use the <code>iscsi interface enable</code> command to enable the iSCSI service on the interface. For example:  <pre>iscsi interface enable -vserver vs1 -lif lif1</pre>
ISCSI: Authentication failed for initiator nodename	CHAP is not configured correctly for the specified initiator.	You should check the CHAP settings; you cannot use the same user name and password for inbound and outbound settings on the storage system: <ul style="list-style-type: none"> <li>• Inbound credentials on the storage system must match outbound credentials on the initiator.</li> <li>• Outbound credentials on the storage system must match inbound credentials on the initiator.</li> </ul>

### iSCSI LIF failover for ASA platforms

Beginning with ONTAP 9.11.1 on All SAN Array (ASA) platforms, the iSCSI LIF failover feature supports automatic and manual migration of iSCSI LIFs in an SFO partner failover (when an iSCSI LIF moves from its home node/port to its HA partner node/port and back again) and in a local failover (when an iSCSI LIF moves from its unhealthy port to a healthy port on its current home node and back again). This feature provides faster I/O resumption for SAN workloads running on iSCSI.

#### About enabling iSCSI LIF failover

You should familiarize yourself with aspects of when iSCSI LIF failover is automatically enabled and when you must manually enable it, including how newly created iSCSI LIFs and existing iSCSI LIFs are affected.

- The automatic migration of an iSCSI LIF is a LIF failover and auto-revert, which is triggered in certain events, such as planned or unplanned failover, a physical ethernet link down, or a node dropping out of replicated database (RDB) quorum.
  - After upgrading your ASA HA pair to ONTAP 9.11.1, this feature is automatically enabled on newly created iSCSI LIFs if no iSCSI LIFs exist in the specified storage VM or if all existing iSCSI LIFs in the specified storage VM are already enabled with iSCSI LIF failover.
  - For iSCSI LIFs created prior to upgrading to ONTAP 9.11.1, to use the iSCSI LIF failover feature, you must enable it using the ONTAP CLI. (Enabling the failover feature and auto-revert capability means changing the failover policy to `sfo-partner-only` and designating the auto-revert value to `true`.)

[Manage iSCSI LIFs using the ONTAP CLI](#)

If you do not enable iSCSI LIF failover on the existing iSCSI LIFs, when there is a failover event, the iSCSI LIFs will not failover.

Additionally, if after upgrading to ONTAP 9.11.1 or later you have existing iSCSI LIFs in a storage VM that have not been enabled with the iSCSI LIF failover feature and you create new iSCSI LIFs in the same storage VM, the new iSCSI LIFs assume the same failover policy (`disabled`) of the existing iSCSI LIFs in the storage VM.

- The manual migration of an iSCSI LIF is a LIF migrate and revert, which is initiated by the cluster admin using the ONTAP CLI or System Manager.

### Migrate and revert an iSCSI LIF

You manually migrate and revert an iSCSI LIF under the following circumstances:

- When scheduled maintenance or replacement is needed.
- When you have a pre-existing iSCSI LIF, meaning that the iSCSI LIF was created before you upgraded your HA pair to ONTAP 9.11.1 or later, and you have not enabled the iSCSI LIF failover feature on the LIF.

### How iSCSI LIF failover works

For LIFs with iSCSI LIF failover enabled (either automatically or manually), the following applies.

- For LIFs using the `data-iscsi` service policy, the failover-policy is restricted to `sfo-partner-only`, `local-only`, and `disabled`.
- iSCSI LIFs can failover only to the HA partner when their failover policy is set to `sfo-partner-only`.
- Auto-revert of LIFs happens when the `auto-revert` is set to `true` and when the LIF's home port is healthy and able to host the LIF.
- On a planned or unplanned node takeover, the iSCSI LIF on the node which is taken-over fails over to the HA partner. The port on which the LIF fails over is determined by VIF Manager.
- Once the failover is complete, the iSCSI LIF operates normally.
- When a giveback is initiated, the iSCSI LIF reverts back to its home node and port, if `auto-revert` is set to `true`.
- When an ethernet link goes down on a port hosting one or more iSCSI LIFs, VIF Manager migrates the LIFs from the down port to a different port in the same broadcast domain. The new port could be in the same node or its HA partner. Once the link is restored and if `auto-revert` is set to `true`, VIF Manager reverts the iSCSI LIFs back to their home node and home port.
- When a node drops out of replicated database (RDB) quorum, VIF Manager migrates the iSCSI LIFs from the out of quorum node to its HA partner. Once the node comes back into quorum and if `auto-revert` is set to `true`, VIF Manager reverts the iSCSI LIFs back to their home node and home port.

### Migrate and revert an iSCSI LIF

You can use System Manager or the ONTAP CLI to manually migrate an iSCSI LIF to a different port on the same node or to a different port on the HA partner, and then revert the LIF back to its home node and home port.



## Migrate and revert an iSCSI LIF using System Manager


You can use System Manager to manually migrate and revert one or more iSCSI LIFs (network interfaces) to another port on the same node or to a port on the HA partner.

### Before you begin

You must have an ASA platform HA pair and it must be running ONTAP 9.11.1 or later.

### Migrate a LIF

#### Steps

1. In System Manager, click **Network > Overview > Network Interfaces**
2. Select the LIF you want to migrate, click , and then click **Migrate**.
3. In the **Migrate Interface** dialog box, select the destination node and port of the HA partner.




You have the option of permanently migrating the iSCSI LIF by checking the checkbox. Understand that the iSCSI LIF must be offline before it is permanently migrated. Additionally, once an iSCSI LIF is permanently migrated, it cannot be undone. There is no revert option.

4. Click **Migrate**.

### Revert a LIF

#### Steps

1. In System Manager, click **Network > Overview > Network Interfaces**.
2. Select the LIF you want to revert, click  and then click **Revert Network Interface**.
3. In the **Revert Network Interface** dialog box, click **Revert**.

## Migrate and revert an iSCSI LIF using the ONTAP CLI

You can use the ONTAP CLI to manually migrate and revert one or more iSCSI LIFs to another port on the same node or to a port on the HA partner.

### Before you begin

You must have an ASA platform HA pair and it must be running ONTAP 9.11.1 or later.

If you want to...	Use this command...
Migrate an iSCSI LIF to another node/port	See <a href="#">Migrate a LIF</a> for the available commands.
Revert an iSCSI LIF back to its home node/port	See <a href="#">Revert a LIF to its home port</a> for the available commands.

### Manage iSCSI LIFs using the ONTAP CLI

You can use the ONTAP CLI to manage iSCSI LIFs, including creating new iSCSI LIFs and enabling the iSCSI LIF failover feature for pre-existing LIFs.

### Before you Begin

You must have an ASA platform HA pair and it must be running ONTAP 9.11.1 or later.

### About this task

See the [ONTAP 9.11.1 Command Reference](#) for a full list of `network interface` commands.

If you want to...	Use this command...
Create an iSCSI LIF	<pre>network interface create -vserver vserver_name -lif iscsi_lif -service -policy default-data-blocks -data -protocol iscsi -home-node node_name -home-port port_name -address IP_address -netmask netmask_value</pre> <p>If needed, see <a href="#">Create a LIF</a> for more information.</p>
Verify that the LIF was created successfully	<pre>network interface show -vserver vserver_name -fields failover- policy,failover-group,auto-revert,is- home</pre>
Verify if you can override the auto-revert default on iSCSI LIFs	<pre>network interface modify -vserver vserver_name -lif iscsi_lif -auto-revert false</pre>
Perform a storage failover on an iSCSI LIF	<pre>storage failover takeover -ofnode node_name -option normal</pre> <p>You receive a warning: A takeover will be initiated. Once the partner node reboots, a giveback will be automatically initiated. Do you want to continue? {y/n}:</p> <p>A <code>y</code> response displays a takeover message from its HA partner.</p>
Enable iSCSI LIF failover feature for pre-existing LIFs	<p>For iSCSI LIFs created before you upgraded your cluster to ONTAP 9.11.1 or later, you can enable the iSCSI LIF failover feature (by modifying the failover policy to <code>sfo-partner-only</code> and by modifying the auto-revert capability to <code>true</code>):</p> <pre>network interface modify -vserver vserver_name -lif iscsi_lif -failover- policy sfo-partner-only -auto-revert true</pre> <p>This command can be run on all the iSCSI LIFs in a Storage VM by specifying “-lif*” and keeping all other parameters the same.</p>

Disable iSCSI LIF failover feature for pre-existing LIFs	<p>For iSCSI LIFs created before you upgraded your cluster to ONTAP 9.11.1 or later, you can disable the iSCSI LIF failover feature and the auto-revert capability:</p> <pre>network interface modify -vserver vserver_name -lif iscsi_lif -failover- policy disabled -auto-revert false</pre> <p>This command can be run on all the iSCSI LIFs in a storage VM by specifying “-lif*” and keeping all other parameters the same.</p>
--	--

## Manage FC protocol

### Configure an SVM for FC

To configure a storage virtual machine (SVM) for FC, you must create LIFs for the SVM and assign the FC protocol to those LIFs.

#### Before you begin

You must have an FC license and it must be enabled. If the FC license is not enabled, the LIFs and SVMs appear to be online but the operational status is `down`. The FC service must be enabled for your LIFs and SVMs to be operational. You must use single initiator zoning for all of the FC LIFs in the SVM to host the initiators.


#### About this task

NetApp supports a minimum of one FC LIF per node for each SVM serving data with the FC protocol. You must use two LIFs per node and two fabrics, with one LIF per node attached. This provides for redundancy at the node layer and the fabric.

## Example 6. Steps

### System Manager

Configure an storage VM for iSCSI with ONTAP System Manager (9.7 and later).

To configure FC on a new storage VM	To configure FC on an existing storage VM
<ol style="list-style-type: none"><li>1. In System Manager, click <b>Storage &gt; Storage VMs</b> and then click <b>Add</b>.</li><li>2. Enter a name for the storage VM.</li><li>3. Select <b>FC</b> for the <b>Access Protocol</b>.</li><li>4. Click <b>Enable FC</b>. + The FC ports are automatically assigned.</li><li>5. Click <b>Save</b>.</li></ol>	<ol style="list-style-type: none"><li>1. In System Manager, click <b>Storage &gt; Storage VMs</b>.</li><li>2. Click on the storage VM you want to configure.</li><li>3. Click on the <b>Settings</b> tab, and then click  next to the FC protocol.</li><li>4. Click <b>Enable FC</b> and enter the IP address and subnet mask for the network interface. + The FC ports are automatically assigned.</li><li>5. Click <b>Save</b>.</li></ol>

### CLI

1. Enable FC service on the SVM:

```
vserver fcp create -vserver vserver_name -status-admin up
```

2. Create two LIFs for the SVMs on each node serving FC:

```
network interface create -vserver vserver_name -lif lif_name -role data  
-data-protocol fcp -home-node node_name -home-port port
```

The `-role` parameter should be `data` and the `data-protocol` parameter should be `fcp`.

3. Verify that your LIFs have been created and that their operational status is online:

```
network interface show -vserver vserver_name lif_name
```

### Related information

[NetApp Support](#)

[NetApp Interoperability Matrix Tool](#)

[Considerations for LIFs in cluster SAN environments](#)

### Delete an FC service for an SVM

You can delete an FC service for a storage virtual machine (SVM) if it is no longer required.

### What you'll need

The administration status must be “down” before you can delete a FC service for an SVM. You can set the administration status to down with either the `vserver fcp modify` command or the `vserver fcp stop`

command.

### Steps

1. Use the `vserver fcp stop` command to stop the I/O to the LUN.

```
vserver fcp stop -vserver vs_1
```

2. Use the `vserver fcp delete` command to remove the service from the SVM.

```
vserver fcp delete -vserver vs_1
```

3. Use the `vserver fcp show` to verify that you deleted the FC service from your SVM:

```
vserver fcp show -vserver vs_1
```

### Recommended MTU configurations for FCoE jumbo frames

For Fibre Channel over Ethernet (FCoE), jumbo frames for the Ethernet adapter portion of the CNA should be configured at 9000 MTU. Jumbo frames for the FCoE adapter portion of the CNA should be configured at greater than 1500 MTU. Only configure jumbo frames if the initiator, target, and all intervening switches support and are configured for jumbo frames.

## Manage NVMe protocol

### Start the NVMe service for an SVM

Before you can use the NVMe protocol on your storage virtual machine (SVM), you must start the NVMe service on the SVM.

#### Before you begin

NVMe must be allowed as a protocol on your system.

The following NVMe protocols are supported:

Protocol	Beginning with ...	Allowed by...
TCP	ONTAP 9.10.1	Default
FCP	ONTAP 9.4	Default

### Steps

1. Change the privilege setting to advanced:

```
set -privilege advanced
```

2. Verify that NVMe is allowed as a protocol:

```
vserver nvme show
```

3. Create the NVMe protocol service:

```
vserver nvme create
```

4. Start the NVMe protocol service on the SVM:

```
vserver nvme modify -status -admin up
```

### Delete NVMe service from an SVM

If needed, you can delete the NVMe service from your storage virtual machine (SVM).

#### Steps

1. Change the privilege setting to advanced:

```
set -privilege advanced
```

2. Stop the NVMe service on the SVM:

```
vserver nvme modify -status -admin down
```

3. Delete the NVMe service:


```
vserver nvme delete
```

### Resize a namespace

Beginning with ONTAP 9.10.1, you can use the ONTAP CLI to increase or decrease the size of a NVMe namespace. You can use System Manager to increase the size of a NVMe namespace.

#### Increase the size of a namespace

##### System Manager

1. Click **Storage > NVMe Namespaces**.
2. Hoover over the namespace you want to increase, click , and then click **Edit**.
3. Under **CAPACITY**, change the size of the namespace.

##### CLI

1. Enter the following command: 

```
vserver nvme namespace modify -vserver SVM_name -path path -size new_size_of_namespace
```

#### Decrease the size of a namespace

You must use the ONTAP CLI to decrease the size of a NVMe namespace.

1. Change the privilege setting to advanced:

```
set -privilege advanced
```

2. Decrease the size of the namespace:

```
vserver nvme namespace modify -vserver SVM_name -path namespace_path -size new_size_of_namespace
```

## Convert a namespace into a LUN

Beginning with ONTAP 9.11.1, you can use the ONTAP CLI to in-place convert an existing NVMe namespace to a LUN.

### Before you start

- Specified NVMe namespace should not have any existing maps to a Subsystem.
- Namespace should not be part of a snapshot or on the destination side of SnapMirror relationship as a read-only namespace.
- Since NVMe namespaces are only supported with specific platforms and network cards, this feature only works with specific hardware.

### Steps

1. You enter the following command to convert an NVMe namespace to a LUN:

```
lun convert-from-namespace -vserver -namespace-path
```

## Manage systems with FC adapters

### Manage systems with FC adapters

Commands are available to manage onboard FC adapters and FC adapter cards. These commands can be used to configure the adapter mode, display adapter information, and change the speed.

Most storage systems have onboard FC adapters that can be configured as initiators or targets. You can also use FC adapter cards configured as initiators or targets. Initiators connect to back-end disk shelves, and possibly foreign storage arrays (FlexArray). Targets connect only to FC switches. Both the FC target HBA ports and the switch port speed should be set to the same value and should not be set to auto.

### Related information

[SAN configuration](#)

### Commands for managing FC adapters

You can use FC commands to manage FC target adapters, FC initiator adapters, and onboard FC adapters for your storage controller. The same commands are used to manage FC adapters for the FC protocol and the FC-NVMe protocol.

FC initiator adapter commands work only at the node level. You must use the `run -node node_name` command before you can use the FC initiator adapter commands.

### Commands for managing FC target adapters

If you want to...	Use this command...
Display FC adapter information on a node	<code>network fcp adapter show</code>
Modify FC target adapter parameters	<code>network fcp adapter modify</code>
Display FC protocol traffic information	<code>run -node <i>node_name</i> sysstat -f</code>
Display how long the FC protocol has been running	<code>run -node <i>node_name</i> uptime</code>
Display adapter configuration and status	<code>run -node <i>node_name</i> sysconfig -v <i>adapter</i></code>
Verify which expansion cards are installed and whether there are any configuration errors	<code>run -node <i>node_name</i> sysconfig -ac</code>
View a man page for a command	<code>man <i>command_name</i></code>

#### Commands for managing FC initiator adapters

If you want to...	Use this command...
Display information for all initiators and their adapters in a node	<code>run -node <i>node_name</i> storage show adapter</code>
Display adapter configuration and status	<code>run -node <i>node_name</i> sysconfig -v <i>adapter</i></code>
Verify which expansion cards are installed and whether there are any configuration errors	<code>run -node <i>node_name</i> sysconfig -ac</code>

#### Commands for managing onboard FC adapters

If you want to...	Use this command...
Display the status of the onboard FC ports	<code>run -node <i>node_name</i> system hardware unified-connect show</code>

#### Configure FC adapters

Each onboard FC port can be individually configured as an initiator or a target. Ports on certain FC adapters can also be individually configured as either a target port or an initiator port, just like the onboard FC ports. A list of adapters that can be configured for target mode is available in the [NetApp Hardware Universe](#).

Target mode is used to connect the ports to FC initiators. Initiator mode is used to connect the ports to tape



drives, tape libraries, or third-party storage with FlexArray Virtualization or Foreign LUN Import (FLI).

The same steps are used when configuring FC adapters for the FC protocol and the FC-NVMe protocol. However, only certain FC adapters support FC-NVMe. See the [NetApp Hardware Universe](#) for a list of adapters that support the FC-NVMe protocol.

### Configure FC adapters for target mode

#### Steps

1. Take the adapter offline:

```
node run -node node_name storage disable adapter adapter_name
```

If the adapter does not go offline, you can also remove the cable from the appropriate adapter port on the system.

2. Change the adapter from initiator to target:

```
system hardware unified-connect modify -t target -node node_name adapter adapter_name
```

3. Reboot the node hosting the adapter you changed.
4. Verify that the target port has the correct configuration:

```
network fcp adapter show -node node_name
```

5. Bring your adapter online:

```
network fcp adapter modify -node node_name -adapter adapter_port -state up
```

### Configure FC adapters for initiator mode

#### What you'll need

- LIFs on the adapter must be removed from any port sets of which they are members.
- All LIF's from every storage virtual machine (SVM) using the physical port to be modified must be migrated or destroyed before changing the personality of the physical port from target to initiator.



NVMe/FC does support initiator mode.

#### Steps

1. Remove all LIFs from the adapter:

```
network interface delete -vserver SVM_name -lif LIF_name,LIF_name
```

2. Take your adapter offline:

```
network fcp adapter modify -node node_name -adapter adapter_port -status-admin down
```

If the adapter does not go offline, you can also remove the cable from the appropriate adapter port on the system.

3. Change the adapter from target to initiator:

```
system hardware unified-connect modify -t initiator adapter_port
```

4. Reboot the node hosting the adapter you changed.
5. Verify that the FC ports are configured in the correct state for your configuration:

```
system hardware unified-connect show
```

6. Bring the adapter back online:

```
node run -node node_name storage enable adapter adapter_port
```

## View adapter settings

You can use specific commands to view information about your FC/UTA adapters.

### FC target adapter

#### Step

1. Use the `network fcp adapter show` command to display adapter information: `network fcp adapter show -instance -node node1 -adapter 0a`

The output displays system configuration information and adapter information for each slot that is used.

### Unified Target Adapter (UTA) X1143A-R6

#### Steps

1. Boot your controller without the cables attached.
2. Run the `system hardware unified-connect show` command to see the port configuration and modules.
3. View the port information before configuring the CNA and ports.

### Change the UTA2 port from CNA mode to FC mode

You should change the UTA2 port from Converged Network Adapter (CNA) mode to Fibre Channel (FC) mode to support the FC initiator and FC target mode. You should change the personality from CNA mode to FC mode when you need to change the physical medium that connects the port to its network.

#### Steps

1. Take the adapter offline:

```
network fcp adapter modify -node node_name -adapter adapter_name -status-admin down
```

2. Change the port mode:

```
ucadmin modify -node node_name -adapter adapter_name -mode fcp
```

### 3. Reboot the node, and then bring the adapter online:

```
network fcp adapter modify -node node_name -adapter adapter_name -status-admin  
up
```

### 4. Notify your admin or VIF manager to delete or remove the port, as applicable:

- If the port is used as a home port of a LIF, is a member of an interface group (ifgrp), or hosts VLANs, then an admin should do the following:
  - i. Move the LIFs, remove the port from the ifgrp, or delete the VLANs, respectively.
  - ii. Manually delete the port by running the `network port delete` command.

If the `network port delete` command fails, the admin should address the errors, and then run the command again.

- If the port is not used as the home port of a LIF, is not a member of an ifgrp, and does not host VLANs, then the VIF manager should remove the port from its records at the time of reboot.

If the VIF manager does not remove the port, then the admin must remove it manually after the reboot by using the `network port delete` command.

```
net-f8040-34::> network port show

Node: net-f8040-34-01

Port          IPspace      Broadcast Domain  Link MTU  Speed (Mbps)  Health
-----
...
e0i           Default      Default           down 1500  auto/10       -
e0f           Default      Default           down 1500  auto/10       -
...

net-f8040-34::> ucadmin show

Admin
Node          Adapter      Current      Current      Pending      Pending
Status
-----
net-f8040-34-01  0e          cna          target       -            -
offline
net-f8040-34-01  0f          cna          target       -            -
offline
...

net-f8040-34::> network interface create -vs net-f8040-34 -lif m
-role
```

```
node-mgmt-home-node net-f8040-34-01 -home-port e0e -address 10.1.1.1
-netmask 255.255.255.0
```

```
net-f8040-34::> network interface show -fields home-port, curr-port
```

```
vserver lif                               home-port curr-port
-----
Cluster net-f8040-34-01_clus1 e0a      e0a
Cluster net-f8040-34-01_clus2 e0b      e0b
Cluster net-f8040-34-01_clus3 e0c      e0c
Cluster net-f8040-34-01_clus4 e0d      e0d
net-f8040-34
      cluster_mgmt      e0M      e0M
net-f8040-34
      m      e0e      e0i
net-f8040-34
      net-f8040-34-01_mgmt1 e0M      e0M
7 entries were displayed.
```

```
net-f8040-34::> uconfig modify local 0e fc
```

Warning: Mode on adapter 0e and also adapter 0f will be changed to fc.

```
Do you want to continue? {y|n}: y
```

Any changes will take effect after rebooting the system. Use the "system node reboot" command to reboot.

```
net-f8040-34::> reboot local
(system node reboot)
```

```
Warning: Are you sure you want to reboot node "net-f8040-34-01"?
{y|n}: y
```

##### 5. Verify that you have the correct SFP+ installed:

```
network fcp adapter show -instance -node -adapter
```

For CNA, you should use a 10Gb Ethernet SFP. For FC, you should either use an 8 Gb SFP or a 16 Gb SFP, before changing the configuration on the node.

### Change the CNA/UTA2 target adapter optical modules

You should change the optical modules on the unified target adapter (CNA/UTA2) to support the personality mode you have selected for the adapter.

#### Steps

1. Verify the current SFP+ used in the card. Then, replace the current SFP+ with the appropriate SFP+ for the preferred personality (FC or CNA).
2. Remove the current optical modules from the X1143A-R6 adapter.
3. Insert the correct modules for your preferred personality mode (FC or CNA) optics.
4. Verify that you have the correct SFP+ installed:

```
network fcp adapter show -instance -node -adapter
```

Supported SFP+ modules and Cisco-branded Copper (Twinax) cables are listed in the *Hardware Universe*.

#### Related information

[NetApp Hardware Universe](#)

#### Supported port configurations for X1143A-R6 adapters

The FC target mode is the default configuration for X1143A-R6 adapter ports. However, ports on this adapter can be configured as either 10-Gb Ethernet and FCoE ports or as 16-Gb FC ports.

When configured for Ethernet and FCoE, X1143A-R6 adapters support concurrent NIC and FCoE target traffic on the same 10-GBE port. When configured for FC, each two-port pair that shares the same ASIC can be individually configured for FC target or FC initiator mode. This means that a single X1143A-R6 adapter can support FC target mode on one two-port pair and FC initiator mode on another two-port pair.

#### Related information

[NetApp Hardware Universe](#)

[SAN configuration](#)

#### Configure the ports

To configure the unified target adapter (X1143A-R6), you must configure the two adjacent ports on the same chip in the same personality mode.

#### Steps

1. Configure the ports as needed for Fibre Channel (FC) or Converged Network Adapter (CNA) using the `system node hardware unified-connect modify` command.
2. Attach the appropriate cables for FC or 10 Gb Ethernet.
3. Verify that you have the correct SFP+ installed:

```
network fcp adapter show -instance -node -adapter
```

For CNA, you should use a 10Gb Ethernet SFP. For FC, you should either use an 8 Gb SFP or a 16 Gb SFP, based on the FC fabric being connected to.

#### Prevent loss of connectivity when using the X1133A-R6 adapter

You can prevent loss of connectivity during a port failure by configuring your system with redundant paths to separate X1133A-R6 HBAs.

The X1133A-R6 HBA is a 4-port, 16 Gb FC adapter consisting of two 2-port pairs. The X1133A-R6 adapter can be configured as target mode or initiator mode. Each 2-port pair is supported by a single ASIC (for example, Port 1 and Port 2 on ASIC 1 and Port 3 and Port 4 on ASIC 2). Both ports on a single ASIC must be configured to operate in the same mode, either target mode or initiator mode. If an error occurs with the ASIC supporting a pair, both ports in the pair go offline.

To prevent this loss of connectivity, you configure your system with redundant paths to separate X1133A-R6 HBAs, or with redundant paths to ports supported by different ASICs on the HBA.

## Manage LIFs for all SAN protocols

### Manage LIFs for all SAN protocols

LIFs are connected to the SAN hosts. They can be removed from port sets, moved to different nodes within a storage virtual machine (SVM), and deleted.

#### Related information

[Network management](#)

### Configure an NVMe LIF

Certain requirements must be met when configuring NVMe LIFs.

#### What you'll need

NVMe must be supported by the FC adapter on which you create the LIF. Supported adapters are listed in the *Hardware Universe*.

[NetApp Hardware Universe](#)

#### About this task

The following rules apply when creating an NVMe LIF:

- NVMe can be the only data protocol on data LIFs.
- You should configure one management LIF for every SVM that supports SAN.
- For ONTAP 9.5 and later:
  - You can only configure two NVMe LIFs per node on a maximum of four nodes.
  - You must configure an NVMe LIF on the node containing the namespace and on node's HA partner.
- For ONTAP 9.4 only:
  - NVMe LIFs and namespaces must be hosted on the same node.
  - Only one NVMe data LIF can be configured per SVM.

#### Steps

1. Create the LIF:

```
network interface create -vserver SVM_name -lif LIF_name -role LIF_role -data  
-protocol fc-nvme -home-node home_node -home-port
```

```
home_port
```

2. Verify that the LIF was created:

```
network interface show -vserver SVM_name
```

### What to know before moving a SAN LIF

You only need to perform a LIF movement if you are changing the contents of your cluster, for example, adding nodes to the cluster or deleting nodes from the cluster. If you perform a LIF movement, you do not have to re-zone your FC fabric or create new iSCSI sessions between the attached hosts of your cluster and the new target interface.

You cannot move a SAN LIF using the `network interface move` command. SAN LIF movement must be performed by taking the LIF offline, moving the LIF to a different home node or port, and then bringing it back online in its new location. Asymmetric Logical Unit Access (ALUA) provides redundant paths and automatic path selection as part of any ONTAP SAN solution. Therefore, there is no I/O interruption when the LIF is taken offline for the movement. The host simply retries and then moves I/O to another LIF.

Using LIF movement, you can nondisruptively do the following:

- Replace one HA pair of a cluster with an upgraded HA pair in a way that is transparent to hosts accessing LUN data
- Upgrade a target interface card
- Shift the resources of a storage virtual machine (SVM) from one set of nodes in a cluster to another set of nodes in the cluster

### Remove a SAN LIF from a port set

If the LIF you want to delete or move is in a port set, you must remove the LIF from the port set before you can delete or move the LIF.

#### About this task

You need to do Step 1 in the following procedure only if one LIF is in the port set. You cannot remove the last LIF in a port set if the port set is bound to an initiator group. Otherwise, you can start with Step 2 if multiple LIFs are in the port set.

#### Steps

1. If only one LIF is in the port set, use the `lun igroup unbind` command to unbind the port set from the initiator group.



When you unbind an initiator group from a port set, all of the initiators in the initiator group have access to all target LUNs mapped to the initiator group on all network interfaces.

```
cluster1::>lun igroup unbind -vserver vs1 -igroup ig1
```

2. Use the `lun portset remove` command to remove the LIF from the port set.

```
cluster1::> port set remove -vserver vs1 -portset ps1 -port-name lif1
```

## Move a SAN LIF

If a node needs to be taken offline, you can move a SAN LIF to preserve its configuration information, such as its WWPN, and avoid rezoning the switch fabric. Because a SAN LIF must be taken offline before it is moved, host traffic must rely on host multipathing software to provide nondisruptive access to the LUN. You can move SAN LIFs to any node in a cluster, but you cannot move the SAN LIFs between storage virtual machines (SVMs).

### What you'll need

If the LIF is a member of a port set, the LIF must have been removed from the port set before the LIF can be moved to a different node.

### About this task

The destination node and physical port for a LIF that you want to move must be on the same FC fabric or Ethernet network. If you move a LIF to a different fabric that has not been properly zoned, or if you move a LIF to an Ethernet network that does not have connectivity between iSCSI initiator and target, the LUN will be inaccessible when you bring it back online.

### Steps

1. View the administrative and operational status of the LIF:

```
network interface show -vserver vserver_name
```

2. Change the status of the LIF to down (offline):

```
network interface modify -vserver vserver_name -lif LIF_name -status-admin down
```

3. Assign the LIF a new node and port:

```
network interface modify -vserver vserver_name -lif LIF_name -home-node node_name -home-port port_name
```

4. Change the status of the LIF to up (online):

```
network interface modify -vserver vserver_name -lif LIF_name -status-admin up
```

5. Verify your changes:

```
network interface show -vserver vserver_name
```

## Delete a LIF in a SAN environment

Before you delete a LIF, you should ensure that the host connected to the LIF can access the LUNs through another path.

### What you'll need


If the LIF you want to delete is a member of a port set, you must first remove the LIF from the port set before you can delete the LIF.



## Example 7. Steps

### System Manager

Delete a LIF with ONTAP System Manager (9.7 and later).

1. In System Manager, click **Network > Overview**, and then select **Network Interfaces**.
2. Select the storage VM from which you want to delete the LIF.
3. Click  and select **Delete**.

### CLI

Delete a LIF with the ONTAP CLI.

1. Verify the name of the LIF and current port to be deleted:

```
network interface show -vserver vserver_name
```

2. Delete the LIF:

```
network interface delete
```

```
network interface delete -vserver vs1 -lif lif1
```

3. Verify that you deleted the LIF:

```
network interface show
```

```
network interface show -vserver vs1
```

Logical Status	Network	Current	Current Is
Vserver Interface	Admin/Oper	Address/Mask	Node Port
Home			
-----	-----	-----	-----
vs1			
lif2	up/up	192.168.2.72/24	node-01 e0b
true			
lif3	up/up	192.168.2.73/24	node-01 e0b
true			

= SAN LIF requirements for adding nodes to a cluster

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You need to be aware of certain considerations when adding nodes to a cluster.

- You must create LIFs on the new nodes as appropriate before you create LUNs on those new nodes.
- You must discover those LIFs from the hosts as dictated by the host stack and protocol.

- You must create LIFs on the new nodes so that the LUN and volume movements are possible without using the cluster interconnect network.

= Configure iSCSI LIFs to return FQDN to host iSCSI SendTargets Discovery Operation

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

Beginning with ONTAP 9, iSCSI LIFs can be configured to return a Fully Qualified Domain Name (FQDN) when a host OS sends an iSCSI SendTargets Discovery Operation. Returning a FQDN is useful when there is a Network Address Translation (NAT) device between the host OS and the storage service.

#### **About this task**

IP addresses on one side of the NAT device are meaningless on the other side, but FQDNs can have meaning on both sides.

The FQDN value interoperability limit is 128 characters on all host OS.

## Steps

1. Change the privilege setting to advanced:

```
set -privilege advanced
```

2. Configure iSCSI LIFs to return FQDN:

```
vserver iscsi interface modify -vserver SVM_name -lif iscsi_LIF_name  
-sendtargets_fqdn FQDN
```

In the following example, the iSCSI LIFs are configured to return storagehost-005.example.com as the FQDN.

```
vserver iscsi interface modify -vserver vs1 -lif vs1_iscsi1 -sendtargets  
-fqdn storagehost-005.example.com
```

3. Verify that sendtargets is the FQDN:

```
vserver iscsi interface show -vserver SVM_name -fields sendtargets-fqdn
```

In this example, storagehost-005.example.com is displayed in the sendtargets-fqdn output field.

```
cluster::vserver*> vserver iscsi interface show -vserver vs1 -fields  
sendtargets-fqdn  
vserver lif          sendtargets-fqdn  
-----  
vs1      vs1_iscsi1  storagehost-005.example.com  
vs1      vs1_iscsi2  storagehost-006.example.com
```

## Related information

### [ONTAP 9 Commands](#)

= Recommended volume and file or LUN configuration combinations

= Recommended volume and file or LUN configuration combinations overview

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

There are specific combinations of FlexVol volume and file or LUN configurations you can use, depending on your application and administration requirements. Understanding the benefits and costs of these combinations can help you determine the right volume and LUN configuration combination for your environment.

The following volume and LUN configuration combinations are recommended:

- Space-reserved files or LUNs with thick volume provisioning
- Non-space-reserved files or LUNs with thin volume provisioning

- Space-reserved files or LUNs with semi-thick volume provisioning

You can use SCSI thin provisioning on your LUNs in conjunction with any of these configuration combinations.

== Space-reserved files or LUNs with thick volume provisioning

**Benefits:**

- All write operations within space-reserved files are guaranteed; they will not fail due to insufficient space.
- There are no restrictions on storage efficiency and data protection technologies on the volume.

**Costs and limitations:**

- Enough space must be set aside from the aggregate up front to support the thickly provisioned volume.
- Space equal to twice the size of the LUN is allocated from the volume at LUN creation time.

== Non-space-reserved files or LUNs with thin volume provisioning

**Benefits:**

- There are no restrictions on storage efficiency and data protection technologies on the volume.
- Space is allocated only as it is used.

**Costs and restrictions:**

- Write operations are not guaranteed; they can fail if the volume runs out of free space.
- You must manage the free space in the aggregate effectively to prevent the aggregate from running out of free space.

== Space-reserved files or LUNs with semi-thick volume provisioning

**Benefits:**

Less space is reserved up front than for thick volume provisioning, and a best-effort write guarantee is still provided.

**Costs and restrictions:**

- Write operations can fail with this option.

You can mitigate this risk by properly balancing free space in the volume against data volatility.

- You cannot rely on retention of data protection objects such as Snapshot copies and FlexClone files and LUNs.
- You cannot use ONTAP block-sharing storage efficiency capabilities that cannot be automatically deleted, including deduplication, compression, and ODX/Copy Offload.

= Determine the correct volume and LUN configuration combination for your environment

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

Answering a few basic questions about your environment can help you determine the best FlexVol volume and LUN configuration for your environment.

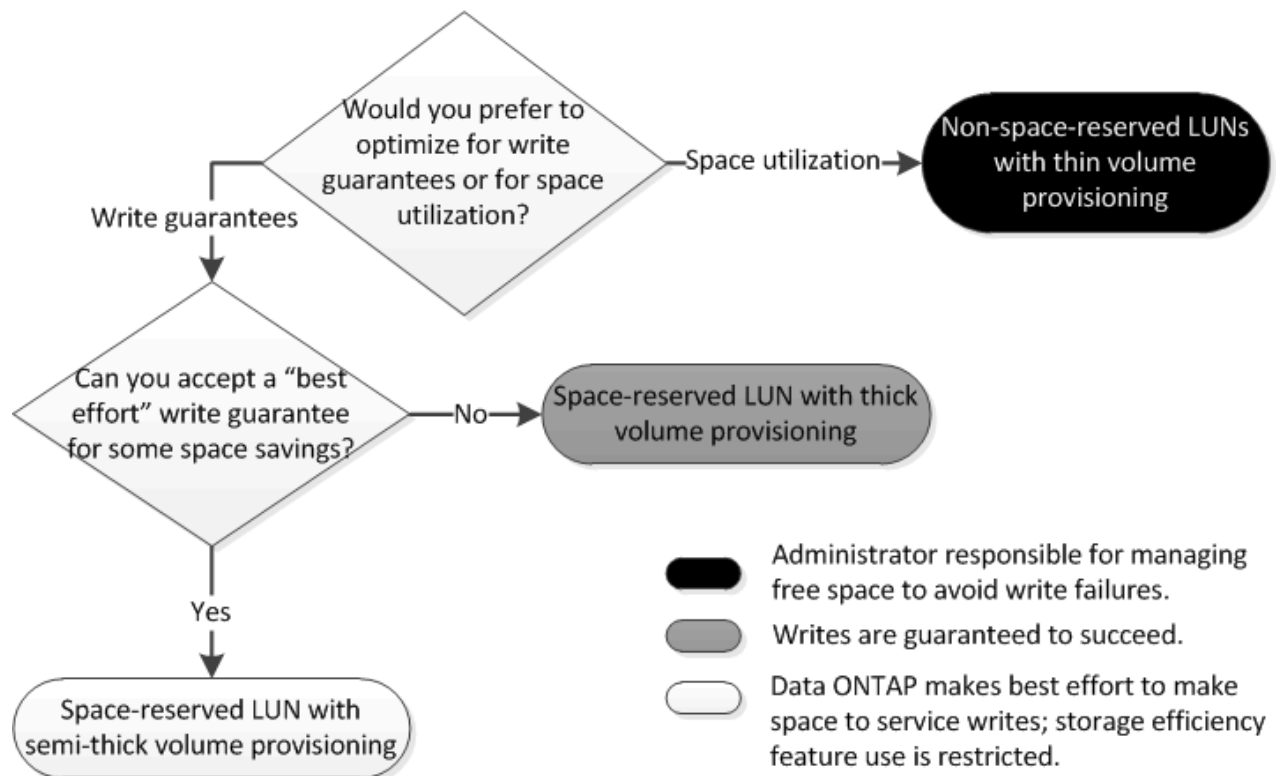
**About this task**

You can optimize your LUN and volume configurations for maximum storage utilization or for the security of write guarantees. Based on your requirements for storage utilization and your ability to monitor and replenish free space quickly, you must determine the FlexVol volume and LUN volumes appropriate for your installation.

You do not need a separate volume for each LUN.

## Step

1. Use the following decision tree to determine the best volume and LUN configuration combination for your environment:



= Calculate rate of data growth for LUNs

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You need to know the rate at which your LUN data is growing over time to determine whether you should use space-reserved LUNs or non-space-reserved LUNs.

### About this task

If you have a consistently high rate of data growth, then space-reserved LUNs might be a better option for you. If you have a low rate of data growth, then you should consider non-space-reserved LUNs.

You can use tools such as OnCommand Insight to calculate your rate of data growth or you can calculate it manually. The following steps are for manual calculation.

### Steps

1. Set up a space-reserved LUN.
2. Monitor the data on the LUN for a set period of time, such as one week.

Make sure that your monitoring period is long enough to form a representative sample of regularly occurring increases in data growth. For instance, you might consistently have a large amount of data growth at the end of each month.

3. Each day, record in GB how much your data grows.

4. At the end of your monitoring period, add the totals for each day together, and then divide by the number of days in your monitoring period.

This calculation yields your average rate of growth.

### Example

In this example, you need a 200 GB LUN. You decide to monitor the LUN for a week and record the following daily data changes:

- Sunday: 20 GB
- Monday: 18 GB
- Tuesday: 17 GB
- Wednesday: 20 GB
- Thursday: 20 GB
- Friday: 23 GB
- Saturday: 22 GB

In this example, your rate of growth is  $(20+18+17+20+20+23+22) / 7 = 20$  GB per day.

= Configuration settings for space-reserved files or LUNs with thick-provisioned volumes

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

This FlexVol volume and file or LUN configuration combination provides the ability to use storage efficiency technologies and does not require you to actively monitor your free space, because sufficient space is allocated up front.

The following settings are required to configure a space-reserved file or LUN in a volume using thick provisioning:

Volume setting	Value
Guarantee	Volume
Fractional reserve	100
Snapshot reserve	Any
Snapshot autodelete	Optional
Autogrow	Optional; if enabled, aggregate free space must be actively monitored.

File or LUN setting	Value
Space reservation	Enabled

= Configuration settings for non-space-reserved files or LUNs with thin-provisioned volumes

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

This FlexVol volume and file or LUN configuration combination requires the smallest amount of storage to be allocated up front, but requires active free space management to prevent errors due to lack of space.

The following settings are required to configure a non-space-reserved files or LUN in a thin-provisioned volume:

Volume setting	Value
Guarantee	None
Fractional reserve	0
Snapshot reserve	Any
Snapshot autodelete	Optional
Autogrow	Optional

File or LUN setting	Value
Space reservation	Disabled

== Additional considerations

When the volume or aggregate runs out of space, write operations to the file or LUN can fail.

If you do not want to actively monitor free space for both the volume and the aggregate, you should enable Autogrow for the volume and set the maximum size for the volume to the size of the aggregate. In this configuration, you must monitor aggregate free space actively, but you do not need to monitor the free space in the volume.

= Configuration settings for space-reserved files or LUNs with semi-thick volume provisioning

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

This FlexVol volume and file or LUN configuration combination requires less storage to be allocated up front than the fully provisioned combination, but places restrictions on the efficiency technologies you can use for the volume. Overwrites are fulfilled on a best-effort basis for this configuration combination.

The following settings are required to configure a space-reserved LUN in a volume using semi-thick provisioning:



Volume setting	Value
Guarantee	Volume
Fractional reserve	0
Snapshot reserve	0
Snapshot autodelete	On, with a commitment level of destroy, a destroy list that includes all objects, the trigger set to volume, and all FlexClone LUNs and FlexClone files enabled for automatic deletion.
Autogrow	Optional; if enabled, aggregate free space must be actively monitored.

File or LUN setting	Value
Space reservation	Enabled

== Technology restrictions

You cannot use the following volume storage efficiency technologies for this configuration combination:

- Compression
- Deduplication
- ODX and FlexClone Copy Offload
- FlexClone LUNs and FlexClone files not marked for automatic deletion (active clones)
- FlexClone subfiles
- ODX/Copy Offload

== Additional considerations

The following facts must be considered when employing this configuration combination:

- When the volume that supports that LUN runs low on space, protection data (FlexClone LUNs and files, Snapshot copies) is destroyed.
- Write operations can time out and fail when the volume runs out of free space.

Compression is enabled by default for AFF platforms. You must explicitly disable compression for any volume for which you want to use semi-thick provisioning on an AFF platform.

= Data protection methods in SAN environments

= Data protection methods in SAN environments overview

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You can protect your data by making copies of it so that it is available for restoration in the event of accidental deletion, application crashes, data corruption, or disaster. Depending on your data protection and backup needs, ONTAP offers a variety of methods that enable you to protect your data.

== SnapMirror Business Continuity (SM-BC)

Beginning with general availability in ONTAP 9.9.1, provides Zero Recovery Time Objective (Zero RTO) or Transparent Application Failover (TAF) to enable automatic failover of business-critical applications in SAN environments. SM-BC requires the installation of ONTAP Mediator 1.2 in a configuration with either two AFF clusters or two All SAN Array (ASA) clusters.

[NetApp Documentation: SnapMirror Business Continuity](#)

== Snapshot copy

Enables you to manually or automatically create, schedule, and maintain multiple backups of your LUNs. Snapshot copies use only a minimal amount of additional volume space and do not have a performance cost. If your LUN data is accidentally modified or deleted, that data can easily and quickly be restored from one of the latest Snapshot copies.

== FlexClone LUNs (FlexClone license required)

Provides point-in-time, writable copies of another LUN in an active volume or in a Snapshot copy. A clone and its parent can be modified independently without affecting each other.

== SnapRestore (license required)

Enables you to perform fast, space-efficient, on-request data recovery from Snapshot copies on an entire volume. You can use SnapRestore to restore a LUN to an earlier preserved state without rebooting the storage system.

== Data protection mirror copies (SnapMirror license required)

Provides asynchronous disaster recovery by enabling you to periodically create Snapshot copies of data on your volume; copy those Snapshot copies over a local or wide area network to a partner volume, usually on another cluster; and retain those Snapshot copies. The mirror copy on the partner volume provides quick availability and restoration of data from the time of the last Snapshot copy, if the data on the source volume is corrupted or lost.

== SnapVault backups (SnapMirror license required)

Provides storage efficient and long-term retention of backups. SnapVault relationships enable you to back up selected Snapshot copies of volumes to a destination volume and retain the backups.

If you conduct tape backups and archival operations, you can perform them on the data that is already backed up on the SnapVault secondary volume.

== SnapDrive for Windows or UNIX (SnapDrive license required)

Configures access to LUNs, manages LUNs, and manages storage system Snapshot copies directly from a Windows or UNIX hosts.

== Native tape backup and recovery

Support for most existing tape drives are included in ONTAP, as well as a method for tape vendors to dynamically add support for new devices. ONTAP also supports the Remote Magnetic Tape (RMT) protocol, enabling backup and recovery to any capable system.

### Related information

[NetApp Documentation: SnapDrive for UNIX](#)

[NetApp Documentation: SnapDrive for Windows \(current releases\)](#)

### Data protection using tape backup

= Effect of moving or copying a LUN on Snapshot copies

= Effect of moving or copying a LUN on Snapshot copies overview

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

Snapshot copies are created at the volume level. If you copy or move a LUN to a different volume, the Snapshot copy policy of the destination volume is applied to the copied or moved volume. If Snapshot copies are not established for the destination volume, Snapshot copies will not be created of the moved or copied LUN.

= Restore a single LUN from a Snapshot copy

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You can restore a single LUN from a Snapshot copy without restoring the entire volume that contains the single LUN. You can restore the LUN in place or to a new path in the volume. The operation restores only the single LUN without impacting other files or LUNs in the volume. You can also restore files with streams.

### What you'll need

- You must have enough space on your volume to complete the restore operation:
  - If you are restoring a space-reserved LUN where the fractional reserve is 0%, you require one times the size of the restored LUN.
  - If you are restoring a space-reserved LUN where the fractional reserve is 100%, you require two times the size of the restored LUN.
  - If you are restoring a non-space-reserved LUN, you only require the actual space used for the restored LUN.
- A Snapshot copy of the destination LUN must have been created.

If the restore operation fails, the destination LUN might be truncated. In such cases, you can use the Snapshot copy to prevent data loss.

- A Snapshot copy of the source LUN must have been created.

In rare cases, the LUN restore can fail, leaving the source LUN unusable. If this occurs, you can use the Snapshot copy to return the LUN to the state just before the restore attempt.

- The destination LUN and source LUN must have the same OS type.

If your destination LUN has a different OS type from your source LUN, your host can lose data access to the destination LUN after the restore operation.

### Steps

1. From the host, stop all host access to the LUN.
2. Unmount the LUN on its host so that the host cannot access the LUN.
3. Unmap the LUN:

```
lun mapping delete -vserver vserver_name -volume volume_name -lun lun_name  
-igroup igroup_name
```

4. Determine the Snapshot copy you want to restore your LUN to:

```
volume snapshot show -vserver vserver_name -volume volume_name
```

5. Create a Snapshot copy of the LUN prior to restoring the LUN:

```
volume snapshot create -vserver vserver_name -volume volume_name -snapshot  
snapshot_name
```

6. Restore the specified LUN in a volume:

```
volume snapshot restore-file -vserver vserver_name -volume volume_name  
-snapshot snapshot_name -path lun_path
```

7. Follow the steps on the screen.

8. If necessary, bring the LUN online:

```
lun modify -vserver vserver_name -path lun_path -state online
```

9. If necessary, remap the LUN:

```
lun mapping create -vserver vserver_name -volume volume_name -lun lun_name  
-igroup igroup_name
```

10. From the host, remount the LUN.

11. From the host, restart access to the LUN.

= Restore all LUNs in a volume from a Snapshot copy

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You can use `volume snapshot restore` command to restore all the LUNs in a specified volume from a Snapshot copy.

### Steps

1. From the host, stop all host access to the LUNs.

Using SnapRestore without stopping all host access to LUNs in the volume can cause data corruption and system errors.

2. Unmount the LUNs on that host so that the host cannot access the LUNs.
3. Unmap your LUNs:

```
lun mapping delete -vserver vserver_name -volume volume_name -lun lun_name  
-igroup igroup_name
```

4. Determine the Snapshot copy to which you want to restore your volume:

```
volume snapshot show -vserver vserver_name -volume volume_name
```

5. Change your privilege setting to advanced:

```
set -privilege advanced
```

6. Restore your data:

```
volume snapshot restore -vserver vserver_name -volume volume_name -snapshot  
snapshot_name
```

7. Follow the instructions on the screen.

8. Remap your LUNs:

```
lun mapping create -vserver vserver_name -volume volume_name -lun lun_name  
-igroup igroup_name
```

9. Verify that your LUNs are online:

```
lun show -vserver vserver_name -path lun_path -fields state
```

10. If your LUNs are not online, bring them online:

```
lun modify -vserver vserver_name -path lun_path -state online
```

11. Change your privilege setting to admin:

```
set -privilege admin
```

12. From the host, remount your LUNs.

13. From the host, restart access to your LUNs.

= Delete one or more existing Snapshot copies from a volume

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You can manually delete one or more existing Snapshot copies from the volume. You might want to do this if you need more space on your volume.

## Steps

1. Use the `volume snapshot show` command to verify which Snapshot copies you want to delete.

```
cluster::> volume snapshot show -vserver vs3 -volume vol3
```

Vserver	Volume	Snapshot	Size	---Blocks---	
				Total%	Used%
vs3	vol3	snap1.2013-05-01_0015	100KB	0%	38%
		snap1.2013-05-08_0015	76KB	0%	32%
		snap2.2013-05-09_0010	76KB	0%	32%
		snap2.2013-05-10_0010	76KB	0%	32%
		snap3.2013-05-10_1005	72KB	0%	31%
		snap3.2013-05-10_1105	72KB	0%	31%
		snap3.2013-05-10_1205	72KB	0%	31%
		snap3.2013-05-10_1305	72KB	0%	31%
		snap3.2013-05-10_1405	72KB	0%	31%
		snap3.2013-05-10_1505	72KB	0%	31%

10 entries were displayed.

2. Use the `volume snapshot delete` command to delete Snapshot copies.

If you want to...	Enter this command...
Delete a single Snapshot copy	<code>volume snapshot delete -vserver <i>svm_name</i> -volume <i>vol_name</i> -snapshot <i>snapshot_name</i></code>
Delete multiple Snapshot copies	<code>volume snapshot delete -vserver <i>svm_name</i> -volume <i>vol_name</i> -snapshot <i>snapshot_name1</i> [, <i>snapshot_name2</i>, ...]</code>
Delete all Snapshot copies	<code>volume snapshot delete -vserver <i>svm_name</i> -volume <i>vol_name</i> -snapshot *</code>

The following example deletes all Snapshot copies on the volume vol3.

```
cluster::> volume snapshot delete -vserver vs3 -volume vol3 *
```

10 entries were acted on.

= Use FlexClone LUNs to protect your data

= Use FlexClone LUNs to protect your data overview

```
:icons: font
:relative_path: ./san-admin/
:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/
```

A FlexClone LUN is a point-in-time, writeable copy of another LUN in an active volume or in a Snapshot copy. The clone and its parent can be modified independently without affecting each other.

A FlexClone LUN shares space initially with its parent LUN. By default, the FlexClone LUN inherits the space-reserved attribute of the parent LUN. For example, if the parent LUN is non-space-reserved, the FlexClone LUN is also non-space-reserved by default. However, you can create a non-space-reserved FlexClone LUN from a parent that is a space-reserved LUN.

When you clone a LUN, block sharing occurs in the background and you cannot create a volume Snapshot copy until the block sharing is finished.

You must configure the volume to enable the FlexClone LUN automatic deletion function with the `volume snapshot autodelete modify` command. Otherwise, if you want FlexClone LUNs to be deleted automatically but the volume is not configured for FlexClone auto delete, none of the FlexClone LUNs are deleted.

When you create a FlexClone LUN, the FlexClone LUN automatic deletion function is disabled by default. You must manually enable it on every FlexClone LUN before that FlexClone LUN can be automatically deleted. If you are using semi-thick volume provisioning and you want the “best effort” write guarantee provided by this option, you must make *all* FlexClone LUNs available for automatic deletion.

When you create a FlexClone LUN from a Snapshot copy, the LUN is automatically split from the Snapshot copy by using a space-efficient background process so that the LUN does not continue to depend on the Snapshot copy or consume any additional space. If this background split has not been completed and this Snapshot copy is automatically deleted, that FlexClone LUN is deleted even if you have disabled the FlexClone auto delete function for that FlexClone LUN. After the background split is complete, the FlexClone LUN is not deleted even if that Snapshot copy is deleted.

## Related information

### [Logical storage management](#)

= Reasons for using FlexClone LUNs

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You can use FlexClone LUNs to create multiple read/write copies of a LUN.

You might want to do this for the following reasons:

- You need to create a temporary copy of a LUN for testing purposes.
- You need to make a copy of your data available to additional users without giving them access to the production data.
- You want to create a clone of a database for manipulation and projection operations, while preserving the original data in an unaltered form.
- You want to access a specific subset of a LUN's data (a specific logical volume or file system in a volume group, or a specific file or set of files in a file system) and copy it to the original LUN, without restoring the rest of the data in the original LUN. This works on operating systems that support mounting a LUN and a clone of the LUN at the same time. SnapDrive for UNIX supports this with the `snap connect` command.
- You need multiple SAN boot hosts with the same operating system.

= How a FlexVol volume can reclaim free space with autodelete setting

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You can enable the autodelete setting of a FlexVol volume to automatically delete FlexClone files and FlexClone LUNs. By enabling autodelete, you can reclaim a target amount of free space in the volume when a volume is nearly full.

You can configure a volume to automatically start deleting FlexClone files and FlexClone LUNs when the free space in the volume decreases below a particular threshold value, and automatically stop deleting clones when a target amount of free space in the volume is reclaimed. Although, you cannot specify the threshold value that starts the automatic deletion of clones, you can specify whether a clone is eligible for deletion, and you can specify the target amount of free space for a volume.

A volume automatically deletes FlexClone files and FlexClone LUNs when the free space in the volume decreases below a particular threshold and when *both* of the following requirements are met:

- The autodelete capability is enabled for the volume that contains the FlexClone files and FlexClone LUNs.

You can enable the autodelete capability for a FlexVol volume by using the `volume snapshot autodelete modify` command. You must set the `-trigger` parameter to `volume` or `snap_reserve` for a volume to automatically delete FlexClone files and FlexClone LUNs.

- The autodelete capability is enabled for the FlexClone files and FlexClone LUNs.



You can enable autodelete for a FlexClone file or FlexClone LUN by using the `file clone create` command with the `-autodelete` parameter. As a result, you can preserve certain FlexClone files and FlexClone LUNs by disabling autodelete for the clones and ensuring that other volume settings do not override the clone setting.

= Configure a FlexVol volume to automatically delete FlexClone files and FlexClone LUNs

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You can enable a FlexVol volume to automatically delete FlexClone files and FlexClone LUNs with autodelete enabled when the free space in the volume decreases below a particular threshold.

### What you'll need

- The FlexVol volume must contain FlexClone files and FlexClone LUNs and be online.
- The FlexVol volume must not be a read-only volume.

### Steps

1. Enable automatic deletion of FlexClone files and FlexClone LUNs in the FlexVol volume by using the `volume snapshot autodelete modify` command.
  - For the `-trigger` parameter, you can specify `volume` or `snap_reserve`.
  - For the `-destroy-list` parameter, you must always specify `lun_clone`, `file_clone` regardless of whether you want to delete only one type of clone.

The following example shows how you can enable volume `vol1` to trigger the automatic deletion of FlexClone files and FlexClone LUNs for space reclamation until 25% of the volume consists of free space:

```
cluster1::> volume snapshot autodelete modify -vserver vs1
-volume vol1 -enabled true -commitment disrupt -trigger volume
-target-free-space 25 -destroy-list lun_clone,file_clone

Volume modify successful on volume:vol1
```

While enabling FlexVol volumes for automatic deletion, if you set the value of the `-commitment` parameter to `destroy`, all the FlexClone files and FlexClone LUNs with the `-autodelete` parameter set to `true` might be deleted when the free space in the volume decreases below the specified threshold value. However, FlexClone files and FlexClone LUNs with the `-autodelete` parameter set to `false` will not be deleted.

1. Verify that automatic deletion of FlexClone files and FlexClone LUNs is enabled in the FlexVol volume by using the `volume snapshot autodelete show` command.

The following example shows that volume `vol1` is enabled for automatic deletion of FlexClone files and FlexClone LUNs:

```
cluster1::> volume snapshot autodelete show -vserver vs1 -volume
vol1

      Vserver Name: vs1
      Volume Name: vol1
      Enabled: true
      Commitment: disrupt
      Defer Delete: user_created
      Delete Order: oldest_first
      Defer Delete Prefix: (not specified)*
      Target Free Space: 25%
      Trigger: volume
      Destroy List: lun_clone,file_clone
      Is Constituent Volume: false
```

2. Ensure that autodelete is enabled for the FlexClone files and FlexClone LUNs in the volume that you want to delete by performing the following steps:

- a. Enable automatic deletion of a particular FlexClone file or FlexClone LUN by using the `volume file clone autodelete` command.

You can force a specific FlexClone file or FlexClone LUN to be automatically deleted by using the `volume file clone autodelete` command with the `-force` parameter.

The following example shows that automatic deletion of the FlexClone LUN `lun1_clone` contained in volume `vol1` is enabled:

```
cluster1::> volume file clone autodelete -vserver vs1 -clone-path
/vol/vol1/lun1_clone -enabled true
```

You can enable autodelete when you create FlexClone files and FlexClone LUNs.

- b. Verify that the FlexClone file or FlexClone LUN is enabled for automatic deletion by using the `volume file clone show-autodelete` command.

The following example shows that the FlexClone LUN `lun1_clone` is enabled for automatic deletion:

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone
-path vol/vol1/lun1_clone

Vserver Name: vs1
                                                    Clone

Path: vol/vol1/lun1_clone

**Autodelete Enabled: true**
```

For more information about using the commands, see the respective man pages.

= Clone LUNs from an active volume

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You can create copies of your LUNs by cloning the LUNs in the active volume. These FlexClone LUNs are readable and writeable copies of the original LUNs in the active volume.

### What you'll need

A FlexClone license must be installed.

### About this task

A space-reserved FlexClone LUN requires as much space as the space-reserved parent LUN. If the FlexClone LUN is not space-reserved, you must ensure that the volume has enough space to accommodate changes to the FlexClone LUN.

### Steps

1. You must have verified that the LUNs are not mapped to an igroup or are written to before making the clone.
2. Use the `lun show` command to verify that the LUN exists.

```
lun show -vserver vs1
```

Vserver	Path	State	Mapped	Type	Size
vs1	/vol/vol1/lun1	online	unmapped	windows	47.07MB

3. Use the `volume file clone create` command to create the FlexClone LUN.

```
volume file clone create -vserver vs1 -volume vol1 -source-path lun1
-destination-path/lun1_clone
```

If you need the FlexClone LUN to be available for automatic deletion, you include `-autodelete true`. If you are creating this FlexClone LUN in a volume using semi-thick provisioning, you must

enable automatic deletion for all FlexClone LUNs.

4. Use the `lun show` command to verify that you created a LUN.

```
lun show -vserver vs1
```

Vserver	Path	State	Mapped	Type	Size
vs1	/vol/volX/lun1	online	unmapped	windows	47.07MB
vs1	/vol/volX/lun1_clone	online	unmapped	windows	47.07MB

= Create FlexClone LUNs from a Snapshot copy in a volume

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You can use a Snapshot copy in your volume to create FlexClone copies of your LUNs. FlexClone copies of LUNs are both readable and writeable.

### What you'll need

A FlexClone license must be installed.

### About this task

The FlexClone LUN inherits the space reservations attribute of the parent LUN. A space-reserved FlexClone LUN requires as much space as the space-reserved parent LUN. If the FlexClone LUN is not space-reserved, the volume must have enough space to accommodate changes to the clone.

### Steps

1. Verify that the LUN is not mapped or being written to.
2. Create a Snapshot copy of the volume that contains the LUNs:

```
volume snapshot create -vserver vserver_name -volume volume_name -snapshot snapshot_name
```

You must create a Snapshot copy (the backing Snapshot copy) of the LUN you want to clone.

3. Create the FlexClone LUN from the Snapshot copy:

```
file clone create -vserver vserver_name -volume volume_name -source-path source_path -snapshot-name snapshot_name -destination-path destination_path
```

If you need the FlexClone LUN to be available for automatic deletion, you include `-autodelete true`. If you are creating this FlexClone LUN in a volume using semi-thick provisioning, you must enable automatic deletion for all FlexClone LUNs.

4. Verify that the FlexClone LUN is correct:

```
lun show -vserver vserver_name
```

Vserver	Path	State	Mapped	Type	Size
vs1	/vol/vol1/lun1_clone	online	unmapped	windows	47.07MB
vs1	/vol/vol1/lun1_snap_clone	online	unmapped	windows	47.07MB

= Prevent a specific FlexClone file or FlexClone LUN from being automatically deleted

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

If you configure a FlexVol volume to automatically delete FlexClone files and FlexClone LUNs, any clone that fits the criteria you specify might be deleted. If you have specific FlexClone files or FlexClone LUNs that you want to preserve, you can exclude them from the automatic FlexClone deletion process.

#### What you'll need

A FlexClone license must be installed.

#### About this task

When you create a FlexClone file or FlexClone LUN, by default the autodelete setting for the clone is disabled. FlexClone files and FlexClone LUNs with autodelete disabled are preserved when you configure a FlexVol volume to automatically delete clones to reclaim space on the volume.

If you set the `commitment` level on the volume to `try` or `disrupt`, you can individually preserve specific FlexClone files or FlexClone LUNs by disabling autodelete for those clones. However, if you set the `commitment` level on the volume to `destroy` and the `destroy` lists include `lun_clone`, `file_clone`, the volume setting overrides the clone setting, and all FlexClone files and FlexClone LUNs can be deleted regardless of the autodelete setting for the clones.

## Steps

1. Prevent a specific FlexClone file or FlexClone LUN from being automatically deleted by using the `volume file clone autodelete` command.

The following example shows how you can disable autodelete for FlexClone LUN `lun1_clone` contained in `vol1`:

```
cluster1::> volume file clone autodelete -vserver vs1 -volume vol1
-clone-path lun1_clone -enable false
```

A FlexClone file or FlexClone LUN with autodelete disabled cannot be deleted automatically to reclaim space on the volume.

2. Verify that autodelete is disabled for the FlexClone file or FlexClone LUN by using the `volume file clone show-autodelete` command.

The following example shows that autodelete is false for the FlexClone LUN `lun1_clone`:

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone
-path vol/vol1/lun1_clone
Name: vs1
Path: vol/vol1/lun1_clone
Autodelete Enabled: false
Vserver
Clone
```

= Configure and use SnapVault backups in a SAN environment

= Configure and use SnapVault backups in a SAN environment overview

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

SnapVault configuration and use in a SAN environment is very similar to configuration and use in a NAS environment, but restoring LUNs in a SAN environment requires some special procedures.

SnapVault backups contain a set of read-only copies of a source volume. In a SAN environment you always back up entire volumes to the SnapVault secondary volume, not individual LUNs.

The procedure for creating and initializing the SnapVault relationship between a primary volume containing LUNs and a secondary volume acting as a SnapVault backup is identical to the procedure used with FlexVol volumes used for file protocols. This procedure is described in detail in [Data Protection](#).

It is important to ensure that LUNs being backed up are in a consistent state before the Snapshot copies are created and copied to the SnapVault secondary volume. Automating the Snapshot copy creation with

SnapCenter ensures that backed up LUNs are complete and usable by the original application.

There are three basic choices for restoring LUNs from a SnapVault secondary volume:

- You can map a LUN directly from the SnapVault secondary volume and connect a host to the LUN to access the contents of the LUN.

The LUN is read-only and you can map only from the most recent Snapshot copy in the SnapVault backup. Persistent reservations and other LUN metadata are lost. If desired, you can use a copy program on the host to copy the LUN contents back to the original LUN if it is still accessible.

The LUN has a different serial number from the source LUN.

- You can clone any Snapshot copy in the SnapVault secondary volume to a new read-write volume.

You can then map any of the LUNs in the volume and connect a host to the LUN to access the contents of the LUN. If desired, you can use a copy program on the host to copy the LUN contents back to the original LUN if it is still accessible.

- You can restore the entire volume containing the LUN from any Snapshot copy in the SnapVault secondary volume.

Restoring the entire volume replaces all of the LUNs, and any files, in the volume. Any new LUNs created since the Snapshot copy was created are lost.

The LUNs retain their mapping, serial numbers, UUIDs, and persistent reservations.

= Access a read-only LUN copy from a SnapVault backup

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You can access a read-only copy of a LUN from the latest Snapshot copy in a SnapVault backup. The LUN ID, path, and serial number are different from the source LUN and must first be mapped. Persistent reservations, LUN mappings, and igroups are not replicated to the SnapVault secondary volume.

#### What you'll need

- The SnapVault relationship must be initialized and the latest Snapshot copy in the SnapVault secondary volume must contain the desired LUN.
- The storage virtual machine (SVM) containing the SnapVault backup must have one or more LIFs with the desired SAN protocol accessible from the host used to access the LUN copy.
- If you plan to access LUN copies directly from the SnapVault secondary volume, you must create your igroups on the SnapVault SVM in advance.

You can access a LUN directly from the SnapVault secondary volume without having to first restore or clone the volume containing the LUN.

#### About this task

If a new Snapshot copy is added to the SnapVault secondary volume while you have a LUN mapped from a previous Snapshot copy, the contents of the mapped LUN changes. The LUN is still mapped with the same identifiers, but the data is taken from the new Snapshot copy. If the LUN size changes, some hosts

automatically detect the size change; Windows hosts require a disk rescan to pick up any size change.

## Steps

1. Run the `lun show` command to list the available LUNs in the SnapVault secondary volume.

In this example, you can see both the original LUNs in the primary volume `srcvolA` and the copies in the SnapVault secondary volume `dstvolB`:

```
cluster::> lun show
```

Vserver	Path	State	Mapped	Type	Size
vserverA	/vol/srcvolA/lun_A	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_B	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_C	online	mapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_A	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_B	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_C	online	unmapped	windows	300.0GB

```
6 entries were displayed.
```

2. If the `igroup` for the desired host does not already exist on the SVM containing the SnapVault secondary volume, run the `igroup create` command to create an `igroup`.

This command creates an `igroup` for a Windows host that uses the iSCSI protocol:

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup  
-protocol iscsi -ostype windows  
-initiator iqn.1991-05.com.microsoft:hostA
```

3. Run the `lun mapping create` command to map the desired LUN copy to the `igroup`.

```
cluster::> lun mapping create -vserver vserverB -path  
/vol/dstvolB/lun_A  
-igroup temp_igroup
```

4. Connect the host to the LUN and access the contents of the LUN as desired.

= Restore a single LUN from a SnapVault backup

```
:icons: font
```

```
:relative_path: ./san-admin/
```

```
:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/
```

You can restore a single LUN to a new location or to the original location. You can restore from any Snapshot copy in the SnapVault secondary volume. To restore the LUN to the original location, you first restore it to a new location and then copy it.



## What you'll need

- The SnapVault relationship must be initialized and the SnapVault secondary volume must contain an appropriate Snapshot copy to restore.
- The storage virtual machine (SVM) containing the SnapVault secondary volume must have one or more LIFs with the desired SAN protocol that are accessible from the host used to access the LUN copy.
- The igroups must already exist on the SnapVault SVM.

## About this task

The process includes creating a read-write volume clone from a Snapshot copy in the SnapVault secondary volume. You can use the LUN directly from the clone, or you can optionally copy the LUN contents back to the original LUN location.

The LUN in the clone has a different path and serial number from the original LUN. Persistent reservations are not retained.

## Steps

1. Run the `snapmirror show` command to verify the secondary volume that contains the SnapVault backup.

```
cluster::> snapmirror show
```

Source Path	Type	Dest Path	Mirror State	Relation Status	Total Progress	Healthy	Last Updated
vserverA:srcvolA	XDP	vserverB:dstvolB	Snapmirrored	Idle	-	true	-

2. Run the `volume snapshot show` command to identify the Snapshot copy that you want to restore the LUN from.

```
cluster::> volume snapshot show
```

Vserver	Volume	Snapshot	State	Size	Total%	Used%
vserverB	dstvolB	snap2.2013-02-10_0010	valid	124KB	0%	0%
		snap1.2013-02-10_0015	valid	112KB	0%	0%
		snap2.2013-02-11_0010	valid	164KB	0%	0%

3. Run the `volume clone create` command to create a read-write clone from the desired Snapshot copy.

The volume clone is created in the same aggregate as the SnapVault backup. There must be enough space in the aggregate to store the clone.

```
cluster::> volume clone create -vserver vserverB
  -flexclone dstvolB_clone -type RW -parent-volume dstvolB
  -parent-snapshot daily.2013-02-10_0010
[Job 108] Job succeeded: Successful
```

4. Run the `lun show` command to list the LUNs in the volume clone.

```
cluster::> lun show -vserver vserverB -volume dstvolB_clone

Vserver      Path                                     State   Mapped   Type
-----
vserverB     /vol/dstvolB_clone/lun_A               online  unmapped windows
vserverB     /vol/dstvolB_clone/lun_B               online  unmapped windows
vserverB     /vol/dstvolB_clone/lun_C               online  unmapped windows

3 entries were displayed.
```

5. If the `igroup` for the desired host does not already exist on the SVM containing the SnapVault backup, run the `igroup create` command to create an `igroup`.

This example creates an `igroup` for a Windows host that uses the iSCSI protocol:

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup
  -protocol iscsi -ostype windows
  -initiator iqn.1991-05.com.microsoft:hostA
```

6. Run the `lun mapping create` command to map the desired LUN copy to the `igroup`.

```
cluster::> lun mapping create -vserver vserverB
  -path /vol/dstvolB_clone/lun_C -igroup temp_igroup
```

7. Connect the host to the LUN and access the contents of the LUN, as desired.

The LUN is read-write and can be used in place of the original LUN. Because the LUN serial number is different, the host interprets it as a different LUN from the original.

8. Use a copy program on the host to copy the LUN contents back to the original LUN.

= Restore all LUNs in a volume from a SnapVault backup

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

If one or more LUNs in a volume need to be restored from a SnapVault backup, you can restore the entire volume. Restoring the volume affects all LUNs in the volume.

### What you'll need

The SnapVault relationship must be initialized and the SnapVault secondary volume must contain an appropriate Snapshot copy to restore.

### About this task

Restoring an entire volume returns the volume to the state it was in when the Snapshot copy was made. If a LUN was added to the volume after the Snapshot copy, that LUN is removed during the restore process.

After restoring the volume, the LUNs remain mapped to the igroups they were mapped to just before the restore. The LUN mapping might be different from the mapping at the time of the Snapshot copy. Persistent reservations on the LUNs from host clusters are retained.

### Steps

1. Stop I/O to all LUNs in the volume.
2. Run the `snapmirror show` command to verify the secondary volume that contains the SnapVault secondary volume.

```
cluster::> snapmirror show
```

Source Path	Type	Dest Path	Mirror State	Relation Status	Total Progress	Healthy	Last Updated
vserverA:srcvolA	XDP	vserverB:dstvolB	Snapmirrored	Idle	-	true	-

3. Run the `volume snapshot show` command to identify the Snapshot copy that you want to restore from.

```
cluster::> volume snapshot show
```

Vserver	Volume	Snapshot	State	Size	Total%	Used%
vserverB	dstvolB	snap2.2013-02-10_0010	valid	124KB	0%	0%
		snap1.2013-02-10_0015	valid	112KB	0%	0%
		snap2.2013-02-11_0010	valid	164KB	0%	0%

4. Run the `snapmirror restore` command and specify the `-source-snapshot` option to specify the Snapshot copy to use.

The destination you specify for the restore is the original volume you are restoring to.

```
cluster::> snapmirror restore -destination-path vserverA:srcvolA
  -source-path vserverB:dstvolB -source-snapshot daily.2013-02-
10_0010
```

```
Warning: All data newer than Snapshot copy hourly.2013-02-11_1205 on
volume vserverA:src_volA will be deleted.
```

```
Do you want to continue? {y|n}: y
```

```
[Job 98] Job is queued: snapmirror restore from source
"vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.
```

5. If you are sharing LUNs across a host cluster, restore the persistent reservations on the LUNs from the affected hosts.

== Restoring a volume from a SnapVault backup

In the following example, the LUN named lun\_D was added to the volume after the Snapshot copy was created. After restoring the entire volume from the Snapshot copy, lun\_D no longer appears.

In the `lun show` command output, you can see the LUNs in the primary volume srcvolA and the read-only copies of those LUNs in the SnapVault secondary volume dstvolB. There is no copy of lun\_D in the SnapVault backup.

```
cluster::> lun show
```

Vserver	Path	State	Mapped	Type	Size
vserverA	/vol/srcvolA/lun_A	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_B	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_C	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_D	online	mapped	windows	250.0GB
vserverB	/vol/dstvolB/lun_A	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_B	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_C	online	unmapped	windows	300.0GB

7 entries were displayed.

```
cluster::>snapmirror restore -destination-path vserverA:srcvolA
-source-path vserverB:dstvolB
-source-snapshot daily.2013-02-10_0010
```

Warning: All data newer than Snapshot copy hourly.2013-02-11\_1205 on volume vserverA:src\_volA will be deleted.

Do you want to continue? {y|n}: y

[Job 98] Job is queued: snapmirror restore from source "vserverB:dstvolB" for the snapshot daily.2013-02-10\_0010.

```
cluster::> lun show
```

Vserver	Path	State	Mapped	Type	Size
vserverA	/vol/srcvolA/lun_A	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_B	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_C	online	mapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_A	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_B	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_C	online	unmapped	windows	300.0GB

6 entries were displayed.

After the volume is restored from the SnapVault secondary volume, the source volume no longer contains lun\_D. You do not need to remap the LUNs in the source volume after the restore because they are still mapped.

= How you can connect a host backup system to the primary storage system

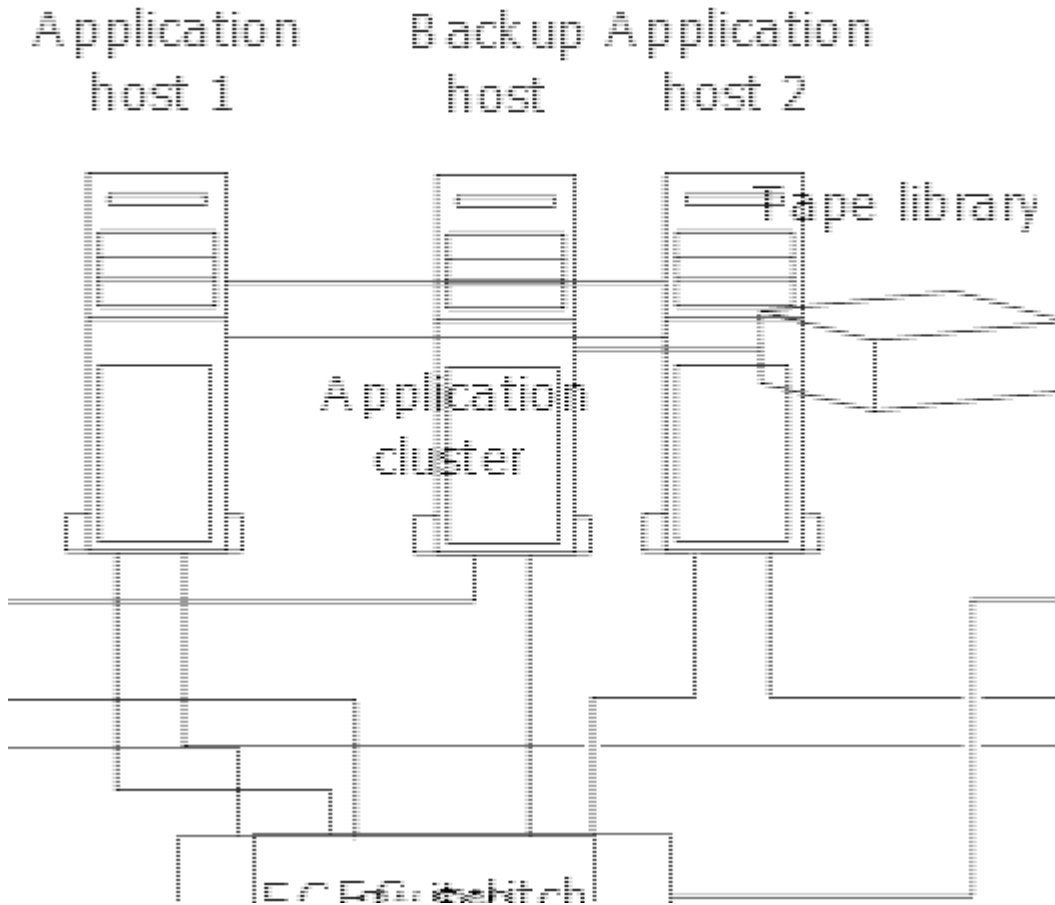
:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You can back up SAN systems to tape through a separate backup host to avoid performance degradation on the application host.

It is imperative that you keep SAN and NAS data separated for backup purposes. The figure below shows the recommended physical configuration for a host backup system to the primary storage system. You must configure volumes as SAN-only. LUNs can be confined to a single volume or the LUNs can be spread across multiple volumes or storage systems.



Volumes on a host can consist of a single LUN mapped from the storage system or multiple LUNs using a volume manager, such as VxVM on HP-UX systems.

= Back up a LUN through a host backup system

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You can use a cloned LUN from a Snapshot copy as source data for the host backup system.

### What you'll need

A production LUN must exist and be mapped to an igroup that includes the WWPN or initiator node name of the application server. The LUN must also be formatted and accessible to the host

### Steps

1. Save the contents of the host file system buffers to disk.

You can use the command provided by your host operating system, or you can use SnapDrive for Windows or SnapDrive for UNIX. You can also opt to make this step part of your SAN backup pre-processing script.

2. Use the `volume snapshot create` command to create a Snapshot copy of the production LUN.

```
volume snapshot create -vserver vs0 -volume vol3 -snapshot vol3_snapshot  
-comment "Single snapshot" -foreground false
```

3. Use the `volume file clone create` command to create a clone of the production LUN.

```
volume file clone create -vserver vs3 -volume vol3 -source-path lun1  
-snapshot-name snap_vol3 -destination-path lun1_backup
```

4. Use the `lun igroup create` command to create an igroup that includes the WWPN of the backup server.

```
lun igroup create -vserver vs3 -igroup igroup3 -protocol fc -ostype windows  
-initiator 10:00:00:00:c9:73:5b:91
```

5. Use the `lun mapping create` command to map the LUN clone you created in Step 3 to the backup host.

```
lun mapping create -vserver vs3 -volume vol3 -lun lun1_backup -igroup  
igroup3
```

You can opt to make this step part of your SAN backup application's post-processing script.

6. From the host, discover the new LUN and make the file system available to the host.

You can opt to make this step part of your SAN backup application's post-processing script.

7. Back up the data in the LUN clone from the backup host to tape by using your SAN backup application.

8. Use the `lun modify` command to take the LUN clone offline.

```
lun modify -vserver vs3 -path /vol/vol3/lun1_backup -state offline
```

9. Use the `lun delete` to remove the LUN clone.

```
lun delete -vserver vs3 -volume vol3 -lun lun1_backup
```

10. Use the `volume snapshot delete` command to remove the Snapshot copy.

```
volume snapshot delete -vserver vs3 -volume vol3 -snapshot vol3_snapshot
```

= SAN configurations in a MetroCluster environment

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You must be aware of certain considerations when using SAN configurations in a MetroCluster environment.

- MetroCluster configurations do not support front-end FC fabric "routed" vSAN configurations.

- MetroCluster configurations do not support front-end NVMe host connectivity.
- Other SAN protocols are supported on MetroCluster configurations.
- When using SAN client configurations, you must check whether any special considerations for MetroCluster configurations are included in the notes that are provided in the Interoperability Matrix Tool (IMT).
- Operating systems and applications must provide an I/O resiliency of 120 seconds to support MetroCluster automatic unplanned switchover and Tiebreaker or Mediator-initiated switchover.
- The MetroCluster is using the same WWPNs on both sides of the front-end SAN.



During switchover, the FC port on the surviving site might log in to the fabric before the fabric has detected that the FC port on the disaster site is offline and has removed this port from the name and directory services. If the FC port on the disaster is not yet removed, the fabric login attempt of the FC port at the surviving site might be rejected due to a duplicate WWPN. This behavior of the FC switches can be changed to honor the login of the previous device and not the existing one. You should verify the effects of this behavior on other fabric devices. Contact the switch vendor for more information.

To learn more, see:

- [Understanding MetroCluster data protection and disaster recovery](#)
- [Performing switchover for tests or maintenance](#)

### Steps

To avoid overlap when the old port goes offline and the new port comes online, use the following steps to configure the front-end switches:

For a...	Use these steps:
----------	------------------



Cisco switch

1. Connect to the switch and log in.

2. Enter configuration mode:

```
switch# config t  
switch(config)#
```

3. Overwrite the first device entry in the name server database with the new device:

```
switch(config)# no fcns reject-duplicate-pwvn vsan 1
```

4. In switches that are running NX-OS 8.x, confirm that the flogi quiesce timeout is set to zero:

a. Display the quiesce timerval:

```
switch(config)# show flogi interval info | i quiesce
```

```
Stats: fs flogi quiesce timerval: 0
```

b. If the output in the previous step does not indicate that the timerval is zero, then set it to zero:

```
switch(config)# flogi scale enable
```

```
switch(config)$ flogi quiesce timeout 0
```

## Brocade switch

1. Connect to the switch and log in.
2. Enter the `switchDisable` command.
3. Enter the `configure` command, and press `y` at the prompt.

```
F-Port login parameters (yes, y, no, n): [no] y
```

4. Choose setting 1:

```
- 0: First login take precedence over the second  
login (default)  
- 1: Second login overrides first login.  
- 2: the port type determines the behavior  
Enforce FLOGI/FDISC login: (0..2) [0] 1
```

5. Respond to the remaining prompts, or press **Ctrl + D**.
6. Enter the `switchEnable` command.

For further MetroCluster-specific host information, refer to the following NetApp Knowledge Base articles:

[What are AIX Host support considerations in a MetroCluster configuration?](#)

[Solaris host support considerations in a MetroCluster configuration](#)

### Related information

[NetApp Interoperability Matrix Tool](#)

= SAN concepts

= About SAN host provisioning

= SAN provisioning with iSCSI

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

In SAN environments, storage systems are targets that have storage target devices. For iSCSI and FC, the storage target devices are referred to as LUNs (logical units). For Non-Volatile Memory Express (NVMe) over Fibre Channel, the storage target devices are referred to as namespaces.

You configure storage by creating LUNs for iSCSI and FC or by creating namespaces for NVMe. The LUNs or namespaces are then accessed by hosts using Internet Small Computer Systems Interface (iSCSI) or Fibre Channel (FC) protocol networks.

To connect to iSCSI networks, hosts can use standard Ethernet network adapters (NICs), TCP offload engine (TOE) cards with software initiators, converged network adapters (CNAs), or dedicated iSCSI host

bus adapters (HBAs).

To connect to FC networks, hosts require FC HBAs or CNAs.

Supported FC protocols include:

- FC
- FCoE
- NVMe

== iSCSI target node network connections and names

iSCSI target nodes can connect to the network in several ways:

- Over Ethernet interfaces using software that is integrated into ONTAP.
- Over multiple system interfaces, with an interface used for iSCSI that can also transmit traffic for other protocols, such as SMB and NFS.
- Using a unified target adapter (UTA) or a converged network adapter (CNA).

Every iSCSI node must have a node name.

The two formats, or type designators, for iSCSI node names are *iqn* and *eui*. The SVM iSCSI target always uses the iqn-type designator. The initiator can use either the iqn-type or eui-type designator.

== Storage system node name

Each SVM running iSCSI has a default node name based on a reverse domain name and a unique encoding number.

The node name is displayed in the following format:

`iqn.1992-08.com.netapp:sn.unique-encoding-number`

The following example shows the default node name for a storage system with a unique encoding number:

`iqn.1992-08.com.netapp:sn.812921059e6c11e097b3123478563412:vs.6`

== TCP port for iSCSI

The iSCSI protocol is configured in ONTAP to use TCP port number 3260.

ONTAP does not support changing the port number for iSCSI. Port number 3260 is registered as part of the iSCSI specification and cannot be used by any other application or service.

### Related information

[NetApp Documentation: ONTAP SAN Host Configuration](#)

= iSCSI service management

= iSCSI service management

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You can manage the availability of the iSCSI service on the iSCSI logical interfaces of the storage virtual machine (SVM) by using the `vserver iscsi interface enable` or `vserver iscsi interface disable` commands.

By default, the iSCSI service is enabled on all iSCSI logical interfaces.

== How iSCSI is implemented on the host

iSCSI can be implemented on the host using hardware or software.

You can implement iSCSI in one of the following ways:

- Using Initiator software that uses the host's standard Ethernet interfaces.
- Through an iSCSI host bus adapter (HBA): An iSCSI HBA appears to the host operating system as a SCSI disk adapter with local disks.
- Using a TCP Offload Engine (TOE) adapter that offloads TCP/IP processing.

The iSCSI protocol processing is still performed by host software.

= How iSCSI authentication works

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

During the initial stage of an iSCSI session, the initiator sends a login request to the storage system to begin an iSCSI session. The storage system then either permits or denies the login request, or determine that a login is not required.

iSCSI authentication methods are:

- Challenge Handshake Authentication Protocol (CHAP)--The initiator logs in using a CHAP user name and password.

You can specify a CHAP password or generate a hexadecimal secret password. There are two types of CHAP user names and passwords:

- Inbound—The storage system authenticates the initiator.

Inbound settings are required if you are using CHAP authentication.

- Outbound—This is an optional setting to enable the initiator to authenticate the storage system.

You can use outbound settings only if you define an inbound user name and password on the storage system.

- deny—The initiator is denied access to the storage system.
- none—The storage system does not require authentication for the initiator.

You can define the list of initiators and their authentication methods. You can also define a default authentication method that applies to initiators that are not on this list.

#### **Related information**

= iSCSI initiator security management

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

ONTAP provides a number of features for managing security for iSCSI initiators. You can define a list of iSCSI initiators and the authentication method for each, display the initiators and their associated authentication methods in the authentication list, add and remove initiators from the authentication list, and define the default iSCSI initiator authentication method for initiators not in the list.

= iSCSI endpoint isolation

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

Beginning with ONTAP 9.1 existing iSCSI security commands were enhanced to accept an IP address range, or multiple IP addresses.

All iSCSI initiators must provide origination IP addresses when establishing a session or connection with a target. This new functionality prevents an initiator from logging into the cluster if the origination IP address is unsupported or unknown, providing a unique identification scheme. Any initiator originating from an unsupported or unknown IP address will have their login rejected at the iSCSI session layer, preventing the initiator from accessing any LUN or volume within the cluster.

Implement this new functionality with two new commands to help manage pre-existing entries.

== Add initiator address range

Improve iSCSI initiator security management by adding an IP address range, or multiple IP addresses with the `vserver iscsi security add-initiator-address-range` command.

```
cluster1::> vserver iscsi security add-initiator-address-range
```

== Remove initiator address range

Remove an IP address range, or multiple IP addresses, with the `vserver iscsi security remove-initiator-address-range` command.

```
cluster1::> vserver iscsi security remove-initiator-address-range
```

= What CHAP authentication is

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

The Challenge Handshake Authentication Protocol (CHAP) enables authenticated communication between iSCSI initiators and targets. When you use CHAP authentication, you define CHAP user names and passwords on both the initiator and the storage system.

During the initial stage of an iSCSI session, the initiator sends a login request to the storage system to begin the session. The login request includes the initiator's CHAP user name and CHAP algorithm. The storage system responds with a CHAP challenge. The initiator provides a CHAP response. The storage system verifies the response and authenticates the initiator. The CHAP password is used to compute the response.

= Guidelines for using CHAP authentication

You should follow certain guidelines when using CHAP authentication.

- If you define an inbound user name and password on the storage system, you must use the same user name and password for outbound CHAP settings on the initiator. If you also define an outbound user name and password on the storage system to enable bidirectional authentication, you must use the same user name and password for inbound CHAP settings on the initiator.
- You cannot use the same user name and password for inbound and outbound settings on the storage system.
- CHAP user names can be 1 to 128 bytes.

A null user name is not allowed.

- CHAP passwords (secrets) can be 1 to 512 bytes.

Passwords can be hexadecimal values or strings. For hexadecimal values, you should enter the value with a prefix of "0x" or "0X". A null password is not allowed.

- For additional restrictions, you should see the initiator's documentation.

For example, the Microsoft iSCSI software initiator requires both the initiator and target CHAP passwords to be at least 12 bytes if IPsec encryption is not being used. The maximum password length is 16 bytes regardless of whether IPsec is used.

= How using iSCSI interface access lists to limit initiator interfaces can increase performance and security

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

iSCSI interface access lists can be used to limit the number of LIFs in an SVM that an initiator can access, thereby increasing performance and security.

When an initiator begins a discovery session using an iSCSI `SendTargets` command, it receives the IP addresses associated with the LIF (network interface) that is in the access list. By default, all initiators have access to all iSCSI LIFs in the SVM. You can use the access list to restrict the number of LIFs in an SVM that an initiator has access to.

= iSNS server registration requirement

= What iSNS is

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

The Internet Storage Name Service (iSNS) is a protocol that enables automated discovery and management of iSCSI devices on a TCP/IP storage network. An iSNS

server maintains information about active iSCSI devices on the network, including their IP addresses, iSCSI node names IQN's, and portal groups.

You can obtain an iSNS server from a third-party vendor. If you have an iSNS server on your network configured and enabled for use by the initiator and target, you can use the management LIF for a storage virtual machine (SVM) to register all the iSCSI LIFs for that SVM on the iSNS server. After the registration is complete, the iSCSI initiator can query the iSNS server to discover all the LIFs for that particular SVM.

If you decide to use an iSNS service, you must ensure that your storage virtual machines (SVMs) are properly registered with an Internet Storage Name Service (iSNS) server.

If you do not have an iSNS server on your network, you must manually configure each target to be visible to the host.

== What an iSNS server does

An iSNS server uses the Internet Storage Name Service (iSNS) protocol to maintain information about active iSCSI devices on the network, including their IP addresses, iSCSI node names (IQNs), and portal groups.

The iSNS protocol enables automated discovery and management of iSCSI devices on an IP storage network. An iSCSI initiator can query the iSNS server to discover iSCSI target devices.

NetApp does not supply or resell iSNS servers. You can obtain these servers from a vendor supported by NetApp.

= How SVMs interact with an iSNS server

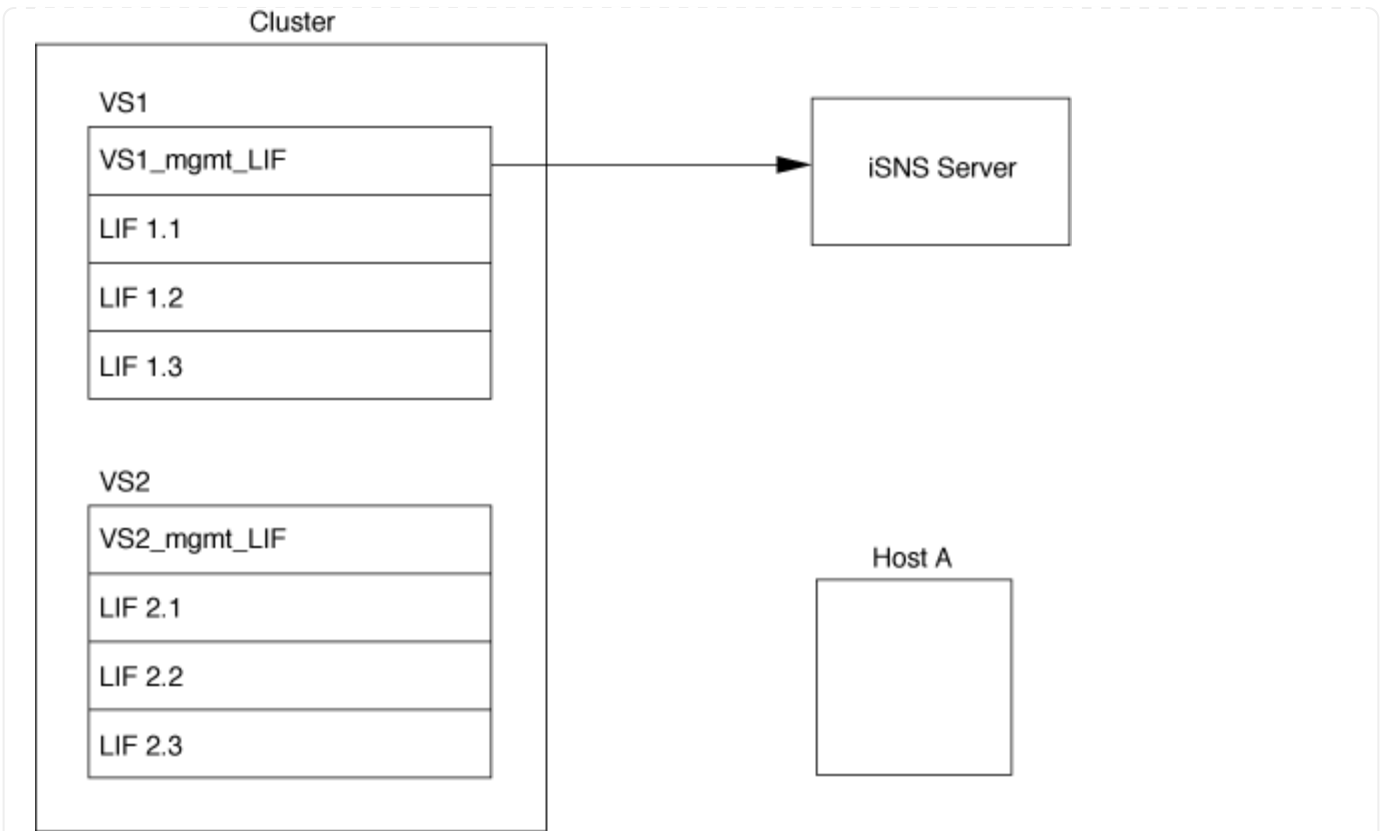
:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

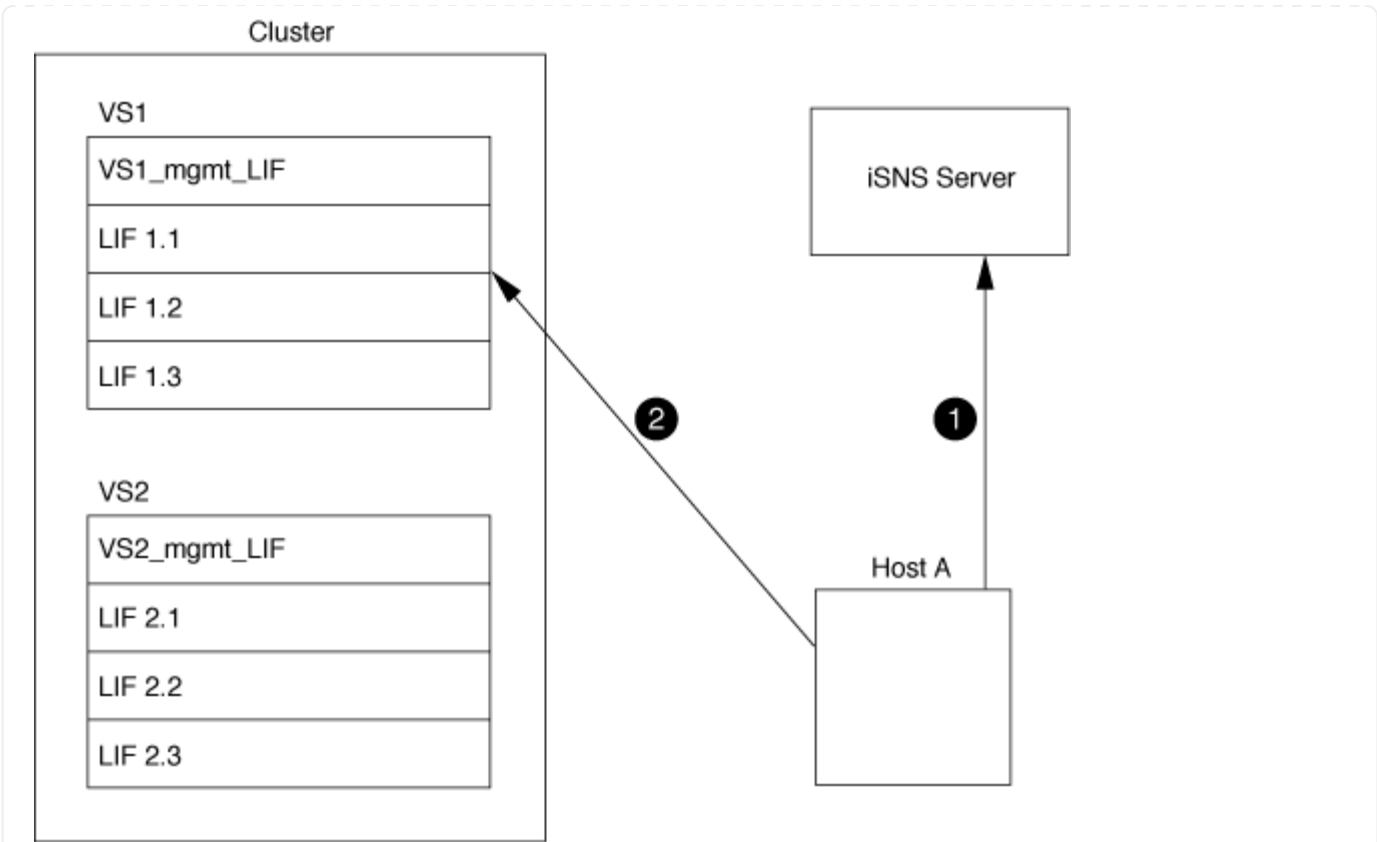
The iSNS server communicates with each storage virtual machine (SVM) through the SVM management LIF. The management LIF registers all iSCSI target node name, alias, and portal information with the iSNS service for a specific SVM.

In the following example, SVM VS1 uses the SVM management LIF vs1\_mgmt\_lif to register with the iSNS server. During iSNS registration, an SVM sends all the iSCSI LIFs through the SVM management LIF to the iSNS Server. After the iSNS registration is complete, the iSNS server has a list of all the LIFs serving iSCSI in VS1. If a cluster contains multiple SVMs, each SVM must register individually with the iSNS server to use the iSNS service.



In the next example, after the iSNS server completes the registration with the target, Host A can discover all the LIFs for VS1 through the iSNS server as indicated in step 1. After Host A completes the discovery of the LIFs for VS1, Host A can establish a connection with any of the LIFs in VS1 as shown in step 2. Host A is not aware of any of the LIFs in VS2 until the management LIF VS2\_mgmt\_LIF for VS2 registers with the iSNS server.





However, if you define the interface access lists, the host can only use the defined LIFs in the interface access list to access the target.

After iSNS is initially configured, ONTAP automatically updates the iSNS server when the SVM configuration settings change.

A delay of a few minutes can occur between the time you make the configuration changes and when ONTAP sends the update to the iSNS server. Force an immediate update of the iSNS information on the iSNS server: `vserver iscsi isns update`

- = Commands for managing iSNS
- :icons: font
- :relative\_path: ./san-admin/
- :imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

ONTAP provides commands to manage your iSNS service.

If you want to...	Use this command...
Configure an iSNS service	<code>vserver iscsi isns create</code>
Start an iSNS service	<code>vserver iscsi isns start</code>
Modify an iSNS service	<code>vserver iscsi isns modify</code>
Display iSNS service configuration	<code>vserver iscsi isns show</code>

If you want to...	Use this command...
Force an update of registered iSNS information	<code>vserver iscsi isns update</code>
Stop an iSNS service	<code>vserver iscsi isns stop</code>
Remove an iSNS service	<code>vserver iscsi isns delete</code>
View the man page for a command	<code>man <i>command name</i></code>

See the man page for each command for more information.

= SAN provisioning with FC

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You should be aware of the important concepts that are required to understand how ONTAP implements an FC SAN.

== How FC target nodes connect to the network

Storage systems and hosts have adapters so that they can be connected to FC switches with cables.

When a node is connected to the FC SAN, each SVM registers the World Wide Port Name (WWPN) of its LIF with the switch Fabric Name Service. The WWNN of the SVM and the WWPN of each LIF is automatically assigned by ONTAP.

Direct-connection to nodes from hosts with FC is not supported, NPIV is required and this requires a switch to be used. With iSCSI sessions, communication works with connections that are either network routed or direct-connect. However, both of these methods are supported with ONTAP.

## == How FC nodes are identified

Each SVM configured with FC is identified by a worldwide node name (WWNN).

## == How WWPNs are used

WWPNs identify each LIF in an SVM configured to support FC. These LIFs utilize the physical FC ports in each node in the cluster, which can be FC target cards, UTA or UTA2 configured as FC or FCoE in the nodes.

- Creating an initiator group

The WWPNs of the host's HBAs are used to create an initiator group (igroup). An igroup is used to control host access to specific LUNs. You can create an igroup by specifying a collection of WWPNs of initiators in an FC network. When you map a LUN on a storage system to an igroup, you can grant all the initiators in that group access to that LUN. If a host's WWPN is not in an igroup that is mapped to a LUN, that host does not have access to the LUN. This means that the LUNs do not appear as disks on that host.

You can also create port sets to make a LUN visible only on specific target ports. A port set consists of a group of FC target ports. You can bind an igroup to a port set. Any host in the igroup can access the LUNs only by connecting to the target ports in the port set.

- Uniquely identifying FC LIFs

WWPNs uniquely identify each FC logical interface. The host operating system uses the combination of the WWNN and WWPN to identify SVMs and FC LIFs. Some operating systems require persistent binding to ensure that the LUN appears at the same target ID on the host.

## == How worldwide name assignments work

Worldwide names are created sequentially in ONTAP. However, because of the way ONTAP assigns them, they might appear to be assigned in a non-sequential order.

Each adapter has a pre-configured WWPN and WWNN, but ONTAP does not use these pre-configured values. Instead, ONTAP assigns its own WWPNs or WWNNs, based on the MAC addresses of the onboard Ethernet ports.

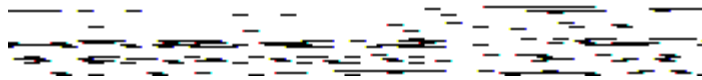
The worldwide names might appear to be non-sequential when assigned for the following reasons:

- Worldwide names are assigned across all the nodes and storage virtual machines (SVMs) in the cluster.
- Freed worldwide names are recycled and added back to the pool of available names.

## == How FC switches are identified

Fibre Channel switches have one worldwide node name (WWNN) for the device itself, and one worldwide port name (WWPN) for each of its ports.

For example, the following diagram shows how the WWPNs are assigned to each of the ports on a 16-port Brocade switch. For details about how the ports are numbered for a particular switch, see the vendor-supplied documentation for that switch.



Port **0**, WWPN 20:**00**:00:60:69:51:06:b4

Port **1**, WWPN 20:**01**:00:60:69:51:06:b4

Port **14**, WWPN 20:**0e**:00:60:69:51:06:b4

Port **15**, WWPN 20:**0f**:00:60:69:51:06:b4

= SAN provisioning with NVMe

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

Beginning with ONTAP 9.4, NVMe/FC is supported in SAN environment. NVMe/FC enables storage administrators to provision namespaces and subsystems and then map the namespaces to subsystems, similar to the way LUNs are provisioned and mapped to igroups for FC and iSCSI.

An NVMe namespace is a quantity of non-volatile memory that can be formatted into logical blocks. Namespaces are the equivalent of LUNs for FC and iSCSI protocols, and an NVMe subsystem is analogous to an igroup. An NVMe subsystem can be associated with initiators so that namespaces within the subsystem can be accessed by the associated initiators.

Although analogous in function, NVMe namespaces do not support all features supported by LUNs.

Beginning with ONTAP 9.5 a license is required to support host-facing data access with NVMe. If NVMe is enabled in ONTAP 9.4, a 90 day grace period is given to acquire the license after upgrading to ONTAP 9.5. You can enable the license using the following command:

```
system license add -license-code NVMe_license_key
```

#### **Related information**

[NetApp Technical Report 4684: Implementing and Configuring Modern SANs with NVMe/FC](#)

= About SAN volumes

= About SAN volumes overview

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

ONTAP provides three basic volume provisioning options: thick provisioning, thin provisioning, and semi-thick provisioning. Each option uses different ways to manage the volume space and the space requirements for ONTAP block sharing technologies. Understanding how the options work enables you to choose the best option for your environment.

Putting SAN LUNs and NAS shares in the same FlexVol volume is not recommended. You should provision separate FlexVol volumes specifically for your SAN LUNs and you should provision separate FlexVol volumes specifically to your NAS shares. This simplifies management and replication deployments and parallels the way FlexVol volumes are supported in Active IQ Unified Manager (formerly OnCommand Unified Manager).

## == Thin provisioning for volumes

When a thinly provisioned volume is created, ONTAP does not reserve any extra space when the volume is created. As data is written to the volume, the volume requests the storage it needs from the aggregate to accommodate the write operation. Using thin-provisioned volumes enables you to overcommit your aggregate, which introduces the possibility of the volume not being able to secure the space it needs when the aggregate runs out of free space.

You create a thin-provisioned FlexVol volume by setting its `-space-guarantee` option to `none`.

## == Thick provisioning for volumes

When a thick-provisioned volume is created, ONTAP sets aside enough storage from the aggregate to ensure that any block in the volume can be written to at any time. When you configure a volume to use thick provisioning, you can employ any of the ONTAP storage efficiency capabilities, such as compression and deduplication, to offset the larger upfront storage requirements.

You create a thick-provisioned FlexVol volume by setting its `-space-slo` (service level objective) option to `thick`.

## == Semi-thick provisioning for volumes

When a volume using semi-thick provisioning is created, ONTAP sets aside storage space from the aggregate to account for the volume size. If the volume is running out of free space because blocks are in use by block-sharing technologies, ONTAP makes an effort to delete protection data objects (Snapshot copies and FlexClone files and LUNs) to free up the space they are holding. As long as ONTAP can delete the protection data objects fast enough to keep pace with the space required for overwrites, the write operations continue to succeed. This is called a “best effort” write guarantee.

**Note:** The following functionality is not supported on volumes that use semi-thick provisioning:

- storage efficiency technologies such as deduplication, compression, and compaction
- Microsoft Offloaded Data Transfer (ODX)

You create a semi-thick-provisioned FlexVol volume by setting its `-space-slo` (service level objective) option to `semi-thick`.

## == Use with space-reserved files and LUNs

A space-reserved file or LUN is one for which storage is allocated when it is created. Historically, NetApp has used the term “thin-provisioned LUN” to mean a LUN for which space reservation is disabled (a non-space-reserved LUN).

**Note:** Non-space-reserved files are not generally referred to as “thin-provisioned files”.

The following table summarizes the major differences in how the three volume provisioning options can be used with space-reserved files and LUNs:

Volume provisioning	LUN/file space reservation	Overwrites	Protection data <sup>2</sup>	Storage efficiency <sup>3</sup>
Thick	Supported	Guaranteed <sup>1</sup>	Guaranteed	Supported

Volume provisioning	LUN/file space reservation	Overwrites	Protection data <sup>2</sup>	Storage efficiency <sup>3</sup>
Thin	No effect	None	Guaranteed	Supported
Semi-thick	Supported	Best effort <sup>1</sup>	Best effort	Not supported

## Notes

1. The ability to guarantee overwrites or provide a best-effort overwrite assurance requires that space reservation is enabled on the LUN or file.
2. Protection data includes Snapshot copies, and FlexClone files and LUNs marked for automatic deletion (backup clones).
3. Storage efficiency includes deduplication, compression, any FlexClone files and LUNs not marked for automatic deletion (active clones), and FlexClone subfiles (used for Copy Offload).

== Support for SCSI thin-provisioned LUNs

ONTAP supports T10 SCSI thin-provisioned LUNs as well as NetApp thin-provisioned LUNs. T10 SCSI thin provisioning enables host applications to support SCSI features including LUN space reclamation and LUN space monitoring capabilities for blocks environments. T10 SCSI thin provisioning must be supported by your SCSI host software.

You use the ONTAP `space-allocation` setting to enable/disable support for the T10 thin provisioning on a LUN. You use the ONTAP `space-allocation enable` setting to enable T10 SCSI thin provisioning on a LUN.

The `[-space-allocation {enabled|disabled}]` command in the ONTAP Command Reference Manual has more information to enable/disable support for the T10 thin provisioning and to enable T10 SCSI thin provisioning on a LUN.

## ONTAP 9 commands

= Configure volume provisioning options

```
:icons: font
```

```
:relative_path: ./san-admin/
```

```
:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/
```

You can configure a volume for thin provisioning, thick provisioning, or semi-thick provisioning.

### About this task

Setting the `-space-slo` option to `thick` ensures the following:

- The entire volume is preallocated in the aggregate. You cannot use the `volume create` or `volume modify` command to configure the volume's `-space-guarantee` option.
- 100% of the space required for overwrites is reserved. You cannot use the `volume modify` command to configure the volume's `-fractional-reserve` option

Setting the `-space-slo` option to `semi-thick` ensures the following:

- The entire volume is preallocated in the aggregate. You cannot use the `volume create` or `volume modify` command to configure the volume's `-space-guarantee` option.
- No space is reserved for overwrites. You can use the `volume modify` command to configure the volume's `-fractional-reserve` option.
- Automatic deletion of Snapshot copies is enabled.

## Step

1. Configure volume provisioning options:

```
volume create -vserver vserver_name -volume volume_name -aggregate
aggregate_name -space-slo none|thick|semi-thick -space-guarantee
none|volume
```

The `-space-guarantee` option defaults to `none` for AFF systems and for non-AFF DP volumes. Otherwise, it defaults to `volume`. For existing FlexVol volumes, use the `volume modify` command to configure provisioning options.

The following command configures `vol1` on SVM `vs1` for thin provisioning:

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-guarantee
none
```

The following command configures `vol1` on SVM `vs1` for thick provisioning:

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-slo thick
```

The following command configures `vol1` on SVM `vs1` for semi-thick provisioning:

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-slo semi-
thick
```

= SAN volume configuration options

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You must set various options on the volume containing your LUN. The way you set the volume options determines the amount of space available to LUNs in the volume.

== Autogrow

You can enable or disable Autogrow. If you enable it, autogrow allows ONTAP to automatically increase the size of the volume up to a maximum size that you predetermine. There must be space available in the containing aggregate to support the automatic growth of the volume. Therefore, if you enable autogrow, you must monitor the free space in the containing aggregate and add more when needed.



Autogrow cannot be triggered to support Snapshot creation. If you attempt to create a Snapshot copy and there is insufficient space on the volume, the Snapshot creation fails, even with autogrow enabled.

If autogrow is disabled, the size of your volume will remain the same.

#### == Autoshrink

You can enable or disable Autoshrink. If you enable it, autoshrink allows ONTAP to automatically decrease the overall size of a volume when the amount of space consumed in the volume decreases a predetermined threshold. This increases storage efficiency by triggering volumes to automatically release unused free space.

#### == Snapshot autodelete

Snapshot autodelete automatically deletes Snapshot copies when one of the following occurs:

- The volume is nearly full.
- The Snapshot reserve space is nearly full.
- The overwrite reserve space is full.

You can configure Snapshot autodelete to delete Snapshot copies from oldest to newest or from newest to oldest. Snapshot autodelete does not delete Snapshot copies that are linked to Snapshot copies in cloned volumes or LUNs.

If your volume needs additional space and you have enabled both autogrow and Snapshot autodelete, by default, ONTAP attempts to acquire the needed space by triggering autogrow first. If enough space is not acquired through autogrow, then Snapshot autodelete is triggered.

#### == Snapshot reserve

Snapshot reserve defines the amount of space in the volume reserved for Snapshot copies. Space allocated to Snapshot reserve cannot be used for any other purpose. If all of the space allocated for Snapshot reserve is used, then Snapshot copies begin to consume additional space on the volume.

#### = Requirement for moving volumes in SAN environments

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

**Before you move a volume that contains LUNs or namespaces, you must meet certain requirements.**

- For volumes containing one or more LUNs, you should have a minimum of two paths per LUN (LIFs) connecting to each node in the cluster.

This eliminates single points of failure and enables the system to survive component failures.

- For volumes containing namespaces, the cluster must be running ONTAP 9.6 or later.

Volume move is not supported for NVMe configurations running ONTAP 9.5.

#### = Considerations for setting fractional reserve

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

Fractional reserve, also called *LUN overwrite reserve*, enables you to turn off overwrite reserve for space-reserved LUNs and files in a FlexVol volume. This can help you maximize your storage utilization, but if your environment is negatively affected by write operations failing due to lack of space, you must understand the requirements that this configuration imposes.

The fractional reserve setting is expressed as a percentage; the only valid values are 0 and 100 percent. The fractional reserve setting is an attribute of the volume.

Setting fractional reserve to 0 increases your storage utilization. However, an application accessing data residing in the volume could experience a data outage if the volume is out of free space, even with the volume guarantee set to `volume`. With proper volume configuration and use, however, you can minimize the chance of writes failing. ONTAP provides a “best effort” write guarantee for volumes with fractional reserve set to 0 when *all* of the following requirements are met:

- Deduplication is not in use
- Compression is not in use
- FlexClone sub-files are not in use
- All FlexClone files and FlexClone LUNs are enabled for automatic deletion

This is not the default setting. You must explicitly enable automatic deletion, either at creation time or by modifying the FlexClone file or FlexClone LUN after it is created.

- ODX and FlexClone copy offload are not in use
- Volume guarantee is set to `volume`
- File or LUN space reservation is `enabled`
- Volume Snapshot reserve is set to 0
- Volume Snapshot copy automatic deletion is enabled with a commitment level of `destroy`, a destroy list of `lun_clone, vol_clone, cifs_share, file_clone, sfsr`, and a trigger of `volume`

This setting also ensures that FlexClone files and FlexClone LUNs are deleted when necessary.

Note that if your rate of change is high, in rare cases the Snapshot copy automatic deletion could fall behind, resulting in the volume running out of space, even with all of the above required configuration settings in use.

In addition, you can optionally use the volume autogrow capability to decrease the likelihood of volume Snapshot copies needing to be deleted automatically. If you enable the autogrow capability, you must monitor the free space in the associated aggregate. If the aggregate becomes full enough that the volume is prevented from growing, more Snapshot copies will probably be deleted as the free space in the volume is depleted.

If you cannot meet all of the above configuration requirements and you need to ensure that the volume does not run out of space, you must set the volume’s fractional reserve setting to 100. This requires more free space up front, but guarantees that data modification operations will succeed even when the technologies listed above are in use.

The default value and allowed values for the fractional reserve setting depend on the guarantee of the volume:

Volume guarantee	Default fractional reserve	Allowed values
Volume	100	0, 100
None	0	0, 100

= About host-side space management

= Host-side space management overview

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

In a thinly provisioned environment, host side space management completes the process of managing space from the storage system that has been freed in the host file system.

A host file system contains metadata to keep track of which blocks are available to store new data and which blocks contain valid data that must not be overwritten. This metadata is stored within the LUN. When a file is deleted in the host file system, the file system metadata is updated to mark that file's blocks as free space. Total file system free space is then recalculated to include the newly freed blocks. To the storage system, these metadata updates appear no different from any other writes being performed by the host. Therefore, the storage system is unaware that any deletions have occurred.

This creates a discrepancy between the amount of free space reported by the host and the amount of free space reported by the underlying storage system. For example, suppose you have a newly provisioned 200-GB LUN assigned to your host by your storage system. Both the host and the storage system report 200 GB of free space. Your host then writes 100 GB of data. At this point, both the host and storage system report 100 GB of used space and 100 GB of unused space.

Then you delete 50 GB of data from your host. At this point, your host will report 50 GB of used space and 150 GB of unused space. However, your storage system will report 100 GB of used space and 100 GB of unused space.

Host-side space management uses various methods to reconcile the space differential between the host and the storage system.

= Automatic host-side space management with SCSI thinly provisioned LUNs

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

If your host supports SCSI thin provisioning, you can enable the `space-allocation` option in ONTAP to turn on automatic host-side space management.

Enabling SCSI thin provisioning enables you to do the following.

- Automatic host-side space management

When data is deleted on a host that supports SCSI thin provisioning, host-side space management identifies the blocks of deleted data on the host file system and automatically issues one or more SCSI UNMAP commands to free corresponding blocks on the storage system.

- Notify the host when a LUN runs out of space while keeping the LUN online

On hosts that do not support SCSI thin provisioning, when the volume containing LUN runs out of space and cannot automatically grow, ONTAP takes the LUN offline. However, on hosts that support SCSI thin provisioning, ONTAP does not take the LUN offline when it runs out of space. The LUN remains online in read-only mode and the host is notified that the LUN can no longer accept writes.

## Related information

### [ONTAP SAN host configuration](#)

= Enable space allocation for SCSI thinly provisioned LUNs

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

If you set the `space-allocation` option to `enabled`, ONTAP notifies the host when the volume has run out of space and the LUN in the volume cannot accept writes. This option also enables ONTAP to reclaim space automatically when your host deletes data.

## About this task

The `space-allocation` option is set to `disabled` by default, and you must take the LUN offline to enable space allocation. After you enable space allocation, you must perform discovery on the host before the host will recognize that space allocation has been enabled.

## Steps

1. Set the `-space-allocation` parameter to `enabled`:

```
lun modify -vserver vserver_name -volume volume_name -lun lun_name -space-allocation enabled
```

2. Verify that space allocation is enabled:

```
lun show -vserver vserver_name -volume volume_name -lun lun_name -fields space-allocation
```

3. Bring the LUN online:

```
lun modify -vserver vserver_name -volume volume_name -lun lun_name -state online
```

4. On the host, rescan all disks to ensure that the change to the `-space-allocation` option is correctly discovered.

= Host support for SCSI thin provisioning

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

To leverage the benefits of SCSI thin provisioning, it must be supported by your host. SCSI thin provisioning uses the Logical Block Provisioning feature as defined in the SCSI SBC-3 standard. Only hosts that support this standard can use SCSI thin provisioning in ONTAP.

The following hosts currently support SCSI thin provisioning when you enable space allocation:

- VMware ESX 5.0 and later
- Red Hat Enterprise Linux 6.2 and later
- Citrix XenServer 6.5 and later
- Microsoft Windows 2012
- Microsoft Windows 2016

When you enable the space allocation functionality in ONTAP, you turn on the following SCSI thin provisioning features:

- Unmapping and reporting space usage for space reclamation
- Reporting resource exhaustion errors

= Simplified host management with SnapCenter

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You can use SnapCenter software to simplify some of the management and data protection tasks associated with iSCSI and FC storage. SnapCenter is an optional management package for Windows and UNIX hosts.

You can use SnapCenter Software to easily create virtual disks from pools of storage that can be distributed among several storage systems and to automate storage provisioning tasks and simplify the process of creating Snapshot copies and clones from Snapshot copies consistent with host data.

See NetApp product documentation for more information on [SnapCenter](#).

= About igroups

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

Initiator groups (igroups) are tables of FC protocol host WWPNs or iSCSI host node names. You can define igroups and map them to LUNs to control which initiators have access to LUNs.

Typically, you want all of the host's initiator ports or software initiators to have access to a LUN. If you are using multipathing software or have clustered hosts, each initiator port or software initiator of each clustered host needs redundant paths to the same LUN.

You can create igroups that specify which initiators have access to the LUNs either before or after you create LUNs, but you must create igroups before you can map a LUN to an igroup.

Initiator groups can have multiple initiators, and multiple igroups can have the same initiator. However, you cannot map a LUN to multiple igroups that have the same initiator. An initiator cannot be a member of igroups of differing otypes.

= Example of how igroups give LUN access

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You can create multiple igroups to define which LUNs are available to your hosts. For example, if you have a host cluster, you can use igroups to ensure that specific LUNs are visible to only one host in the cluster or to all of the hosts in the cluster.

The following table illustrates how four igroups give access to the LUNs for four different hosts that are accessing the storage system. The clustered hosts (Host3 and Host4) are both members of the same igroup (group3) and can access the LUNs mapped to this igroup. The igroup named group4 contains the WWPNs of Host4 to store local information that is not intended to be seen by its partner.

Hosts with HBA WWPNs, IQNs, or EUIs	igroups	WWPNs, IQNs, EUIs added to igroups	LUNs mapped to igroups
Host1, single-path (iSCSI software initiator)  iqn.1991-05.com.microsoft:host1	group1	iqn.1991-05.com.microsoft:host1	/vol/vol2/lun1
Host2, multipath (two HBAs)  10:00:00:00:c9:2b:6b:3c  10:00:00:00:c9:2b:02:3c	group2	10:00:00:00:c9:2b:6b:3c  10:00:00:00:c9:2b:02:3c	/vol/vol2/lun2
Host3, multipath, clustered with host 4  10:00:00:00:c9:2b:32:1b  10:00:00:00:c9:2b:41:02	group3	10:00:00:00:c9:2b:32:1b  10:00:00:00:c9:2b:41:02  10:00:00:00:c9:2b:51:2c  10:00:00:00:c9:2b:47:a2	/vol/vol2/qtrees1/lun3
Host4, multipath, clustered (not visible to Host3)  10:00:00:00:c9:2b:51:2c  10:00:00:00:c9:2b:47:a2	group4	10:00:00:00:c9:2b:51:2c  10:00:00:00:c9:2b:47:a2	/vol/vol2/qtrees2/lun4  /vol/vol2/qtrees1/lun5

= Specify initiator WWPNs and iSCSI node names for an igroup

:icons: font

```
:relative_path: ./san-admin/  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/
```

You can specify the iSCSI node names and WWPNs of the initiators when you create an igroup or you can add them later. If you choose to specify the initiator iSCSI node names and WWPNs when you create the LUN, they can be removed later, if needed.

Follow the instructions in your Host Utilities documentation to obtain WWPNs and to find the iSCSI node names associated with a specific host. For hosts running ESX software, use Virtual Storage Console.

= Storage virtualization with VMware and Microsoft copy offload

= Storage virtualization with VMware and Microsoft copy offload overview

:icons: font

```
:relative_path: ./san-admin/  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/
```

VMware and Microsoft support copy offload operations to increase performance and network throughput. You must configure your system to meet the requirements of the VMware and Windows operating system environments to use their respective copy offload functions.

When using VMware and Microsoft copy offload in virtualized environments, your LUNs must be aligned. Unaligned LUNs can degrade performance.

== Advantages of using a virtualized SAN environment

Creating a virtualized environment by using storage virtual machines (SVMs) and LIFs enables you to expand your SAN environment to all of the nodes in your cluster.

- Distributed management

You can log in to any node in the SVM to administer all of the nodes in a cluster.

- Increased data access

With MPIO and ALUA, you have access to your data through any active iSCSI or FC LIFs for the SVM.

- Controlled LUN access

If you use SLM and portsets, you can limit which LIFs an initiator can use to access LUNs.

= How LUN access works in a virtualized environment

:icons: font

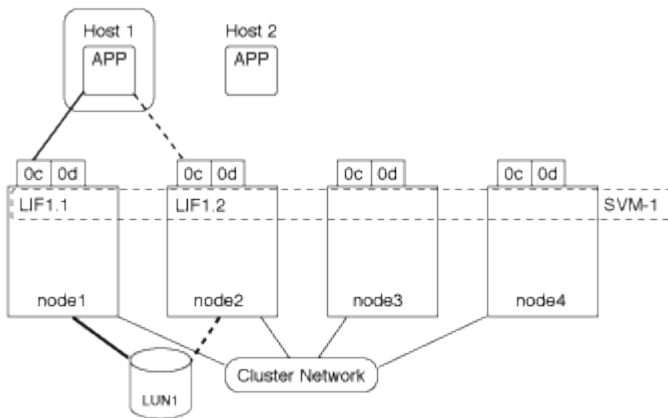
```
:relative_path: ./san-admin/  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/
```

In a virtualized environment, LIFs enable hosts (clients) to access LUNs through optimized and unoptimized paths.

A LIF is a logical interface that connects the SVM to a physical port. Although multiple SVMs can have multiple LIFs on the same port, a LIF belongs to one SVM. You can access LUNs through the SVMs LIFs.

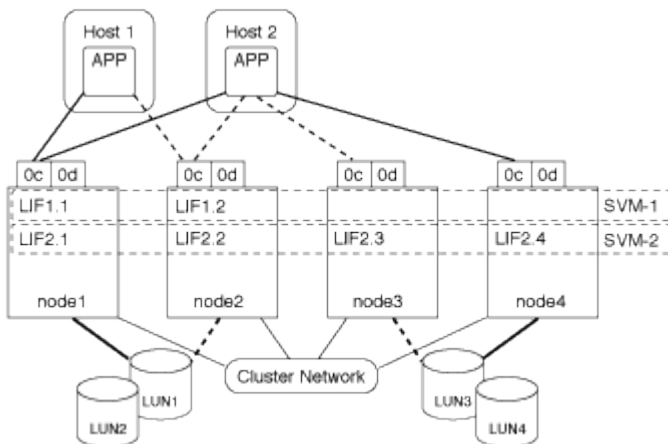
### Example of LUN access with a single SVM in a cluster

In the following example, Host 1 connects to LIF1.1 and LIF1.2 in SVM-1 to access LUN1. LIF1.1 uses the physical port node1:0c and LIF1.2 uses the node2:0c. LIF1.1 and LIF1.2 belongs only to SVM-1. If a new LUN is created on node 1 or node 2, for SVM-1, then it can use these same LIFs. If a new SVM is created, then new LIFs can be created using physical ports 0c or 0d on both the nodes.



### Example of LUN access with multiple SVMs in a cluster

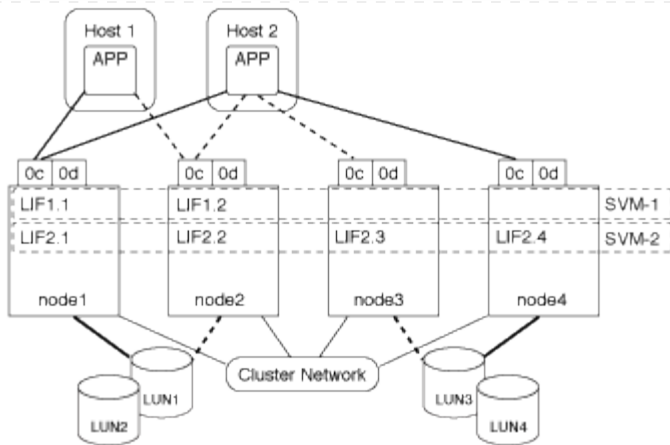
A physical port can support multiple LIFs serving different SVMs. Because LIFs are associated with a particular SVM, the cluster nodes can send the incoming data traffic to the correct SVM. In the following example, each node from 1 through 4 has a LIF for SVM-2 using the physical port 0c on each node. Host 1 connects to LIF1.1 and LIF1.2 in SVM-1 to access LUN1. Host 2 connects to LIF2.1 and LIF2.2 in SVM-2 to access LUN2. Both SVMs are sharing the physical port 0c on the nodes 1 and 2. SVM-2 has additional LIFs that Host 2 is using to access LUNs 3 and 4. These LIFs are using physical port 0c on nodes 3 and 4. Multiple SVMs can share the physical ports on the nodes.



### Example of an active or optimized path to a LUN from a host system

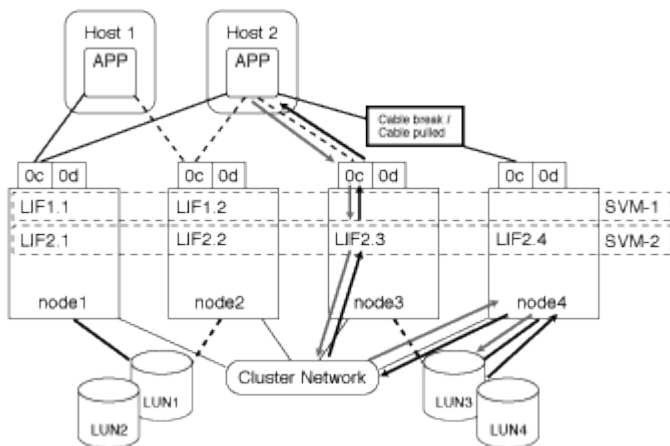
In an active or optimized path, the data traffic does not travel over the cluster network; it travels the most direct route to the LUN. The active or optimized path to LUN1 is through LIF1.1 in node1, using physical port 0c. Host 2 has two active or optimized paths, one path to node1, LIF2.1, which is sharing physical port 0c and the other path to node4, LIF2.4, which is using physical port 0c.





### Example of an active or unoptimized path (indirect) path to a LUN from a host system

In an active or unoptimized path (indirect) path, the data traffic travels over the cluster network. This issue occurs only if all the active or optimized paths from a host are unavailable to handle traffic. If the path from Host 2 to SVM-2 LIF2.4 is lost, then access to LUN3 and LUN4 traverses the cluster network. Access from Host 2 uses LIF2.3 on node3. Then the traffic enters the cluster network switch and backs up to node4 for access to the LUN3 and LUN4. It will then traverse back over the cluster network switch and then back out through LIF2.3 to Host 2. This active or unoptimized path is used until the path to LIF2.4 is restored or a new LIF is established for SVM-2 on another physical port on node 4.



= Considerations for LIFs in cluster SAN environments

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You must be aware of certain LIF considerations in a SAN environment.

- Initiators must use Multipath I/O (MPIO) and asymmetric logical unit access(ALUA) for failover capability for clusters in a SAN iSCSI or FC environment because SAN does not support automatic failover for LIFs.
- At least one SAN LIF of the appropriate protocol must be configured on each node that hosts a mapped LUN and the node's HA partner.

You can configure two LIFs per node, one for each fabric being used with FC and to separate Ethernet networks for iSCSI.

- Some options are not applicable for iSCSI or FC.

For example, you cannot use IP addresses with FC.

= Improve VMware VAAI performance for ESX hosts

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

ONTAP supports certain VMware vStorage APIs for Array Integration (VAAI) features when the ESX host is running ESX 4.1 or later. These features help offload operations from the ESX host to the storage system and increase the network throughput. The ESX host enables the features automatically in the correct environment.

The VAAI feature supports the following SCSI commands:

- EXTENDED\_COPY

This feature enables the host to initiate the transfer of data between the LUNs or within a LUN without involving the host in the data transfer. This results in saving ESX CPU cycles and increasing the network throughput. The extended copy feature, also known as "copy offload," is used in scenarios such as cloning a virtual machine. When invoked by the ESX host, the copy offload feature copies the data within the storage system rather than going through the host network. Copy offload transfers data in the following ways:

- Within a LUN
- Between LUNs within a volume
- Between LUNs on different volumes within a storage virtual machine (SVM)
- Between LUNs on different SVMs within a cluster

If this feature cannot be invoked, the ESX host automatically uses the standard READ and WRITE commands for the copy operation.

- WRITE\_SAME

This feature offloads the work of writing a repeated pattern, such as all zeros, to a storage array. The ESX host uses this feature in operations such as zero-filling a file.

- COMPARE\_AND\_WRITE

This feature bypasses certain file access concurrency limits, which speeds up operations such as booting up virtual machines.

== Requirements for using the VAAI environment

The VAAI features are part of the ESX operating system and are automatically invoked by the ESX host when you have set up the correct environment.

The environment requirements are as follows:

- The ESX host must be running ESX 4.1 or later.

- The NetApp storage system that is hosting the VMware datastore must be running ONTAP.
- (Copy offload only) The source and the destination of the VMware copy operation must be hosted on the same storage system within the same cluster.

The copy offload feature currently does not support copying data between VMware datastores that are hosted on different storage systems.

== Determine if VAAI features are supported by ESX

To confirm whether the ESX operating system supports the VAAI features, you can check the vSphere Client or use any other means of accessing the host. ONTAP supports the SCSI commands by default.

You can check your ESX host advanced settings to determine whether VAAI features are enabled. The table indicates which SCSI commands correspond to ESX control names.

SCSI command	ESX control name (VAAI feature)
EXTENDED_COPY	HardwareAcceleratedMove
WRITE_SAME	HardwareAcceleratedInit
COMPARE_AND_WRITE	HardwareAcceleratedLocking

= Microsoft Offloaded Data Transfer (ODX)

= Microsoft Offloaded Data Transfer (ODX) overview

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

Microsoft Offloaded Data Transfer (ODX), also known as *copy offload*, enables direct data transfers within a storage device or between compatible storage devices without transferring the data through the host computer.

ONTAP supports ODX for both the SMB and SAN protocols.

In non-ODX file transfers, the data is read from the source and is transferred across the network to the host. The host transfers the data back over the network to the destination. In ODX file transfer, the data is copied directly from the source to the destination without passing through the host.

Because ODX offloaded copies are performed directly between the source and destination, significant performance benefits are realized, including faster copy time, reduced utilization of CPU and memory on the client, and reduced network I/O bandwidth utilization.

For SAN environments, ODX is only available when it is supported by both the host and the storage system. Client computers that support ODX and have ODX enabled automatically and transparently use offloaded file transfer when moving or copying files. ODX is used regardless of whether you drag-and-drop files through Windows Explorer or use command-line file copy commands, or whether a client application initiates file copy requests.

= Requirements for using ODX

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

If you plan to use ODX for copy offloads, you need to be familiar with volume support considerations, system requirements, and software capability requirements.

To use ODX, your system must have the following:

- ONTAP

ODX is automatically enabled in supported versions of ONTAP.

- Minimum source volume of 2 GB

For optimal performance, the source volume should be greater than 260 GB.

- Deduplication

ODX uses deduplication as part of the copy process. If you do not want deduplication on your SVM, you should disable ODX on that SVM.

- ODX support on the Windows client

ODX is supported in Windows Server 2012 or later and in Windows 8 or later. The Interoperability Matrix contains the latest information about supported Windows clients.

[NetApp Interoperability Matrix Tool](#)

- Copy application support for ODX

The application that performs the data transfer must support ODX. Application operations that support ODX include the following:

- Hyper-V management operations, such as creating and converting virtual hard disks (VHDs), managing Snapshot copies, and copying files between virtual machines
- Windows Explorer operations
- Windows PowerShell copy commands
- Windows command prompt copy commands

The Microsoft TechNet Library contains more information about supported ODX applications on Windows servers and clients.

- If you use compressed volumes, the compression group size must be 8K.

32K compression group size is not supported.

ODX does not work with the following volume types:

- Source volumes with capacities of less than 2 GB
- Read-only volumes
- [FlexCache volumes](#)
- [Semi-thick provisioned volumes](#)

= Use cases for ODX

:icons: font

:relative\_path: ./san-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You should be aware of the use cases for using ODX on SVMs so that you can

determine under what circumstances ODX provides you with performance benefits.

Windows servers and clients that support ODX use copy offload as the default way of copying data across remote servers. If the Windows server or client does not support ODX or the ODX copy offload fails at any point, the copy or move operation falls back to traditional reads and writes for the copy or move operation.

The following use cases support using ODX copies and moves:

- Intra-volume

The source and destination files or LUNs are within the same volume.

- Inter-volume, same node, same SVM

The source and destination files or LUNs are on different volumes that are located on the same node. The data is owned by the same SVM.

- Inter-volume, different nodes, same SVM

The source and destination files or LUNs are on different volumes that are located on different nodes. The data is owned by the same SVM.

- Inter-SVM, same node

The source and destination file or LUNs are on different volumes that are located on the same node. The data is owned by different SVMs.

- Inter-SVM, different nodes

The source and destination file or LUNs are on different volumes that are located on different nodes. The data is owned by different SVMs.

- Inter-cluster

The source and destination LUNs are on different volumes that are located on different nodes across clusters. This is only supported for SAN and does not work for SMB.

There are some additional special use cases:

- With the ONTAP ODX implementation, you can use ODX to copy files between SMB shares and FC or iSCSI attached virtual drives.

You can use Windows Explorer, the Windows CLI or PowerShell, Hyper-V, or other applications that support ODX to copy or move files seamlessly using ODX copy offload between SMB shares and connected LUNs, provided that the SMB shares and LUNs are on the same cluster.

- Hyper-V provides some additional use cases for ODX copy offload:

- You can use ODX copy offload pass-through with Hyper-V to copy data within or across virtual hard disk (VHD) files or to copy data between mapped SMB shares and connected iSCSI LUNs within the same cluster.

This allows copies from guest operating systems to pass through to the underlying storage.

- When creating fixed-sized VHDs, ODX is used for initializing the disk with zeros, using a well-known zeroed token.

- ODX copy offload is used for virtual machine storage migration if the source and destination storage is on the same cluster.

To take advantage of the use cases for ODX copy offload pass-through with Hyper-V, the guest operating system must support ODX and the guest operating system's disks must be SCSI disks backed by storage (either SMB or SAN) that supports ODX. IDE disks on the guest operating system do not support ODX pass-through.

## == Special system file requirements

You can delete ODX files found in qtrees. You must not remove or modify any other ODX system files unless you are told by technical support to do so.

When using the ODX feature, there are ODX system files that exist in every volume of the system. These files enable point-in-time representation of data used during the ODX transfer. The following system files are in the root level of each volume that contains LUNs or files to which data was offloaded:

- `.copy-offload` (a hidden directory)
- `.tokens` (file under the hidden `.copy-offload` directory)

You can use the `copy-offload delete-tokens -path dir_path -node node_name` command to delete a qtree containing an ODX file.

## = SAN configuration reference

### = SAN configuration reference

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

The following sections describe supported FC-NVMe, FC, iSCSI, and FCoE topologies for connecting host computers to nodes, and list supported limits for SAN components.

You should use this information in conjunction with basic SAN configuration documentation:

- [SAN administration overview](#)

## = Considerations for iSCSI configurations

### = Considerations for iSCSI configurations overview

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You should consider several things when setting up your iSCSI configuration.

- You can set up your iSCSI configuration with single nodes or with HA pairs.

Direct connect or the use of Ethernet switches is supported for connectivity. You must create LIFs for both types of connectivity

- You should configure one management LIF for every storage virtual machine (SVM) supporting SAN.
- Selective LUN mapping (SLM) limits the paths that are being utilized in accessing the LUNs owned by an HA pair.

This is the default behavior for LUNs created with ONTAP releases.

- HA pairs are defined as the reporting nodes for the Active/Optimized and the Active/Unoptimized paths that will be used by the host in accessing the LUNs through ALUA.



- It is recommended that all SVMs in iSCSI configurations have a minimum of two LIF's per node in separate Ethernet networks for redundancy and MPIO across multiple paths.
- You need to create one or more iSCSI paths from each node in an HA pair, using logical interfaces (LIFs) to allow access to LUNs that are serviced by the HA pair.

If a node fails, LIFs do not migrate or assume the IP addresses of the failed partner node. Instead, the MPIO software, using ALUA on the host, is responsible for selecting the appropriate paths for LUN access through LIFs.

- VLANs offer specific benefits, such as increased security and improved network reliability that you might want to leverage in iSCSI.

= Ways to configure iSCSI SAN hosts with single nodes

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

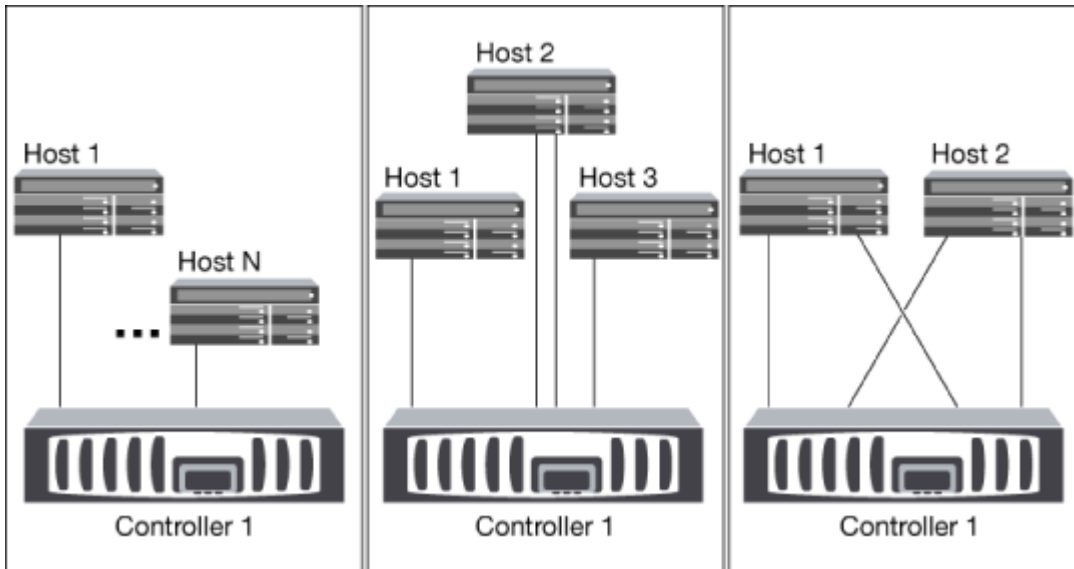
You can configure the iSCSI SAN hosts to connect directly to a single node or by using either one or multiple IP switches. You should determine whether you want a single-switch configuration that is not completely redundant or a multi-switch configuration that is completely redundant.

You can configure iSCSI SAN hosts in a direct-attached, single-switch, or multi-switch environment. If there are multiple hosts connecting to the node, each host can be configured with a different operating system. For single and multi-network configurations, the node can have multiple iSCSI connections to the switch, but multipathing software that supports ALUA is required.

If there are multiple paths from the host to the controller, then ALUA must be enabled on the host.

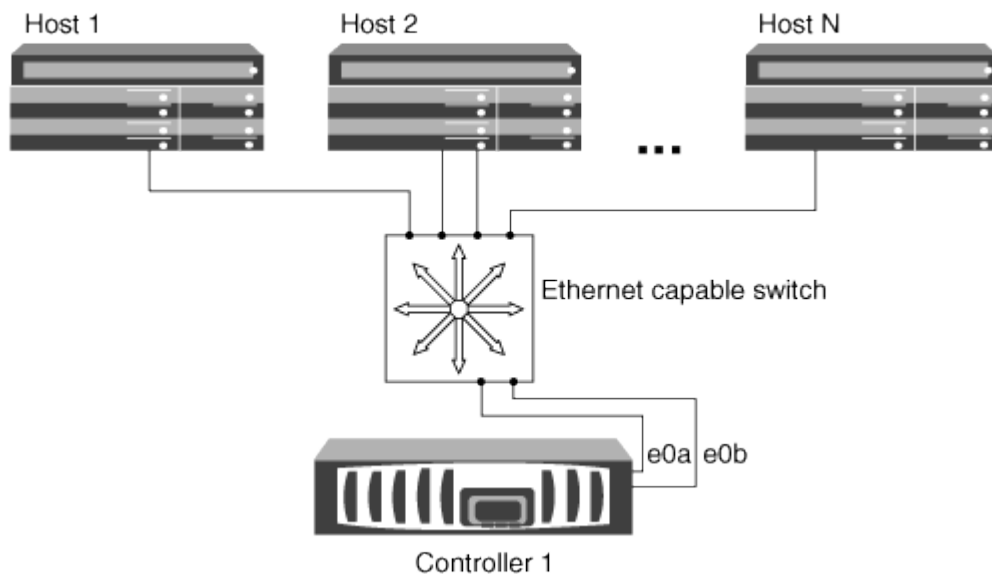
== Direct-attached single-node configurations

In direct-attached configurations, one or more hosts are directly connected to the node.



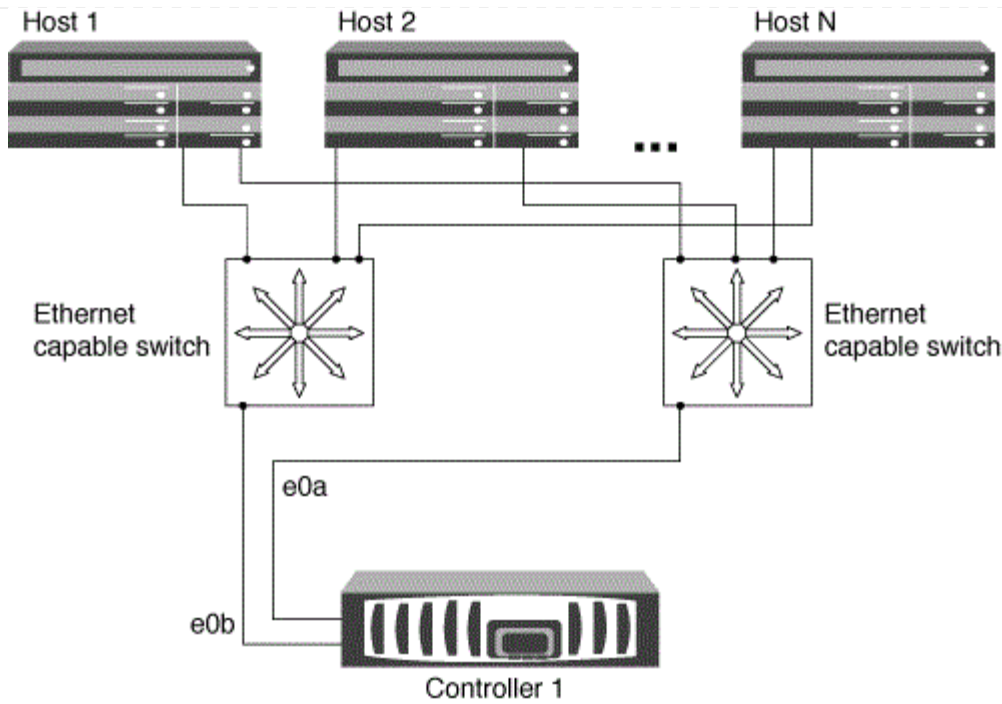
== Single-network single-node configurations

In single-network single-node configurations, one switch connects a single node to one or more hosts. Because there is a single switch, this configuration is not fully redundant.



== Multi-network single-node configurations

In multi-network single-node configurations, two or more switches connect a single node to one or more hosts. Because there are multiple switches, this configuration is fully redundant.



= Ways to configure iSCSI SAN hosts with HA pairs

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

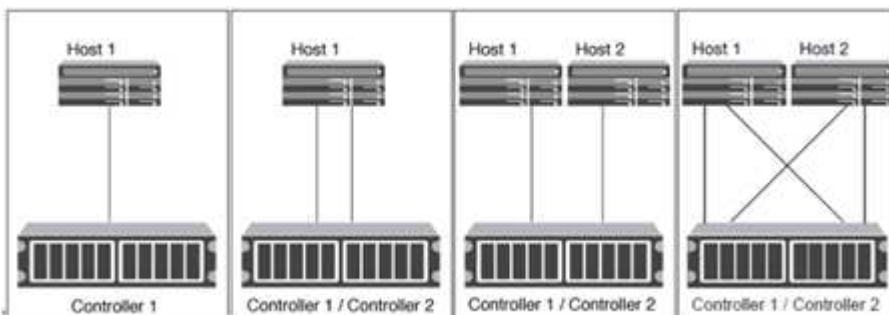
You can configure the iSCSI SAN hosts to connect to dual-node or multi-node configurations by using either one or multiple IP switches. You should determine whether you want a single-switch configuration that is not completely redundant or a multi-switch configuration that is completely redundant.

You can configure iSCSI SAN hosts with single controllers and HA pairs on direct-attached, single-network, or multi-network environments. HA pairs can have multiple iSCSI connections to each switch, but multipathing software that supports ALUA is required on each host. If there are multiple hosts, you can configure each host with a different operating system by checking the NetApp Interoperability Matrix Tool.

### [NetApp Interoperability Matrix Tool](#)

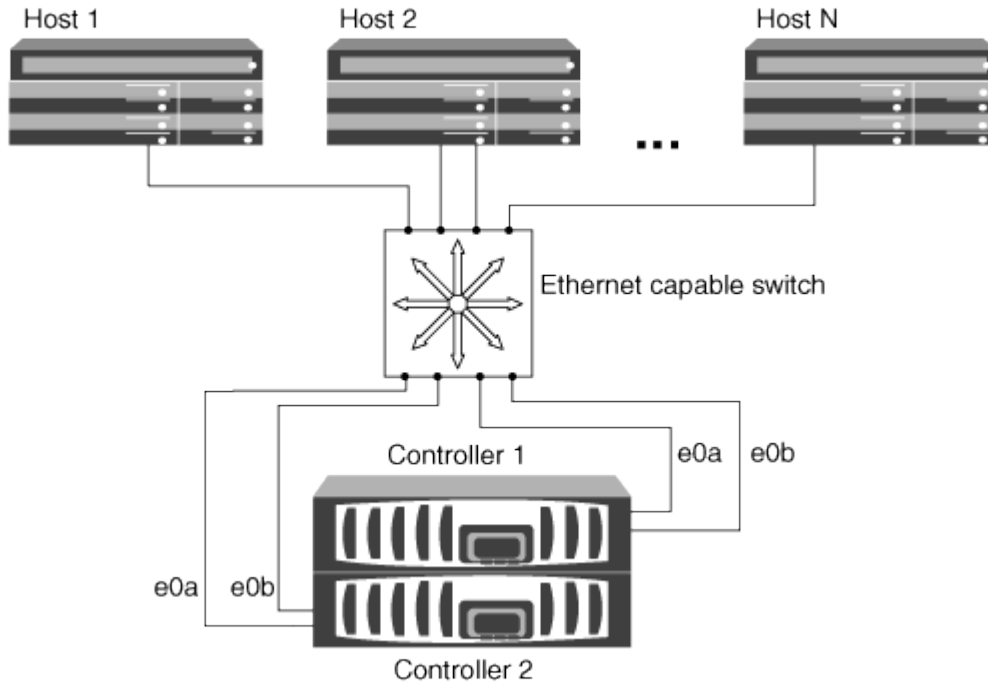
== Direct-attachment

In a direct-attached configuration, one or more hosts are directly connected to the controllers.



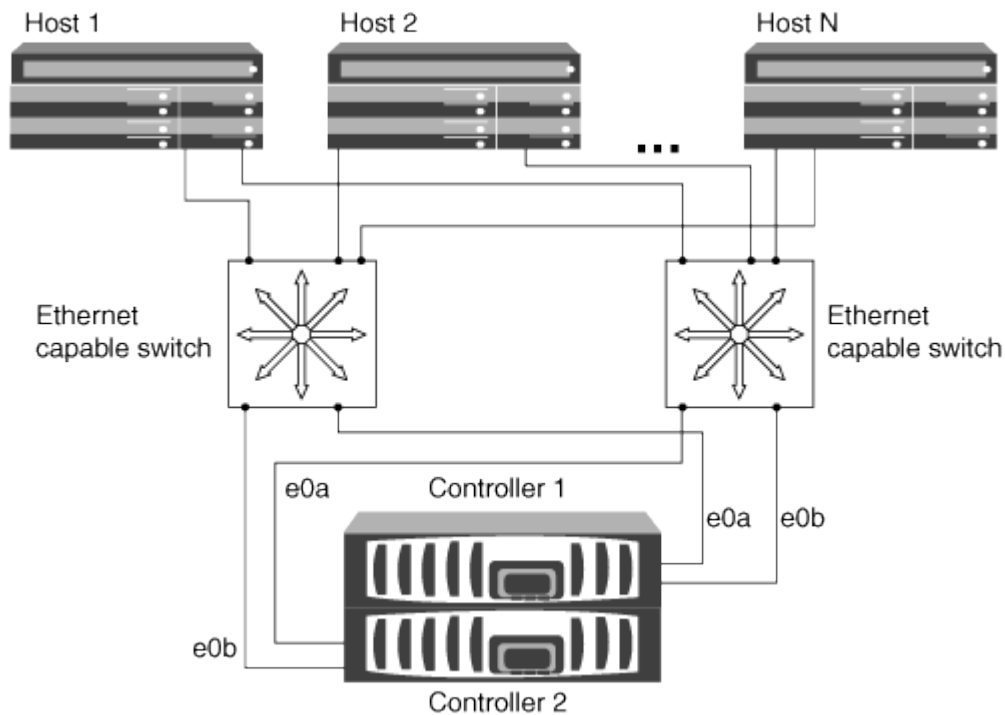
== Single-network HA pairs

In single-network HA pair configurations, one switch connects the HA pair to one or more hosts. Because there is a single switch, this configuration is not fully redundant.



== Multi-network HA pairs

In multi-network HA pair configurations, two or more switches connect the HA pair to one or more hosts. Because there are multiple switches, this configuration is fully redundant.



= Benefits of using VLANs in iSCSI configurations

:icons: font  
:relative\_path: ./san-config/  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

A VLAN consists of a group of switch ports grouped together into a broadcast domain. A VLAN can be on a single switch or it can span multiple switch chassis. Static and dynamic VLANs enable you to increase security, isolate problems, and limit available paths within your IP network infrastructure.

When you implement VLANs in large IP network infrastructures, you derive the following benefits:

- Increased security.

VLANs enable you to leverage existing infrastructure while still providing enhanced security because they limit access between different nodes of an Ethernet network or an IP SAN.

- Improved Ethernet network and IP SAN reliability by isolating problems.
- Reduction of problem resolution time by limiting the problem space.
- Reduction of the number of available paths to a particular iSCSI target port.
- Reduction of the maximum number of paths used by a host.

Having too many paths slows reconnect times. If a host does not have a multipathing solution, you can use VLANs to allow only one path.

#### == Dynamic VLANs

Dynamic VLANs are MAC address-based. You can define a VLAN by specifying the MAC address of the members you want to include.

Dynamic VLANs provide flexibility and do not require mapping to the physical ports where the device is physically connected to the switch. You can move a cable from one port to another without reconfiguring the VLAN.

#### == Static VLANs

Static VLANs are port-based. The switch and switch port are used to define the VLAN and its members.

Static VLANs offer improved security because it is not possible to breach VLANs using media access control (MAC) spoofing. However, if someone has physical access to the switch, replacing a cable and reconfiguring the network address can allow access.

In some environments, it is easier to create and manage static VLANs than dynamic VLANs. This is because static VLANs require only the switch and port identifier to be specified, instead of the 48-bit MAC address. In addition, you can label switch port ranges with the VLAN identifier.

#### = Considerations for FC-NVMe configurations

:icons: font  
:relative\_path: ./san-config/  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

Beginning with ONTAP 9.4, the non-volatile memory express (NVMe) protocol is available for SAN environments. FC-NVMe allows you to run NVMe over an existing

FC network with an AFF system. FC-NVMe uses the same physical setup and zoning practice as traditional FC networks but allows for greater bandwidth, increased IOPs and reduced latency than FC-SCSI.

Supported configurations:

- NVMe is supported on AFF platforms that have 32G FC ports.
- You can set up your FC-NVMe configuration with single nodes or HA pairs using a single fabric or multifabric.
- NVMe is supported on 4-node clusters or smaller.
- NVMe can be the only data protocol on the storage virtual machine (SVM).
- Up to 8 NVMe SVMs are supported per cluster.
- FC-NVMe can be the only data protocol on data LIFs.
- LUNs and namespaces cannot be mixed on the same volume.
- You should configure one management LIF for every SVM supporting SAN.
- The use of heterogeneous FC switch fabrics is not supported, except in the case of embedded blade switches.

Specific exceptions are listed on the [NetApp Interoperability Matrix Tool](#).

- Cascade, partial mesh, full mesh, core-edge, and director fabrics are all industry-standard methods of connecting FC switches to a fabric, and all are supported.

A fabric can consist of one or multiple switches, and the storage controllers can be connected to multiple switches.

Functionality enhancements:

<b>This functionality is supported...</b>	<b>Starting with...</b>
volume move with mapped namespaces	ONTAP 9.6
Namespaces support 512 byte blocks and 4096 byte blocks. 4096 is the default value. 512 should only be used if the host operating system does not support 4096 byte blocks.	ONTAP 9.6
Multipath HA pair failover/giveback	ONTAP 9.5

The following applies only to nodes running ONTAP 9.4:

- NVMe LIFs and namespaces must be hosted on the same node.
- The NVMe service must be created before the NVMe LIF is created.

The following ONTAP features are not supported by NVMe configurations:

- NVMe namespace move
- NVMe namespaces (Copy on Demand)

- Creating namespaces on a volume transitioned from Data ONTAP operating in 7-mode.
- Sync
- Virtual Storage Console

See the [NetApp Hardware Universe](#) for a complete list of NVMe limits.

#### Related information

[How to configure and Connect SUSE Enterprise Linux to ONTAP NVMe/FC namespaces](#)

[Licensing information for NVMe protocol on ONTAP](#)

[NetApp Technical Report 4684: Implementing and Configuring Modern SANs with NVMe/FC](#)

= Considerations for FC configurations

= Considerations for FC configurations overview

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You should be aware of several things when setting up your FC configuration.

- You can set up your FC configuration with single nodes or HA pairs using a single fabric or multifabric.
- You should configure two FC data LIFs per node.

This creates redundancy and protects against loss of data access.

- You should configure one management LIF for every storage virtual machine (SVM) supporting SAN.
- Multiple hosts, using different operating systems, such as Windows, Linux, or UNIX, can access the storage solution at the same time.

Hosts require that a supported multipathing solution be installed and configured. Supported operating systems and multipathing solutions can be verified on the Interoperability Matrix.

- ONTAP supports single, dual, or multiple node solutions that are connected to multiple physically independent storage fabrics; a minimum of two are recommended for SAN solutions.

This provides redundancy at the fabric and storage system layers. Redundancy is particularly important because these layers typically support many hosts.

- The use of heterogeneous FC switch fabrics is not supported, except in the case of embedded blade switches.

Specific exceptions are listed on the Interoperability Matrix.

- Cascade, partial mesh, full mesh, core-edge, and director fabrics are all industry-standard methods of connecting FC switches to a fabric, and all are supported.

A fabric can consist of one or multiple switches, and the storage controllers can be connected to multiple switches.

#### Related information

= Ways to configure FC and FC-NVMe SAN hosts with single nodes

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

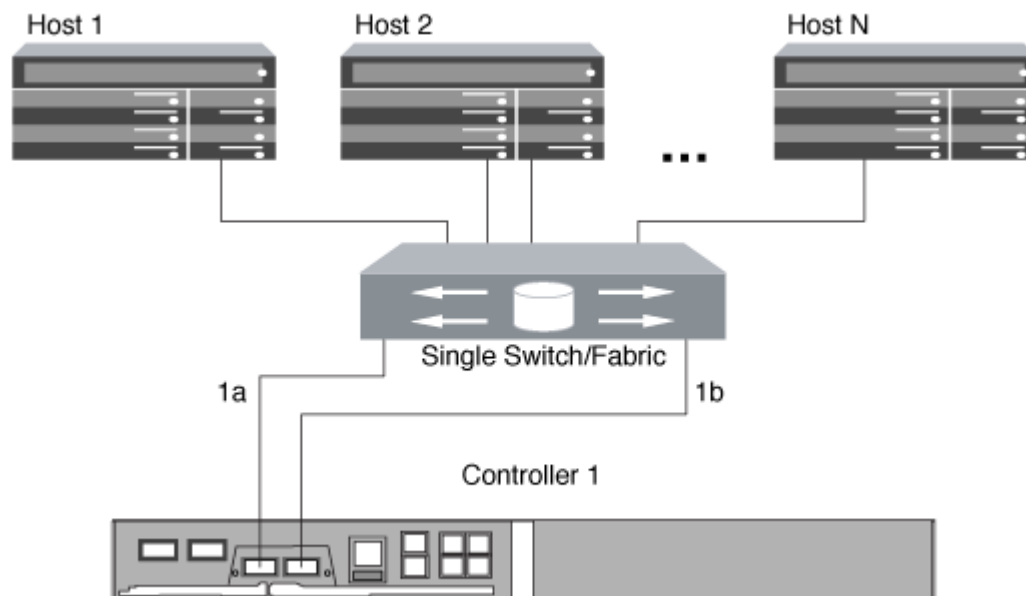
You can configure FC and FC-NVMe SAN hosts with single nodes through one or more fabrics. N-Port ID Virtualization (NPIV) is required and must be enabled on all FC switches in the fabric. You cannot directly attach FC or FC-NMVE SAN hosts to single nodes without using an FC switch.

You can configure FC or FC-NVMe SAN hosts with single nodes through a single fabric or multifabrics. The FC target ports (0a, 0c, 0b, 0d) in the illustrations are examples. The actual port numbers vary depending on the model of your storage node and whether you are using expansion adapters.

== Single-fabric single-node configurations

In single-fabric single-node configurations, there is one switch connecting a single node to one or more hosts. Because there is a single switch, this configuration is not fully redundant. All hardware platforms that support FC and FC-NVMe support single-fabric single-node configurations. However, the FAS2240 platform requires the X1150A-R6 expansion adapter to support a single-fabric single-node configuration.

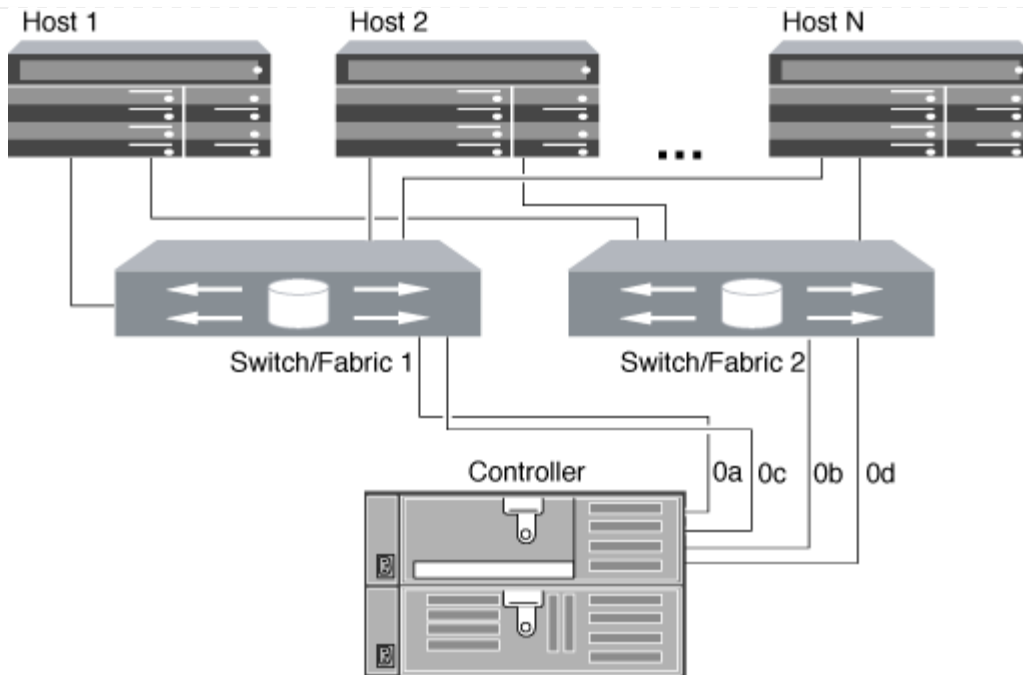
The following figure shows a FAS2240 single-fabric single-node configuration. It shows the storage controllers side by side, which is how they are mounted in the FAS2240-2. For the FAS2240-4, the controllers are mounted one above the other. There is no difference in the SAN configuration for the two models.



== Multifabric single-node configurations

In multifabric single-node configurations, there are two or more switches connecting a single node to one or more hosts. For simplicity, the following figure shows a multifabric single-node configuration with only two fabrics, but you can have two or more fabrics in any multifabric configuration. In this figure, the storage controller is mounted in the top chassis and the bottom chassis can be empty or can have an IOMX module, as it does in this example.





### Related information

[NetApp Technical Report 4684: Implementing and Configuring Modern SANs with NVMe/FC](#)

= Ways to configure FC & FC-NVMe SAN hosts with HA pairs

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

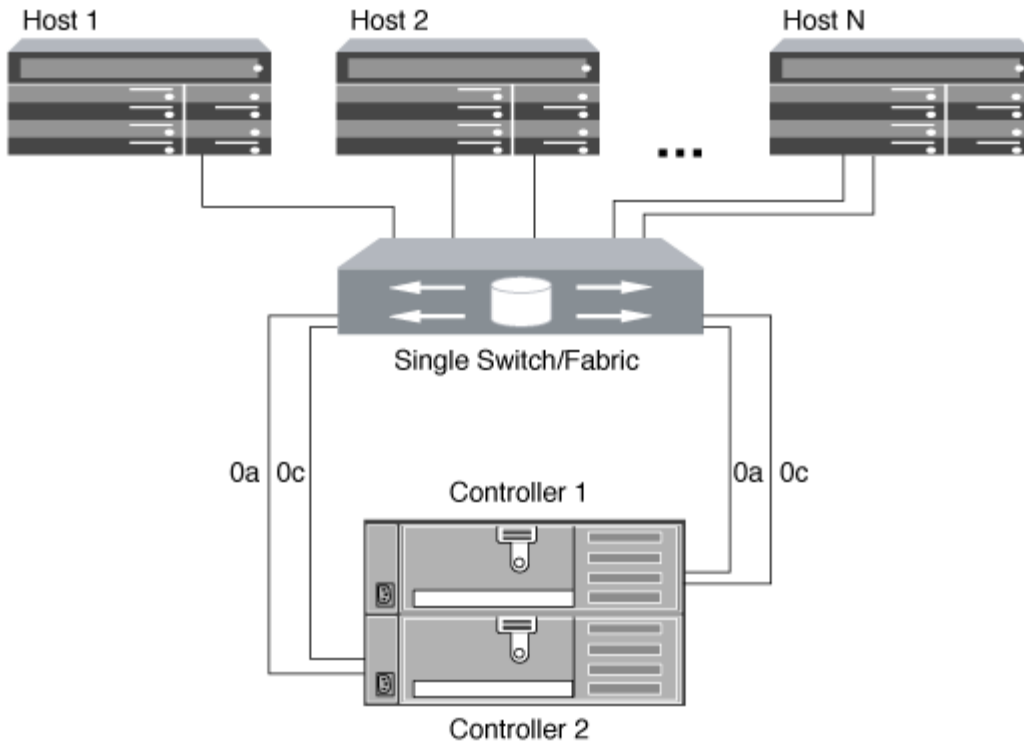
You can configure FC and FC-NVMe SAN hosts to connect to HA pairs through one or more fabrics. You cannot directly attach FC or FC-NVMe SAN hosts to HA pairs without using a switch.

You can configure FC and FC-NVMe SAN hosts with single fabric HA pairs or with multifabric HA pairs. The FC target port numbers (0a, 0c, 0d, 1a, 1b) in the illustrations are examples. The actual port numbers vary depending on the model of your storage node and whether you are using expansion adapters.

== Single-fabric HA pairs

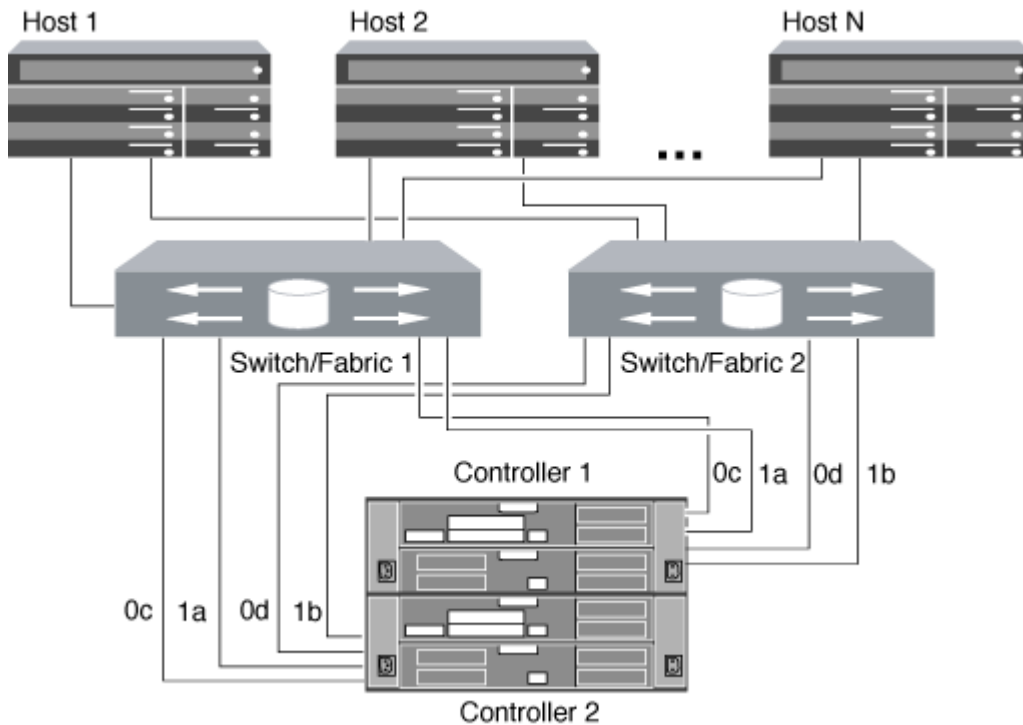
In single-fabric HA pair configurations, there is one fabric connecting both controllers in the HA pair to one or more hosts. Because the hosts and controllers are connected through a single switch, single-fabric HA pairs are not fully redundant.

All platforms that support FC configurations support single-fabric HA pair configurations, except the FAS2240 platform. The FAS2240 platform only supports single-fabric single-node configurations.



== Multifabric HA pairs

In multifabric HA pairs, there are two or more switches connecting HA pairs to one or more hosts. For simplicity, the following multifabric HA pair figure shows only two fabrics, but you can have two or more fabrics in any multifabric configuration:



= FC switch configuration best practices

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

For best performance, you should consider certain best practices when configuring your FC switch.

A fixed link speed setting is the best practice for FC switch configurations, especially for large fabrics because it provides the best performance for fabric rebuilds and can significantly save time. Although autonegotiation provides the greatest flexibility, FC switch configuration does not always perform as expected, and it adds time to the overall fabric-build sequence.

All of the switches that are connected to the fabric must support N\_Port ID virtualization (NPIV) and must have NPIV enabled. ONTAP uses NPIV to present FC targets to a fabric.

For details about which environments are supported, see the [NetApp Interoperability Matrix Tool](#).

For FC and iSCSI best practices, see [Best Practices for Scalable SAN - ONTAP 9](#).

= Supported number of FC hop counts

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

The maximum supported FC hop count between a host and storage system depends on the switch supplier and storage system support for FC configurations.

The hop count is defined as the number of switches in the path between the initiator (host) and target (storage system). Cisco also refers to this value as the *diameter of the SAN fabric*.

Switch supplier	Supported hop count
Brocade	7 for FC5 for FCoE
Cisco	7 for FCUp to 3 of the switches can be FCoE switches.

#### Related information

[NetApp Downloads: Brocade Scalability Matrix Documents](#)

[NetApp Downloads: Cisco Scalability Matrix Documents](#)

= FC target port supported speeds

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

FC target ports can be configured to run at different speeds. You should set the target port speed to match the speed of the device to which it connects. All target ports used by a given host should be set to the same speed.

FC target ports can be used for FC-NVMe configurations in the exact same way they are used for FC configurations.

You should set the target port speed to match the speed of the device to which it connects instead of using autonegotiation. A port that is set to autonegotiation can take longer to reconnect after a takeover/giveback or other interruption.

You can configure onboard ports and expansion adapters to run at the following speeds. Each controller and expansion adapter port can be configured individually for different speeds as needed.

4 Gb ports	8 Gb ports	16 Gb ports	32 Gb ports
<ul style="list-style-type: none"><li>• 4 Gb</li></ul>	<ul style="list-style-type: none"><li>• 8 Gb</li></ul>	<ul style="list-style-type: none"><li>• 16 Gb</li></ul>	<ul style="list-style-type: none"><li>• 32 Gb</li></ul>
<ul style="list-style-type: none"><li>• 2 Gb</li></ul>	<ul style="list-style-type: none"><li>• 4 Gb</li></ul>	<ul style="list-style-type: none"><li>• 8 Gb</li></ul>	<ul style="list-style-type: none"><li>• 16 Gb</li></ul>
<ul style="list-style-type: none"><li>• 1 Gb</li></ul>	<ul style="list-style-type: none"><li>• 2 Gb</li></ul>	<ul style="list-style-type: none"><li>• 4 Gb</li></ul>	<ul style="list-style-type: none"><li>• 8 Gb</li></ul>

UTA2 ports can use an 8 Gb SFP+ adapter to support 8, 4, and 2 Gb speeds, if required.

= FC Target port configuration recommendations

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

For best performance and highest availability, you should use the recommended FC target port configuration.

The following table shows the preferred port usage order for onboard FC and FC-NVMe target ports. For expansion adapters, the FC ports should be spread so that they do not use the same ASIC for connectivity. The preferred slot order is listed in [NetApp Hardware Universe](#) for the version of ONTAP software used by your controller.

FC-NVMe is supported on the following models:

- AFF A300

The AFF A300 onboard ports do not support FC-NVMe.

- AFF A700
- AFF A700s
- AFF A800

The FAS22xx and FAS2520 systems do not have onboard FC ports and do not support add-on adapters.

Controller	Port pairs with shared ASIC	Number of target ports: Preferred ports
FAS9000, AFF A700, AFF A700s and AFF A800	None	All data ports are on expansion adapters. See <a href="#">NetApp Hardware Universe</a> for more information.
8080, 8060 and 8040	0e+0f 0g+0h	1: 0e 2: 0e, 0g 3: 0e, 0g, 0h 4: 0e, 0g, 0f, 0h
FAS8200 and AFF A300	0g+0h	1: 0g 2: 0g, 0h
8020	0c+0d	1: 0c 2: 0c, 0d
62xx	0a+0b 0c+0d	1: 0a 2: 0a, 0c 3: 0a, 0c, 0b 4: 0a, 0c, 0b, 0d
32xx	0c+0d	1: 0c 2: 0c, 0d
FAS2554, FAS2552, FAS2600 series, FAS2720, FAS2750, AFF A200 and AFF A220	0c+0d 0e+0f	1: 0c 2: 0c, 0e 3: 0c, 0e, 0d 4: 0c, 0e, 0d, 0f

= Manage systems with FC adapters

= Managing systems with FC adapters overview

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

Commands are available to manage onboard FC adapters and FC adapter cards.

These commands can be used to configure the adapter mode, display adapter information, and change the speed.

Most storage systems have onboard FC adapters that can be configured as initiators or targets. You can also use FC adapter cards configured as initiators or targets. Initiators connect to back-end disk shelves, and possibly foreign storage arrays (FlexArray). Targets connect only to FC switches. Both the FC target HBA ports and the switch port speed should be set to the same value and should not be set to auto.

= Commands for managing FC adapters

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You can use FC commands to manage FC target adapters, FC initiator adapters, and onboard FC adapters for your storage controller. The same commands are used to manage FC adapters for the FC protocol and the FC-NVMe protocol.

FC initiator adapter commands work only at the node level. You must use the `run -node node_name` command before you can use the FC initiator adapter commands.

== Commands for managing FC target adapters

If you want to...	Use this command...
Display FC adapter information on a node	<code>network fcp adapter show</code>
Modify FC target adapter parameters	<code>network fcp adapter modify</code>
Display FC protocol traffic information	<code>run -node node_name sysstat -f</code>
Display how long the FC protocol has been running	<code>run -node node_name uptime</code>
Display adapter configuration and status	<code>run -node node_name sysconfig -v adapter</code>
Verify which expansion cards are installed and whether there are any configuration errors	<code>run -node node_name sysconfig -ac</code>
View a man page for a command	<code>man command_name</code>

== Commands for managing FC initiator adapters

If you want to...	Use this command...
Display information for all initiators and their adapters in a node	<code>run -node node_name storage show adapter</code>

If you want to...	Use this command...
Display adapter configuration and status	<code>run -node <i>node_name</i> sysconfig -v <i>adapter</i></code>
Verify which expansion cards are installed and whether there are any configuration errors	<code>run -node <i>node_name</i> sysconfig -ac</code>

== Commands for managing onboard FC adapters

If you want to...	Use this command...
Display the status of the onboard FC ports	<code>system node hardware unified-connect show</code>

= Configure FC adapters for initiator mode

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You can configure individual FC ports of onboard adapters and certain FC adapter cards for initiator mode. Initiator mode is used to connect the ports to tape drives, tape libraries, or third-party storage with FlexArray Virtualization or Foreign LUN Import (FLI).

#### What you'll need

- LIFs on the adapter must be removed from any port sets of which they are members.
- All LIF's from every storage virtual machine (SVM) using the physical port to be modified must be migrated or destroyed before changing the personality of the physical port from target to initiator.

#### About this task

Each onboard FC port can be individually configured as an initiator or a target. Ports on certain FC adapters can also be individually configured as either a target port or an initiator port, just like the onboard FC ports. A list of adapters that can be configured for target mode is available in [NetApp Hardware Universe](#).

NVMe/FC does support initiator mode.

## Steps

1. Remove all LIFs from the adapter:

```
network interface delete -vserver SVM_name -lif lif_name,lif_name
```

2. Take your adapter offline:

```
network fcp adapter modify -node node_name -adapter adapter_port -status  
-admin down
```

If the adapter does not go offline, you can also remove the cable from the appropriate adapter port on the system.

3. Change the adapter from target to initiator:

```
system hardware unified-connect modify -t initiator adapter_port
```

4. Reboot the node hosting the adapter you changed.
5. Verify that the FC ports are configured in the correct state for your configuration:

```
system hardware unified-connect show
```

6. Bring the adapter back online:

```
node run -node node_name storage enable adapter adapter_port
```

= Configure FC adapters for target mode

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You can configure individual FC ports of onboard adapters and certain FC adapter cards for target mode. Target mode is used to connect the ports to FC initiators.

### About this task

Each onboard FC port can be individually configured as an initiator or a target. Ports on certain FC adapters can also be individually configured as either a target port or an initiator port, just like the onboard FC ports. A list of adapters that can be configured for target mode is available in the [NetApp Hardware Universe](#).

The same steps are used when configuring FC adapters for the FC protocol and the FC-NVMe protocol. However, only certain FC adapters support FC-NVMe. See the [NetApp Hardware Universe](#) for a list of adapters that support the FC-NVMe protocol.

## Steps

1. Take the adapter offline:

```
node run -node node_name storage disable adapter adapter_name
```

If the adapter does not go offline, you can also remove the cable from the appropriate adapter port on the system.



## 2. Change the adapter from initiator to target:

```
system node hardware unified-connect modify -t target -node node_name  
adapter adapter_name
```

## 3. Reboot the node hosting the adapter you changed.

## 4. Verify that the target port has the correct configuration:

```
network fcp adapter show -node node_name
```

## 5. Bring your adapter online:

```
network fcp adapter modify -node node_name -adapter adapter_port -state up
```

= Display information about an FC target adapter

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You can use the `network fcp adapter show` command to display system configuration and adapter information for any FC adapter in the system.

### Step

#### 1. Display information about the FC adapter by using the `network fcp adapter show` command.

The output displays system configuration information and adapter information for each slot that is used.

```
network fcp adapter show -instance -node node1 -adapter 0a
```

= Change the FC adapter speed

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You should set your adapter target port speed to match the speed of the device to which it connects, instead of using autonegotiation. A port that is set to autonegotiation can take longer time to reconnect after a takeover/giveback or other interruption.

### What you'll need

All LIFs that use this adapter as their home port must be offline.

### About this task

Because this task encompasses all storage virtual machines (SVMs) and all LIFs in a cluster, you must use the `-home-port` and `-home-lif` parameters to limit the scope of this operation. If you do not use these parameters, the operation applies to all LIFs in the cluster, which might not be desirable.

### Steps

#### 1. Take all of the LIFs on this adapter offline:

```
network interface modify -vserver * -lif * { -home-node node1 -home-port 0c
} -status-admin down
```

2. Take the adapter offline:

```
network fcp adapter modify -node node1 -adapter 0c -state down
```

If the adapter does not go offline, you can also remove the cable from the appropriate adapter port on the system.

3. Determine the maximum speed for the port adapter:

```
fcp adapter show -instance
```

You cannot modify the adapter speed beyond the maximum speed.

4. Change the adapter speed:

```
network fcp adapter modify -node node1 -adapter 0c -speed 16
```

5. Bring the adapter online:

```
network fcp adapter modify -node node1 -adapter 0c -state up
```

6. Bring all of the LIFs on the adapter online:

```
network interface modify -vserver * -lif * { -home-node node1 -home-port 0c
} -status-admin up
```

= Supported FC ports

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

The number of onboard FC ports and CNA/UTA2 ports configured for FC varies based on the model of the controller. FC ports are also available through supported FC target expansion adapters or additional UTA2 cards configured with FC SFP+ adapters.

== Onboard FC, UTA, and UTA2 ports

- Onboard ports can be individually configured as either target or initiator FC ports.
- The number of onboard FC ports differs depending on controller model.

The [NetApp Hardware Universe](#) contains a complete list of onboard FC ports on each controller model.

- FC ports are only available on FAS2240 systems through the X1150A-R6 expansion adapter.

FAS2220 and FAS2520 systems do not support FC.

== Target expansion adapter FC ports

- Available target expansion adapters differ depending on controller model.

The [NetApp Hardware Universe](#) contains a complete list of target expansion adapters for each controller model.

- The ports on some FC expansion adapters are configured as initiators or targets at the factory and cannot be changed.

Others can be individually configured as either target or initiator FC ports, just like the onboard FC ports. A complete list is available in [NetApp Hardware Universe](#).

= Prevent loss of connectivity when using the X1133A-R6 adapter

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You can prevent loss of connectivity during a port failure by configuring your system with redundant paths to separate X1133A-R6 HBAs.

The X1133A-R6 HBA is a 4-port, 16 Gb FC adapter consisting of two 2-port pairs. The X1133A-R6 adapter can be configured as target mode or initiator mode. Each 2-port pair is supported by a single ASIC (for example, Port 1 and Port 2 on ASIC 1 and Port 3 and Port 4 on ASIC 2). Both ports on a single ASIC must be configured to operate in the same mode, either target mode or initiator mode. If an error occurs with the ASIC supporting a pair, both ports in the pair go offline.

To prevent this loss of connectivity, you configure your system with redundant paths to separate X1133A-R6 HBAs, or with redundant paths to ports supported by different ASICs on the HBA.

= Manage X1143A-R6 adapters

= Supported port configurations for X1143A-R6 adapters overview

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

By default the X1143A-R6 adapter is configured in FC target mode, but you can configure its ports as either 10 Gb Ethernet and FCoE (CNA) ports or as 16 Gb FC initiator or target ports. This requires different SFP+ adapters.

When configured for Ethernet and FCoE, X1143A-R6 adapters support concurrent NIC and FCoE target traffic on the same 10-GBE port. When configured for FC, each two-port pair that shares the same ASIC can be individually configured for FC target or FC initiator mode. This means that a single X1143A-R6 adapter can support FC target mode on one two-port pair and FC initiator mode on another two-port pair. Port pairs connected to the same ASIC must be configured in the same mode.

In FC mode, the X1143A-R6 adapter behaves just like any existing FC device with speeds up to 16 Gbps. In CNA mode, you can use the X1143A-R6 adapter for concurrent NIC and FCoE traffic sharing the same 10 GbE port. CNA mode only supports FC target mode for the FCoE function.

= Configure the ports

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

To configure the unified target adapter (X1143A-R6), you must configure the two adjacent ports on the same chip in the same personality mode.

### Steps

1. Configure the ports as needed for Fibre Channel (FC) or Converged Network Adapter (CNA) using the `system node hardware unified-connect modify` command.
2. Attach the appropriate cables for FC or 10 Gb Ethernet.
3. Verify that you have the correct SFP+ installed:

```
network fcp adapter show -instance -node -adapter
```

For CNA, you should use a 10Gb Ethernet SFP. For FC, you should either use an 8 Gb SFP or a 16 Gb SFP, based on the FC fabric being connected to.

= Change the UTA2 port from CNA mode to FC mode

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You should change the UTA2 port from Converged Network Adapter (CNA) mode to Fibre Channel (FC) mode to support the FC initiator and FC target mode. You should change the personality from CNA mode to FC mode when you need to change the physical medium that connects the port to its network.

### Steps

1. Take the adapter offline:

```
network fcp adapter modify -node node_name -adapter adapter_name -status  
-admin down
```

2. Change the port mode:

```
ucadmin modify -node node_name -adapter adapter_name -mode fcp
```

3. Reboot the node, and then bring the adapter online:

```
network fcp adapter modify -node node_name -adapter adapter_name -status  
-admin up
```

4. Notify your admin or VIF manager to delete or remove the port, as applicable:

- If the port is used as a home port of a LIF, is a member of an interface group (ifgrp), or hosts VLANs, then an admin should do the following:
  - i. Move the LIFs, remove the port from the ifgrp, or delete the VLANs, respectively.
  - ii. Manually delete the port by running the `network port delete` command.

If the `network port delete` command fails, the admin should address the errors, and then run the command again.

- If the port is not used as the home port of a LIF, is not a member of an ifgrp, and does not host

VLANs, then the VIF manager should remove the port from its records at the time of reboot.

If the VIF manager does not remove the port, then the admin must remove it manually after the reboot by using the `network port delete` command.

```
net-f8040-34::> network port show
```

```
Node: net-f8040-34-01
```

Health	Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Speed (Mbps)
Status	-----	-----	-----	-----	-----	-----	-----	-----
...								
	e0i	Default	Default		down	1500	auto/10	-
	e0f	Default	Default		down	1500	auto/10	-
...								

```
net-f8040-34::> ucadmin show
```

Admin	Node	Adapter	Mode	Type	Pending	Pending
Status	-----	-----	-----	-----	-----	-----
	net-f8040-34-01					
		0e	cna	target	-	-
offline						
	net-f8040-34-01					
		0f	cna	target	-	-
offline						
...						

```
net-f8040-34::> network interface create -vs net-f8040-34 -lif m
-role
node-mgmt-home-node net-f8040-34-01 -home-port e0e -address 10.1.1.1
-netmask 255.255.255.0
```

```
net-f8040-34::> network interface show -fields home-port, curr-
port
```

vserver	lif	home-port	curr-port
-----	-----	-----	-----
Cluster	net-f8040-34-01_clus1	e0a	e0a
Cluster	net-f8040-34-01_clus2	e0b	e0b

```

Cluster net-f8040-34-01_clus3 e0c      e0c
Cluster net-f8040-34-01_clus4 e0d      e0d
net-f8040-34
      cluster_mgmt      e0M      e0M
net-f8040-34
      m                  e0e      e0i
net-f8040-34
      net-f8040-34-01_mgmt1 e0M      e0M
7 entries were displayed.

```

```
net-f8040-34::> ucadmin modify local 0e fc
```

Warning: Mode on adapter 0e and also adapter 0f will be changed to fc.

```
Do you want to continue? {y|n}: y
```

Any changes will take effect after rebooting the system. Use the "system node reboot" command to reboot.

```
net-f8040-34::> reboot local
(system node reboot)
```

```
Warning: Are you sure you want to reboot node "net-f8040-34-01"?
{y|n}: y
```

##### 5. Verify that you have the correct SFP+ installed:

```
network fcp adapter show -instance -node -adapter
```

For CNA, you should use a 10Gb Ethernet SFP. For FC, you should either use an 8 Gb SFP or a 16 Gb SFP, before changing the configuration on the node.

= Change the CNA/UTA2 target adapter optical modules

```
:icons: font
```

```
:relative_path: ./san-config/
```

```
:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/
```

You should change the optical modules on the unified target adapter (CNA/UTA2) to support the personality mode you have selected for the adapter.

##### Steps

1. Verify the current SFP+ used in the card. Then, replace the current SFP+ with the appropriate SFP+ for the preferred personality (FC or CNA).
2. Remove the current optical modules from the X1143A-R6 adapter.
3. Insert the correct modules for your preferred personality mode (FC or CNA) optics.
4. Verify that you have the correct SFP+ installed:

```
network fcp adapter show -instance -node -adapter
```

Supported SFP+ modules and Cisco-branded Copper (Twinax) cables are listed in the [NetApp Hardware Universe](#).

= View adapter settings

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

To view the settings for your unified target adapter (X1143A-R6), you must run the `system hardware unified-connect show` command to display all modules on your controller.

### Steps

1. Boot your controller without the cables attached.
2. Run the `system hardware unified-connect show` command to see the port configuration and modules.
3. View the port information before configuring the CNA and ports.

= Ways to Configure FCoE

= Ways to Configure FCoE overview

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

FCoE can be configured in various ways using FCoE switches. Direct-attached configurations are not supported in FCoE.

All FCoE configurations are dual-fabric, fully redundant, and require host-side multipathing software. In all FCoE configurations, you can have multiple FCoE and FC switches in the path between the initiator and target, up to the maximum hop count limit. To connect switches to each other, the switches must run a firmware version that supports Ethernet ISLs. Each host in any FCoE configuration can be configured with a different operating system.

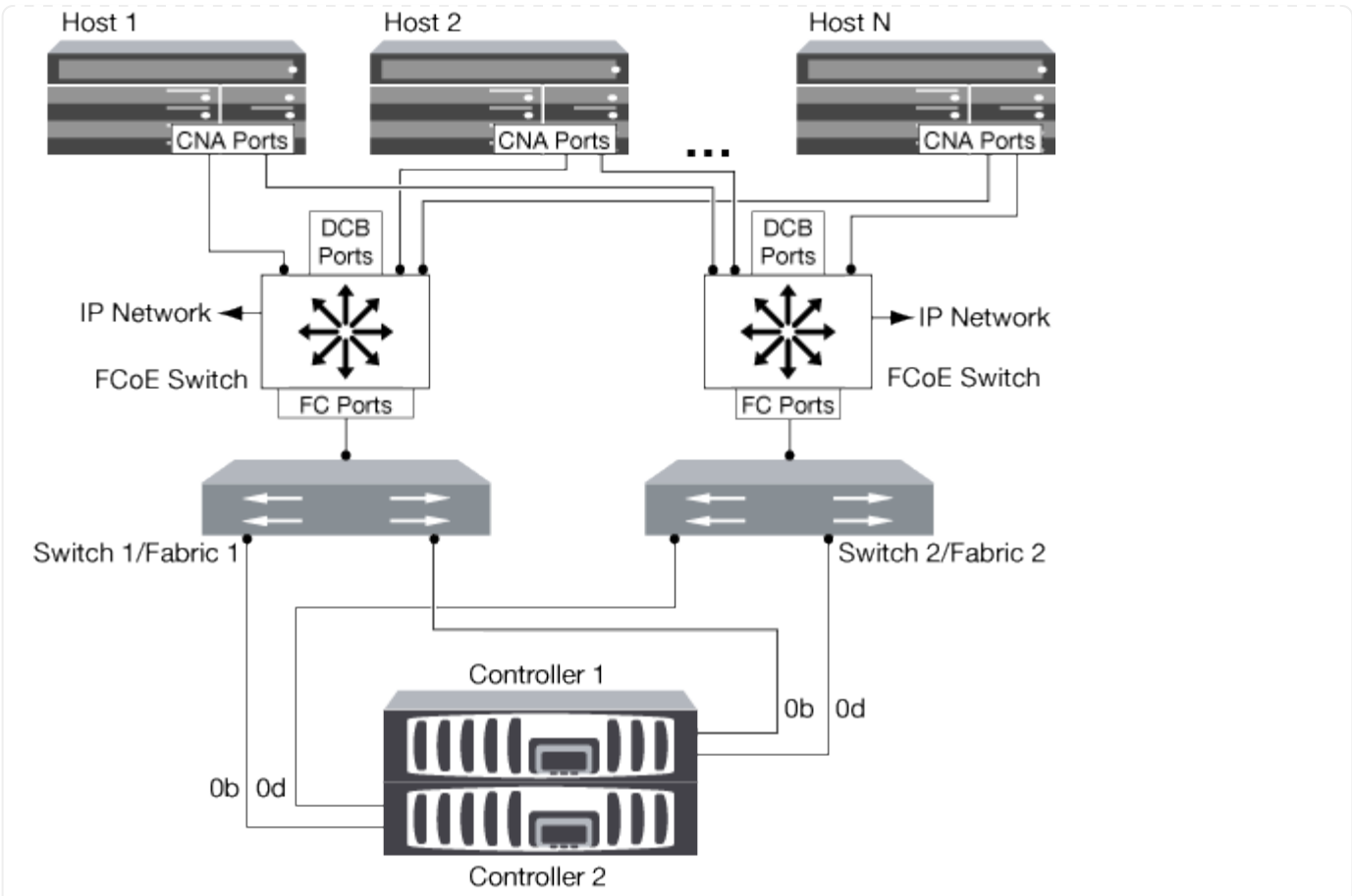
FCoE configurations require Ethernet switches that explicitly support FCoE features. FCoE configurations are validated through the same interoperability and quality assurance process as FC switches. Supported configurations are listed in the Interoperability Matrix. Some of the parameters included in these supported configurations are the switch model, the number of switches that can be deployed in a single fabric, and the supported switch firmware version.

The FC target expansion adapter port numbers in the illustrations are examples. The actual port numbers might vary, depending on the expansion slots in which the FCoE target expansion adapters are installed.

== FCoE initiator to FC target

Using FCoE initiators (CNAs), you can connect hosts to both controllers in an HA pair through FCoE switches to FC target ports. The FCoE switch must also have FC ports. The host FCoE initiator always connects to the FCoE switch. The FCoE switch can connect directly to the FC target or can connect to the FC target through FC switches.

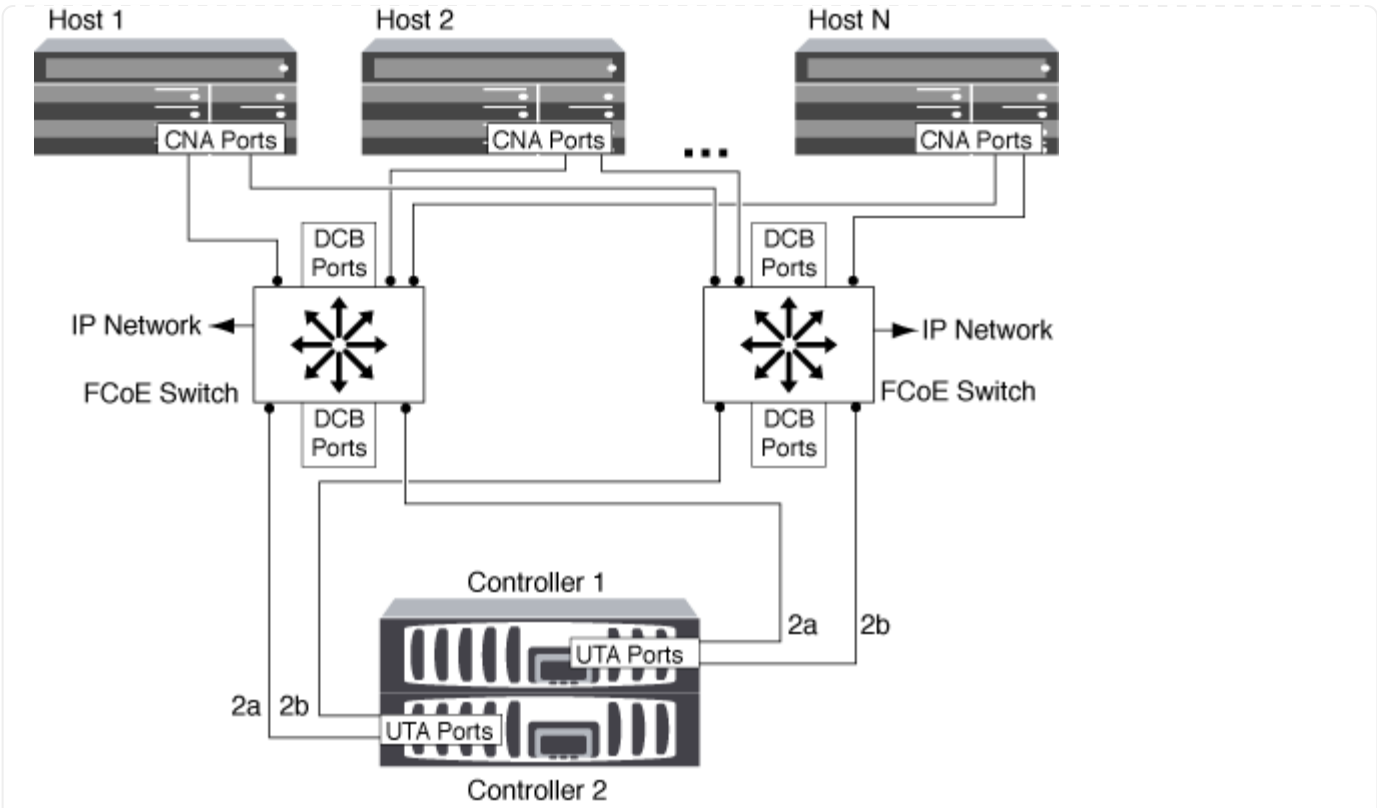
The following illustration shows host CNAs connecting to an FCoE switch, and then to an FC switch before connecting to the HA pair:



== FCoE initiator to FCoE target

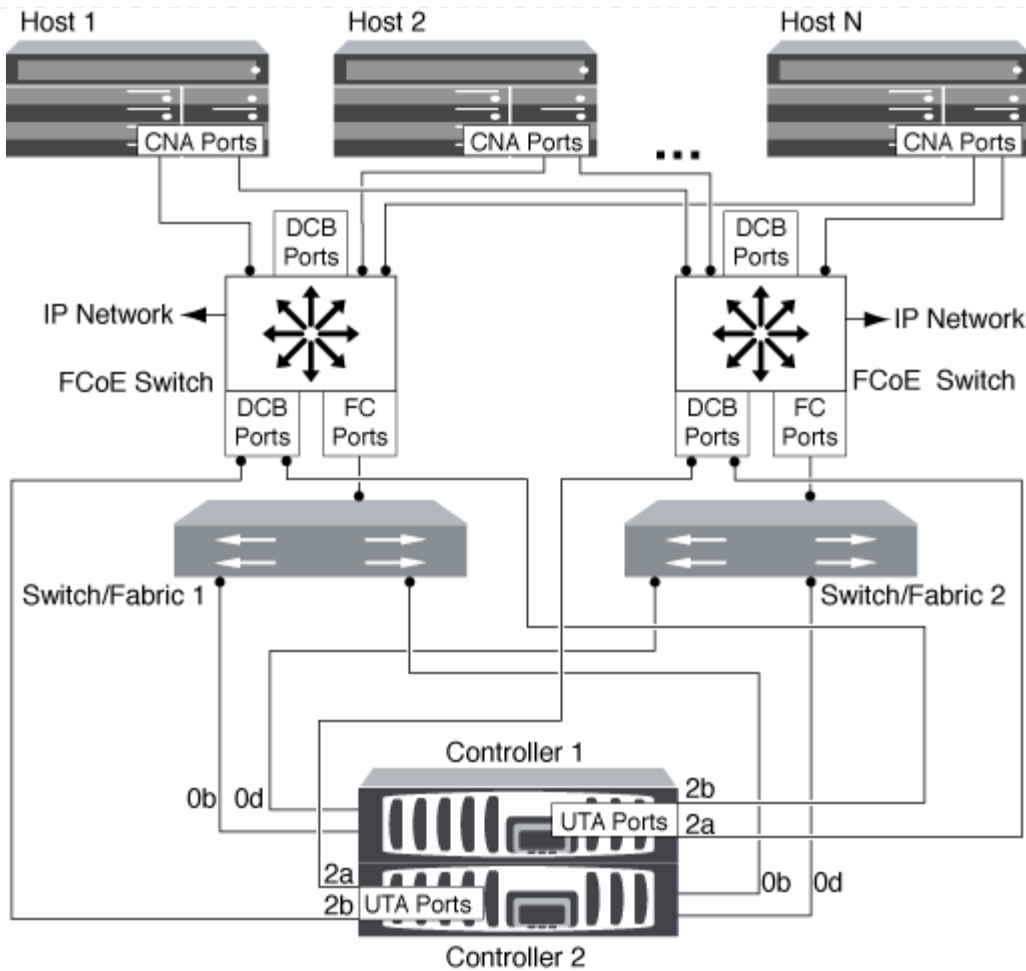
Using host FCoE initiators (CNAs), you can connect hosts to both controllers in an HA pair to FCoE target ports (also called UTAs or UTA2s) through FCoE switches.





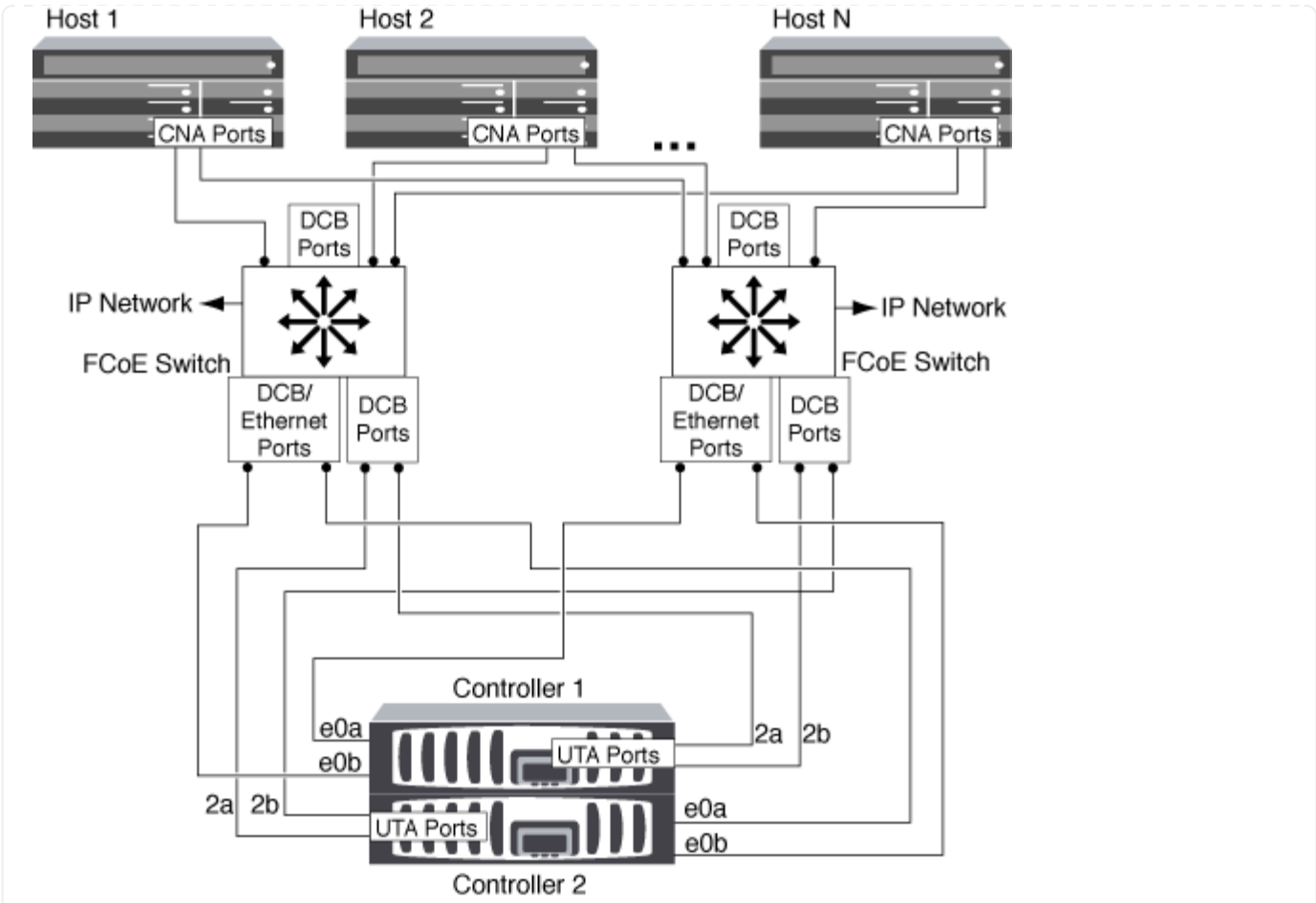
== FCoE initiator to FCoE and FC targets

Using host FCoE initiators (CNAs), you can connect hosts to both controllers in an HA pair to FCoE and FC target ports (also called UTAs or UTA2s) through FCoE switches.



== FCoE mixed with IP storage protocols

Using host FCoE initiators (CNAs), you can connect hosts to both controllers in an HA pair to FCoE target ports (also called UTAs or UTA2s) through FCoE switches. FCoE ports cannot use traditional link aggregation to a single switch. Cisco switches support a special type of link aggregation (Virtual Port Channel) that does support FCoE. A Virtual Port Channel aggregates individual links to two switches. You can also use Virtual Port Channels for other Ethernet traffic. Ports used for traffic other than FCoE, including NFS, SMB, iSCSI, and other Ethernet traffic, can use regular Ethernet ports on the FCoE switches.



```

= FCoE initiator and target combinations
:icons: font
:relative_path: ./san-config/
:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

```

Certain combinations of FCoE and traditional FC initiators and targets are supported.

== FCoE initiators

You can use FCoE initiators in host computers with both FCoE and traditional FC targets in storage controllers. The host FCoE initiator must connect to an FCoE DCB (data center bridging) switch; direct connection to a target is not supported.

The following table lists the supported combinations:

Initiator	Target	Supported?
FC	FC	Yes
FC	FCoE	Yes
FCoE	FC	Yes
FCoE	FCoE	Yes

## == FCoE targets

You can mix FCoE target ports with 4-Gb, 8-Gb, or 16-Gb FC ports on the storage controller regardless of whether the FC ports are add-in target adapters or onboard ports. You can have both FCoE and FC target adapters in the same storage controller.

The rules for combining onboard and expansion FC ports still apply.

= FCoE supported hop count

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

The maximum supported Fibre Channel over Ethernet (FCoE) hop count between a host and storage system depends on the switch supplier and storage system support for FCoE configurations.

The hop count is defined as the number of switches in the path between the initiator (host) and target (storage system). Documentation from Cisco Systems also refers to this value as the *diameter of the SAN fabric*.

For FCoE, you can have FCoE switches connected to FC switches.

For end-to-end FCoE connections, the FCoE switches must be running a firmware version that supports Ethernet inter-switch links (ISLs).

The following table lists the maximum supported hop counts:

Switch supplier	Supported hop count
Brocade	7 for FC 5 for FCoE
Cisco	7 Up to 3 of the switches can be FCoE switches.

= Fibre Channel and FCoE zoning

= Fibre Channel and FCoE zoning overview

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

An FC, FC-NVMe or FCoE zone is a logical grouping of one or more ports within a fabric. For devices to be able see each other, connect, create sessions with one another, and communicate, both ports need to have a common zone membership. Single initiator zoning is recommended.

== Reasons for zoning

- Zoning reduces or eliminates *crosstalk* between initiator HBAs.

This occurs even in small environments and is one of the best arguments for implementing zoning. The logical fabric subsets created by zoning eliminate crosstalk problems.

- Zoning reduces the number of available paths to a particular FC, FC-NVMe, or FCoE port and reduces the number of paths between a host and a particular LUN that is visible.

For example, some host OS multipathing solutions have a limit on the number of paths they can manage. Zoning can reduce the number of paths that an OS multipathing driver sees. If a host does not have a multipathing solution installed, you need to verify that only one path to a LUN is visible by using either zoning in the fabric or a combination of Selective LUN Mapping (SLM) and portsets in the SVM.

- Zoning increases security by limiting access and connectivity to end-points that share a common zone.

Ports that have no zones in common cannot communicate with one another.

- Zoning improves SAN reliability by isolating problems that occur and helps to reduce problem resolution time by limiting the problem space.

== Recommendations for zoning

- You should implement zoning any time, if four or more hosts are connected to a SAN or if SLM is not implemented on the nodes to a SAN.
- Although World Wide Node Name zoning is possible with some switch vendors, World Wide Port Name zoning is required to properly define a specific port and to use NPIV effectively.
- You should limit the zone size while still maintaining manageability.

Multiple zones can overlap to limit size. Ideally, a zone is defined for each host or host cluster.

- You should use single-initiator zoning to eliminate crosstalk between initiator HBAs.

= World Wide Name-based zoning

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

Zoning based on World Wide Name (WWN) specifies the WWN of the members to be included within the zone. When zoning in ONTAP, you must use World Wide Port Name (WWPN) zoning.

WWPN zoning provides flexibility because access is not determined by where the device is physically connected to the fabric. You can move a cable from one port to another without reconfiguring zones.

For Fibre Channel paths to storage controllers running ONTAP, be sure the FC switches are zoned using the WWPNs of the target logical interfaces (LIFs), not the WWPNs of the physical ports on the node. For more information on LIFs, see the *ONTAP Network Management Guide*.

## Network management

= Individual zones

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

In the recommended zoning configuration, there is one host initiator per zone. The zone consists of the host initiator port and one or more target LIFs on the storage nodes that are providing access to the LUNs up to the desired number of paths per target. This means that hosts accessing the same nodes cannot see each other's

ports, but each initiator can access any node.

You should add all LIF's from the storage virtual machine (SVM) into the zone with the host initiator. This allows you to move volumes or LUNs without editing your existing zones or creating new zones.

For Fibre Channel paths to nodes running ONTAP, be sure that the FC switches are zoned using the WWPNs of the target logical interfaces (LIFs), not the WWPNs of the physical ports on the node. The WWPNs of the physical ports start with "50" and the WWPNs of the LIFs start with "20".

= Single-fabric zoning

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

In a single-fabric configuration, you can still connect each host initiator to each storage node. Multipathing software is required on the host to manage multiple paths. Each host should have two initiators for multipathing to provide resiliency in the solution.

Each initiator should have a minimum of one LIF from each node that the initiator can access. The zoning should allow at least one path from the host initiator to the HA pair of nodes in the cluster to provide a path for LUN connectivity. This means that each initiator on the host might only have one target LIF per node in its zone configuration. If there is a requirement for multipathing to the same node or multiple nodes in the cluster, then each node will have multiple LIFs per node in its zone configuration. This enables the host to still access its LUNs if a node fails or a volume containing the LUN is moved to a different node. This also requires the reporting nodes to be set appropriately.

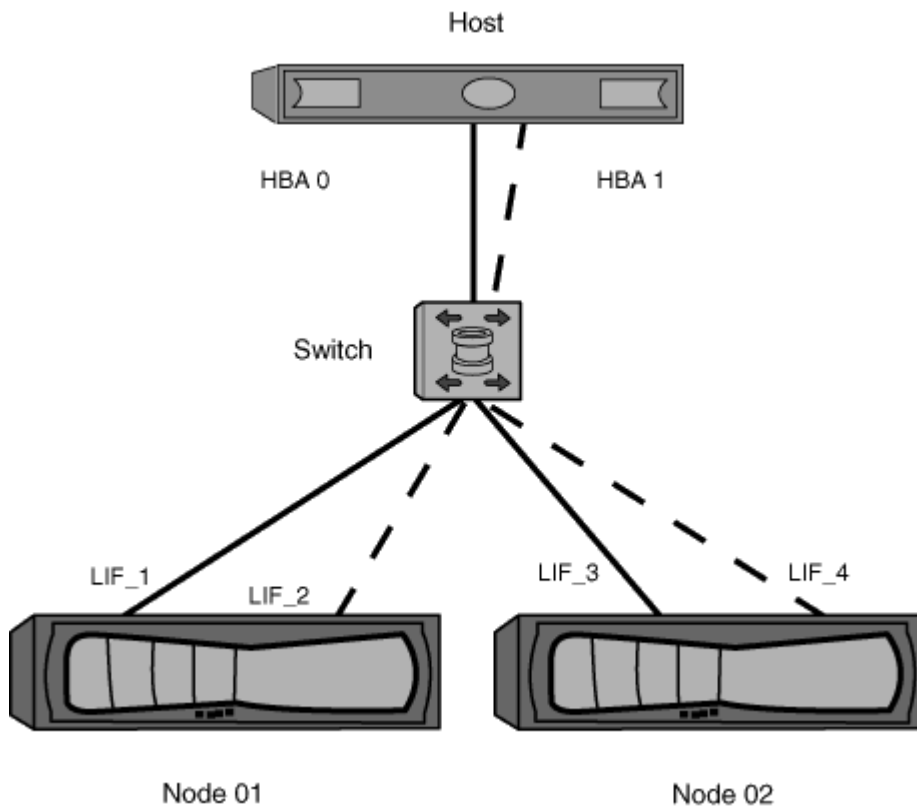
Single-fabric configurations are supported, but are not considered highly available. The failure of a single component can cause loss of access to data.

In the following figure, the host has two initiators and is running multipathing software. There are two zones:

The naming convention used in this figure is just a recommendation of one possible naming convention that you can choose to use for your ONTAP solution.

- Zone 1: HBA 0, LIF\_1, and LIF\_3
- Zone 2: HBA 1, LIF\_2, and LIF\_4

If the configuration included more nodes, the LIFs for the additional nodes would be included in these zones.



In this example, you could also have all four LIFs in each zone. In that case, the zones would be as follows:

- Zone 1: HBA 0, LIF\_1, LIF\_2, LIF\_3, and LIF\_4
- Zone 2: HBA 1, LIF\_1, LIF\_2, LIF\_3, and LIF\_4

The host operating system and multipathing software have to support the number of supported paths that are being used to access the LUNs on the nodes. To determine the number of paths used to access the LUNs on nodes, see the SAN configuration limits section.



## Related information

[NetApp Hardware Universe](#)

= Dual-fabric HA pair zoning

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

In dual-fabric configurations, you can connect each host initiator to each cluster node. Each host initiator uses a different switch to access the cluster nodes. Multipathing software is required on the host to manage multiple paths.

Dual-fabric configurations are considered high availability because access to data is maintained if a single component fails.

In the following figure, the host has two initiators and is running multipathing software. There are two zones. SLM is configured so that all nodes are considered as reporting nodes.

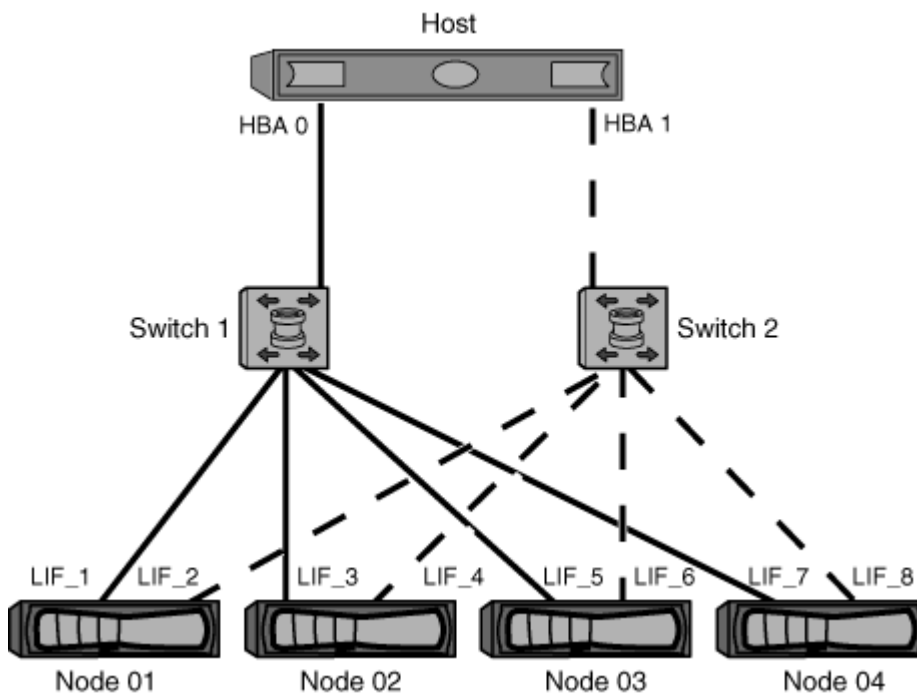
The naming convention used in this figure is just a recommendation of one possible naming convention that you can choose to use for your ONTAP solution.

- Zone 1: HBA 0, LIF\_1, LIF\_3, LIF\_5, and LIF\_7
- Zone 2: HBA 1, LIF\_2, LIF\_4, LIF\_6, and LIF\_8

Each host initiator is zoned through a different switch. Zone 1 is accessed through Switch 1. Zone 2 is accessed through Switch 2.

Each initiator can access a LIF on every node. This enables the host to still access its LUNs if a node fails. SVMs have access to all iSCSI and FC LIFs on every node in a clustered solution based on the setting for Selective LUN Map (SLM) and the reporting node configuration. You can use SLM, portsets, or FC switch zoning to reduce the number of paths from an SVM to the host and the number of paths from an SVM to a LUN.

If the configuration included more nodes, the LIFs for the additional nodes would be included in these zones.



The host operating system and multipathing software have to support the number of paths that is being used to access the LUNs on the nodes.

## Related information

[NetApp Hardware Universe](#)

= Zoning restrictions for Cisco FC and FCoE switches

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

When using Cisco FC and FCoE switches, a single fabric zone must not contain more than one target LIF for the same physical port. If multiple LIFs on the same port are in the same zone, then the LIF ports might fail to recover from a connection loss.

Regular FC switches are used for the FC-NVMe protocol in the exact same way they are used for the FC protocol.

- Multiple LIFs for the FC and FCoE protocols, can share physical ports on a node as long as they are in different zones.
- FC-NVMe and FCoE cannot share the same physical port.
- FC and FC-NVMe can share the same 32 Gb physical port.
- Cisco FC and FCoE switches require each LIF on a given port to be in a separate zone from the other LIFs on that port.
- A single zone can have both FC and FCoE LIFs. A zone can contain a LIF from every target port in the cluster, but be careful to not exceed the host's path limits and verify the SLM configuration.
- LIFs on different physical ports can be in the same zone.
- Cisco switches require that LIFs be separated.

Though not required, separating LIFs is recommended for all switches

= Requirements for shared SAN configurations

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

Shared SAN configurations are defined as hosts that are attached to both ONTAP storage systems and other vendors' storage systems. Accessing ONTAP storage systems and other vendors' storage systems from a single host is supported as long as several requirements are met.

For all of the host operating systems, it is a best practice to use separate adapters to connect to each vendor's storage systems. Using separate adapters reduces the chances of conflicting drivers and settings. For connections to an ONTAP storage system, the adapter model, BIOS, firmware, and driver must be listed as supported in the NetApp Interoperability Matrix Tool.

You should set the required or recommended timeout values and other storage parameters for the host. You must always install the NetApp software or apply the NetApp settings last.

- For AIX, you should apply the values from the AIX Host Utilities version that is listed in the Interoperability Matrix Tool for your configuration.

- For ESX, you should apply host settings by using Virtual Storage Console for VMware vSphere.
- For HP-UX, you should use the HP-UX default storage settings.
- For Linux, you should apply the values from the Linux Host Utilities version that is listed in the Interoperability Matrix Tool for your configuration.
- For Solaris, you should apply the values from the Solaris Host Utilities version that is listed in the Interoperability Matrix Tool for your configuration.
- For Windows, you should install the Windows Host Utilities version that is listed in the Interoperability Matrix Tool for your configuration.

### Related information

[NetApp Interoperability Matrix Tool](#)

= Host support for multipathing

= Host support for multipathing overview

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

ONTAP always uses Asymmetric Logical Unit Access (ALUA) for both FC and iSCSI paths. Be sure to use host configurations that support ALUA for FC and iSCSI protocols.

Beginning with ONTAP 9.5 multipath HA pair failover/giveback is supported for NVMe configurations using Asynchronous Namespace Access (ANA). In ONTAP 9.4, NVMe only supports one path from host to target. The application host needs to manage path failover to its high availability (HA) partner.

For information about which specific host configurations support ALUA or ANA, see the [NetApp Interoperability Matrix Tool](#) and [ONTAP SAN Host Configuration](#) for your host operating system.

= When host multipathing software is required

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

If there is more than one path from the storage virtual machine (SVM) logical interfaces (LIFs) to the fabric, multipathing software is required. Multipathing software is required on the host any time the host can access a LUN through more than one path.

The multipathing software presents a single disk to the operating system for all paths to a LUN. Without multipathing software, the operating system could treat each path as a separate disk, which can lead to data corruption.

Your solution is considered to have multiple paths if you have any of the following:

- A single initiator port in the host attaching to multiple SAN LIFs in the SVM
- Multiple initiator ports attaching to a single SAN LIF in the SVM
- Multiple initiator ports attaching to multiple SAN LIFs in the SVM

In single-fabric single-node configurations, multipathing software is not required if you only have a single path from the host to the node.

Multipathing software is recommended in HA configurations. In addition to Selective LUN Map, using FC switch zoning or portsets to limit the paths used to access LUNs is recommended.

Multipathing software is also known as MPIO (multipath I/O) software.

= Recommended number of paths from host to nodes in cluster

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You should not exceed more than eight paths from your host to each node in your cluster, paying attention to the total number of paths that can be supported for the host OS and the multipathing used on the host.

You should have a minimum of two paths per LUN connecting to each reporting node through Selective LUN Map (SLM) being used by the storage virtual machine (SVM) in your cluster. This eliminates single points of failure and enables the system to survive component failures.

If you have four or more nodes in your cluster or more than four target ports being used by the SVMs in any of your nodes, you can use the following methods to limit the number of paths that can be used to access LUNs on your nodes so that you do not exceed the recommended maximum of eight paths.

- SLM

SLM reduces the number of paths from the host to LUN to only paths on the node owning the LUN and the owning node's HA partner. SLM is enabled by default.

- Portsets for iSCSI
- FC igroup mappings from your host
- FC switch zoning

## Related information

[SAN administration](#)

= Configuration limits

= Determine the number of supported nodes for SAN configurations

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

The number of nodes per cluster supported by ONTAP varies depending on your version of ONTAP, the storage controller models in your cluster, and the protocol of your cluster nodes.

## About this task

If any node in the cluster is configured for FC, FC-NVMe, FCoE, or iSCSI, that cluster is limited to the SAN node limits. Node limits based on the controllers in your cluster are listed in the *Hardware Universe*.

## Steps

1. Go to [NetApp Hardware Universe](#).
2. Click **Platforms** in the upper left (next to the **Home** button) and select the platform type.
3. Select the check box next to your version of ONTAP.

A new column is displayed for you to choose your platforms.

4. Select the check boxes next to the platforms used in your solution.
5. Unselect the **Select All** check box in the **Choose Your Specifications** column.
6. Select the **Max Nodes per Cluster (NAS/SAN)** check box.
7. Click **Show Results**.

#### Related information

[NetApp Hardware Universe](#)

= Determine the number of supported hosts per cluster in FC and FC-NVMe configurations

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

The maximum number of SAN hosts that can be connected to a cluster varies greatly based upon your specific combination of multiple cluster attributes, such as the number of hosts connected to each cluster node, initiators per host, sessions per host, and nodes in the cluster.

#### About this task

For FC and FC-NVMe configurations, you should use the number of initiator-target nexuses (ITNs) in your system to determine whether you can add more hosts to your cluster.

An ITN represents one path from the host's initiator to the storage system's target. The maximum number of ITNs per node in FC and FC-NVMe configurations is 2,048. As long as you are below the maximum number of ITNs, you can continue to add hosts to your cluster.

To determine the number of ITNs used in your cluster, perform the following steps for each node in the cluster.

#### Steps

1. Identify all the LIFs on a given node.
2. Run the following command for every LIF on the node:

```
fcip initiator show -fields wwpn, lif
```

The number of entries displayed at the bottom of the command output represents your number of ITNs for that LIF.

3. Record the number of ITNs displayed for each LIF.
4. Add the number of ITNs for each LIF on every node in your cluster.

This total represents the number of ITNs in your cluster.

= Determine the supported number of hosts in iSCSI configurations

:icons: font  
:relative\_path: ./san-config/  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

The maximum number of SAN hosts that can be connected in iSCSI configurations varies greatly based on your specific combination of multiple cluster attributes, such as the number of hosts connected to each cluster node, initiators per host, logins per host, and nodes in the cluster.

### About this task

The number of hosts that can be directly connected to a node or that can be connected through one or more switches depends on the number of available Ethernet ports. The number of available Ethernet ports is determined by the model of the controller and the number and type of adapters installed in the controller. The number of supported Ethernet ports for controllers and adapters is available in the *Hardware Universe*.

For all multi-node cluster configurations, you must determine the number of iSCSI sessions per node to know whether you can add more hosts to your cluster. As long as your cluster is below the maximum number of iSCSI sessions per node, you can continue to add hosts to your cluster. The maximum number of iSCSI sessions per node varies based on the types of controllers in your cluster.

### Steps

1. Identify all of the target portal groups on the node.
2. Check the number of iSCSI sessions for every target portal group on the node:

```
iscsi session show -tpgroup tpgroup
```

The number of entries displayed at the bottom of the command output represents your number of iSCSI sessions for that target portal group.

3. Record the number of iSCSI sessions displayed for each target portal group.
4. Add the number of iSCSI sessions for each target portal group on the node.

The total represents the number of iSCSI sessions on your node.

= FC switch configuration limits

:icons: font  
:relative\_path: ./san-config/  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

Fibre Channel switches have maximum configuration limits, including the number of logins supported per port, port group, blade, and switch. The switch vendors document their supported limits.

Each FC logical interface (LIF) logs into an FC switch port. The total number of logins from a single target on the node equals the number of LIFs plus one login for the underlying physical port. Do not exceed the switch vendor's configuration limits for logins or other configuration values. This also holds true for the initiators being used on the host side in virtualized environments with NPIV enabled. Do not exceed the switch vendor's configuration limits for logins for either the target or the initiators being used in the solution.

## == Brocade switch limits

You can find the configuration limits for Brocade switches in the *Brocade Scalability Guidelines*.

## == Cisco Systems switch limits

You can find the configuration limits for Cisco switches in the [Cisco Configuration Limits](#) guide for your version of Cisco switch software.

## = Calculate queue depth overview

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You might need to tune your FC queue depth on the host to achieve the maximum values for ITNs per node and FC port fan-in. The maximum number of LUNs and the number of HBAs that can connect to an FC port are limited by the available queue depth on the FC target ports.

### About this task

Queue depth is the number of I/O requests (SCSI commands) that can be queued at one time on a storage controller. Each I/O request from the host's initiator HBA to the storage controller's target adapter consumes a queue entry. Typically, a higher queue depth equates to better performance. However, if the storage controller's maximum queue depth is reached, that storage controller rejects incoming commands by returning a QFULL response to them. If a large number of hosts are accessing a storage controller, you should plan carefully to avoid QFULL conditions, which significantly degrade system performance and can lead to errors on some systems.

In a configuration with multiple initiators (hosts), all hosts should have similar queue depths. Because of the inequality in queue depth between hosts connected to the storage controller through the same target port, hosts with smaller queue depths are being deprived of access to resources by hosts with larger queue depths.

The following general recommendations can be made about "tuning" queue depths:

- For small to mid-size systems, use an HBA queue depth of 32.
- For large systems, use an HBA queue depth of 128.
- For exception cases or performance testing, use a queue depth of 256 to avoid possible queuing problems.
- All hosts should have the queue depths set to similar values to give equal access to all hosts.
- To avoid performance penalties or errors, the storage controller target FC port queue depth must not be exceeded.

### Steps

1. Count the total number of FC initiators in all of the hosts that connect to one FC target port.
2. Multiply by 128.
  - If the result is less than 2,048, set the queue depth for all initiators to 128.  
You have 15 hosts with one initiator connected to each of two target ports on the storage controller.  $15 \times 128 = 1,920$ . Because 1,920 is less than the total queue depth limit of 2,048, you can set the queue depth for all of your initiators to 128.



- If the result is greater than 2,048, go to step 3.  
You have 30 hosts with one initiator connected to each of two target ports on the storage controller.  $30 \times 128 = 3,840$ . Because 3,840 is greater than the total queue depth limit of 2,048, you should choose one of the options under step 3 for remediation.

3. Choose one of the following options to add more hosts to the storage controller.

- Option 1:
  - i. Add more FC target ports.
  - ii. Redistribute your FC initiators.
  - iii. Repeat steps 1 and 2.

The desired queue depth of 3,840 exceeds the available queue depth per port. To remedy this, you can add a two-port FC target adapter to each controller, then rezone your FC switches so that 15 of your 30 hosts connect to one set of ports, and the remaining 15 hosts connect to a second set of ports. The queue depth per port is then reduced to  $15 \times 128 = 1,920$ .

- Option 2:
  - i. Designate each host as “large” or “small” based on its expected I/O need.
  - ii. Multiply the number of large initiators by 128.
  - iii. Multiply the number of small initiators by 32.
  - iv. Add the two results together.
  - v. If the result is less than 2,048, set the queue depth for large hosts to 128 and the queue depth for small hosts to 32.
  - vi. If the result is still greater than 2,048 per port, reduce the queue depth per initiator until the total queue depth is less than or equal to 2,048.

To estimate the queue depth needed to achieve a certain I/O per second throughput, use this formula:

Needed queue depth = (Number of I/O per second) × (Response time)

For example, if you need 40,000 I/O per second with a response time of 3 milliseconds, the needed queue depth =  $40,000 \times (.003) = 120$ .

The maximum number of hosts that you can connect to a target port is 64, if you decide to limit the queue depth to the basic recommendation of 32. However, if you decide to have a queue depth of 128, then you can have a maximum of 16 hosts connected to one target port. The larger the queue depth, the fewer hosts that a single target port can support. If your requirement is such that you cannot compromise on the queue depth, then you should get more target ports.

The desired queue depth of 3,840 exceeds the available queue depth per port. You have 10 “large” hosts that have high storage I/O needs, and 20 “small” hosts that have low I/O needs. Set the initiator queue depth on the large hosts to 128 and the initiator queue depth on the small hosts to 32.

Your resulting total queue depth is  $(10 \times 128) + (20 \times 32) = 1,920$ .

You can spread the available queue depth equally across each initiator.

Your resulting queue depth per initiator is  $2,048 \div 30 = 68$ .

= Set queue depths on SAN hosts

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You might need to change the queue depths on your host to achieve the maximum values for ITNs per node and FC port fan-in.

== AIX hosts

You can change the queue depth on AIX hosts using the `chdev` command. Changes made using the `chdev` command persist across reboots.

Examples:

- To change the queue depth for the `hdisk7` device, use the following command:

```
chdev -l hdisk7 -a queue_depth=32
```

- To change the queue depth for the `fcs0` HBA, use the following command:

```
chdev -l fcs0 -a num_cmd_elems=128
```

The default value for `num_cmd_elems` is 200. The maximum value is 2,048.

It might be necessary to take the HBA offline to change `num_cmd_elems` and then bring it back online using the `rmdev -l fcs0 -R` and `makdev -l fcs0 -P` commands.

## == HP-UX hosts

You can change the LUN or device queue depth on HP-UX hosts using the kernel parameter `scsi_max_qdepth`. You can change the HBA queue depth using the kernel parameter `max_fcp_reqs`.

- The default value for `scsi_max_qdepth` is 8. The maximum value is 255.

`scsi_max_qdepth` can be dynamically changed on a running system using the `-u` option on the `kmtune` command. The change will be effective for all devices on the system. For example, use the following command to increase the LUN queue depth to 64:

```
kmtune -u -s scsi_max_qdepth=64
```

It is possible to change queue depth for individual device files using the `scsictl` command. Changes using the `scsictl` command are not persistent across system reboots. To view and change the queue depth for a particular device file, execute the following command:

```
scsictl -a /dev/rdisk/c2t2d0
```

```
scsictl -m queue_depth=16 /dev/rdisk/c2t2d0
```

- The default value for `max_fcp_reqs` is 512. The maximum value is 1024.

The kernel must be rebuilt and the system must be rebooted for changes to `max_fcp_reqs` to take effect. To change the HBA queue depth to 256, for example, use the following command:

```
kmtune -u -s max_fcp_reqs=256
```

## == Solaris hosts

You can set the LUN and HBA queue depth for your Solaris hosts.

- For LUN queue depth: The number of LUNs in use on a host multiplied by the per-LUN throttle (`lun-queue-depth`) must be less than or equal to the `tgt-queue-depth` value on the host.
- For queue depth in a Sun stack: The native drivers do not allow for per LUN or per target `max_throttle` settings at the HBA level. The recommended method for setting the `max_throttle` value for native drivers is on a per-device type (`VID_PID`) level in the `/kernel/drv/sd.conf` and `/kernel/drv/ssd.conf` files. The host utility sets this value to 64 for MPxIO configurations and 8 for Veritas DMP configurations.

### Steps

1. # `cd/kernel/drv`
2. # `vi lpfc.conf`
3. Search for `/tft-queue (/tgt-queue)`

```
tgt-queue-depth=32
```

The default value is set to 32 at installation.

1. Set the desired value based on the configuration of your environment.
2. Save the file.
3. Reboot the host using the `sync; sync; sync; reboot -- -r` command.

== VMware hosts for a QLogic HBA

Use the `esxcfg-module` command to change the HBA timeout settings. Manually updating the `esx.conf` file is not recommended.

#### Steps

1. Log on to the service console as the root user.
2. Use the `#vmkload_mod -l` command to verify which QLogic HBA module is currently loaded.
3. For a single instance of a QLogic HBA, run the following command:

```
#esxcfg-module -s ql2xmaxqdepth=64 qla2300_707
```

This example uses `qla2300_707` module. Use the appropriate module based on the output of `vmkload_mod -l`.

1. Save your changes using the following command:

```
#!/usr/sbin/esxcfg-boot -b
```

2. Reboot the server using the following command:

```
#reboot
```

3. Confirm the changes using the following commands:

a. `#esxcfg-module -g qla2300_707`

b. `qla2300_707 enabled = 1 options = 'ql2xmaxqdepth=64'`

== VMware hosts for an Emulex HBA

Use the `esxcfg-module` command to change the HBA timeout settings. Manually updating the `esx.conf` file is not recommended.

#### Steps

1. Log on to the service console as the root user.
2. Use the `#vmkload_mod -l grep lpfc` command to verify which Emulex HBA is currently loaded.
3. For a single instance of an Emulex HBA, enter the following command:

```
#esxcfg-module -s lpfc0_lun_queue_depth=16 lpfcdd_7xx
```

Depending on the model of the HBA, the module can be either `lpfcdd_7xx` or `lpfcdd_732`. The above command

uses the `lpfcdd_7xx` module. You should use the appropriate module based on the outcome of `vmkload_mod -l`.

+

Running this command will set the LUN queue depth to 16 for the HBA represented by `lpfc0`.

1. For multiple instances of an Emulex HBA, run the following command:

```
a esxcfg-module -s "lpfc0_lun_queue_depth=16 lpfc1_lun_queue_depth=16"
lpfcdd_7xx
```

The LUN queue depth for `lpfc0` and the LUN queue depth for `lpfc1` is set to 16.

2. Enter the following command:

```
#esxcfg-boot -b
```

3. Reboot using `#reboot`.

== Windows hosts for an Emulex HBA

On Windows hosts, you can use the `LPUTILNT` utility to update the queue depth for Emulex HBAs.

### Steps

1. Run the `LPUTILNT` utility located in the `C:\WINNT\system32` directory.
2. Select **Drive Parameters** from the menu on the right side.
3. Scroll down and double-click **QueueDepth**.

If you are setting **QueueDepth** greater than 150, the following Windows Registry value also need to be increased appropriately:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lpxnds\Parameters\Device\NumberOfRequests
```

## == Windows hosts for a Qlogic HBA

On Windows hosts, you can use the `SANsurfer` HBA manager utility to update the queue depths for Qlogic HBAs.

### Steps

1. Run the `SANsurfer` HBA manager utility.
2. Click on **HBA port > Settings**.
3. Click **Advanced HBA port settings** in the list box.
4. Update the `Execution Throttle` parameter.

## == Linux hosts for Emulex HBA

You can update the queue depths of an Emulex HBA on a Linux host. To make the updates persistent across reboots, you must then create a new RAM disk image and reboot the host.

### Steps

1. Identify the queue depth parameters to be modified:

```
modinfo lpfc|grep queue_depth
```

The list of queue depth parameters with their description is displayed. Depending on your operating system version, you can modify one or more of the following queue depth parameters:

- `lpfc_lun_queue_depth`: Maximum number of FC commands that can be queued to a specific LUN (uint)
- `lpfc_hba_queue_depth`: Maximum number of FC commands that can be queued to an lpfc HBA (uint)
- `lpfc_tgt_queue_depth`: Maximum number of FC commands that can be queued to a specific target port (uint)

The `lpfc_tgt_queue_depth` parameter is applicable only for Red Hat Enterprise Linux 7.x systems, SUSE Linux Enterprise Server 11 SP4 systems and 12.x systems.

2. Update the queue depths by adding the queue depth parameters to the `/etc/modprobe.conf` file for a Red Hat Enterprise Linux 5.x system and to the `/etc/modprobe.d/scsi.conf` file for a Red Hat Enterprise Linux 6.x or 7.x system, or a SUSE Linux Enterprise Server 11.x or 12.x system.

Depending on your operating system version, you can add one or more of the following commands:

- `options lpfc lpfc_hba_queue_depth=new_queue_depth`
- `options lpfc lpfc_lun_queue_depth=new_queue_depth`
- `options lpfc lpfc_tgt_queue_depth=new_queue_depth`

3. Create a new RAM disk image, and then reboot the host to make the updates persistent across reboots.

For more information, see the [System administration](#) for your version of Linux operating system.

4. Verify that the queue depth values are updated for each of the queue depth parameter that you have modified:

```
cat /sys/class/scsi_host/host_number/lpfc_lun_queue_depthcat
/sys/class/scsi_host/host_number/lpfc_tgt_queue_depthcat
/sys/class/scsi_host/host_number/lpfc_hba_queue_depth
```

```
root@localhost ~]#cat
/sys/class/scsi_host/host5/lpfc_lun_queue_depth
30
```

The current value of the queue depth is displayed.

== Linux hosts for QLogic HBA

You can update the device queue depth of a QLogic driver on a Linux host. To make the updates persistent across reboots, you must then create a new RAM disk image and reboot the host. You can use the QLogic HBA management GUI or command-line interface (CLI) to modify the QLogic HBA queue depth.

This task shows how to use the QLogic HBA CLI to modify the QLogic HBA queue depth

### Steps

1. Identify the device queue depth parameter to be modified:

```
modinfo qla2xxx | grep ql2xmaxqdepth
```

You can modify only the `ql2xmaxqdepth` queue depth parameter, which denotes the maximum queue depth that can be set for each LUN. The default value is 64 for RHEL 7.5 and later. The default value is 32 for RHEL 7.4 and earlier.

```
root@localhost ~]# modinfo qla2xxx|grep ql2xmaxqdepth
parm:          ql2xmaxqdepth:Maximum queue depth to set for each LUN.
Default is 64. (int)
```

2. Update the device queue depth value:

- If you want to make the modifications persistent, perform the following steps:
  - i. Update the queue depths by adding the queue depth parameter to the `/etc/modprobe.conf` file for a Red Hat Enterprise Linux 5.x system and to the `/etc/modprobe.d/scsi.conf` file for a Red Hat Enterprise Linux 6.x or 7.x system, or a SUSE Linux Enterprise Server 11.x or 12.x system: `options qla2xxx ql2xmaxqdepth=new_queue_depth`
  - ii. Create a new RAM disk image, and then reboot the host to make the updates persistent across reboots.

For more information, see the [System administration](#) for your version of Linux operating system.

- If you want to modify the parameter only for the current session, run the following command:

```
echo new_queue_depth > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

In the following example, the queue depth is set to 128.

```
echo 128 > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

3. Verify that the queue depth values are updated:

```
cat /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

The current value of the queue depth is displayed.

4. Modify the QLogic HBA queue depth by updating the firmware parameter `Execution Throttle` from the QLogic HBA BIOS.

- a. Log in to the QLogic HBA management CLI:

```
/opt/QLogic_Corporation/QConvergeConsoleCLI/qauccli
```

- b. From the main menu, select the `Adapter Configuration` option.



```
[root@localhost ~]#
/opt/QLogic_Corporation/QConvergeConsoleCLI/qauccli
Using config file:
/opt/QLogic_Corporation/QConvergeConsoleCLI/qauccli.cfg
Installation directory:
/opt/QLogic_Corporation/QConvergeConsoleCLI
Working dir: /root

QConvergeConsole

      CLI - Version 2.2.0 (Build 15)

Main Menu

1: Adapter Information
**2: Adapter Configuration**
3: Adapter Updates
4: Adapter Diagnostics
5: Monitoring
6: FabricCache CLI
7: Refresh
8: Help
9: Exit

Please Enter Selection: 2
```

c. From the list of adapter configuration parameters, select the HBA Parameters option.

```
1: Adapter Alias
2: Adapter Port Alias
**3: HBA Parameters**
4: Persistent Names (udev)
5: Boot Devices Configuration
6: Virtual Ports (NPIV)
7: Target Link Speed (iidMA)
8: Export (Save) Configuration
9: Generate Reports
10: Personality
11: FEC
(p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
Please Enter Selection: 3
```

d. From the list of HBA ports, select the required HBA port.

## Fibre Channel Adapter Configuration

```
HBA Model QLE2562 SN: BFD1524C78510
  1: Port    1: WWPN: 21-00-00-24-FF-8D-98-E0 Online
  2: Port    2: WWPN: 21-00-00-24-FF-8D-98-E1 Online
HBA Model QLE2672 SN: RFE1241G81915
  3: Port    1: WWPN: 21-00-00-0E-1E-09-B7-62 Online
  4: Port    2: WWPN: 21-00-00-0E-1E-09-B7-63 Online
```

(p or 0: Previous Menu; m or 98: Main Menu; ex or 99:  
Quit)

Please Enter Selection: 1

The details of the HBA port are displayed.

- e. From the HBA Parameters menu, select the Display HBA Parameters option to view the current value of the Execution Throttle option.

The default value of the Execution Throttle option is 65535.

## HBA Parameters Menu

```
=====
HBA          : 2 Port: 1
SN           : BFD1524C78510
HBA Model    : QLE2562
HBA Desc.    : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version   : 8.01.02
WWPN         : 21-00-00-24-FF-8D-98-E0
WWNN         : 20-00-00-24-FF-8D-98-E0
Link         : Online
=====
```

- 1: Display HBA Parameters
- 2: Configure HBA Parameters
- 3: Restore Defaults

(p or 0: Previous Menu; m or 98: Main Menu; x or 99:  
Quit)

Please Enter Selection: 1

```
-----
-----
HBA Instance 2: QLE2562 Port 1 WWPN 21-00-00-24-FF-8D-98-E0
```

PortID 03-07-00

Link: Online

```
-----  
-----  
Connection Options           : 2 - Loop Preferred, Otherwise  
Point-to-Point  
Data Rate                    : Auto  
Frame Size                   : 2048  
Hard Loop ID                 : 0  
Loop Reset Delay (seconds)   : 5  
Enable Host HBA BIOS        : Enabled  
Enable Hard Loop ID         : Disabled  
Enable FC Tape Support      : Enabled  
Operation Mode              : 0 - Interrupt for every I/O  
completion  
Interrupt Delay Timer (100us) : 0  
**Execution Throttle        : 65535**  
Login Retry Count           : 8  
Port Down Retry Count       : 30  
Enable LIP Full Login       : Enabled  
Link Down Timeout (seconds) : 30  
Enable Target Reset         : Enabled  
LUNs Per Target             : 128  
Out Of Order Frame Assembly : Disabled  
Enable LR Ext. Credits      : Disabled  
Enable Fabric Assigned WWN  : N/A
```

Press <Enter> to continue:

- f. Press **Enter** to continue.
- g. From the HBA Parameters menu, select the `Configure HBA Parameters` option to modify the HBA parameters.
- h. From the `Configure Parameters` menu, select the `Execute Throttle` option and update the value of this parameter.

## Configure Parameters Menu

```
=====
HBA          : 2 Port: 1
SN           : BFD1524C78510
HBA Model    : QLE2562
HBA Desc.    : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version   : 8.01.02
WWPN         : 21-00-00-24-FF-8D-98-E0
WWNN         : 20-00-00-24-FF-8D-98-E0
Link         : Online
=====
```

- 1: Connection Options
- 2: Data Rate
- 3: Frame Size
- 4: Enable HBA Hard Loop ID
- 5: Hard Loop ID
- 6: Loop Reset Delay (seconds)
- 7: Enable BIOS
- 8: Enable Fibre Channel Tape Support
- 9: Operation Mode
- 10: Interrupt Delay Timer (100 microseconds)
- 11: Execution Throttle
- 12: Login Retry Count
- 13: Port Down Retry Count
- 14: Enable LIP Full Login
- 15: Link Down Timeout (seconds)
- 16: Enable Target Reset
- 17: LUNs per Target
- 18: Enable Receive Out Of Order Frame
- 19: Enable LR Ext. Credits
- 20: Commit Changes
- 21: Abort Changes

(p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)

Please Enter Selection: 11

Enter Execution Throttle [1-65535] [65535]: 65500

- i. Press **Enter** to continue.
- j. From the Configure Parameters menu, select the `Commit Changes` option to save the changes.
- k. Exit the menu.

= Considerations for SAN configurations in a MetroCluster environment

:icons: font

:relative\_path: ./san-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You must be aware of certain considerations when using SAN configurations in a MetroCluster environment.

- MetroCluster configurations do not support front-end FC fabric “routed” vSAN configurations.
- MetroCluster configurations do not support front-end NVMe host connectivity.
- Other SAN protocols are supported on MetroCluster configurations.
- When using SAN client configurations, you must check whether any special considerations for MetroCluster configurations are included in the notes that are provided in the Interoperability Matrix Tool (IMT).
- Operating systems and applications must provide an I/O resiliency of 120 seconds to support MetroCluster automatic unplanned switchover and Tiebreaker or Mediator-initiated switchover.
- The MetroCluster is using the same WWPNs on both sides of the front-end SAN.



During switchover, the FC port on the surviving site might log in to the fabric before the fabric has detected that the FC port on the disaster site is offline and has removed this port from the name and directory services. If the FC port on the disaster is not yet removed, the fabric login attempt of the FC port at the surviving site might be rejected due to a duplicate WWPN. This behavior of the FC switches can be changed to honor the login of the previous device and not the existing one. You should verify the effects of this behavior on other fabric devices. Contact the switch vendor for more information.

To learn more, see:

- [Understanding MetroCluster data protection and disaster recovery](#)
- [Performing switchover for tests or maintenance](#)

### Steps

To avoid overlap when the old port goes offline and the new port comes online, use the following steps to configure the front-end switches:

For a...	Use these steps:
----------	------------------

Cisco switch

1. Connect to the switch and log in.
2. Enter configuration mode:

```
switch# config t  
switch(config)#
```

3. Overwrite the first device entry in the name server database with the new device:

```
switch(config)# no fcns reject-duplicate-pwvn vsan 1
```

4. In switches that are running NX-OS 8.x, confirm that the flogi quiesce timeout is set to zero:

- a. Display the quiesce timerval:

```
switch(config)# show flogi interval info | i quiesce
```

```
Stats: fs flogi quiesce timerval: 0
```

- b. If the output in the previous step does not indicate that the timerval is zero, then set it to zero:

```
switch(config)# flogi scale enable
```

```
switch(config)$ flogi quiesce timeout 0
```

## Brocade switch

1. Connect to the switch and log in.
2. Enter the `switchDisable` command.
3. Enter the `configure` command, and press `y` at the prompt.

```
F-Port login parameters (yes, y, no, n): [no] y
```

4. Choose setting 1:

```
- 0: First login take precedence over the second  
login (default)  
- 1: Second login overrides first login.  
- 2: the port type determines the behavior  
Enforce FLOGI/FDISC login: (0..2) [0] 1
```

5. Respond to the remaining prompts, or press **Ctrl + D**.
6. Enter the `switchEnable` command.

For further MetroCluster-specific host information, refer to the following NetApp Knowledge Base articles:

[What are AIX Host support considerations in a MetroCluster configuration?](#)

[Solaris host support considerations in a MetroCluster configuration](#)

### Related information

[NetApp Interoperability Matrix Tool](#)

= S3 object storage management

:hardbreaks:

:linkattrs:

:relative\_path: ./object-storage-management/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

= S3 configuration

= S3 configuration overview

:icons: font

:relative\_path: ./s3-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

Beginning with ONTAP 9.8, you can enable an ONTAP Simple Storage Service (S3) object storage server in an ONTAP cluster.

ONTAP supports two on-premises use case scenarios for serving S3 object storage:

- FabricPool tier to a bucket on local cluster (tier to a local bucket) or remote cluster (cloud tier).
- S3 client app access to a bucket on the local cluster or a remote cluster.

You should use these procedures if you want to configure S3 object storage in the following way:

- You want to provide S3 object storage from an existing cluster running ONTAP.

ONTAP S3 is appropriate if you want S3 capabilities on existing clusters without additional hardware and management. For deployments larger than 300TB, NetApp StorageGRID software continues to be the NetApp flagship solution for object storage. For more information, see the [StorageGRID documentation](#).

- You have cluster administrator privileges, not SVM administrator privileges.

== S3 configuration with System Manager and the ONTAP CLI

You can configure and manage ONTAP S3 with System Manager and the ONTAP CLI. When you enable S3 and create buckets using System Manager, ONTAP selects best-practice defaults for simplified configuration. If you need to specify configuration parameters, you might want to use the ONTAP CLI. If you configure the S3 server and buckets from the CLI, you can still manage them with System Manager if desired, or vice-versa.

When you create an S3 bucket using System Manager, ONTAP configures a default performance service level that is the highest available on your system. For example, on an AFF system, the default setting would be **Extreme**. Performance service levels are predefined adaptive Quality of Service (QoS) policy groups. Instead of one of the default service levels, you can specify a custom QoS policy group or no policy group.

Predefined adaptive QoS policy groups are:

- **Extreme**: Used for applications that expect the lowest latency and highest performance.
- **Performance**: Used for applications with modest performance needs and latency.
- **Value**: Used for applications for which throughput and capacity are more important than latency.
- **Custom**: Specify a custom QoS policy or no QoS policy.

If you select **Use for tiering**, no performance service levels are selected, and the system tries to select low-cost media with optimal performance for the tiered data.

See also: [Use adaptive QoS policy groups](#).

ONTAP tries to provision this bucket on local tiers that have the most appropriate disks, satisfying the chosen service level. However, if you need to specify which disks to include in the bucket, consider configuring S3 object storage from the CLI by specifying the local tiers (aggregate). If you configure the S3 server from the CLI, you can still manage it with System Manager if desired.

If you want the ability to specify which aggregates are used for buckets, you can only do so using the CLI.

== Configuring S3 buckets on Cloud Volumes ONTAP

If you want to serve buckets from Cloud Volumes ONTAP, it is strongly recommended that you manually select the underlying aggregates to ensure that they are using one node only. Using aggregates from both nodes can impact performance, because the nodes will be in geographically separated availability zones and hence susceptible to latency issues. Therefore, in Cloud Volumes ONTAP environments, you should [configure S3 buckets from the CLI](#).

Otherwise, S3 servers on Cloud Volumes ONTAP are configured and maintained the same in Cloud Volumes ONTAP as in on-premises environments.



= S3 support in ONTAP 9

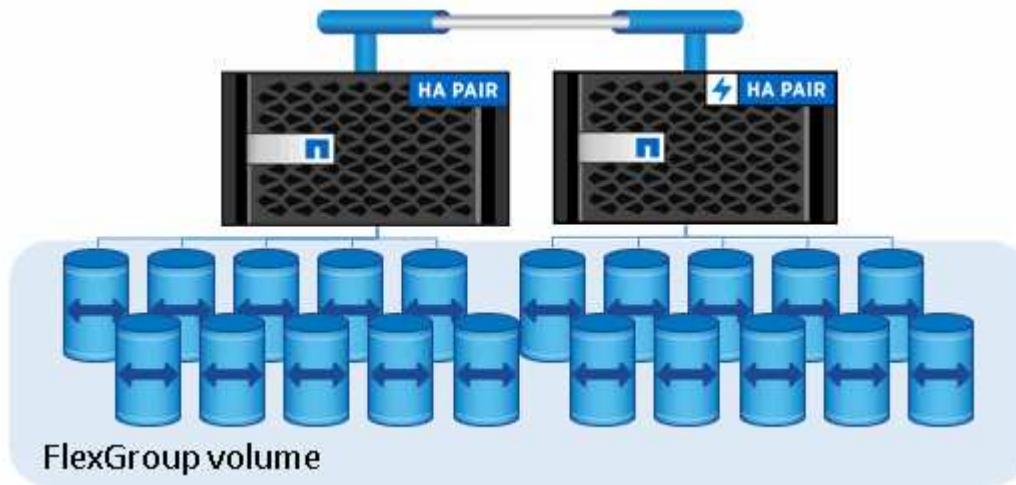
= ONTAP S3 architecture and use cases

:icons: font

:relative\_path: ./s3-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

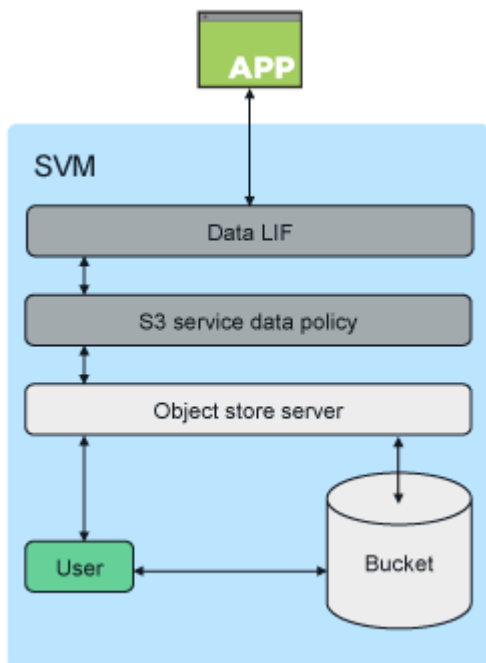
In ONTAP, the underlying architecture for a bucket is a FlexGroup volume—a single namespace that is made up of multiple constituent member volumes but is managed as a single volume.



Buckets are only limited by the physical maximums of the underlying hardware, architectural maximums could be higher. Buckets can take advantage of FlexGroup elastic sizing to automatically grow a constituent of a FlexGroup volume if it is running out of space. There is a limit of 1000 buckets per FlexGroup volume, or 1/3 of the FlexGroup volume's capacity (to account for data growth in buckets).

No NAS or SAN protocol access is permitted to the FlexGroup volume that contain S3 buckets.

Access to the bucket is provided through authorized users and client applications.



There are three primary use cases for client access to ONTAP S3 services:

- For ONTAP systems using ONTAP S3 as a remote FabricPool capacity (cloud) tier

The S3 server and bucket containing the capacity tier (for *cold* data) is on a different cluster than the performance tier (for *hot* data).

- For ONTAP systems using ONTAP S3 as a local FabricPool tier

The S3 server and bucket containing the capacity tier is on the same cluster, but on a different HA pair, as the performance tier.

- For external S3 client apps

ONTAP S3 serves S3 client apps run on non-NetApp systems.

It is a best practice to provide access to ONTAP S3 buckets using HTTPS. When HTTPS is enabled, security certificates are required for proper integration with SSL/TLS. Client users' access and secret keys are then required to authenticate the user with ONTAP S3 as well as authorizing the users' access permissions for operations within ONTAP S3. The client application should also have access to the root CA certificate (the ONTAP S3 server's signed certificate) to be able to authenticate the server and create a secure connection between client and server.

Users are created within the S3-enabled SVM, and their access permissions can be controlled at the bucket or SVM level; that is, they can be granted access to one or more buckets within the SVM.

HTTPS is enabled by default on ONTAP S3 servers. It is possible to disable HTTPS and enable HTTP for client access, in which case authentication using CA certificates is not required. However, when HTTP is enabled and HTTPS is disabled, all communication with the ONTAP S3 server are sent over the network in clear text.

For additional information, see [Technical Report: S3 in ONTAP Best Practices](#)

## Related information

### [FlexGroup volumes management](#)

= ONTAP version support for S3 object storage

:icons: font

:relative\_path: ./s3-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

ONTAP supports S3 object storage for on-premises environments beginning with ONTAP 9.8. Cloud Volumes ONTAP supports S3 object storage for cloud environments beginning with ONTAP 9.9.1.

== S3 support with Cloud Volumes ONTAP

ONTAP S3 is configured and functions the same in Cloud Volumes ONTAP as in on-premises environments, with one exception:

- Underlying aggregates should be from one node only. Learn more about [bucket creation in CVO environments](#).

Cloud Provider	ONTAP Version
Azure	ONTAP 9.9.1 and later
AWS	ONTAP 9.11.0 and later
Google Cloud	Not currently supported

== S3 public preview in ONTAP 9.7

In ONTAP 9.7, S3 object storage was introduced as a public preview. That version was not intended for production environments and will no longer be updated as of ONTAP 9.8. Only ONTAP 9.8 and later releases support S3 object storage in production environments.

S3 buckets created with the 9.7 public preview can be used in ONTAP 9.8 and later, but cannot take advantage of feature enhancements. If you have buckets created with the 9.7 public preview, you should migrate the contents of those buckets to 9.8 buckets for feature support, security, and performance enhancements.

= ONTAP S3 supported actions

:icons: font

:relative\_path: ./s3-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

== Bucket operations

Actions marked with an asterisk are supported by ONTAP, not S3 REST APIs

- CreateBucket (beginning with ONTAP 9.11.1)
- DeleteBucket\* (supported with S3 REST APIs beginning with ONTAP 9.11.1)
- DeleteBucketPolicy\*

- GetBucketAcl
- HeadBucket
- ListBuckets
- PutBucket\*

== Object operations

Beginning with ONTAP 9.9.1, ONTAP S3 supports object metadata and tagging.

- PutObject and CreateMultipartUpload now include key-value pairs using `x-amz-meta-<key>`.

For example: `x-amz-meta-project: ontap_s3`.

- GetObject. and HeadObject now return user-defined metadata.
- Unlike metadata, tags can be read independently of objects using:
  - PutObjectTagging
  - GetObjectTagging
  - DeleteObjectTagging

Beginning with ONTAP 9.11.1, ONTAP S3 supports object versioning and associated actions with these ONTAP APIs:

- PutBucketVersioning
- GetBucketVersioning
- ListBucketVersions

Supported object actions:

- AbortMultipartUpload
- CompleteMultipartUpload
- CreateMultipartUpload
- DeleteObject
- DeleteObjects (supported with S3 REST APIs beginning with ONTAP 9.11.1)
- DeleteObjectTagging (beginning with ONTAP 9.9.1)
- GetBucketVersioning (beginning with ONTAP 9.11.1)
- GetObject
- GetObjectAcl
- GetObjectTagging (beginning with ONTAP 9.9.1)
- HeadObject
- ListMultipartUpload
- ListObjects
- ListObjectsV2
- ListBucketVersions (beginning with ONTAP 9.11.1)

- ListParts
- PutBucketVersioning (beginning with ONTAP 9.11.1)
- PutObject
- PutObjectTagging (beginning with ONTAP 9.9.1)
- UploadPart

== Group policies

These operations are not specific to S3 and are generally associated with Identity and Management (IAM) processes. ONTAP supports these commands but does not use the IAM REST APIs.

- Create Policy
- AttachGroup Policy

== User management

These operations are not specific to S3 and are generally associated with IAM processes.

- CreateUser
- DeleteUser
- CreateGroup
- DeleteGroup

= ONTAP S3 interoperability

:icons: font

:relative\_path: ./s3-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

The ONTAP S3 server interacts normally with other ONTAP functionality except as noted in this table.

Feature area	Supported	Not supported
Cloud Volumes ONTAP	<ul style="list-style-type: none"> <li>• Azure clients in ONTAP 9.9.1 and later releases</li> <li>• AWS clients in ONTAP 9.11.0 and later releases</li> </ul>	<ul style="list-style-type: none"> <li>• Cloud Volumes ONTAP for any client in ONTAP 9.8 and earlier releases</li> <li>• Google Cloud clients</li> </ul>

Feature area	Supported	Not supported
Data protection	<ul style="list-style-type: none"> <li>• Cloud Sync</li> <li>• <a href="#">Object versioning</a> (beginning with ONTAP 9.11.1)</li> <li>• <a href="#">S3 SnapMirror</a> (beginning with ONTAP 9.10.1)</li> </ul>	<ul style="list-style-type: none"> <li>• Erasure coding</li> <li>• Information lifecycle management</li> <li>• MetroCluster</li> <li>• NDMP</li> <li>• SMTape</li> <li>• SnapLock</li> <li>• SnapMirror Cloud</li> <li>• SVM disaster recovery</li> <li>• SyncMirror</li> <li>• User-created Snapshot copies</li> <li>• WORM</li> </ul>
Encryption	<ul style="list-style-type: none"> <li>• NetApp Aggregate Encryption (NAE)</li> <li>• NetApp Volume Encryption (NVE)</li> <li>• NetApp Storage Encryption (NSE)</li> <li>• TLS/SSL</li> </ul>	<ul style="list-style-type: none"> <li>• SLAG</li> </ul>
Storage efficiency	<ul style="list-style-type: none"> <li>• Deduplication</li> <li>• Compression</li> <li>• Compaction</li> </ul>	<ul style="list-style-type: none"> <li>• Aggregate-level efficiencies</li> <li>• Volume clone of the FlexGroup volume containing ONTAP S3 buckets</li> </ul>
Storage virtualization	-	NetApp FlexArray Virtualization
Quality of service (QoS)	<ul style="list-style-type: none"> <li>• QoS maximums (ceilings)</li> <li>• QoS minimums (floors)</li> </ul>	-
Additional features	<ul style="list-style-type: none"> <li>• <a href="#">Audit S3 events</a> (beginning with ONTAP 9.10.1)</li> </ul>	<ul style="list-style-type: none"> <li>• FlexCache volumes</li> <li>• FPolicy</li> <li>• Qtrees</li> <li>• Quotas</li> </ul>

= About the S3 configuration process

= S3 configuration workflow

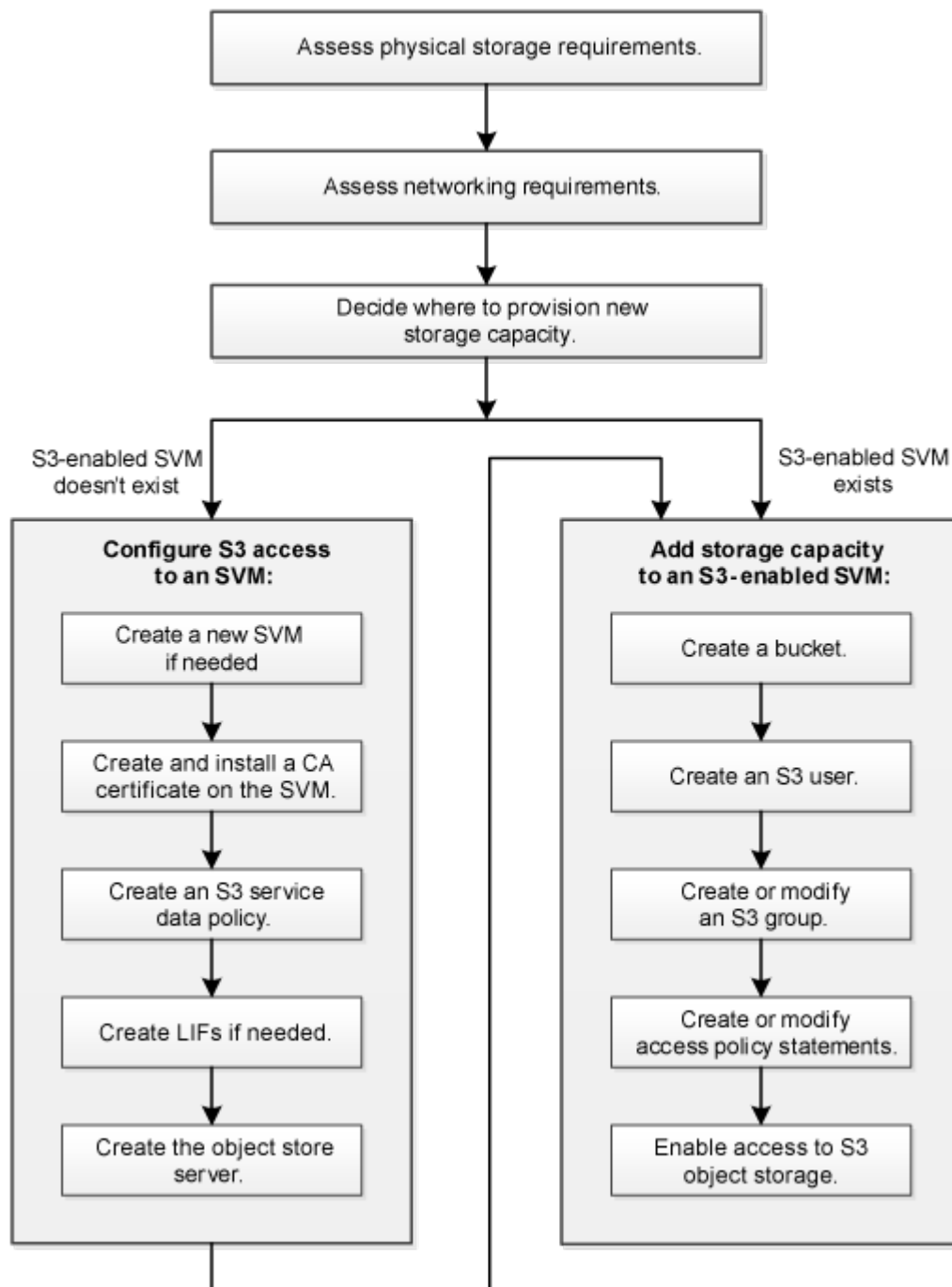
:icons: font

:relative\_path: ./s3-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

Configuring S3 involves assessing physical storage and networking requirements, and then choosing a workflow that is specific to your goal—configuring S3 access to a new or existing SVM, or adding a bucket and users to an existing SVM that is already fully configured for S3 access.

When you configure S3 access to a new storage VM using System Manager, you are prompted to enter certificate and networking information, and the storage VM and S3 object storage server are created in a single operation.



```
= Assess physical storage requirements
:icons: font
:relative_path: ./s3-config/
:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/
```

Before provisioning S3 storage for clients, you must ensure that there is sufficient space in existing aggregates for the new object store. If there is not, you can add disks to existing aggregates or create new aggregates of the desired type and location.

### About this task

When you create an S3 bucket in an S3-enabled SVM, a FlexGroup volume is automatically created to support the bucket. You can let ONTAP select the underlying aggregates and FlexGroup components automatically (the default) or you can select the underlying aggregates and FlexGroup components yourself.

If you decide to specify the aggregates and FlexGroup components — for example, if you have specific performance requirements for the underlying disks — you should make sure that your aggregate configuration conforms to best practice guidelines for provisioning a FlexGroup volume. Learn more:

- [FlexGroup volumes management](#)
- [NetApp Technical Report 4571-a: NetApp ONTAP FlexGroup Volume Top Best Practices](#)

If you are serving buckets from Cloud Volumes ONTAP, it is strongly recommended that you manually select the underlying aggregates to ensure that they are using one node only. Using aggregates from both nodes can impact performance, because the nodes will be in geographically separated availability zones and hence susceptible to latency issues. Learn about [creating buckets for Cloud Volumes ONTAP](#).

You can use the ONTAP S3 server to create a local FabricPool capacity tier; that is, in the same cluster as the performance tier. This can be useful, for example, if you have SSD disks attached to one HA pair and you want to tier *cold* data to HDD disks in another HA pair. In this use case, the S3 server and the bucket containing the local capacity tier should therefore be in a different HA pair than the performance tier. Local tiering is not supported on one-node and two-node clusters.

### Steps

1. Display available space in existing aggregates:

```
storage aggregate show
```

If there is an aggregate with sufficient space or requisite node location, record its name for your S3 configuration.



```

cluster-1::> storage aggregate show
Aggregate      Size Available Used% State  #Vols  Nodes  RAID Status
-----
aggr_0        239.0GB   11.13GB   95% online    1 node1  raid_dp,
normal
aggr_1        239.0GB   11.13GB   95% online    1 node1  raid_dp,
normal
aggr_2        239.0GB   11.13GB   95% online    1 node2  raid_dp,
normal
aggr_3        239.0GB   11.13GB   95% online    1 node2  raid_dp,
normal
aggr_4        239.0GB   238.9GB   95% online    5 node3  raid_dp,
normal
aggr_5        239.0GB   239.0GB   95% online    4 node4  raid_dp,
normal

6 entries were displayed.

```

2. If there are no aggregates with sufficient space or requisite node location, add disks to an existing aggregate by using the `storage aggregate add-disks` command, or create a new aggregate by using the `storage aggregate create` command.

= Assess networking requirements

:icons: font

:relative\_path: ./s3-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

Before providing S3 storage to clients, you must verify that networking is correctly configured to meet the S3 provisioning requirements.

### What you'll need

The following cluster networking objects must be configured:

- Physical and logical ports
- Broadcast domains
- Subnets (if required)
- IPspaces (as required, in addition to the default IPspace)
- Failover groups (as required, in addition to the default failover group for each broadcast domain)
- External firewalls

### About this task

For remote FabricPool capacity (cloud) tiers and remote S3 clients, you must use a data SVM and configure data LIFs. For FabricPool cloud tiers, you must also configure intercluster LIFs; cluster peering is not required.

For local FabricPool capacity tiers, you must use the system SVM (called "Cluster"), but you have two options for LIF configuration:

- You can use the cluster LIFs.

In this option, no further LIF configuration is required, but there will be an increase in traffic on the cluster LIFs. Also, the local tier will not be accessible to other clusters.

- You can use data and intercluster LIFs.

This option requires additional configuration, including enabling the LIFs for the S3 protocol, but the local tier will also be accessible as a remote FabricPool cloud tier to other clusters.

## Steps

1. Display the available physical and virtual ports:

```
network port show
```

- When possible, you should use the port with the highest speed for the data network.
  - All components in the data network must have the same MTU setting for best performance.
2. If you are planning to use a subnet name to allocate the IP address and network mask value for a LIF, verify that the subnet exists and has sufficient addresses available:

```
network subnet show
```

Subnets contain a pool of IP addresses that belong to the same layer 3 subnet. Subnets are created by using the `network subnet create` command.

3. Display available IPspaces:

```
network ipspace show
```

You can use the default IPspace or a custom IPspace.

4. If you want to use IPv6 addresses, verify that IPv6 is enabled on the cluster:

```
network options ipv6 show
```

If required, you can enable IPv6 by using the `network options ipv6 modify` command.

= Decide where to provision new S3 storage capacity

:icons: font

:relative\_path: ./s3-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

Before you create a new S3 bucket, you must decide whether to place it in a new or existing SVM. This decision determines your workflow.

## Choices

- If you want to provision a bucket in a new SVM or an SVM that is not enabled for S3, complete the steps in the following topics.

[Create an SVM for S3](#)

[Create a bucket for S3](#)

Although S3 can coexist in an SVM with NFS and SMB, you might choose to create a new SVM if one of the following is true:

- You are enabling S3 on a cluster for the first time.
- You have existing SVMs in a cluster in which you do not want to enable S3 support.
- You have one or more S3-enabled-SVMs in a cluster, and you want another S3 server with different performance characteristics.  
After enabling S3 on the SVM, proceed to provision a bucket.
- If you want to provision the initial bucket or an additional bucket on an existing S3-enabled SVM, complete the steps in the following topic.

### Create a bucket for S3

= Configure S3 access to an SVM

= Create an SVM for S3

:icons: font

:relative\_path: ./s3-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

Although S3 can coexist in an SVM with other protocols, you might want to create a new SVM to isolate the namespace and workload.

#### About this task

If you are only providing S3 object storage from this SVM, the S3 server does not require any DNS configuration. However, you might want to configure DNS on the SVM if other protocols are used.

When you configure S3 access to a new storage VM using System Manager, you are prompted to enter certificate and networking information, and the storage VM and S3 object storage server are created in a single operation.

## CLI

1. Verify that S3 is licensed on your cluster:

```
system license show -package s3
```

If it is not, contact your sales representative.

2. Create an SVM:

```
vserver create -vserver svm_name -rootvolume root_volume_name -aggregate  
aggregate_name -rootvolume-security-style unix -language C.UTF-8 -ip  
ipspace_name
```

- Use the UNIX setting for the `-rootvolume-security-style` option.
- Use the default `C.UTF-8` `-language` option.
- The `ipspace` setting is optional.

3. Verify the configuration and status of the newly created SVM:

```
vserver show -vserver svm_name
```

The `Vserver Operational State` field must display the `running` state. If it displays the `initializing` state, it means that some intermediate operation such as root volume creation failed, and you must delete the SVM and re-create it.

## Examples

The following command creates an SVM for data access in the IPspace `ipSpaceA`:

```
cluster-1::> vserver create -vserver svm1.example.com -rootvolume  
root_svm1 -aggregate aggr1 -rootvolume-security-style unix -language  
C.UTF-8 -ipSpace ipSpaceA
```

```
[Job 2059] Job succeeded:  
Vserver creation completed
```

The following command shows that an SVM was created with a root volume of 1 GB, and it was started automatically and is in `running` state. The root volume has a default export policy that does not include any rules, so the root volume is not exported upon creation. By default, the `vsadmin` user account is created and is in the `locked` state. The `vsadmin` role is assigned to the default `vsadmin` user account.

```

cluster-1::> vserver show -vserver svml.example.com
                Vserver: svml.example.com
                Vserver Type: data
                Vserver Subtype: default
                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                Root Volume: root_svml
                Aggregate: aggr1
                NIS Domain: -
                Root Volume Security Style: unix
                LDAP Client: -
                Default Volume Language Code: C.UTF-8
                Snapshot Policy: default
                Comment:
                Quota Policy: default
                List of Aggregates Assigned: -
                Limit on Maximum Number of Volumes allowed: unlimited
                Vserver Admin State: running
                Vserver Operational State: running
                Vserver Operational State Stopped Reason: -
                Allowed Protocols: nfs, cifs
                Disallowed Protocols: -
                QoS Policy Group: -
                Config Lock: false
                IPspace Name: ipspaceA

```

## System Manager

You should be prepared to enter the S3 server name as a Fully Qualified Domain Name (FQDN), which clients will use for S3 access. The S3 server FQDN must not begin with a bucket name.


You should be prepared to enter IP addresses for interface role Data.

If you are using an external-CA signed certificate, you will be prompted to enter it during this procedure; you also have the option to use a system-generated certificate.

### 1. Enable S3 on a storage VM.

- a. Add a new storage VM: click **Storage > Storage VMs**, then click **Add**.

If this is a new system with no existing storage VMs: click **Dashboard > Configure Protocols**.

If you are adding an S3 server to an existing storage VM: click **Storage > Storage VMs**, select a storage VM, click **Settings**, and then click  under **S3**.

- b. Click **Enable S3**, then enter the S3 Server Name.

- c. Select the certificate type.

Whether you select system-generated certificate or one of your own, it will be required for client access.

- d. Enter the network interfaces.
2. If you selected the system-generated certificate, you see the certificate information when the new storage VM creation is confirmed. Click **Download** and save it for client access.
- The secret key will not be displayed again.
  - If you need the certificate information again: click **Storage > Storage VMs**, select the storage VM, and click **Settings**.

= Create and install a CA certificate on the SVM

:icons: font

:relative\_path: ./s3-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

A Certificate Authority (CA) certificate is required to enable HTTPS traffic from S3 clients to the S3-enabled SVM.

### About this task

Although it is possible to configure an S3 server to use HTTP only, and although it is possible to configure clients without a CA certificate requirement, it is a best practice to secure HTTPS traffic to ONTAP S3 servers with a CA certificate.

A CA certificate is not necessary for a local tiering use case, where IP traffic is going over cluster LIFs only.

The instructions in this procedure will create and install an ONTAP self-signed certificate. CA certificates from third-party vendors are also supported; see the administrator authentication documentation for more information.

### Administrator authentication and RBAC

See the `security certificate` man pages for additional configuration options.

### Steps

1. Create a self-signed digital certificate:

```
security certificate create -vserver svm_name -type root-ca -common-name ca_cert_name
```

The `-type root-ca` option creates and installs a self-signed digital certificate to sign other certificates by acting as a certificate authority (CA).

The `-common-name` option creates the SVM's Certificate Authority (CA) name and will be used when generating the certificate's complete name.

The default certificate size is 2048 bits.

### Example

```
cluster-1::> security certificate create -vserver svm1.example.com  
-type root-ca -common-name svm1_ca
```

The certificate's generated name for reference:

```
svm1_ca_159D1587CE21E9D4_svm1_ca
```

When the certificate's generated name is displayed; be sure to save it for later steps in this procedure.

2. Generate a certificate signing request:

```
security certificate generate-csr -common-name s3_server_name  
[additional_options]
```

The `-common-name` parameter for the signing request must be the S3 server name (FQDN).

You can provide the location and other detailed information about the SVM if desired.

You are prompted to keep a copy of your certificate request and private key for future reference.

3. Sign the CSR using SVM\_CA to generate S3 Server's certificate:

```
security certificate sign -vserver svm_name -ca ca_cert_name -ca-serial  
ca_cert_serial_number [additional_options]
```

Enter the command options that you used in previous steps:

- `-ca` — the common name of the CA that you entered in Step 1.
- `-ca-serial` — the CA serial number from Step 1. For example, if the CA certificate name is `svm1_ca_159D1587CE21E9D4_svm1_ca`, the serial number is `159D1587CE21E9D4`.

By default, the signed certificate will expire in 365 days. You can select another value, and specify other signing details.

When prompted, copy and enter the certificate request string you saved in Step 2.

A signed certificate is displayed; save it for later use.

4. Install the signed certificate on the S3-enabled SVM:

```
security certificate install -type server -vserver svm_name
```

When prompted, enter the certificate and private key.

You have the option to enter intermediate certificates if a certificate chain is desired.

When the private key and the CA-signed digital certificate are displayed; save them for future reference.

5. Get the public key certificate:

```
security certificate show -vserver svm_name -common-name ca_cert_name -type  
root-ca -instance
```

Save the public key certificate for later client-side configuration.

Example



```

cluster-1::> security certificate show -vserver svml.example.com
-common-name svml_ca -type root-ca -instance

                Name of Vserver: svml.example.com
                FQDN or Custom Common Name: svml_ca
                Serial Number of Certificate: 159D1587CE21E9D4
                Certificate Authority: svml_ca
                Type of Certificate: root-ca
                (DEPRECATED)-Certificate Subtype: -
                Unique Certificate Name:
svml_ca_159D1587CE21E9D4_svml_ca
                Size of Requested Certificate in Bits: 2048
                Certificate Start Date: Thu May 09 10:58:39 2020
                Certificate Expiration Date: Fri May 08 10:58:39 2021
                Public Key Certificate: -----BEGIN CERTIFICATE-----
MIIDZ ...==
-----END CERTIFICATE-----

                Country Name: US
                State or Province Name:
                Locality Name:
                Organization Name:
                Organization Unit:
                Contact Administrator's Email Address:
                Protocol: SSL
                Hashing Function: SHA256
                Self-Signed Certificate: true
                Is System Internal Certificate: false

```

= Create an S3 service data policy

:icons: font

:relative\_path: ./s3-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You can create service policies for S3 data and management services. An S3 service data policy is required to enable S3 data traffic on LIFs.

#### About this task

An S3 service data policy is required if you are using data LIFs and intercluster LIFs. It is not required if you are using cluster LIFs for the local tiering use case.

When a service policy is specified for a LIF, the policy is used to construct a default role, failover policy, and data protocol list for the LIF.

Although multiple protocols can be configured for SVMs and LIFs, it is a best practice for S3 to be the only protocol when serving object data.

#### Steps

## 1. Change the privilege setting to advanced:

```
set -privilege advanced
```

## 2. Create a service data policy:

```
network interface service-policy create -vserver svm_name -policy  
policy_name -services data-core,data-s3-server
```

The `data-core` and `data-s3-server` services are the only ones required to enable ONTAP S3, although other services can be included as needed.

= Create data LIFs

:icons: font

:relative\_path: ./s3-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

If you created a new SVM, the dedicated LIFs you create for S3 access should be data LIFs.

### What you'll need

- The underlying physical or logical network port must have been configured to the administrative up status.
- If you are planning to use a subnet name to allocate the IP address and network mask value for a LIF, the subnet must already exist.

Subnets contain a pool of IP addresses that belong to the same layer 3 subnet. They are created using the `network subnet create` command.

- The LIF service policy must already exist.

### About this task

- You can create both IPv4 and IPv6 LIFs on the same network port.
- If you have a large number of LIFs in your cluster, you can verify the LIF capacity supported on the cluster by using the `network interface capacity show` command and the LIF capacity supported on each node by using the `network interface capacity details show` command (at the advanced privilege level).
- If you are enabling remote FabricPool capacity (cloud) tiering, you must also configure intercluster LIFs.

### Steps

#### 1. Create a LIF:

```
network interface create -vserver svm_name -lif lif_name -service-policy  
service_policy_names -home-node node_name -home-port port_name {-address  
IP_address -netmask IP_address | -subnet-name subnet_name} -firewall-policy  
data -auto-revert {true|false}
```

- `-home-node` is the node to which the LIF returns when the `network interface revert` command is run on the LIF.

You can also specify whether the LIF should automatically revert to the home-node and home-port with the `-auto-revert` option.

- `-home-port` is the physical or logical port to which the LIF returns when the `network interface revert` command is run on the LIF.
- You can specify an IP address with the `-address` and `-netmask` options, or you enable allocation from a subnet with the `-subnet_name` option.
- When using a subnet to supply the IP address and network mask, if the subnet was defined with a gateway, a default route to that gateway is added automatically to the SVM when a LIF is created using that subnet.
- If you assign IP addresses manually (without using a subnet), you might need to configure a default route to a gateway if there are clients or domain controllers on a different IP subnet. The `network route create man` page contains information about creating a static route within an SVM.
- For the `-firewall-policy` option, use the same default data as the LIF role.

You can create and add a custom firewall policy later if desired.

- `-auto-revert` allows you to specify whether a data LIF is automatically reverted to its home node under circumstances such as startup, changes to the status of the management database, or when the network connection is made. The default setting is `false`, but you can set it to `false` depending on network management policies in your environment.
  - The `-service-policy` option specifies the data and management services policy you created and any other policies you need.
2. If you want to assign an IPv6 address in the `-address` option:

- a. Use the `network ndp prefix show` command to view the list of RA prefixes learned on various interfaces.

The `network ndp prefix show` command is available at the advanced privilege level.

- b. Use the format `prefix:id` to construct the IPv6 address manually.

`prefix` is the prefix learned on various interfaces.

For deriving the `id`, choose a random 64-bit hexadecimal number.

3. Verify that the LIF was created successfully by using the `network interface show` command.
4. Verify that the configured IP address is reachable:

To verify an...	Use...
IPv4 address	<code>network ping</code>
IPv6 address	<code>network ping6</code>

## Examples

The following command shows how to create an S3 data LIF that is assigned with the `my-S3-policy`

service policy:

```
network interface create -vserver svml.example.com -lif lif2 -home-node
node2 -homeport e0d -service-policy my-S3-policy -subnet-name ipspacel
```

The following command shows all the LIFs in cluster-1. Data LIFs datalif1 and datalif3 are configured with IPv4 addresses, and datalif4 is configured with an IPv6 address:

```
cluster-1::> network interface show
```

Is	Logical	Status	Network	Current	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----
----					
cluster-1					
true	cluster_mgmt	up/up	192.0.2.3/24	node-1	e1a
node-1					
true	clus1	up/up	192.0.2.12/24	node-1	e0a
true	clus2	up/up	192.0.2.13/24	node-1	e0b
true	mgmt1	up/up	192.0.2.68/24	node-1	e1a
node-2					
true	clus1	up/up	192.0.2.14/24	node-2	e0a
true	clus2	up/up	192.0.2.15/24	node-2	e0b
true	mgmt1	up/up	192.0.2.69/24	node-2	e1a
vs1.example.com					
true	datalif1	up/down	192.0.2.145/30	node-1	e1c
vs3.example.com					
true	datalif3	up/up	192.0.2.146/30	node-2	e0c
true	datalif4	up/up	2001::2/64	node-2	e0c

5 entries were displayed.

= Create intercluster LIFs for remote FabricPool tiering

:icons: font

```
:relative_path: ./s3-config/
```

```
:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/
```

If you are enabling remote FabricPool capacity (cloud) tiering using ONTAP S3, you must configure intercluster LIFs. You can configure intercluster LIFs on ports shared with the data network. Doing so reduces the number of ports you need for intercluster networking.

#### What you'll need

- The underlying physical or logical network port must have been configured to the administrative up status.
- The LIF service policy must already exist.

#### About this task

Intercluster LIFs are not required for local Fabric pool tiering or for serving external S3 apps.

#### Steps

1. List the ports in the cluster:

```
network port show
```

The following example shows the network ports in `cluster01`:

```
cluster01::> network port show
```

(Mbps)					Speed
Node	Port	IPspace	Broadcast Domain	Link	MTU
Admin/Oper					
-----					
cluster01-01					
	e0a	Cluster	Cluster	up	1500
auto/1000					
	e0b	Cluster	Cluster	up	1500
auto/1000					
	e0c	Default	Default	up	1500
auto/1000					
	e0d	Default	Default	up	1500
auto/1000					
cluster01-02					
	e0a	Cluster	Cluster	up	1500
auto/1000					
	e0b	Cluster	Cluster	up	1500
auto/1000					
	e0c	Default	Default	up	1500
auto/1000					
	e0d	Default	Default	up	1500
auto/1000					

## 2. Create intercluster LIFs on the system SVM:

```
network interface create -vserver Cluster -lif LIF_name -service-policy  
default-intercluster -home-node node -home-port port -address port_IP  
-netmask netmask
```

The following example creates intercluster LIFs `cluster01_icl01` and `cluster01_icl02`:

```

cluster01::> network interface create -vserver Cluster -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver Cluster -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0

```

### 3. Verify that the intercluster LIFs were created:

```
network interface show -service-policy default-intercluster
```

```

cluster01::> network interface show -service-policy default-
intercluster

```

Current	Is	Logical	Status	Network	Current	
Vserver	Port	Home	Interface	Admin/Oper	Address/Mask	Node
cluster01	e0c	true	cluster01_icl01	up/up	192.168.1.201/24	cluster01-01
cluster01	e0c	true	cluster01_icl02	up/up	192.168.1.202/24	cluster01-02

### 4. Verify that the intercluster LIFs are redundant:

```
network interface show -service-policy default-intercluster -failover
```

The following example shows that the intercluster LIFs cluster01\_icl01 and cluster01\_icl02 on the e0c port will fail over to the e0d port.

```

cluster01::> network interface show -service-policy default-
intercluster -failover
          Logical          Home          Failover
Failover
Vserver  Interface          Node:Port          Policy          Group
-----  -----
cluster01
          cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                                     Failover Targets: cluster01-01:e0c,
                                                         cluster01-01:e0d
          cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                                     Failover Targets: cluster01-02:e0c,
                                                         cluster01-02:e0d

```

= Create the S3 object store server

:icons: font

:relative\_path: ./s3-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

The ONTAP object store server manages data as S3 objects, as opposed to file or block storage provided by ONTAP NAS and SAN servers.

### What you'll need

You should be prepared to enter the S3 server name as a Fully Qualified Domain Name (FQDN), which clients will use for S3 access. The FQDN must not begin with a bucket name.

You should have a self-signed CA certificate (created in previous steps) or a certificate signed by an external CA vendor. A CA certificate is not necessary for a local tiering use case, where IP traffic is going over cluster LIFs only.

### About this task

When an object store server is created, a root user with UID 0 is created. No access key or secret key is generated for this root user. The ONTAP administrator must run the `object-store-server users regenerate-keys` command to set the access key and secret key for this user.

As a NetApp best practice, do not use this root user. Any client application that uses the access key or secret key of the root user has full access to all buckets and objects in the object store.

See the `vserver object-store-server` man pages for additional configuration and display options.

## CLI

1. Create the S3 server:



```
vserver object-store-server create -vserver svm_name -object-store-server
s3_server_fqdn -certificate-name ca_cert_name -comment text
[additional_options]
```

You can specify additional options when creating the S3 server or at any time later.

- The SVM name can be either a data SVM or `Cluster` (the system SVM name) if you are configuring local tiering.
- HTTPS is enabled by default on port 443. You can change the port number with the `-secure -listener-port` option.

When HTTPS is enabled, CA certificates are required for proper integration with SSL/TLS.

- HTTP is disabled by default; when enabled, the server listens on port 80. You can enable it with the `-is-http-enabled` option or change the port number with the `-listener-port` option.

When HTTP is enabled, all the request and responses are sent over the network in clear text.

## 2. Verify that S3 is configured as desired:

```
vserver object-store-server show
```

### Example

The following command verifies the configuration values of all object storage servers:

```
cluster1::> vserver object-store-server show


Vserver: vs1

Object Store Server Name: s3.example.com
Administrative State: up
Listener Port For HTTP: 80
Secure Listener Port For HTTPS: 443
HTTP Enabled: false
HTTPS Enabled: true
Certificate for HTTPS Connections: svm1_ca
Comment: Server comment
```

### System Manager

Use this procedure if you are adding an S3 server to an existing storage VM. To add an S3 server to a new storage VM, see [Create a storage SVM for S3](#).

You should be prepared to enter IP addresses for interface role Data.

1. Enable S3 on an existing storage VM.
  - a. Select the storage VM: click **Storage > Storage VMs**, select a storage VM, click **Settings**, and then click  under **S3**.
  - b. Click **Enable S3**, then enter the S3 Server Name.

c. Select the certificate type.

Whether you select system-generated certificate or one of your own, it will be required for client access.

d. Enter the network interfaces.

2. If you selected the system-generated certificate, you see the certificate information when the new storage VM creation is confirmed. Click **Download** and save it for client access.
  - The secret key will not be displayed again.
  - If you need the certificate information again: click **Storage > Storage VMs**, select the storage VM, and click **Settings**.

= Add storage capacity to an S3-enabled SVM

= Create a bucket

:icons: font

:relative\_path: ./s3-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

S3 objects are kept in *buckets*--they are not nested as files inside a directory inside other directories.

### Before you begin

An SVM containing an S3 server must already exist.

### About this task

For the CLI, when you create a bucket, you have two provisioning options:

- Let ONTAP select the underlying aggregates and FlexGroup components (default)
  - ONTAP creates and configures a FlexGroup volume for the first bucket by automatically selecting the aggregates. It will automatically select the highest service level available for your platform, or you can specify the storage service level. Any additional buckets you add later in the SVM will have the same underlying FlexGroup volume.
  - Alternatively, you can specify whether the bucket will be used for tiering, in which case ONTAP tries to select low-cost media with optimal performance for the tiered data.
- You select the underlying aggregates and FlexGroup components (requires advanced privilege command options)
  - You have the option to manually select the aggregates on which the bucket and containing FlexGroup volume must be created, and then specifying the number of constituents on each aggregate. When adding additional buckets:
    - If you specify aggregates and constituents for a new bucket, a new FlexGroup will be created for the new bucket.
    - If you do not specify aggregates and constituents for a new bucket, the new bucket will be added to an existing FlexGroup.See [FlexGroup volumes management](#) for more information.

When you specify aggregates and constituents when creating a bucket, no QoS policy groups, default or custom, are applied. You can do so later with the `vserver object-store-server bucket modify` command.

**Note:** If you are serving buckets from Cloud Volumes ONTAP, you should use the CLI procedure. It is strongly recommended that you manually select the underlying aggregates to ensure that they are using one node only. Using aggregates from both nodes can impact performance, because the nodes will be in geographically separated availability zones and hence susceptible to latency issues.

Storage service levels are predefined adaptive Quality of Service (QoS) policy groups, with *value*, *performance*, and *extreme* default levels. Instead of one of the default storage service levels, you can also define a custom QoS policy group and apply it to a bucket.

Beginning with ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

## Storage service definitions

If you are configuring local capacity tiering, you create buckets and users in a data SVM, not in the system SVM where the S3 server is located.

For remote client access, you must configure buckets in an S3-enabled storage VM. If you create a bucket in a storage VM that is not S3-enabled, it will only be available for local tiering.

## Performance management

See the `vserver object-store-server bucket man` pages for additional configuration and display options.

== Process to create buckets

## CLI

1. If you plan to select aggregates and FlexGroup components yourself, set the privilege level to advanced (otherwise, admin privilege level is sufficient): `set -privilege advanced`
2. Create a bucket:

```
vserver object-store-server bucket create -vserver svm_name -bucket
bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

The SVM name can be either a data SVM or `Cluster` (the system SVM name) if you are configuring local tiering.

If you specify no options, ONTAP creates a 5GB bucket with the service level set to the highest level available for your system.

If you want ONTAP to create a bucket based on performance or usage, use one of the following options:

- service level

Include the `-storage-service-level` option with one of the following values: `value`, `performance`, or `extreme`.

- tiering

Include the `-used-as-capacity-tier true` option.

If you want to specify the aggregates on which to create the underlying FlexGroup volume, use the following options:

- The `-aggr-list` parameter specifies the list of aggregates to be used for FlexGroup volume constituents.

Each entry in the list creates a constituent on the specified aggregate. You can specify an aggregate multiple times to have multiple constituents created on the aggregate.

For consistent performance across the FlexGroup volume, all of the aggregates must use the same disk type and RAID group configurations.

- The `-aggr-list-multiplier` parameter specifies the number of times to iterate over the aggregates that are listed with the `-aggr-list` parameter when creating a FlexGroup volume.

The default value of the `-aggr-list-multiplier` parameter is 4.

### 3. Add a QoS policy group if needed:

```
vserver object-store-server bucket modify -bucket bucket_name -qos-policy  
-group qos_policy_group
```

### 4. Verify bucket creation:

```
vserver object-store-server bucket show [-instance]
```

## Example

The following example creates a bucket for SVM vs1 of size 1TB and specifying the aggregate:

```
cluster-1::*> vserver object-store-server bucket create -vserver  
svm1.example.com -bucket testbucket -aggr-list aggr1 -size 1TB
```

## System Manager

### 1. Add a new bucket on an S3-enabled storage VM.

a. Click **Storage > Buckets**, then click **Add**.

b. Enter a name, select the storage VM, and enter a size.

- If you click **Save** at this point, a bucket is created with these default settings:
  - No users are granted access to the bucket unless any group policies are already in effect.



You should not use the S3 root user to manage ONTAP object storage and share its permissions, because it has unlimited access to the object store. Instead, create a user or group with administrative privileges that you assign.

- A Quality of Service (performance) level that is the highest available for your system.
- You can click **More Options** to configure user permissions and performance level when you configure the bucket, or you can modify these settings later.
  - You must have already created user and groups before using **More Options** to configure their permissions.
  - If you intend to use the S3 object store for FabricPool tiering, consider selecting **Use for tiering** (use low-cost media with optimal performance for the tiered data) rather than a performance service level.

### 2. On S3 client apps – another ONTAP system or an external 3rd-party app – verify access to the new bucket by entering the following:

- The S3 server CA certificate.
- The user's access key and secret key.
- The S3 server FQDN name and bucket name.

= Create an S3 user

:icons: font

:relative\_path: ./s3-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

:hardbreaks-option:

User authorization is required on all ONTAP object stores in order to restrict connectivity to authorized clients.

#### **Before you begin.**

An S3-enabled SVM must already exist.

#### **About this task**

An S3 user can be granted access to any bucket in an SVM but not in multiple SVMs.

When you create an S3 user, an access-key and a secret-key will be generated. They must be shared with the user along with the object store's FQDN and bucket name. S3 users' keys can be displayed with the `vserver object-store-server user show` command.

You can grant specific access permissions to S3 users in a bucket policy or an object server policy.

When an object store server is created, a root user (UID 0) is created, a privileged user with access all buckets. Rather than administering ONTAP S3 as root user, it is a best practice to create an admin user role with specific privileges.


## **CLI**

1. Create an S3 user:

```
vserver object-store-server user create -vserver svm_name -user user_name [-comment text]
```

2. Be sure to save the access key and secret key, they will be required for access from S3 clients.

## **System Manager**

1. Edit the storage VM: click **Storage > storage VMs**, click the storage VM, click **Settings** and then click  under S3.
2. Add a user: click **Users**, then click **Add**.
3. Enter a name and click **Save**.
4. Be sure to save the access key and secret key, they will be required for access from S3 clients.

## Next steps

- [Create or modify S3 groups](#)

= Create or modify S3 groups

:icons: font

:relative\_path: ./s3-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

:hardbreaks-option:

You can simplify bucket access by creating groups of users with appropriate access authorizations.

## Before you begin

S3 users in an S3-enabled SVM must already exist.

## About this task

Users in an S3 group can be granted access to any bucket in an SVM but not in multiple SVMs. Group access permissions can be configured in two ways:

- At the bucket level

After creating a group of S3 users, you specify group permissions in bucket policy statements and they apply only to that bucket.

- At the SVM level

After creating a group of S3 users, you specify object server policy names in the group definition. Those policies determine the buckets and access for the group members.

## CLI


1. Create an S3 group:

```
vserver object-store-server group create -vserver svm_name -name group_name -users user_name\(s\) [-policies policy_names] [-comment text]
```

The `-policies` option can be omitted in configurations with only one bucket in an object store; the group name can be added to the bucket policy.

The `-policies` option can be added later with the `vserver object-store-server group modify` command after object storage server policies are created.

## System Manager

1. Edit the storage VM: click **Storage > storage VMs**, click the storage VM, click **Settings** and then click  under S3.
2. Add a group: select **Groups**, then select **Add**.
3. Enter a group name and select from a list of users.
4. You can select an existing group policy or add one now, or you can add a policy later.

= Create or modify access policy statements

= About bucket and object store server policies

:icons: font

:relative\_path: ./s3-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

User and group access to S3 resources is controlled by bucket and object store server policies. If you have a small number of users or groups, controlling access at the bucket level is probably sufficient, but if you have many users and groups, it is easier to control access at the object store server level.

= Modify a bucket policy

:icons: font

:relative\_path: ./s3-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You can add access rules to the default bucket policy. The scope of its access control is the containing bucket, so it is most appropriate when there is a single bucket.

### Before you begin

An S3-enabled SVM containing an S3 server and a bucket must already exist.

You must have already created users or groups before granting permissions.

### About this task

You can add new statements for new users and groups, or you can modify the attributes of existing statements. For more options, see the `vserver object-store-server bucket policy man` pages.

User and group permissions can be granted when the bucket is created or as needed later. You can also modify the bucket capacity and QoS policy group assignment.

Beginning with ONTAP 9.9.1 and later releases, if you plan to support AWS client object tagging functionality with the ONTAP S3 server, the actions `GetObjectTagging`, `PutObjectTagging`, and `DeleteObjectTagging` need to be allowed using the bucket or group policies.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

## System Manager

### Steps

1. Edit the bucket: click **Storage > Buckets**, click the desired bucket, and then click **Edit**.

When adding or modifying permissions, you can specify the following parameters:

- **Principal:** the user or group to whom access is granted.
- **Effect:** allows or denies access to a user or group.
- **Actions:** permissible actions in the bucket for a given user or group.
- **Resources:** paths and names of objects within the bucket for which access is granted or denied.

The defaults *bucketname* and *bucketname/\** grant access to all objects in the bucket. You can also



grant access to single objects; for example, *bucketname/\*\_readme.txt*.

- **Conditions** (optional): expressions that are evaluated when access is attempted. For example, you can specify a list of IP addresses for which access will be allowed or denied.

## CLI

### Steps

1. Add a statement to a bucket policy:

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid text]
[-index integer]
```

The following parameters define access permissions:

-effect	The statement may allow or deny access
-action	You can specify * to mean all actions, or a list of one or more of the following: GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, and ListMultipartUploadParts.
-principal	A list of one or more S3 users or groups. <ul style="list-style-type: none"><li>• A maximum of 10 users or groups can be specified.</li><li>• If an S3 group is specified, it must be in the form group/group_name.</li><li>• * can be specified to mean public access; that is, access without an access-key and secret-key.</li><li>• If no principal is specified, all S3 users in the SVM are granted access.</li></ul>
-resource	The bucket and any object it contains. The wildcard characters * and ? can be used to form a regular expression for specifying a resource.

You can optionally specify a text string as comment with the `-sid` option.

### Examples

The following example creates an object store server bucket policy statement for the SVM `svm1.example.com` and `bucket1` which specifies allowed access to a `readme` folder for object store server user `user1`.

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal user1 -resource
bucket1/readme/* -sid "fullAccessToReadmeForUser1"
```

The following example creates an object store server bucket policy statement for the SVM `svm1.example.com`

and bucket1 which specifies allowed access to all objects for object store server group group1.

```
cluster1::> vservers object-store-server bucket policy statement create
-vserver svml.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal group/group1
-resource bucket1/* -sid "fullAccessForGroup1"
```

= Create or modify an object store server policy

:icons: font

:relative\_path: ./s3-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You can create policies that can apply to one or more buckets in an object store. Object store server policies can be attached to groups of users, thereby simplifying the management of resource access across multiple buckets.

### Before you begin

An S3-enabled SVM containing an S3 server and a bucket must already exist.

### About this task

You can enable access policies at the SVM level by specifying a default or custom policy in an object storage server group. The policies do not take effect until they are specified in the group definition.



When you use object storage server policies, you specify principals (that is, users and groups) in the group definition, not in the policy itself.

There are three read-only default policies for access to ONTAP S3 resources:

- FullAccess
- NoS3Access
- ReadOnlyAccess

You can also create new custom policies, then add new statements for new users and groups, or you can modify the attributes of existing statements. For more options, see the `vservers object-store-server policy` [command reference](#).

Beginning with ONTAP 9.9.1 and later releases, if you plan to support AWS client object tagging functionality with the ONTAP S3 server, the actions `GetObjectTagging`, `PutObjectTagging`, and `DeleteObjectTagging` need to be allowed using the bucket or group policies.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

## System Manager

### Use System Manager to create or modify an object store server policy

#### Steps

1. Edit the storage VM: click **Storage > storage VMs**, click the storage VM, click **Settings** and then click 

under S3.

2. Add a user: click **Policies**, then click **Add**.
  - a. Enter a policy name and select from a list of groups.
  - b. Select an existing default policy or add a new one.

When adding or modifying a group policy, you can specify the following parameters:

- **Group**: the groups to whom access is granted.
- **Effect**: allows or denies access to one or more groups.
- **Actions**: permissible actions in one or more buckets for a given group.
- **Resources**: paths and names of objects within one or more buckets for which access is granted or denied.

For example:

- `*` grants access to all buckets in the storage VM.
  - `bucketname` and `bucketname/*` grant access to all objects in a specific bucket.
  - `bucketname/readme.txt` grants access to an object in a specific bucket.
- c. If desired, add statements to existing policies.

## CLI

### Use the CLI to create or modify an object store server policy

#### Steps

1. Create an object storage server policy:

```
vserver object-store-server policy create -vserver svm_name -policy policy_name [-comment text]
```

2. Create a statement for the policy:

```
vserver object-store-server policy statement create -vserver svm_name -policy policy_name -effect {allow|deny} -action object_store_actions -resource object_store_resources [-sid text]
```

The following parameters define access permissions:

<code>-effect</code>	The statement may allow or deny access
<code>-action</code>	You can specify <code>*</code> to mean all actions, or a list of one or more of the following: <code>GetObject</code> , <code>PutObject</code> , <code>DeleteObject</code> , <code>ListBucket</code> , <code>GetBucketAcl</code> , <code>GetObjectAcl</code> , <code>ListAllMyBuckets</code> , <code>ListBucketMultipartUploads</code> , and <code>ListMultipartUploadParts</code> .

<code>-resource</code>	The bucket and any object it contains. The wildcard characters * and ? can be used to form a regular expression for specifying a resource.
------------------------	--

You can optionally specify a text string as comment with the `-sid` option.

By default, new statements are added to the end of the list of statements, which are processed in order. When you add or modify statements later, you have the option to modify the statement's `-index` setting to change the processing order.

= Enable client access to S3 object storage

= Enable ONTAP S3 access for remote FabricPool tiering

:icons: font

:relative\_path: ./s3-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

For ONTAP S3 to be used as a remote FabricPool capacity (cloud) tier, the ONTAP S3 administrator must provide information about the S3 server configuration to the remote ONTAP cluster administrator.

### About this task

The following S3 server information is required to configure FabricPool cloud tiers:

- server name (FQDN)
- bucket name
- CA certificate
- access key
- password (secret access key)

In addition, the following networking configuration is required:

- There must be an entry for the remote ONTAP S3 server's hostname in the DNS server configured for the admin SVM, including the S3 server's FQDN name and the IP addresses on its LIFs.
- Intercluster LIFs must be configured on both local and remote clusters, although cluster peering is not required.

See the FabricPool documentation about configuring ONTAP S3 as a cloud tier.

### Managing Storage Tiers By Using FabricPool

= Enable ONTAP S3 access for local FabricPool tiering

:icons: font

:relative\_path: ./s3-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

For ONTAP S3 to be used as a local FabricPool capacity tier, you must define an object store based on the bucket you created, and then attach the object store to a performance tier aggregate to create a FabricPool.

### Before you begin

You must have the ONTAP S3 server name and a bucket name, and the S3 server must have been created using cluster LIFs (with the `-vserver Cluster` parameter).

### About this task

The object-store configuration contains information about the local capacity tier, including the S3 server and bucket names and authentication requirements.

An object-store configuration once created must not be reassociated with a different object-store or

bucket. You can create multiple buckets for local tiers, but you cannot create multiple object stores in a single bucket.

A FabricPool license is not required for a local capacity tier.

## Steps

1. Create the object store for the local capacity tier:

```
storage aggregate object-store config create -object-store-name store_name
-ipospace Cluster -provider-type ONTAP_S3 -server S3_server_name -container
-name bucket_name -access-key access_key -secret-password password
```

- The `-container-name` is the S3 bucket you created.
- The `-access-key` parameter authorizes requests to the ONTAP S3 server.
- The `-secret-password` parameter (secret access key) authenticates requests to the ONTAP S3 server.
- You can set the `-is-certificate-validation-enabled` parameter to `false` to disable certificate checking for ONTAP S3.

```
cluster1::> storage aggregate object-store config create
-object-store-name MyLocalObjStore -ipospace Cluster -provider-type
ONTAP_S3 -server s3.example.com
-container-name bucket1 -access-key myS3key -secret-password
myS3pass
```

2. Display and verify the object store configuration information:

```
storage aggregate object-store config show
```

3. Optional: To see how much data in a volume is inactive, follow the steps in [Determining how much data in a volume is inactive by using inactive data reporting](#).

Seeing how much data in a volume is inactive can help you decide which aggregate to use for FabricPool local tiering.

4. Attach the object store to an aggregate:

```
storage aggregate object-store attach -aggregate aggr_name -object-store
-name store_name
```

You can use the `allow-flexgroup true` option to attach aggregates that contain FlexGroup volume constituents.

```
cluster1::> storage aggregate object-store attach
-aggregate aggr1 -object-store-name MyLocalObjStore
```

5. Display the object store information and verify that the attached object store is available:

```
storage aggregate object-store show
```

```
cluster1::> storage aggregate object-store show
```

Aggregate	Object Store Name	Availability State
-----	-----	-----
aggr1	MyLocalObjStore	available

= Enable client access from an S3 app

:icons: font

:relative\_path: ./s3-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

For S3 client apps to access the ONTAP S3 server, the ONTAP S3 administrator must provide configuration information to the S3 user.

### What you'll need

The S3 client app must be capable of authenticating with the ONTAP S3 server using the following AWS signature versions:

- Signature Version 4, ONTAP 9.8 and later
- Signature Version 2, ONTAP 9.11.1 and later

Other signature versions are not supported by ONTAP S3.

The ONTAP S3 administrator must have created S3 users and granted them access permissions, as an individual users or as a group member, in the bucket policy or the object storage server policy.

The S3 client app must be capable of resolving the ONTAP S3 server name, which requires that ONTAP S3 administrator provide the S3 server name (FQDN) and IP addresses for the S3 server's LIFs.

### About this task

To access an ONTAP S3 bucket, a user on the S3 client app enters information provided by the ONTAP S3 administrator.

Beginning with ONTAP 9.9.1, the ONTAP S3 server supports the following AWS client functionality:

- user-defined object metadata

A set of key-value pairs can be assigned to objects as metadata when they are created using PUT (or POST). When a GET/HEAD operation is performed on the object, the user-defined metadata is returned along with the system metadata.

- object tagging

A separate set of key-value pairs can be assigned as tags for categorizing objects. Unlike metadata, tags are created and read with REST APIs independently of the object, and they implemented when objects are created or any time after.

To enable clients to get and put tagging information, the actions `GetObjectTagging`, `PutObjectTagging`, and `DeleteObjectTagging` need to be allowed using the bucket or group policies.



For more information, see the AWS S3 documentation.

### Steps

1. Authenticate the S3 client app with the ONTAP S3 server by entering the S3 server name and the CA certificate.
2. Authenticate a user on the S3 client app by entering the following information:
  - S3 server name (FQDN) and bucket name
  - the user's access key and secret key

= Storage service definitions

:icons: font

:relative\_path: ./s3-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

ONTAP includes predefined storage services that are mapped to corresponding minimum performance factors.

The actual set of storage services available in a cluster or SVM is determined by the type of storage that makes up an aggregate in the SVM.

The following table shows how the minimum performance factors are mapped to the predefined storage services:

Storage service	Expected IOPS (SLA)	Peak IOPS (SLO)	Minimum volume IOPS	Estimated latency	Are expected IOPS enforced?
value	128 per TB	512 per TB	75	17 ms	On AFF: Yes Otherwise: No
performance	2048 per TB	4096 per TB	500	2 ms	Yes
extreme	6144 per TB	12288 per TB	1000	1 ms	Yes

The following table defines the available storage service level for each type of media or node:

Media or node	Available storage service level
Disk	value
Virtual machine disk	value
FlexArray LUN	value
Hybrid	value

Media or node	Available storage service level
Capacity-optimized Flash	value
Solid-state drive (SSD) - non-AFF	value
Performance-optimized Flash - SSD (AFF)	extreme, performance, value

= Protect buckets with S3 SnapMirror

= S3 SnapMirror overview

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./s3-snapmirror/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

Beginning with ONTAP 9.10.1, you can protect buckets in ONTAP S3 object stores using familiar SnapMirror mirroring and backup functionality. In addition, unlike standard SnapMirror, S3 SnapMirror can have non-NetApp destinations.

S3 SnapMirror supports active mirrors and backup tiers from ONTAP S3 buckets to the following destinations:

Target	Supports active mirrors and takeover?	Supports backup and restore?
ONTAP S3 <ul style="list-style-type: none"> <li>• buckets in the same SVM</li> <li>• buckets in different SVMs on the same cluster</li> <li>• buckets in SVMs on different clusters</li> </ul>	✓	✓
StorageGRID		✓
AWS S3		✓
Cloud Volumes ONTAP for Azure		✓

You can protect existing buckets on ONTAP S3 servers or you can create new buckets with data protection enabled immediately.

S3 SnapMirror supports fan-out and cascade relationships. For an overview, see [Fan-out and cascade data protection deployments](#).

== S3 SnapMirror requirements

- ONTAP version  
ONTAP 9.10.1 or later must be running source and destination clusters.

- Licensing

The following license bundles are required on ONTAP source and destination systems:

- Core Bundle  
For ONTAP S3 protocol and storage.
  - Data Protection Bundle  
For S3 SnapMirror to target other NetApp object store targets (ONTAP S3, StorageGRID, and Cloud Volumes ONTAP).
  - Data Protection Bundle and Hybrid Cloud Bundle  
For S3 SnapMirror to target 3rd party object stores (AWS S3).
- ONTAP S3
    - ONTAP S3 servers must be running source and destination SVMs.
    - It is recommended but not required that CA certificates for TLS access are installed on systems that host S3 servers.
      - The CA certificates used to sign the S3 servers' certificates must be installed on the admin storage VM of the clusters that host S3 servers.
      - You can use a self-signed CA certificate or a certificate signed by an external CA vendor.
      - If the source or destination storage VMs are not listening on HTTPS, it is not necessary to install CA certificates.
  - Peering (for ONTAP S3 targets)
    - Intercluster LIFs must be configured (for remote ONTAP targets).
    - Source and destination clusters are peered (for remote ONTAP targets).
    - Source and destination storage VMs are peered (for all ONTAP targets).
  - SnapMirror policy
    - An S3-specific SnapMirror policy is required for all S3 SnapMirror relationships, but you can use the same policy for multiple relationships.
    - You can create your own policy or accept the default **Continuous** policy, which includes the following values:
      - Throttle (upper limit on throughput/bandwidth) - unlimited.
      - Time for recovery point objective: 1 hour (3600 seconds).
  - Root user keys  
Storage VM root user access keys are required for S3 SnapMirror relationships; ONTAP does not assign them by default. The first time you create an S3 SnapMirror relationship, you must verify that the keys exist on both source and destination storage VMs and regenerate them if they do not. If you need to regenerate them, you must ensure that all clients and all SnapMirror object-store configurations using the access and secret key pair are updated with the new keys.

For information about S3 server configuration, see the following topics:

- [Enable an S3 server on a storage VM](#)
- [About the S3 configuration process](#)

For information about cluster and storage VM peering, see the following topic:

- [Prepare for mirroring and vaulting \(System Manager, steps 1-6\)](#)

- [Cluster and SVM peering \(CLI\)](#)

== S3 SnapMirror considerations and restrictions

When you create new buckets, you can control access by creating users and groups. For more information, see the following topics:

- [Add S3 users and groups \(System Manager\)](#)
- [Create an S3 user \(CLI\)](#)
- [Create or modify S3 groups \(CLI\)](#)

The following standard SnapMirror functionality is not supported in the current S3 SnapMirror release:

- Fan-in deployments (data protection relationships between multiple source buckets and a single destination bucket)

S3 Snapmirror can support multiple bucket mirrors from multiple clusters to a single secondary cluster, but each source bucket must have its own destination bucket on the secondary cluster.

= Mirror and backup protection on a remote cluster

= Create a mirror relationship for a new bucket (remote cluster)

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./s3-snapmirror/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

When you create new S3 buckets, you can protect them immediately to an S3 SnapMirror destination on a remote cluster.



### What you'll need

- Requirements for ONTAP versions, licensing, and S3 server configuration have been completed.
- A peering relationship exists between source and destination clusters, and a peering relationship exists between source and destination storage VMs.
- CA Certificates are needed for the source and destination VMs. You can use self-signed CA certificates or certificates signed by an external CA vendor.

### About this task

You will need to perform tasks on both source and destination systems.

== System Manager procedure

1. If this is the first S3 SnapMirror relationship for this storage VM, verify that root user keys exist for both source and destination storage VMs and regenerate them if they do not:
  - a. Click **Storage > Storage VMs** and then select the storage VM.
  - b. In the **Settings** tab, click  in the **S3** tile.
  - c. In the **Users** tab, verify that there is an access key for the root user.
  - d. If there is not, click  next to **root**, then click **Regenerate Key**.

Do not regenerate the key if one already exists.

2. Edit the storage VM to add users, and to add users to groups, in both the source and destination storage VMs:

Click **Storage > storage VMs**, click the storage VM, click **Settings** and then click  under S3.

See [Add S3 users and groups](#) for more information.

3. On the source cluster, create an S3 SnapMirror policy if you don't have an existing one and you don't want to use the default policy:

- a. Click **Protection > Overview**, and then click **Local Policy Settings**.

- b. Click  next to **Protection Policies**, then click **Add**.

- Enter the policy name and description.
- Select the policy scope, cluster or SVM
- Select **Continuous** for S3 SnapMirror relationships.
- Enter your **Throttle** and **Recovery Point Objective** values.

4. Create a bucket with SnapMirror protection:

- a. Click **Storage > Buckets**, then click **Add**. Verifying permissions is optional but recommended.

- b. Enter a name, select the storage VM, enter a size, then click **More Options**.

- c. Under **Permissions**, click **Add**.

- **Principal** and **Effect** - select values corresponding to your user group settings or accept the defaults.
- **Actions**- make sure the following values are shown:  
`GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts`
- **Resources** - use the defaults (`bucketname, bucketname/*`) or other values you need.

See [Manage user access to buckets](#) for more information about these fields.

- d. Under **Protection**, check **Enable SnapMirror (ONTAP or Cloud)**. Then enter the following values:

- Destination
  - **TARGET: ONTAP System**
  - **CLUSTER**: Select the remote cluster.
  - **STORAGE VM**: Select a storage VM on the remote cluster.
  - **S3 SERVER CA CERTIFICATE**: Copy and paste the contents of the *source* certificate.
- Source
  - **S3 SERVER CA CERTIFICATE**: Copy and paste the contents of the *destination* certificate.

Check **Use the same certificate on the destination** if you are using a certificate signed by an external CA vendor.

If you click **Destination Settings**, you can also enter your own values in place of the defaults for bucket name, capacity, and performance service level.

When you click **Save**, a new bucket is created in the source storage VM, and it is mirrored to a new bucket that is created the destination storage VM.

== CLI procedure

1. If this is the first S3 SnapMirror relationship for this SVM, verify that root user keys exist for both source and destination SVMs and regenerate them if they do not:

```
vserver object-store-server user show
```

Verify that there is an access key for the root user. If there is not, enter:

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root
```

Do not regenerate the key if one already exists.

2. Create buckets in both the source and destination SVMs:

```
vserver object-store-server bucket create -vserver svm_name -bucket bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]
```

3. Add access rules to the default bucket policies in both the source and destination SVMs:

```
vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]
```

#### Example

```
src_cluster::> vserver object-store-server bucket policy add-statement -bucket test-bucket -effect allow -action GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts -principal - -resource test-bucket, test-bucket /*
```

4. On the source SVM, create an S3 SnapMirror policy if you don't have an existing one and you don't want to use the default policy:

```
snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]
```

Parameters:

- `type continuous` – the only policy type for S3 SnapMirror relationships (required).
- `-rpo` – specifies the time for recovery point objective, in seconds (optional).
- `-throttle` – specifies the upper limit on throughput/bandwidth, in kilobytes/seconds (optional).

### Example

```
src_cluster::> snapmirror policy create -vserver vs0 -type
continuous -rpo 0 -policy test-policy
```

5. Install CA server certificates on the admin SVMs of the source and destination clusters:

- a. On the source cluster, install the CA certificate that signed the *destination* S3 server certificate:  
security certificate install -type server-ca -vserver *src\_admin\_svm* -cert-name *dest\_server\_certificate*
- b. On the destination cluster, install the CA certificate that signed the *source* S3 server certificate:  
security certificate install -type server-ca -vserver *dest\_admin\_svm* -cert-name *src\_server\_certificate*

If you are using a certificate signed by an external CA vendor, install the same certificate on the source and destination admin SVM.

See the `security certificate install` man page for details.

6. On the source SVM, create an S3 SnapMirror relationship:

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name
-destination-path dest_peer_svm_name:/bucket/bucket_name, ...} [-policy
policy_name]
```

You can use a policy you created or accept the default.

### Example

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
bucket -destination-path vs1-dest:bucket/test-bucket-mirror -policy
test-policy
```

7. Verify that mirroring is active:

```
snapmirror show -policy-type continuous -fields status
```

= Create a mirror relationship for an existing bucket (remote cluster)

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./s3-snapmirror/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You can begin protecting existing S3 buckets at any time; for example, if you upgraded an S3 configuration from a release earlier than ONTAP 9.10.1.

### What you'll need



- Requirements for ONTAP versions, licensing, and S3 server configuration have been completed.


- A peering relationship exists between source and destination clusters, and a peering relationship exists between source and destination storage VMs.
- CA Certificates are needed for the source and destination VMs. You can use self-signed CA certificates or certificates signed by an external CA vendor.

### About this task


You will need to perform tasks on both source and destination clusters.

== System Manager procedure

1. If this is the first S3 SnapMirror relationship for this storage VM, verify that root user keys exist for both source and destination storage VMs and regenerate them if they do not:
  - a. Click **Storage > Storage VMs** and then select the storage VM.
  - b. In the **Settings** tab, click  in the **S3** tile.
  - c. In the **Users** tab, verify that there is an access key for the root user.
  - d. If there is not, click  next to **root**, then click **Regenerate Key**. Do not regenerate the key if one already exists.

2. Verify that user and group access is correct in both the source and destination storage VMs: Click **Storage > storage VMs**, click the storage VM, click **Settings** and then click  under **S3**.

See [Add S3 users and groups](#) for more information.

3. On the source cluster, create an S3 SnapMirror policy if you don't have an existing one and you don't want to use the default policy:
  - a. Click **Protection > Overview**, and then click **Local Policy Settings**.
  - b. Click  next to **Protection Policies**, then click **Add**.
  - c. Enter the policy name and description.
  - d. Select the policy scope, cluster or SVM
  - e. Select **Continuous** for S3 SnapMirror relationships.
  - f. Enter your **Throttle** and **Recovery Point Objective** values.

4. Verify that the bucket access policy of the existing bucket still meets your needs:

- a. Click **Storage > Buckets** and then select the bucket you want to protect.

- b. In the **Permissions** tab, click  **Edit**, then click **Add** under **Permissions**.

- **Principal and Effect:** select values corresponding to your user group settings, or accept the defaults.
- **Actions:** make sure the following values are shown:  
`GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts`
- **Resources:** use the defaults (`bucketname, bucketname/*`) or other values you need.

See [Manage user access to buckets](#) for more information about these fields.

5. Protect an existing bucket with S3 SnapMirror protection:

- a. Click **Storage > Buckets** and then select the bucket you want to protect..

- b. Click **Protect** and enter the following values:



- Destination
  - **TARGET:** ONTAP System
  - **CLUSTER:** Select the remote cluster.
  - **STORAGE VM:** Select a storage VM on the remote cluster.
  - **S3 SERVER CA CERTIFICATE:** Copy and paste the contents of the *source* certificate.
- Source
  - **S3 SERVER CA CERTIFICATE:** Copy and paste the contents of the *destination* certificate.

Check **Use the same certificate on the destination** if you are using a certificate signed by an external CA vendor.

If you click **Destination Settings**, you can also enter your own values in place of the defaults for bucket name, capacity, and performance service level.

When you click **Save**, the existing bucket is mirrored to a new bucket in the destination storage VM.

== CLI procedure

1. If this is the first S3 SnapMirror relationship for this SVM, verify that root user keys exist for both source and destination SVMs and regenerate them if they do not:

```
vserver object-store-server user show
```

Verify that there is an access key for the root user. If there is not, enter:

```
vserver object-store-server user regenerate-keys -vserver svm_name -user
root
```

Do not regenerate the key if one already exists.

2. Create a bucket on the destination SVM to be the mirror target:

```
vserver object-store-server bucket create -vserver svm_name -bucket
dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

3. Verify that the access rules of the default bucket policies are correct in both the source and destination SVMs:

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
text] [-index integer]
```

### Example

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. On the source SVM, create an S3 SnapMirror policy if you don't have an existing one and you don't want to use the default policy:

```
snapmirror policy create -vserver svm_name -policy policy_name -type
continuous [-rpo integer] [-throttle throttle_type] [-comment text]
[additional_options]
```

**Parameters:**

- `continuous` – the only policy type for S3 SnapMirror relationships (required).
- `-rpo` – specifies the time for recovery point objective, in seconds (optional).
- `-throttle` – specifies the upper limit on throughput/bandwidth, in kilobytes/seconds (optional).

**Example**

```
src_cluster::> snapmirror policy create -vserver vs0 -type
continuous -rpo 0 -policy test-policy
```

5. Install CA certificates on the admin SVMs of source and destination clusters:

- a. On the source cluster, install the CA certificate that signed the *destination* S3 server certificate:

```
security certificate install -type server-ca -vserver src_admin_svm
-cert-name dest_server_certificate
```

- b. On the destination cluster, install the CA certificate that signed the *source* S3 server certificate:

```
security certificate install -type server-ca -vserver dest_admin_svm
-cert-name src_server_certificate
```

If you are using a certificate signed by an external CA vendor, install the same certificate on the source and destination admin SVM.

See the `security certificate install` man page for details.

6. On the source SVM, create an S3 SnapMirror relationship:

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name
-destination-path dest_peer_svm_name:/bucket/bucket_name, ...} [-policy
policy_name]
```

You can use a policy you created or accept the default.

**Example**

```
src_cluster::> snapmirror create -source-path vs0:/bucket/test-
bucket -destination-path vs1:/bucket/test-bucket-mirror -policy
test-policy
```

7. Verify that mirroring is active:

```
snapmirror show -policy-type continuous -fields status
```

= Takeover and serve data from the destination bucket (remote cluster)

:toc: macro  
:toclevels: 1  
:hardbreaks:  
:icons: font  
:linkattrs:  
:relative\_path: ./s3-snapmirror/  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

If the data in a source bucket becomes unavailable, you can break the SnapMirror relationship to make the destination bucket writable and begin serving data.

### About this task


When a takeover operation is performed, source bucket is converted to read-only and original destination bucket is converted to read-write, thereby reversing the S3 SnapMirror relationship.

When the disabled source bucket is available again, S3 SnapMirror automatically resynchronizes the contents of the two buckets. It is not necessary to explicitly resynchronize the relationship, as is required for volume SnapMirror deployments.

The takeover operation must be initiated from the remote cluster.

== System Manager procedure

Failover from the unavailable bucket and begin serving data:

1. Click **Protection > Relationships**, then select **S3 SnapMirror**.
2. Click , select **Failover**, then click **Failover**.

== CLI procedure

1. Initiate a failover operation for the destination bucket:  
`snapmirror failover start -destination-path svm_name:/bucket/bucket_name`
2. Verify the status of the failover operation:  
`snapmirror show -fields status`

### Example

```
dest_cluster::> snapmirror failover start -destination-path  
dest_svm1:/bucket/test-bucket-mirror
```

= Restore a bucket from the destination storage VM (remote cluster)

:toc: macro  
:toclevels: 1  
:hardbreaks:  
:icons: font  
:linkattrs:  
:relative\_path: ./s3-snapmirror/  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

If data in a source bucket is lost or corrupted, you repopulate your data by restoring from a destination bucket.

## About this task


You can restore the destination bucket to an existing bucket or a new bucket. The target bucket for the restore operation must be larger than the destination bucket's logical used space.

If you use an existing bucket, it must be empty when starting a restore operation. Restore does not "roll back" a bucket in time; rather, it populates an empty bucket with its previous contents.

The restore operation must be initiated from the remote cluster.

== System Manager procedure

Restore the back-up data:

1. Click **Protection > Relationships**, then select **S3 SnapMirror**.
2. Click  and then select **Restore**.
3. Under **Source**, select **Existing Bucket** (the default) or **New Bucket**.
  - To restore to an **Existing Bucket** (the default), complete these actions:
    - Select the cluster and storage VM to search for the existing bucket.
    - Select the existing bucket.
    - Copy and paste the contents of the *destination* S3 server CA certificate.
  - To restore to a **New Bucket**, enter the following values:
    - The cluster and storage VM to host the new bucket.
    - The new bucket's name, capacity, and performance service level. See [Storage service levels](#) for more information.
    - The contents of the *destination* S3 server CA certificate.
4. Under **Destination**, copy and paste the contents of the *source* S3 server CA certificate.
5. Click **Protection > Relationships** to monitor the restore progress.

== CLI procedure

1. If you are restoring to a new bucket, create the new bucket. For more information, see [Create a backup relationship for a new bucket \(cloud target\)](#).
2. Initiate a restore operation for the destination bucket:

```
snapmirror restore -source-path svm_name:/bucket/bucket_name -destination  
-path svm_name:/bucket/bucket_name
```

## Example

```
dest_cluster::> snapmirror restore -source-path src_vs1:/bucket/test-  
bucket -destination-path dest_vs1:/bucket/test-bucket-mirror
```

= Mirror and backup protection on the local cluster

= Create a mirror relationship for a new bucket (local cluster)

```
:toc: macro  
:hardbreaks:  
:toclevels: 1
```





```
:icons: font
:linkattrs:
:relative_path: ./s3-snapmirror/
:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/
```

When you create new S3 buckets, you can protect them immediately to an S3 SnapMirror destination on the same cluster. You can mirror data to a bucket in a different storage VM or the same storage VM as the source.

### What you'll need

- Requirements for ONTAP versions, licensing, and S3 server configuration have been completed.
- A peering relationship exists between source and destination storage VMs.
- CA Certificates are needed for the source and destination VMs. You can use self-signed CA certificates or certificates signed by an external CA vendor.

== System Manager procedure

1. If this is the first S3 SnapMirror relationship for this storage VM, verify that root user keys exist for both source and destination storage VMs and regenerate them if they do not:
  - a. Click **Storage > Storage VMs** and then select the storage VM.
  - b. In the **Settings** tab, click  in the S3 tile.
  - c. In the **Users** tab, verify that there is an access key for the root user
  - d. If there is not, click  next to **root**, then click **Regenerate Key**.  
Do not regenerate the key if one already exists.
2. Edit the storage VM to add users, and to add users to groups, in both the source and destination storage VMs:  
Click **Storage > storage VMs**, click the storage VM, click **Settings** and then click  under S3.  
  
See [Add S3 users and groups](#) for more information.
3. Create an S3 SnapMirror policy if you don't have an existing one and you don't want to use the default policy:
  - a. Click **Protection > Overview**, and then click **Local Policy Settings**.
  - b. Click  next to **Protection Policies**, then click **Add**.
    - Enter the policy name and description.
    - Select the policy scope, cluster or SVM
    - Select **Continuous** for S3 SnapMirror relationships.
    - Enter your **Throttle** and **Recovery Point Objective** values.
4. Create a bucket with SnapMirror protection:
  - a. Click **Storage > Buckets** then click **Add**.
  - b. Enter a name, select the storage VM, enter a size, then click **More Options**.
  - c. Under **Permissions**, click **Add**. Verifying permissions is optional but recommended.
    - **Principal** and **Effect** - select values corresponding to your user group settings, or accept the defaults.
    - **Actions** - make sure the following values are shown:

`GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts`

- **Resources** - use the defaults (`bucketname`, `bucketname/*`) or other values you need

See [Manage user access to buckets](#) for more information about these fields.

d. Under **Protection**, check **Enable SnapMirror (ONTAP or Cloud)**. Then enter the following values:

- Destination
  - **TARGET**: ONTAP System
  - **CLUSTER**: Select the remote cluster.
  - **STORAGE VM**: Select a storage VM on the remote cluster.
  - **S3 SERVER CA CERTIFICATE**: Copy and paste the contents of the source certificate.
- Source
  - **S3 SERVER CA CERTIFICATE**: Copy and paste the contents of the destination certificate.

Check **Use the same certificate on the destination** if you are using a certificate signed by an external CA vendor.

If you click **Destination Settings**, you can also enter your own values in place of the defaults for bucket name, capacity, and performance service level.

When you click **Save**, a new bucket is created in the source storage VM, and it is mirrored to a new bucket that is created the destination storage VM.

== CLI procedure

1. If this is the first S3 SnapMirror relationship for this SVM, verify that root user keys exist for both source and destination SVMs and regenerate them if they do not:

```
vserver object-store-server user show
```

Verify that there is an access key for the root user. If there is not, enter:

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root
```

Do not regenerate the key if one already exists.

2. Create buckets in both the source and destination SVMs:

```
vserver object-store-server bucket create -vserver svm_name -bucket bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]
```

3. Add access rules to the default bucket policies in both the source and destination SVMs:

```
vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]
```

### Example

```
src_cluster::> vserver object-store-server bucket policy add-  
statement -bucket test-bucket -effect allow -action  
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc  
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -  
-resource test-bucket, test-bucket /*
```

4. Create an S3 SnapMirror policy if you don't have an existing one and you don't want to use the default policy:

```
snapmirror policy create -vserver svm_name -policy policy_name -type  
continuous [-rpo integer] [-throttle throttle_type] [-comment text]  
[additional_options]
```

#### Parameters:

- `continuous` – the only policy type for S3 SnapMirror relationships (required).
- `-rpo` – specifies the time for recovery point objective, in seconds (optional).
- `-throttle` – specifies the upper limit on throughput/bandwidth, in kilobytes/seconds (optional).

### Example

```
src_cluster::> snapmirror policy create -vserver vs0 -type  
continuous -rpo 0 -policy test-policy
```

5. Install CA server certificates on the admin SVM:

- a. Install the CA certificate that signed the *source* S3 server's certificate on the admin SVM:

```
security certificate install -type server-ca -vserver admin_svm -cert  
-name src_server_certificate
```

- b. Install the CA certificate that signed the *destination* S3 server's certificate on the admin SVM:

```
security certificate install -type server-ca -vserver admin_svm -cert  
-name dest_server_certificate
```

If you are using a certificate signed by an external CA vendor, you only need to install this certificate on the admin SVM.

See the `security certificate install` man page for details.

6. Create an S3 SnapMirror relationship:

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name  
-destination-path dest_peer_svm_name:/bucket/bucket_name, ...} [-policy  
policy_name]`
```

You can use a policy you created or accept the default.

## Example

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-  
bucket -destination-path vs1-dest:/vs1/bucket/test-bucket-mirror  
-policy test-policy
```

### 7. Verify that mirroring is active:

```
snapmirror show -policy-type continuous -fields status
```

= Create a mirror relationship for an existing bucket (local cluster)

:toc: macro

:hardbreaks:

:toclevels: 1

:icons: font

:linkattrs:

:relative\_path: ./s3-snapmirror/





:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You can begin protecting existing S3 buckets on the same cluster at any time; for example, if you upgraded an S3 configuration from a release earlier than ONTAP 9.10.1. You can mirror data to a bucket in a different storage VM or the same storage VM as the source.


### What you'll need

- Requirements for ONTAP versions, licensing, and S3 server configuration have been completed.
- A peering relationship exists between source and destination storage VMs.
- CA Certificates are needed for the source and destination VMs. You can use self-signed CA certificates or certificates signed by an external CA vendor.

== System Manager procedure

1. If this is the first S3 SnapMirror relationship for this storage VM, verify that root user keys exist for both source and destination storage VMs and regenerate them if they do not:
  - a. Click **Storage > Storage VMs** and then select the storage VM.
  - b. In the **Settings** tab, click  in the **S3** tile.
  - c. In the **Users** tab, verify that there is an access key for the root user.
  - d. If there is not, click  next to **root**, then click **Regenerate Key**.  
Do not regenerate the key if one already exists
2. Verify that user and group access is correct in both the source and destination storage VMs:
  - Click **Storage > storage VMs**, click the storage VM, click **Settings** and then click  under S3.  
  
See [Add S3 users and groups](#) for more information.
3. Create an S3 SnapMirror policy if you don't have an existing one and you don't want to use the default policy:
  - a. Click **Protection > Overview**, and then click **Local Policy Setting**.
  - b. Click  next to **Protection Policies**, then click **Add**.



- Enter the policy name and description.
  - Select the policy scope, cluster or SVM
  - Select **Continuous** for S3 Snapmirror relationships.
  - Enter your **Throttle** and **Recovery Point Objective** values.
4. Verify that the bucket access policy of the existing bucket continues to meet your needs:
- a. Click **Storage > Buckets** and then select the bucket you want to protect.
  - b. In the **Permissions** tab, click  **Edit**, then click **Add** under **Permissions**.
    - **Principal** and **Effect** - select values corresponding to your user group settings, or accept the defaults.
    - **Actions** - make sure the following values are shown:  
`GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts`
    - **Resources** - use the defaults (`bucketname, bucketname/*`) or other values you need.

See [Manage user access to buckets](#) for more information about these fields.

5. Protect an existing bucket with S3 SnapMirror:
- a. Click **Storage > Buckets** and then select the bucket you want to protect.
  - b. Click **Protect** and enter the following values:
    - Destination
      - **TARGET:** ONTAP System
      - **CLUSTER:** Select the local cluster.
      - **STORAGE VM:** Select the same or a different storage VM.
      - **S3 SERVER CA CERTIFICATE:** Copy and paste the contents of the *source* certificate.
    - Source
      - **S3 SERVER CA CERTIFICATE:** Copy and paste the contents of the *destination* certificate.

Check **Use the same certificate on the destination** if you are using a certificate signed by an external CA vendor.

If you click **Destination Settings**, you can also enter your own values in place of the defaults for bucket name, capacity, and performance service level.

When you click **Save**, the existing bucket is mirrored to a new bucket in the destination storage VM.

== CLI procedure

1. If this is the first S3 SnapMirror relationship for this SVM, verify that root user keys exist for both source and destination SVMs and regenerate them if they do not:  
`vserver object-store-server user show`

Verify that there is an access key for the root user. If there is not, enter:

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root
```

Do not regenerate the key if one already exists.

2. Create a bucket on the destination SVM to be the mirror target:

```
vserver object-store-server bucket create -vserver svm_name -bucket
dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

3. Verify that the access rules to the default bucket policies are correct in both the source and destination SVMs:

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
text] [-index integer]
```

### Example

```
clusterA::> vserver object-store-server bucket policy add-statement
-bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. Create an S3 SnapMirror policy if you don't have an existing one and you don't want to use the default policy:

```
snapmirror policy create -vserver svm_name -policy policy_name -type
continuous [-rpo integer] [-throttle throttle_type] [-comment text]
[additional_options]
```

### Parameters:

- *continuous* – the only policy type for S3 SnapMirror relationships (required).
- *-rpo* – specifies the time for recovery point objective, in seconds (optional).
- *-throttle* – specifies the upper limit on throughput/bandwidth, in kilobytes/seconds (optional).

### Example

```
clusterA::> snapmirror policy create -vserver vs0 -type
continuous -rpo 0 -policy test-policy
```

5. Install CA server certificates on the admin SVM:

- a. Install the CA certificate that signed the *source* S3 server's certificate on the admin SVM:

```
security certificate install -type server-ca -vserver admin_svm -cert
-name src_server_certificate
```

- b. Install the CA certificate that signed the *destination* S3 server's certificate on the admin SVM:

```
security certificate install -type server-ca -vserver admin_svm -cert
-name dest_server_certificate
```

If you are using a certificate signed by an external CA vendor, you only need to install this certificate on the admin SVM.

See the `security certificate install man` page for details.

6. Create an S3 SnapMirror relationship:

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name  
-destination-path dest_peer_svm_name:/bucket/bucket_name, ...} [-policy  
policy_name]
```

You can use a policy you created or accept the default.

**Example**

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-  
bucket -destination-path vs1-dest:/bucket/test-bucket-mirror -policy  
test-policy
```

7. Verify that mirroring is active:

```
snapmirror show -policy-type continuous -fields status
```

= Takeover and serve data from the destination bucket (local cluster)

:toc: macro

:hardbreaks:

:toclevels: 1

:icons: font

:linkattrs:

:relative\_path: ./s3-snapmirror/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

If the data in a source bucket becomes unavailable, you can break the SnapMirror relationship to make the destination bucket writable and begin serving data.

**About this task**


When a takeover operation is performed, source bucket is converted to read-only and original destination bucket is converted to read-write, thereby reversing the S3 SnapMirror relationship.

When the disabled source bucket is available again, S3 SnapMirror automatically resynchronizes the contents of the two buckets. You don't need to explicitly resynchronize the relationship, as is required for standard volume SnapMirror deployments.

If the destination bucket is on a remote cluster, the takeover operation must be initiated from the remote cluster.

== System Manager procedure

Failover from the unavailable bucket and begin serving data:

1. Click **Protection > Relationships**, then select **S3 SnapMirror**.
2. Click , select **Failover**, then click **Failover**.

== CLI procedure

1. Initiate a failover operation for the destination bucket:

```
snapmirror failover start -destination-path svm_name:/bucket/bucket_name
```

2. Verify the status of the failover operation:

```
snapmirror show -fields status
```

### Example

```
clusterA::> snapmirror failover start -destination-path vs1:/bucket/test-  
bucket-mirror
```

= Restore a bucket from the destination storage VM (remote cluster)

:toc: macro

:hardbreaks:

:toclevels: 1

:icons: font

:linkattrs:

:relative\_path: ./s3-snapmirror/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

When data in a source bucket is lost or corrupted, you repopulate your data by restoring from a destination bucket.

### About this task


You can restore the destination bucket to an existing bucket or a new bucket. The target bucket for the restore operation must be larger than the destination bucket's logical used space.

If you use an existing bucket, it must be empty when starting a restore operation. Restore does not "roll back" a bucket in time; rather, it populates an empty bucket with its previous contents.

The restore operation must be initiated from the remote cluster.

== System Manager procedure

Restore the back-up data:

1. Click **Protection > Relationships**, then select the bucket.
2. Click  and then select **Restore**.
3. Under **Source**, select **Existing Bucket** (the default) or **New Bucket**.
  - To restore to an **Existing Bucket** (the default), complete these actions:
    - Select the cluster and storage VM to search for the existing bucket.
    - Select the existing bucket.
4. Copy and paste the contents of the destination S3 server CA certificate.
  - To restore to a **New Bucket**, enter the following values:
    - The cluster and storage VM to host the new bucket.
    - The new bucket's name, capacity, and performance service level. See [Storage service levels](#) for more information.
    - The contents of the destination S3 server CA certificate.

5. Under **Destination**, copy and paste the contents of the source S3 server CA certificate.
6. Click **Protection** > Relationships to monitor the restore progress.

== CLI procedure

1. If you are restoring to a new bucket, create the new bucket. For more information, see [Create a backup relationship for a new bucket \(cloud target\)](#).
2. Initiate a restore operation for the destination bucket:  

```
snapmirror restore -source-path svm_name:/bucket/bucket_name -destination  
-path svm_name:/bucket/bucket_name
```

### Example

```
clusterA::> snapmirror restore -source-path vs0:/bucket/test-bucket  
-destination-path vs1:/bucket/test-bucket-mirror
```

= Backup protection with cloud targets

= Requirements for cloud target relationships

:toc: macro

:hardbreaks:

:toclevels: 1

:icons: font

:linkattrs:

:relative\_path: ./s3-snapmirror/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

Make sure that your source and target environments meet the requirements for S3 SnapMirror backup protection to cloud targets.

You must have valid account credentials with the object store provider to access the data bucket.

Intercluster network interfaces and an IPspace should be configured on the cluster before the cluster can connect to a cloud object store. You should create cluster network interfaces on each node to seamlessly transfer data from the local storage to the cloud object store.

For StorageGRID targets, you need to know the following information:

- server name, expressed as a fully-qualified domain name (FQDN) or IP address
- bucket name; the bucket must already exist
- access key
- secret key

In addition, the CA certificate used to sign the StorageGRID server certificate needs to be installed on the ONTAP S3 cluster's admin storage VM using the `security certificate install` command. For more information, see [Installing a CA certificate](#) if you use StorageGRID.

For AWS S3 targets, you need to know the following information:

- server name, expressed as a fully-qualified domain name (FQDN) or IP address

- bucket name; the bucket must already exist
- access key
- secret key

The DNS server for the ONTAP cluster's admin storage VM must be able to resolve FQDNs (if used) to IP addresses.

= Create a backup relationship for a new bucket (cloud target)

:toc: macro

:hardbreaks:

:toclevels: 1

:icons: font

:linkattrs:

:relative\_path: ./s3-snapmirror/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

When you create new S3 buckets, you can back them up immediately to an S3 SnapMirror target bucket on an object store provider, which can be a StorageGRID system or an AWS S3 deployment.

#### What you'll need

- You have valid account credentials and configuration information for the object store provider.
- Intercluster network interfaces and an IPspace have been configured on the source system.
- The DNS configuration for the source storage VM must be able to resolve the target's FQDN.

== System Manager procedure

1. Edit the storage VM to add users, and to add users to groups:

- Click **Storage > storage VMs**, click the storage VM, click **Settings** and then click  under **S3**.

See [Add S3 users and groups](#) for more information.


2. Add a Cloud Object Store on the source system:

- Click **Protection > Overview**, then select **Cloud Object Stores**.
- Click **Add**, then select **Amazon S3** or **StorageGRID**.

c. Enter the following values:

- Cloud object store name
- URL style (path or virtual-hosted)
- storage VM (enabled for S3)
- Object store server name (FQDN)
- Object store certificate
- Access key
- Secret key
- Container (bucket) name

3. Create an S3 SnapMirror policy if you don't have an existing one and you don't want to use the default policy:

- a. Click **Protection > Overview**, and then click **Local Policy Settings**.
  - b. Click  next to **Protection Policies**, then click **Add**.
    - Enter the policy name and description.
    - Select the policy scope, cluster or SVM
    - Select **Continuous** for S3 SnapMirror relationships.
    - Enter your **Throttle** and **Recovery Point Objective** values.
4. Create a bucket with SnapMirror protection:
- a. Click **Storage > Buckets**, then click **Add**.
  - b. Enter a name, select the storage VM, enter a size, then click **More Options**.
  - c. Under **Permissions**, click **Add**. Verifying permissions is optional but recommended.
    - **Principal** and **Effect** - select values corresponding to your user group settings or accept the defaults.
    - **Actions** - make sure the following values are shown:  
`GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts`
    - **Resources** - use the defaults `_(bucketname, bucketname/*)` or other values you need.

See [Manage user access to buckets](#) for more information about these fields.
  - d. Under **Protection**, check **Enable SnapMirror (ONTAP or Cloud)**, select **Cloud Storage**, then select the **Cloud Object Store**.

When you click **Save**, a new bucket is created in the source storage VM, and it is backed up to the cloud object store.

== CLI procedure

1. If this is the first S3 SnapMirror relationship for this SVM, verify that root user keys exist for both source and destination SVMs and regenerate them if they do not:

```
vserver object-store-server user show
```

Confirm that there is an access key for the root user. If there is not, enter:

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root
```

Do not regenerate the key if one already exists.

2. Create a bucket in the source SVM:

```
vserver object-store-server bucket create -vserver svm_name -bucket bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]
```

3. Add access rules to the default bucket policy:

```
vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]
```

## Example

```
clusterA::> vsserver object-store-server bucket policy add-statement
-bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. Create an S3 SnapMirror policy if you don't have an existing one and you don't want to use the default policy:

```
snapmirror policy create -vsserver svm_name -policy policy_name -type
continuous [-rpo integer] [-throttle throttle_type] [-comment text]
[additional_options]
```

### Parameters:

- \* `type continuous` – the only policy type for S3 SnapMirror relationships (required).
- \* `-rpo` – specifies the time for recovery point objective, in seconds (optional).
- \* `-throttle` – specifies the upper limit on throughput/bandwidth, in kilobytes/seconds (optional).

## Example

```
clusterA::> snapmirror policy create -vsserver vs0 -type continuous
-rpo 0 -policy test-policy
```

5. If the target is a StorageGRID system, install the StorageGRID CA server certificate on the admin SVM of the source cluster:

```
security certificate install -type server-ca -vsserver src_admin_svm -cert
-name storage_grid_server_certificate
```

See the `security certificate install` man page for details.

6. Define the S3 SnapMirror destination object store:

```
snapmirror object-store config create -vsserver svm_name -object-store-name
target_store_name -usage data -provider-type {AWS_S3|SGWS} -server
target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port
port_number -access-key target_access_key -secret-password
target_secret_key
```

### Parameters:

- \* `-object-store-name` – the name of the object store target on the local ONTAP system.
- \* `-usage` – use data for this workflow.
- \* `-provider-type` – AWS\_S3 and SGWS (StorageGRID) targets are supported.
- \* `-server` – the target server's FQDN or IP address.
- \* `-is-ssl-enabled` – enabling SSL is optional but recommended.

See the `snapmirror object-store config create` man page for details.



### Example

```
src_cluster::> snapmirror object-store config create -vserver vs0
-object-store-name sgws-store -usage data -provider-type SGWS
-server sgws.example.com -container-name target-test-bucket -is-ssl
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

#### 7. Create an S3 SnapMirror relationship:

```
snapmirror create -source-path svm_name:/bucket/bucket_name -destination
-path object_store_name:/objstore -policy policy_name
```

#### Parameters:

\* `-destination-path` – the object store name you created in the previous step and the fixed value `objstore`.

You can use a policy you created or accept the default.

### Example

```
src_cluster::> snapmirror create -source-path vs0:/bucket/test-
bucket -destination-path sgws-store:/objstore -policy test-policy
```

#### 8. Verify that mirroring is active:

```
snapmirror show -policy-type continuous -fields status
```

= Create a backup relationship for an existing bucket (cloud target)

:toc: macro

:hardbreaks:

:toclevels: 1

:icons: font

:linkattrs:

:relative\_path: ./s3-snapmirror/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You can begin backing up existing S3 buckets at any time; for example, if you upgraded an S3 configuration from a release earlier than ONTAP 9.10.1.

#### What you'll need



- You have valid account credentials and configuration information for the object store provider.
- Intercluster network interfaces and an IPspace have been configured on the source system.
- The DNS configuration for the source storage VM must be able to resolve the target's FQDN.

== System Manager procedure

#### 1. Verify that the users and groups are correctly defined:

Click **Storage > storage VMs**, click the storage VM, click **Settings** and then click  under S3.

See [Add S3 users and groups](#) for more information.

2. Create an S3 SnapMirror policy if you don't have an existing one and you don't want to use the default policy:
  - a. Click **Protection > Overview**, and then click **Local Policy Settings**.
  - b. Click  next to **Protection Policies**, then click **Add**.
  - c. Enter the policy name and description.
  - d. Select the policy scope, cluster or SVM
  - e. Select **Continuous** for S3 SnapMirror relationships.
  - f. Enter your **Throttle** and **Recovery Point Objective values**.
3. Add a Cloud Object Store on the source system:
  - a. Click **Protection > Overview**, then select **Cloud Object Store**.
  - b. Click **Add**, then select **Amazon S3** or **Others** for StorageGRID Webscale.
  - c. Enter the following values:
    - Cloud object store name
    - URL style (path or virtual-hosted)
    - storage VM (enabled for S3)
    - Object store server name (FQDN)
    - Object store certificate
    - Access key
    - Secret key
    - Container (bucket) name
4. Verify that the bucket access policy of the existing bucket still meets your needs:
  - a. Click **Storage > Buckets** and then select the bucket you want to protect.
  - b. In the **Permissions** tab, click  **Edit**, then click **Add** under **Permissions**.
    - **Principal** and **Effect** - select values corresponding to your user group settings or accept the defaults.
    - **Actions** - make sure the following values are shown:  
`GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts`
    - **Resources** - use the defaults (`bucketname, bucketname/*`) or other values you need.

See [Manage user access to buckets](#) for more information about these fields.
5. Back up the bucket using S3 SnapMirror:
  - a. Click **Storage > Buckets** and then select the bucket you want to back up.
  - b. Click **Protect**, select **Cloud Storage** under **Target**, then select the **Cloud Object Store**.

When you click **Save**, the existing bucket is backed up to the cloud object store.

== CLI procedure

1. Verify that the access rules in the default bucket policy are correct:
 

```
vserver object-store-server bucket policy add-statement -vserver svm_name
```

```
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
text] [-index integer]
```

### Example

```
clusterA::> vsserver object-store-server bucket policy add-statement
-bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

2. Create an S3 SnapMirror policy if you don't have an existing one and you don't want to use the default policy:

```
snapmirror policy create -vsserver svm_name -policy policy_name -type
continuous [-rpo integer] [-throttle throttle_type] [-comment text]
[additional_options]
```

### Parameters:

- \* `type continuous` – the only policy type for S3 SnapMirror relationships (required).
- \* `-rpo` – specifies the time for recovery point objective, in seconds (optional).
- \* `-throttle` – specifies the upper limit on throughput/bandwidth, in kilobytes/seconds (optional).

### Example

```
clusterA::> snapmirror policy create -vsserver vs0 -type continuous
-rpo 0 -policy test-policy
```

3. If the target is a StorageGRID system, install the StorageGRID CA certificate on the admin SVM of the source cluster:

```
security certificate install -type server-ca -vsserver src_admin_svm -cert
-name storage_grid_server_certificate
```

See the `security certificate install` man page for details.

4. Define the S3 SnapMirror destination object store:

```
snapmirror object-store config create -vsserver svm_name -object-store-name
target_store_name -usage data -provider-type {AWS_S3|SGWS} -server
target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port
port_number -access-key target_access_key -secret-password
target_secret_key
```

### Parameters:

- \* `-object-store-name` – the name of the object store target on the local ONTAP system.
- \* `-usage` – use data for this workflow.
- \* `-provider-type` – AWS\_S3 and SGWS (StorageGRID) targets are supported.
- \* `-server` – the target server's FQDN or IP address.
- \* `-is-ssl-enabled` –enabling SSL is optional but recommended.

See the `snapmirror object-store config create` man page for details.

### Example

```
src_cluster::> snapmirror object-store config create -vserver vs0
-object-store-name sgws-store -usage data -provider-type SGWS
-server sgws.example.com -container-name target-test-bucket -is-ssl
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

#### 5. Create an S3 SnapMirror relationship:

```
snapmirror create -source-path svm_name:/bucket/bucket_name -destination
-path object_store_name:/objstore -policy policy_name
```

#### Parameters:

\* `-destination-path` – the object store name you created in the previous step and the fixed value `objstore`.

You can use a policy you created or accept the default.

### Example

```
src_cluster::> snapmirror create -source-path vs0:/bucket/buck-evp
-destination-path sgws-store:/objstore -policy test-policy
```

#### 6. Verify that mirroring is active:

```
snapmirror show -policy-type continuous -fields status
```

= Restore a bucket from a cloud target

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./s3-snapmirror/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

When data in a source bucket is lost or corrupted, you repopulate your data by restoring from a destination bucket.


#### About this task

You can restore the destination bucket to an existing bucket or a new bucket. The target bucket for the restore operation must be larger than the destination bucket's logical used space.

If you use an existing bucket, it must be empty when starting a restore operation. Restore does not "roll back" a bucket in time; rather, it populates an empty bucket with its previous contents.

== System Manager procedure

Restore the back-up data:

1. Click **Protection > Relationships**, then select **S3 SnapMirror**.
2. Click  and then select **Restore**.

3. Under **Source**, select **Existing Bucket** (the default) or **New Bucket**.

- To restore to an **Existing Bucket** (the default), complete these actions:
  - Select the cluster and storage VM to search for the existing bucket.
  - Select the existing bucket.
  - Copy and paste the contents of the *destination* S3 server CA certificate.
- To restore to a **New Bucket**, enter the following values:
  - The cluster and storage VM to host the new bucket.
  - The new bucket's name, capacity, and performance service level.  
See [Storage service levels](#) for more information.
  - The contents of the destination S3 server CA certificate.

4. Under **Destination**, copy and paste the contents of the *source* S3 server CA certificate.

5. Click **Protection > Relationships** to monitor the restore progress.

== CLI procedure

. If you are restoring to a new bucket, create the new bucket. For more information, see [Create a backup relationship for a bucket \(cloud target\)](#).

. Initiate a restore operation for the destination bucket:

```
snapmirror restore -source-path object_store_name:/objstore -destination-path  
svm_name:/bucket/bucket_name
```

+

.Example

+

The following example restores a destination bucket to an existing bucket.

```
clusterA::> snapmirror restore -source-path sgws.store:/objstore -destination  
-path vs0:/bucket/test-bucket
```

= Modify a mirror policy

```
:toc: macro
```

```
:toclevels: 1
```

```
:hardbreaks:
```

```
:icons: font
```

```
:linkattrs:
```


```
:relative_path: ./s3-snapmirror/
```

```
:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/
```

You might want to modify an S3 mirror policy; for example, if you want to adjust the RPO and throttle values.

== System Manager procedure

If you want to adjust these values, you can edit an existing protection policy.

1. Click **Protection > Relationships**, and then select the protection policy for the relationship you want to modify.
2. Click  next to the policy name, then click **Edit**.

== CLI procedure

Modify an S3 SnapMirror policy:

```
snapmirror policy modify -vserver svm_name -policy policy_name [-rpo integer]
[-throttle throttle_type] [-comment text]
```

Parameters:

- `-rpo` – specifies the time for recovery point objective, in seconds.
- `-throttle` – specifies the upper limit on throughput/bandwidth, in kilobytes/seconds.

### Example

```
clusterA::> snapmirror policy modify -vserver vs0 -policy test-policy
-rpo 60
```

= Audit S3 events

= Audit S3 events

:icons: font

:relative\_path: ./s3-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

Beginning with ONTAP 9.10.1, you can audit data and management events in ONTAP S3 environments. S3 audit functionality is similar to existing NAS auditing capabilities, and S3 and NAS auditing can coexist in a cluster.

When you create and enable an S3 auditing configuration on an SVM, S3 events are recorded in a log file. The you can specify the following events to be logged:

- Object access (data) events
  - GetObject, PutObject, and DeleteObject
- Management events
  - PutBucket and DeleteBucket

The log format is JavaScript Object Notation (JSON).

The combined limit for S3 and NFS auditing configurations is 50 SVMs per cluster.

The following license bundle is required:

\* Core Bundle, for ONTAP S3 protocol and storage

For more information, see [How the ONTAP auditing process works](#).

== Guaranteed auditing

By default, S3 and NAS auditing is guaranteed. ONTAP guarantees that all auditable bucket access events are recorded, even if a node is unavailable. A requested bucket operation cannot be completed until the audit record for that operation is saved to the staging volume on persistent storage. If audit records cannot be committed in the staging files, either because of insufficient space or because of other issues, client operations are denied.

## == Space requirements for auditing

In the ONTAP auditing system, audit records are initially stored in binary staging files on individual nodes. Periodically, they are consolidated and converted to user-readable event logs, which are stored in the audit event log directory for the SVM.

The staging files are stored in a dedicated staging volume, which is created by ONTAP when the auditing configuration is created. There is one staging volume per aggregate.

You must plan for sufficient available space in the auditing configuration:

- For the staging volumes in aggregates that contain audited buckets.
- For the volume containing the directory where converted event logs are stored.

You can control the number of event logs, and hence the available space in the volume, using one of two methods when creating the S3 auditing configuration:

- A numerical limit; the `-rotate-limit` parameter controls the minimum number of audit files that must be preserved.
- A time limit; the `-retention-duration` parameter controls the maximum period that files can be preserved.

In both parameters, once that configured is exceeded, older audit files can be deleted to make room for newer ones. For both parameters, the value is 0, indicating that all files must be maintained. In order to ensure sufficient space, it is therefore a best practice to set one of the parameters to a non-zero value.

Because of guaranteed auditing, if the space available for audit data runs out before the rotation limit, newer audit data cannot be created, resulting in failure to clients accessing data. Therefore, the choice of this value and of the space allocated to auditing must be chosen carefully, and you must respond to warnings about available space from the auditing system.

For more information, see [Basic auditing concepts](#).

## = Plan an S3 auditing configuration

:icons: font

:relative\_path: ./s3-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You must specify a number of parameters for the S3 auditing configuration or accept the defaults. In particular, you should consider which log rotation parameters will help ensure adequate free space.

See the `vserver object-store-server audit create` man page for syntax details.

## == General parameters

There are two required parameters that you must specify when you create the auditing configuration. There are also three optional parameters that you can specify.

Type of information	Option	Required
---------------------	--------	----------

<p><i>SVM name</i></p> <p>Name of the SVM on which to create the auditing configuration.</p> <p>The SVM must already exist and be enabled for S3.</p>	<p><code>-verserver svm_name</code></p>	<p>Yes</p>
<p><i>Log destination path</i></p> <p>Specifies where the converted audit logs are stored. The path must already exist on the SVM.</p> <p>The path can be up to 864 characters in length and must have read-write permissions.</p> <p>If the path is not valid, the audit configuration command fails.</p>	<p><code>-destination text</code></p>	<p>Yes</p>
<p><i>Categories of events to audit</i></p> <p>The following event categories can be audited:</p> <ul style="list-style-type: none"> <li>• data GetObject, PutObject, and DeleteObject events</li> <li>• management PutBucket and DeleteBucket events</li> </ul> <p>The default is to audit data events only.</p>	<p><code>-events {data management}, ...</code></p>	<p>No</p>

You can enter one of the following parameters to control the number of audit log files. If no value is entered, all log files are retained.

<b>Type of information</b>	<b>Option</b>	<b>Required</b>
<p><i>Log files rotation limit</i></p> <p>Determines how many audit log files to retain before rotating the oldest log file out. For example, if you enter a value of 5, the last five log files are retained.</p> <p>A value of 0 indicates that all the log files are retained. The default value is 0.</p>	<p><code>-rotate-limit integer</code></p>	<p>No</p>
<p><i>Log files duration limit</i></p> <p>Determines how long a log file can be retained before being deleted. For example, if you enter a value of 5d0h0m, logs more than 5 days old are deleted.</p> <p>A value of 0 indicates that all the log files are retained. The default value is 0.</p>	<p><code>-retention duration integer_time</code></p>	<p>No</p>



## == Parameters for audit log rotation

You can rotate audit logs based on size or schedule. The default is to rotate audit logs based on size.

### === Rotate logs based on log size

If you want to use the default log rotation method and the default log size, you do not need to configure any specific parameters for log rotation. The default log size is 100 MB.

If you do not want to use the default log size, you can configure the `-rotate-size` parameter to specify a custom log size.

If you want to reset the rotation based on a log size alone, use the following command to unset the `-rotate-schedule-minute` parameter:

```
vserver audit modify -vserver svm_name -destination / -rotate-schedule-minute -
```

### === Rotate logs based on a schedule

If you choose to rotate the audit logs based on a schedule, you can schedule log rotation by using the time-based rotation parameters in any combination.

- If you use time-based rotation, the `-rotate-schedule-minute` parameter is mandatory.
- All other time-based rotation parameters are optional.
  - `-rotate-schedule-month`
  - `-rotate-schedule-dayofweek`
  - `-rotate-schedule-day`
  - `-rotate-schedule-hour`
- The rotation schedule is calculated by using all the time-related values. For example, if you specify only the `-rotate-schedule-minute` parameter, the audit log files are rotated based on the minutes specified on all days of the week, during all hours on all months of the year.
- If you specify only one or two time-based rotation parameters (for example, `-rotate-schedule-month` and `-rotate-schedule-minutes`), the log files are rotated based on the minute values that you specified on all days of the week, during all hours, but only during the specified months.

For example, you can specify that the audit log is to be rotated during the months January, March, and August on all Mondays, Wednesdays, and Saturdays at 10:30 a.m.

- If you specify values for both `-rotate-schedule-dayofweek` and `-rotate-schedule-day`, they are considered independently.

For example, if you specify `-rotate-schedule-dayofweek` as Friday and `-rotate-schedule-day` as 13, then the audit logs would be rotated on every Friday and on the 13th day of the specified month, not just on every Friday the 13th.

- If you want to reset the rotation based on a schedule alone, use the following command to unset the `-rotate-size` parameter:

```
vserver audit modify -vserver svm_name -destination / -rotate-size -
```

### === Rotate logs based on log size and schedule

You can choose to rotate the log files based on log size and a schedule by setting both the `-rotate-size` parameter and the time-based rotation parameters in any combination. For example: if `-rotate-size` is set to 10 MB and `-rotate-schedule-minute` is set to 15, the log files rotate when the log file size reaches 10 MB or on the 15th minute of every hour (whichever event occurs first).

= Create and enable an S3 auditing configuration

:icons: font

:relative\_path: ./s3-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

To implement S3 auditing, you first create a persistent object store auditing configuration on an S3-enabled SVM, then enable the configuration.

#### What you'll need

- An S3-enabled SVM.
- Sufficient space for staging volumes in the aggregate.

#### About this task

An auditing configuration is required for each SVM that contains S3 buckets that you wish to audit. You can enable S3 auditing on new or existing S3 servers. Auditing configurations persist in an S3 environment until removed by the **vserver object-store-server audit delete** command.

The S3 auditing configuration applies to all buckets in the SVM that you select for auditing. An audit-enabled SVM can contain audited and un-audited buckets.

It is recommended that you configure S3 auditing for automatic log rotation, determined by log size or a schedule. If you don't configure automatic log rotation, all log files are retained by default. You can also rotate S3 log files manually using the **vserver object-store-server audit rotate-log** command.

If the SVM is an SVM disaster recovery source, the destination path cannot be on the root volume.

#### Procedure

1. Create the auditing configuration to rotate audit logs based on log size or a schedule.

If you want to rotate audit logs by...	Enter...
Log size	<pre>vserver object-store-server audit create -vserver svm_name -destination path [[-events] {data management}, ...] [[-rotate-limit integer]   [-retention-duration [integer_d] [_integer_h][_integer_m][_integers]]] [-rotate- size {integer[KB MB GB TB PB]}]</pre>

If you want to rotate audit logs by...	Enter...
A schedule	<pre>vserver object-store-server audit create -vserver svm_name -destination path [[-events] {data management}, ...] [[-rotate-limit integer]   [-retention-duration [integerd][integerh] [integerm][integers]] ] [-rotate-schedule-month chron_month] [-rotate-schedule-dayofweek chron_dayofweek] [-rotate-schedule-day chron_dayofmonth] [-rotate-schedule-hour chron_hour] -rotate-schedule-minute chron_minute</pre> <p>The <code>-rotate-schedule-minute</code> parameter is required if you are configuring time-based audit log rotation.</p>

## 2. Enable S3 auditing:

```
vserver object-store-server audit enable -vserver svm_name
```

### Examples

The following example creates an auditing configuration that audits all S3 events (the default) using size-based rotation. The logs are stored in the `/audit_log` directory. The log file size limit is 200 MB. The logs are rotated when they reach 200 MB in size.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -rotate
-size 200MB
```

The following example creates an auditing configuration that audits all S3 events (the default) using size-based rotation. The log file size limit is 100 MB (the default), and the logs are retained for 5 days before being deleted.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-retention-duration 5d0h0m
```

The following example creates an auditing configuration that audits S3 management events, and central access policy staging events using time-based rotation. The audit logs are rotated monthly, at 12:30 p.m. on all days of the week. The log rotation limit is 5.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -events
management -rotate-schedule-month all -rotate-schedule-dayofweek all -rotate
-schedule-hour 12 -rotate-schedule-minute 30 -rotate-limit 5
```

= Select buckets for S3 auditing

```
:icons: font
```

```
:relative_path: ./s3-audit/
```

```
:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/
```

You must specify which buckets to audit in an audit-enabled SVM.

### What you'll need

- An SVM enabled for S3 auditing.

### About this task

S3 auditing configurations are enabled on a per-SVM basis, but you must select the buckets in SVMs that are enabled for audit. If you add buckets to the SVM and you want the new buckets to be audited, you must select them with this procedure. You can also have non-audited buckets in an SVM enabled for S3 auditing.

Auditing configurations persist for buckets until removed by the `vserver object-store-server audit object-select delete` command.

### Procedure

Select a bucket for S3 auditing:

```
vserver object-store-server audit event-selector create -vserver svm_name
-bucket bucket_name [[-access] {read-only|write-only|all}] [[-permission]
{allow-only|deny-only|all}]
```

- `-access` - specifies the type of event access to be audited: `read-only`, `write-only` or `all` (default is `all`).
- `-permission` - specifies the type of event permission to be audited: `allow-only`, `deny-only` or `all` (default is `all`).

### Example

The following example creates a bucket auditing configuration that only logs allowed events with read-only access:

```
cluster1::> vserver object-store-server audit event-selector create -vserver
vs1 -bucket test-bucket -access read-only -permission allow-only
```

= Modify an S3 auditing configuration

:icons: font

:relative\_path: ./s3-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

You can modify the auditing parameters of individual buckets or the auditing configuration of all buckets selected for audit in the SVM.

**Table 2. Procedure**

If you want to modify the audit configuration for...	Enter...
Individual buckets	<code>vserver object-store-server audit event-selector modify -vserver <i>svm_name</i> [-bucket <i>bucket_name</i>] [<i>parameters to modify</i>]</code>
All buckets in the SVM	<code>vserver object-store-server audit modify -vserver <i>svm_name</i> [<i>parameters to modify</i>]</code>

### Examples

The following example modifies an individual bucket auditing configuration to audit only write-only access

events:

```
cluster1::> vserver object-store-server audit event-selector modify
-vserver vs1 -bucket test-bucket -access write-only
```

The following example modifies the auditing configuration of all buckets in the SVM to change the log size limit to 10MB and to retain 3 log files before rotating.

```
cluster1::> vserver object-store-server audit modify -vserver vs1
-rotate-size 10MB -rotate-limit 3
```

= Show S3 auditing configurations

:icons: font

:relative\_path: ./s3-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

After completing the auditing configuration, you can verify that auditing is configured properly and is enabled. You can also display information about all object store auditing configurations in the cluster.

#### About this task

You can display information about bucket and SVM auditing configurations.

- Buckets – use the `vserver object-store-server audit event-selector show` command

Without any parameters, the command displays the following information about buckets in all SVMs in the cluster with object store auditing configurations:

- SVM name
- Bucket name
- Access and permission values

- SVMs – use the `vserver object-store-server audit show` command

Without any parameters, the command displays the following information about all SVMs in the cluster with object store auditing configurations:

- SVM name
- Audit state
- Target directory

You can specify the `-fields` parameter to specify which audit configuration information to display.

#### Procedure

Show information about S3 auditing configurations:

If you want to modify the configuration for...	Enter...
Buckets	<code>vserver object-store-server audit event-selector show [-vserver <i>svm_name</i>] [<i>parameters</i>]</code>
SVMs	<code>vserver object-store-server audit show [-vserver <i>svm_name</i>] [<i>parameters</i>]</code>

### Examples

The following example displays information for a single bucket:

```
cluster1::> vserver object-store-server audit event-selector show
-vserver vs1 -bucket test-bucket
```

Vserver	Bucket	Access	Permission
vs1	bucket1	read-only	allow-only

The following example displays information for all buckets on an SVM:

```
cluster1::> vserver object-store-server audit event-selector show
-vserver vs1
```

Vserver	:vs1
Bucket	:test-bucket
Access	:all
Permission	:all

The following example displays the name, audit state, event types, log format, and target directory for all SVMs.

```
cluster1::> vserver object-store-server audit show
```

Vserver	State	Event Types	Log Format	Target Directory
vs1	false	data	json	/audit_log

The following example displays the SVM names and details about the audit log for all SVMs.

```
cluster1::> vserver object-store-server audit show -log-save-details
```

Vserver	Rotation		Rotation
	File Size	Rotation Schedule	Limit
vs1	100MB	-	0

The following example displays in list form all audit configuration information about all SVMs.

```
cluster1::> vserver object-store-server audit show -instance
```

```
          Vserver: vs1
          Auditing state: true
          Log Destination Path: /audit_log
    Categories of Events to Audit: data
          Log Format: json
          Log File Size Limit: 100MB
    Log Rotation Schedule: Month: -
    Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
          Log Rotation Schedule: Hour: -
    Log Rotation Schedule: Minute: -
          Rotation Schedules: -
          Log Files Rotation Limit: 0
          Log Retention Time: 0s
```

= Security and data encryption

:hardbreaks:

:linkattrs:

:relative\_path: ./security-encryption/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

= Manage security with System Manager

= Security management overview with System Manager

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

Beginning with ONTAP 9.7, you can manage cluster security with System Manager.

With System Manager, you use ONTAP standard methods to secure client and administrator access to storage and to protect against viruses. Advanced technologies are available for encryption of data at rest

and for WORM storage.

If you are using the classic System Manager (available only in ONTAP 9.7 and earlier), refer to [System Manager Classic \(ONTAP 9.0 to 9.7\)](#)

== Client authentication and authorization

ONTAP authenticates a client machine and user by verifying their identities with a trusted source. ONTAP authorizes a user to access a file or directory by comparing the user's credentials with the permissions configured on the file or directory.

== Administrator authentication and RBAC

Administrators use local or remote login accounts to authenticate themselves to the cluster and storage VM. Role-Based Access Control (RBAC) determines the commands to which an administrator has access.

== Virus scanning

You can use integrated antivirus functionality on the storage system to protect data from being compromised by viruses or other malicious code. ONTAP virus scanning, called *Vscan*, combines best-in-class third-party antivirus software with ONTAP features that give you the flexibility you need to control which files get scanned and when.

== Encryption

ONTAP offers both software- and hardware-based encryption technologies for ensuring that data at rest cannot be read if the storage medium is repurposed, returned, misplaced, or stolen.

== WORM storage

*SnapLock* is a high-performance compliance solution for organizations that use *write once, read many (WORM)* storage to retain critical files in unmodified form for regulatory and governance purposes.

= Set up multifactor authentication

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

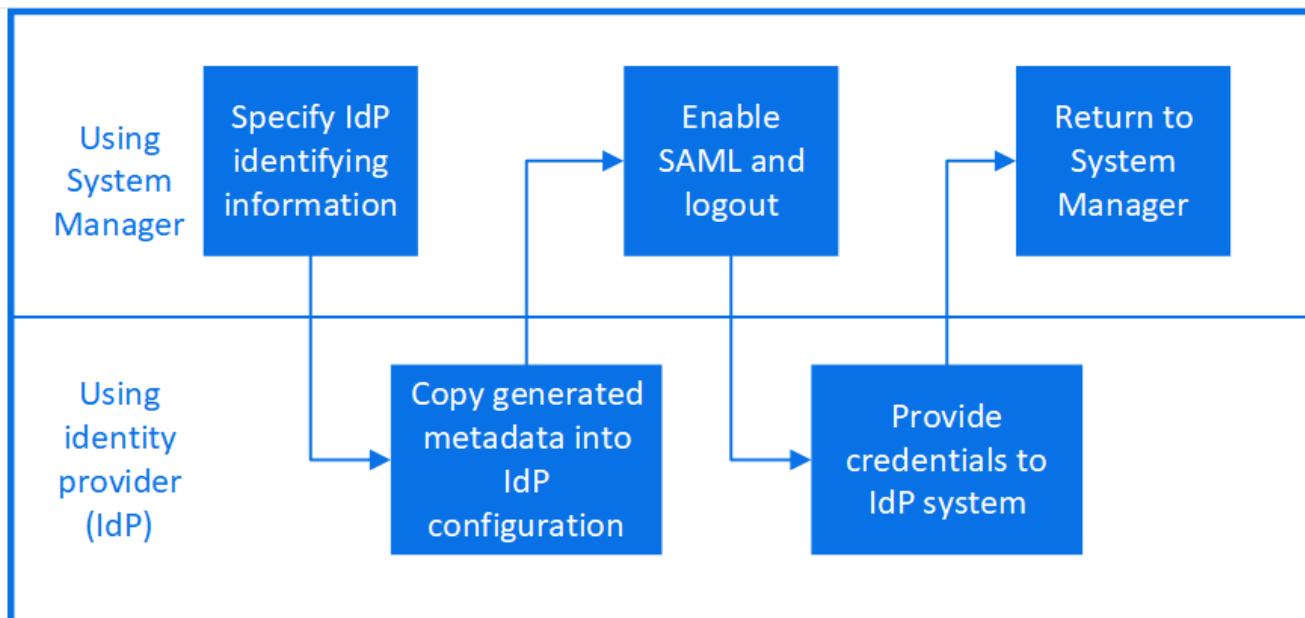
Security Assertion Markup Language (SAML) authentication allows users to log in to an application by using a secure identity provider (IdP).

In System Manager, in addition to standard ONTAP authentication, SAML-based authentication is provided as an option for multifactor authentication.

Security Assertion Markup Language (SAML) is an XML-based framework for authentication and authorization between two entities: a service provider and an identity provider.


== Enable SAML authentication





To enable SAML authentication, perform the following steps:


### Steps

1. Click **Cluster > Settings**.
2. Next to **SAML Authentication**, click .
3. Ensure there is a check in the **Enable SAML Authentication** checkbox.
4. Enter the URL of the IdP URI (including "https://").
5. Modify the host system address, if needed.
6. Ensure the correct certificate is being used:
  - If your system was mapped with only one certificate with type "server", then that certificate is considered the default and it isn't displayed.
  - If your system was mapped with multiple certificates as type "server", then one of the certificates is displayed. To select a different certificate, click **Change**.
7. Click **Save**. A confirmation window displays the metadata information, which has been automatically copied to your clipboard.
8. Go to the IdP system you specified and copy the metadata from your clipboard to update the system metadata.
9. Return to the confirmation window (in System Manager) and check the checkbox **I have configured the IdP with the host URI or metadata**.
10. Click **Logout** to enable SAML-based authentication. The IdP system will display an authentication screen.
11. In the IdP system, enter your SAML-based credentials. After your credentials are verified, you will be directed to the System Manager home page.

== Disable SAML authentication

To disable SAML authentication, perform the following steps:

### Steps

1. Click **Cluster > Settings**.
2. Under **SAML Authentication**, click the **Enabled** toggle button.
3. *Optional:* You can also click  next to **SAML Authentication**, and then uncheck the **Enable SAML Authentication** checkbox.

= Control administrator access

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

The role assigned to an administrator determines which functions the administrator can perform with System Manager. Predefined roles for cluster administrators and storage VM administrators are provided by System Manager. You assign the role when you create the administrator's account, or you can assign a different role later.

Depending on how you have enabled account access, you might need to perform any of the following:



- Associate a public key with a local account.
- Install a CA-signed server digital certificate.
- Configure AD, LDAP, or NIS access.

You can perform these tasks before or after enabling account access.

== Assigning a role to an administrator

Assign a role to an administrator, as follows:


### Steps

1. Click **Cluster > Settings**.
2. Click  next to **Users and Roles**.
3. Click  **Add** under **Users**.
4. Specify a user name, and select a role in the drop-down menu for **Role**.
5. Specify a login method and password for the user.

== Changing an administrator's role

Change the role for an administrator, as follows:

### Steps


1. Click **Cluster > Settings**.
2. Select the name of user whose role you want to change, then click the  that appears next to the user name.
3. Click **Edit**.
4. Select a role in the drop-down menu for **Role**.

= Diagnose and correct file access issues  
:toc: macro  
:toclevels: 1  
:hardbreaks:  
:icons: font  
:linkattrs:  
:relative\_path: ./  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./san-admin/./media/

### Steps

1. In System Manager, select **Storage > Storage VMs**.
2. Select the storage VM on which you want to perform a trace.
3. Click  **More**.
4. Click **Trace File Access**.
5. Provide the user name and client IP address, then click **Start Tracing**.

The trace results are displayed in a table. The **Reasons** column provides the reason why a file could not be accessed.

6. Click  in the left column of the results table to view the file access permissions.

= Manage certificates with System Manager


Beginning with ONTAP 9.10.1, you can use System Manager to manage trusted certificate authorities, client/server certificates, and local (onboard) certificate authorities.

With System Manager, you can manage the certificates received from other applications so you can authenticate communications from those applications. You can also manage your own certificates that identify your system to other applications.

== View certificate information

With System Manager, you can view trusted certificate authorities, client/server certificates, and local certificate authorities that are stored on the cluster.

### Steps

1. In System Manager, click **Cluster > Settings**.
2. Scroll to the **Security** area.  
In the **Certificates** section, the following details are displayed:
  - The number of stored trusted certificate authorities.
  - The number of stored client/server certificates.
  - The number of stored local certificate authorities.
3. Click any number to view details about a category of certificates, or click  to view the **Certificates** page, which contains information about all categories.  
The list displays the information for the entire cluster. If you want to display information for only a specific storage VM, perform the following steps:
  - a. Click **Storage > Storage VMs**.

- b. Select the storage VM.
- c. View the **Settings** tab.
- d. Click a number shown in the **Certificate** section.

### What to do next

- From the **Certificates** page, you can [\[Generate a certificate signing request\]](#).
- The certificate information is separated into three tabs, one for each category. You can perform the following tasks from each tab:

On this tab...	You can perform these procedures...
<b>Trusted certificate authorities</b>	<ul style="list-style-type: none"> <li>• <a href="#">[install-trusted-cert]</a></li> <li>• <a href="#">[Delete a trusted certificate authority]</a></li> <li>• <a href="#">[Renew a trusted certificate authority]</a></li> </ul>
<b>Client/server certificates</b>	<ul style="list-style-type: none"> <li>• <a href="#">[install-cs-cert]</a></li> <li>• <a href="#">[gen-cs-cert]</a></li> <li>• <a href="#">[delete-cs-cert]</a></li> <li>• <a href="#">[renew-cs-cert]</a></li> </ul>
<b>Local certificate authorities</b>	<ul style="list-style-type: none"> <li>• <a href="#">[Create a new local certificate authority]</a></li> <li>• <a href="#">[Sign a certificate using a local certificate authority]</a></li> <li>• <a href="#">[Delete a local certificate authority]</a></li> <li>• <a href="#">[Renew a local certificate authority]</a></li> </ul>

== Generate a certificate signing request

You can generate a certificate signing request (CSR) with System Manager from any tab of the **Certificates** page. A private key and a corresponding CSR are generated, which can be signed using a certificate authority to generate a public certificate.


### Steps

1. View the **Certificates** page. See [\[View certificate information\]](#).
2. Click **+Generate CSR**.
3. Complete the information for the subject name:
  - a. Enter a **common name**.
  - b. Select a **country**.
  - c. Enter an **organization**.
  - d. Enter an **organization unit**.
4. If you want to override defaults, select **More Options** and provide additional information.

== Install (add) a trusted certificate authority

You can install additional trusted certificate authorities in System Manager.

### Steps

1. View the **Trusted Certificate Authorities** tab. See [\[View certificate information\]](#).
2. Click  .
3. On the **Add Trusted Certificate Authority** panel, perform the following:
  - Enter a **name**.
  - For the **scope**, select a storage VM.
  - Enter a **common name**.
  - Select a **type**.
  - Enter or import **certificate details**.


== Delete a trusted certificate authority

With System Manager, you can delete a trusted certificate authority.



You cannot delete trusted certificate authorities that were preinstalled with ONTAP.


### Steps

1. View the **Trusted Certificate Authorities** tab. See [\[View certificate information\]](#).
2. Click the name of the trusted certificate authority.
3. Click  next to the name, then click **Delete**.

== Renew a trusted certificate authority

With System Manager, you can renew a trusted certificate authority that has expired or is about to expire.

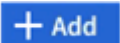
### Steps

1. View the **Trusted Certificate Authorities** tab. See [\[View certificate information\]](#).
2. Click the name of the trusted certificate authority.
3. Click  next to the name, then click **Renew**.

== Install (add) a client/server certificate

With System Manager, you can install additional client/server certificates.

### Steps

1. View the **Client/Server Certificates** tab. See [\[View certificate information\]](#).
2. Click  .
3. On the **Add Client/Server Certificate** panel, perform the following:
  - Enter a **certificate name**.
  - For the **scope**, select a storage VM.
  - Enter a **common name**.
  - Select a **type**.
  - Enter or import **certificate details**.

You can either write in or copy and paste in the certificate details from a text file or you can import

the text from a certificate file by clicking **Import**.

- Enter a the **private key**.

You can either write in or copy and paste in the private key from a text file or you can import the text from a private key file by clicking **Import**.

== Generate (add) a self-signed client/server certificate

With System Manager, you can generate additional self-signed client/server certificates.


### Steps

1. View the **Client/Server Certificates** tab. See [\[View certificate information\]](#).
2. Click **+Generate Self-signed Certificate**.
3. On the **Generate Self-Signed Certificate** panel, perform the following:
  - Enter a **certificate name**.
  - For the **scope**, select a storage VM.
  - Enter a **common name**.
  - Select a **type**.
  - Select a **hash function**.
  - Select a **key size**.
  - Select a **storage VM**.

== Delete a client/server certificate

With System Manager, you can delete client/server certificates.


### Steps

1. View the **Client/Server Certificates** tab. See [\[View certificate information\]](#).
2. Click the name of the client/server certificate.
3. Click  next to the name, then click **Delete**.

== Renew a client/server certificate

With System Manager, you can renew a client/server certificate that has expired or is about to expire.

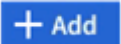
### Steps

1. View the **Client/Server Certificates** tab. See [\[View certificate information\]](#).
2. Click the name of the client/server certificate.
3. Click  next to the name, then click **Renew**.

== Create a new local certificate authority

With System Manager, you can create a new local certificate authority.

### Steps

1. View the **Local Certificate Authorities** tab. See [\[View certificate information\]](#).
2. Click  .

3. On the **Add Local Certificate Authority** panel, perform the following:


- Enter a **name**.
- For the **scope**, select a storage VM.
- Enter a **common name**.

4. If you want to override defaults, select **More Options** and provide additional information.

== Sign a certificate using a local certificate authority

In System Manager, you can use a local certificate authority to sign a certificate.


### Steps

1. View the **Local Certificate Authorities** tab. See [\[View certificate information\]](#).
2. Click the name of the local certificate authority.
3. Click  next to the name, then click **Sign a certificate**.
4. Complete the **Sign a Certificate Signing Request** form.
  - You can either paste in the certificate signing content or import a certificate signing request file by clicking **Import**.
  - Specify the number of days for which the certificate will be valid.

== Delete a local certificate authority

With System Manager, you can delete a local certificate authority.


### Steps

1. View the **Local Certificate Authority** tab. See [\[View certificate information\]](#).
2. Click the name of the local certificate authority.
3. Click  next to the name, then click **Delete**.

== Renew a local certificate authority

With System Manager, you can renew a local certificate authority that has expired or is about to expire.

### Steps

1. View the **Local Certificate Authority** tab. See [\[View certificate information\]](#).
2. Click the name of the local certificate authority.
3. Click  next to the name, then click **Renew**.

= Manage administrator authentication and RBAC with the CLI

= Administrator authentication and RBAC overview with the CLI

```
:icons: font
```

```
:relative_path: ./authentication/
```

```
:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/
```

You can enable login accounts for ONTAP cluster administrators and storage virtual machine (SVM) administrators. You can also use role-based access control (RBAC) to define the capabilities of administrators.

You enable login accounts and RBAC in the following ways:

- You want to use the ONTAP command-line interface (CLI), not System Manager or an automated scripting tool.
- You want to use best practices, not explore every available option.
- You are not using SNMP to collect information about the cluster.

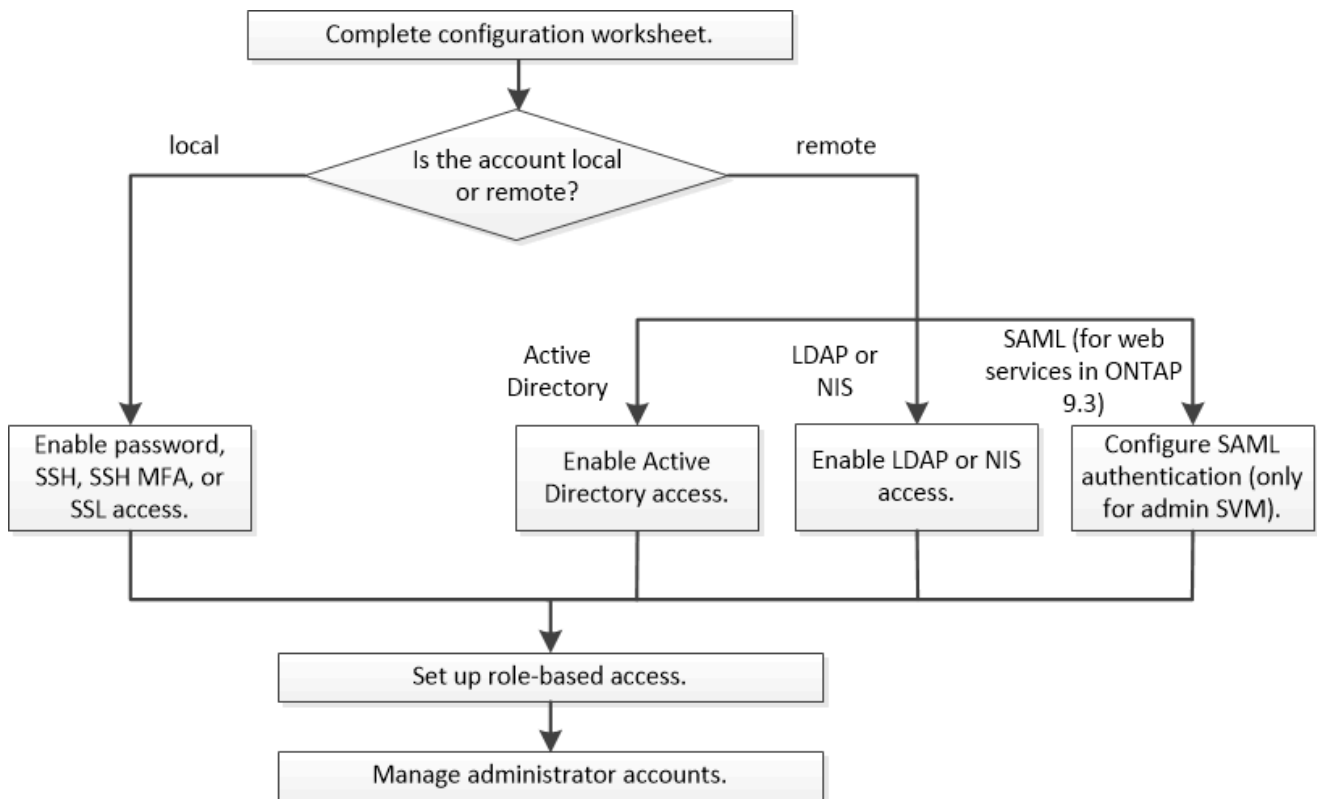
= Administrator authentication and RBAC workflow

:icons: font

:relative\_path: ./authentication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You can enable authentication for local administrator accounts or remote administrator accounts. The account information for a local account resides on the storage system and the account information for a remote account resides elsewhere. Each account can have a predefined role or a custom role.



You can enable local administrator accounts to access an admin storage virtual machine (SVM) or a data SVM with the following types of authentication:

- Password
- SSH public key
- SSL certificate
- SSH multifactor authentication (MFA)

Beginning with ONTAP 9.3, authentication with password and public key is supported.



You can enable remote administrator accounts to access an admin SVM or a data SVM with the following types of authentication:

- Active Directory
- SAML authentication (only for admin SVM)

Beginning with ONTAP 9.3, Security Assertion Markup Language (SAML) authentication can be used for accessing the admin SVM by using any of the following web services: Service Processor Infrastructure, ONTAP APIs, or System Manager.

- Beginning with ONTAP 9.4, SSH MFA can be used for remote users on LDAP or NIS servers. Authentication with nsswitch and public key is supported.

= Worksheets for administrator authentication and RBAC configuration

:icons: font

:relative\_path: ./authentication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

Before creating login accounts and setting up role-based access control (RBAC), you should gather information for each item in the configuration worksheets.

== Create or modify login accounts

You provide these values with the `security login create` command when you enable login accounts to access a storage virtual machine (SVM). You provide the same values with the `security login modify` command when you modify how an account accesses an SVM.

Field	Description	Your value
<code>-vserver</code>	The name of the SVM that the account accesses. The default value is the name of the admin SVM for the cluster.	
<code>-user-or-group-name</code>	The user name or group name of the account. Specifying a group name enables access to each user in the group. You can associate a user name or group name with multiple applications.	
<code>-application</code>	The application that is used to access the SVM: <ul style="list-style-type: none"><li>• <code>http</code></li><li>• <code>ontapi</code></li><li>• <code>snmp</code></li><li>• <code>ssh</code></li></ul>	

-authmethod	<p>The method that is used to authenticate the account:</p> <ul style="list-style-type: none"> <li>• <code>cert</code> for SSL certificate authentication</li> <li>• <code>domain</code> for Active Directory authentication</li> <li>• <code>nsswitch</code> for LDAP or NIS authentication</li> <li>• <code>password</code> for user password authentication</li> <li>• <code>publickey</code> for public key authentication</li> <li>• <code>community</code> for SNMP community strings</li> <li>• <code>usm</code> for SNMP user security model</li> <li>• <code>saml</code> for Security Assertion Markup Language (SAML) authentication</li> </ul>	
-remote-switch-ipaddress	<p>The IP address of the remote switch. The remote switch can be a cluster switch monitored by the cluster switch health monitor (CSHM) or a Fibre Channel (FC) switch monitored by the MetroCluster health monitor (MCC-HM). This option is applicable only when the application is <code>snmp</code> and the authentication method is <code>usm</code>.</p>	
-role	<p>The access control role that is assigned to the account:</p> <ul style="list-style-type: none"> <li>• For the cluster (the admin SVM), the default value is <code>admin</code>.</li> <li>• For a data SVM, the default value is <code>vsadmin</code>.</li> </ul>	
-comment	<p>(Optional) Descriptive text for the account. You should enclose the text in double quotation marks (").</p>	

<code>-is-ns-switch-group</code>	Whether the account is an LDAP group account or NIS group account (yes or no).	
----------------------------------	--	--

Support for nsswitch is available from **ONTAP 9.4**

The order of authentication is always the public key followed by the password.

a|

a|

`-is-ldap-fastbind`

a|

Beginning with ONTAP 9.11.1, when set to true, enables LDAP fast bind for nsswitch authentication; the default is false. To use LDAP fast bind, the `-authentication-method` value must be set to `nsswitch`. [Learn about LDAP fastbind for nsswitch authentication.](#)

a|

== Define custom roles

You provide these values with the `security login role create` command when you define a custom role.

[cols="3\*"]

h  Field	h  Description	h  Your value
----------	----------------	---------------

a|

`-vserver`

a|

(Optional) The name of the SVM that is associated with the role.

a|

a|

`-role`

a|

The name of the role.

a|

a|

`-cmddirname`

a|

The command or command directory to which the role gives access. You should enclose command subdirectory names in double quotation marks ("). For example, `"volume snapshot"`. You must enter `DEFAULT` to specify all command directories.

a|

a|

`-access`

a|

(Optional) The access level for the role. For command directories:

- `none` (the default value for custom roles) denies access to commands in the command directory
- `readonly` grants access to the `show` commands in the command directory and its subdirectories
- `all` grants access to all of the commands in the command directory and its subdirectories

For *nonintrinsic commands* (commands that do not end in `create`, `modify`, `delete`, or `show`):

- `none` (the default value for custom roles) denies access to the command
- `readonly` is not applicable
- `all` grants access to the command

To grant or deny access to intrinsic commands, you must specify the command directory.

a|

a|

`-query`

a|

(Optional) The query object that is used to filter the access level, which is specified in the form of a valid option for the command or for a command in the command directory. You should enclose the query object in double quotation marks ("). For example, if the command directory is `volume`, the query object `"-aggr aggr0"` would enable access for the `aggr0` aggregate only.

a|

== Associate a public key with a user account

You provide these values with the `security login publickey create` command when you associate an SSH public key with a user account.

[cols="3\*"]

h| Field h| Description h| Your value

a|

`-vserver`

a|

(Optional) The name of the SVM that the account accesses.

a|

a|

`-username`

a|

The user name of the account. The default value, `admin`, which is the default name of the cluster administrator.

a|

a|

`-index`

a|

The index number of the public key. The default value is 0 if the key is the first key that is created for the account; otherwise, the default value is one more than the highest existing index number for the account.

a|

a|

`-publickey`

a|

The OpenSSH public key. You should enclose the key in double quotation marks (").

a|

a|

-role

a|

The access control role that is assigned to the account.

a|

a|

-comment

a|

(Optional) Descriptive text for the public key. You should enclose the text in double quotation marks ("").

a|

== Install a CA-signed server digital certificate

You provide these values with the `security certificate generate-csr` command when you generate a digital certificate signing request (CSR) for use in authenticating an SVM as an SSL server.

[cols="3\*"]

h| Field h| Description h| Your value

a|

-common-name

a|

The name of the certificate, which is either a fully qualified domain name (FQDN) or a custom common name.

a|

a|

-size

a|

The number of bits in the private key. The higher the value, the more secure the key. The default value is 2048. Possible values are 512, 1024, 1536, and 2048.

a|

a|

-country

a|

The country of the SVM, in a two-letter code. The default value is `US`. See the man pages for a list of codes.

a|

a|

-state

a|

The state or province of the SVM.

a|

a|

-locality

a|

The locality of the SVM.

a|

a|

-organization

a|

The organization of the SVM.

a|

a|

-unit

a|

The unit in the organization of the SVM.

a|

a|

-email-addr

a|

The email address of the contact administrator for the SVM.

a|

a|

-hash-function

a|

The cryptographic hashing function for signing the certificate. The default value is `SHA256`. Possible values are `SHA1`, `SHA256`, and `MD5`.

a|

You provide these values with the `security certificate install` command when you install a CA-signed digital certificate for use in authenticating the cluster or SVM as an SSL server. Only the options that are relevant to this guide are shown in the following table.

[cols="3\*"]

h  Field h	Description h	Your value
------------	---------------	------------

a		
---	--	--

-vserver		
----------	--	--

a		
---	--	--

The name of the SVM on which the certificate is to be installed.		
--	--	--

a		
---	--	--

a		
---	--	--

-type		
-------	--	--

a		
---	--	--

The certificate type:		
-----------------------	--	--

- `server` for server certificates and intermediate certificates
- `client-ca` for the public key certificate of the root CA of the SSL client
- `server-ca` for the public key certificate of the root CA of the SSL server of which ONTAP is a client
- `client` for a self-signed or CA-signed digital certificate and private key for ONTAP as an SSL client

a|

== Configure Active Directory domain controller access

You provide these values with the `security login domain-tunnel create` command when you have already configured a SMB server for a data SVM and you want to configure the SVM as a gateway or *tunnel* for Active Directory domain controller access to the cluster.

[cols="3\*"]

h| Field h| Description h| Your value

a|

-vserver

a|

The name of the SVM for which the SMB server has been configured.

a|

You provide these values with the `vserver active-directory create` command when you have not configured a SMB server and you want to create an SVM computer account on the Active Directory domain.

[cols="3\*"]

h| Field h| Description h| Your value

a|

-vserver

a|

The name of the SVM for which you want to create an Active Directory computer account.

a|

a|

-account-name

a|

The NetBIOS name of the computer account.

a|

a|

-domain

a|

The fully qualified domain name (FQDN).

a|

a|

-ou

a|

The organizational unit in the domain. The default value is `CN=Computers`. ONTAP appends this value to the domain name to produce the Active Directory distinguished name.

a|



== Configure LDAP or NIS server access

You provide these values with the `vserver services name-service ldap client create` command when you create an LDAP client configuration for the SVM.

[NOTE]

Beginning with ONTAP 9.2, the `-ldap-servers` field replaces the `-servers` field. This new field can take either a host name or an IP address as the value for the LDAP server.

Only the options that are relevant to this guide are shown in the following table:

Field	Description	Your value
<code>-vserver</code>	The name of the SVM for the client configuration.	
<code>-client-config</code>	The name of the client configuration.	
<code>-servers</code>	<b>ONTAP 9.0, 9.1:</b> A comma-separated list of IP addresses for the LDAP servers to which the client connects.	
<code>-ldap-servers</code>	<b>ONTAP 9.2:</b> A comma-separated list of IP addresses and host names for the LDAP servers to which the client connects.	
<code>-schema</code>	The schema that the client uses to make LDAP queries.	

Start TLS is supported for access to data SVMs only. It is not supported for access to admin SVMs.

a|

You provide these values with the `vserver services name-service ldap create` command when you associate an LDAP client configuration with the SVM.

[cols="3\*"]

h| Field h| Description h| Your value

a|

`-vserver`

a|

The name of the SVM with which the client configuration is to be associated.

a|

a|

`-client-config`

a|

The name of the client configuration.

a|

a|

`-client-enabled`

a|

Whether the SVM can use the LDAP client configuration (`true` or `false`).

a|

You provide these values with the `vserver services name-service nis-domain create` command when you create an NIS domain configuration on an SVM.

[NOTE]

Beginning with ONTAP 9.2, the `-nis-servers` field replaces the `-servers` field. This new field can take either a host name or an IP address as the value for the NIS server.

Field	Description	Your value
-vserver	The name of the SVM on which the domain configuration is to be created.	
-domain	The name of the domain.	
-active	Whether the domain is active (true or false).	
-servers	<b>ONTAP 9.0, 9.1:</b> A comma-separated list of IP addresses for the NIS servers that are used by the domain configuration.	
-nis-servers	<b>ONTAP 9.2:</b> A comma-separated list of IP addresses and host names for the NIS servers that are used by the domain configuration.	

You provide these values with the `vserver services name-service ns-switch create` command when you specify the look-up order for name service sources.

Field	Description	Your value
-vserver	The name of the SVM on which the name service look-up order is to be configured.	
-database	The name service database: <ul style="list-style-type: none"> <li>• <code>hosts</code> for files and DNS name services</li> <li>• <code>group</code> for files, LDAP, and NIS name services</li> <li>• <code>passwd</code> for files, LDAP, and NIS name services</li> <li>• <code>netgroup</code> for files, LDAP, and NIS name services</li> <li>• <code>namemap</code> for files and LDAP name services</li> </ul>	

<code>-sources</code>	<p>The order in which to look up name service sources (in a comma-separated list):</p> <ul style="list-style-type: none"> <li>• files</li> <li>• dns</li> <li>• ldap</li> <li>• nis</li> </ul>	
-----------------------	--	--

## == Configure SAML access

Beginning with ONTAP 9.3, you provide these values with the `security saml-sp create` command to configure SAML authentication.

Field	Description	Your value
<code>-idp-uri</code>	The FTP address or HTTP address of the Identity Provider (IdP) host from where the IdP metadata can be downloaded.	
<code>-sp-host</code>	The host name or IP address of the SAML service provider host (ONTAP system). By default, the IP address of the cluster-management LIF is used.	
<code>{[-cert-ca] and [-cert-serial] or [-cert-common-name]}</code>	The server certificate details of the service provider host (ONTAP system).	
<code>-verify-metadata-server</code>	Whether the identity of the IdP metadata server must be validated ( <code>true</code> or <code>false</code> ). The best practice is to always set this value to <code>true</code> .	

## = Create login accounts

### = Create login accounts overview

`:icons: font`

`:relative_path: ./authentication/`

`:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/`

You can enable local or remote cluster and SVM administrator accounts. A local account is one in which the account information, public key, or security certificate resides on the storage system. AD account information is stored on a domain controller. LDAP and NIS accounts reside on LDAP and NIS servers.

## == Cluster and SVM administrators

A *cluster administrator* accesses the admin SVM for the cluster. The admin SVM and a cluster administrator with the reserved name `admin` are automatically created when the cluster is set up.

A cluster administrator with the default `admin` role can administer the entire cluster and its resources. The cluster administrator can create additional cluster administrators with different roles as needed.

An *SVM administrator* accesses a data SVM. The cluster administrator creates data SVMs and SVM administrators as needed.

SVM administrators are assigned the `vsadmin` role by default. The cluster administrator can assign different roles to SVM administrators as needed.

The following generic names cannot be used for remote cluster and SVM administrator accounts: "adm", "bin", "cli", "daemon", "ftp", "games", "halt", "lp", "mail", "man", "naroot", "netapp", "news", "nobody", "operator", "root", "shutdown", "sshd", "sync", "sys", "uucp", and "www".

## == Merged roles

If you enable multiple remote accounts for the same user, the user is assigned the union of all roles specified for the accounts. That is, if an LDAP or NIS account is assigned the `vsadmin` role, and the AD group account for the same user is assigned the `vsadmin-volume` role, the AD user logs in with the more inclusive `vsadmin` capabilities. The roles are said to be *merged*.

### = Enable local account access

#### = Enable local account access overview

:icons: font

:relative\_path: ./authentication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

A local account is one in which the account information, public key, or security certificate resides on the storage system. You can use the `security login create` command to enable local accounts to access an admin or data SVM.

### = Enable password account access

:icons: font

:relative\_path: ./authentication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You can use the `security login create` command to enable administrator accounts to access an admin or data SVM with a password. You are prompted for the password after you enter the command.

## What you'll need

You must be a cluster administrator to perform this task.

## About this task

If you are unsure of the access control role that you want to assign to the login account, you can use the `security login modify` command to add the role later.

## Step

1. Enable local administrator accounts to access an SVM using a password:

```
security login create -vserver SVM_name -user-or-group-name
user_or_group_name -application application -authmethod
authentication_method -role role -comment comment
```

For complete command syntax, see the [worksheet](#).

The following command enables the cluster administrator account `admin1` with the predefined `backup` role to access the admin SVM `engCluster` using a password. You are prompted for the password after you enter the command.

```
cluster1::>security login create -vserver engCluster -user-or-group
-name admin1 -application ssh -authmethod password -role backup
```

= Enable SSH public key accounts

:icons: font

:relative\_path: ./authentication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You can use the `security login create` command to enable administrator accounts to access an admin or data SVM with an SSH public key.

### What you'll need

You must be a cluster administrator to perform this task.

### About this task

- You must associate the public key with the account before the account can access the SVM.

#### [Associating a public key with a user account](#)

You can perform this task before or after you enable account access.

- If you are unsure of the access control role that you want to assign to the login account, you can use the `security login modify` command to add the role later.

If you want to enable SSL FIPS mode on a cluster where administrator accounts authenticate with an SSH public key before accessing SVMs, you must ensure that the host key algorithm is supported before enabling FIPS.

**Note:** Host key algorithm support has changed in ONTAP 9.11.1 and later releases.

ONTAP release	Supported key types	Unsupported key types
9.11.1 and later	ecdsa-sha2-nistp256	rsa-sha2-512 rsa-sha2-256 ssh-ed25519 ssh-dss ssh-rsa
9.10.1 and earlier	ecdsa-sha2-nistp256 ssh-ed25519	ssh-dss ssh-rsa

Existing SSH public key accounts without the supported key algorithms must be reconfigured with a supported key type before enabling FIPS, or the administrator authentication will fail.

For more information, see [Configure network security using FIPS](#).

### Step

1. Enable local administrator accounts to access an SVM using an SSH public key:

```
security login create -vserver SVM_name -user-or-group-name  
user_or_group_name -application application -authmethod  
authentication_method -role role -comment comment
```

For complete command syntax, see the [worksheet](#).

The following command enables the SVM administrator account `svmadmin1` with the predefined `vsadmin-volume` role to access the `SVMengData1` using an SSH public key:

```
cluster1::>security login create -vserver engData1 -user-or-group
-name svmadmin1 -application ssh -authmethod publickey -role
vsadmin-volume
```

### After you finish

If you have not associated a public key with the administrator account, you must do so before the account can access the SVM.

### Associating a public key with a user account

= Enable SSH multifactor authentication (MFA)

:icons: font

:relative\_path: ./authentication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

Beginning with ONTAP 9.3, you can use the `security login create` command to enhance security by requiring that administrators log in to an admin or data SVM with both an SSH public key and a user password.

### Before you begin

You must be a cluster administrator to perform this task.

### About this task

- You must associate the public key with the account before the account can access the SVM.

#### Associate a public key with a user account

You can perform this task before or after you enable account access.

- If you are unsure of the access control role that you want to assign to the login account, you can use the `security login modify` command to add the role later.

#### Modifying the role assigned to an administrator

- The user is always authenticated with public key authentication followed by password authentication.

### Step

1. Require local administrator accounts to access an SVM using SSH MFA:

```
security login create -vserver SVM -user-or-group-name user_name
-application ssh -authentication-method password|publickey -role admin
-second-authentication-method password|publickey
```

The following command requires the SVM administrator account `admin2` with the predefined `admin` role to log in to the `SVMengData1` with both an SSH public key and a user password:



```
cluster-1::> security login create -vserver engData1 -user-or-group
-name admin2 -application ssh -authentication-method publickey -role
admin -second-authentication-method password
```

Please enter a password for user 'admin2':

Please enter it again:

Warning: To use public-key authentication, you must create a public key for user "admin2".

### After you finish

If you have not associated a public key with the administrator account, you must do so before the account can access the SVM.

#### [Associating a public key with a user account](#)

= Enable SSL certificate accounts

:icons: font

:relative\_path: ./authentication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You can use the `security login create` command to enable administrator accounts to access an admin or data SVM with an SSL certificate.

### What you'll need

You must be a cluster administrator to perform this task.

### About this task

- You must install a CA-signed server digital certificate before the account can access the SVM.

#### [Generating and installing a CA-signed server certificate](#)

You can perform this task before or after you enable account access.

- If you are unsure of the access control role you want to assign to the login account, you can add the role later with the `security login modify` command.

#### [Modifying the role assigned to an administrator](#)

For cluster administrator accounts, certificate authentication is supported only with the `http` and `ontapi` applications. For SVM administrator accounts, certificate authentication is supported only with the `ontapi` application.

## Step

1. Enable local administrator accounts to access an SVM using an SSL certificate:

```
security login create -vserver SVM_name -user-or-group-name
user_or_group_name -application application -authmethod
authentication_method -role role -comment comment
```

For complete command syntax, see the [ONTAP man pages by release](#).

The following command enables the SVM administrator account `svmadmin2` with the default `vsadmin` role to access the `SVMengData2` using an SSL digital certificate.

```
cluster1::>security login create -vserver engData2 -user-or-group
-name svmadmin2 -application ontapi -authmethod cert
```

## After you finish

If you have not installed a CA-signed server digital certificate, you must do so before the account can access the SVM.

### [Generating and installing a CA-signed server certificate](#)

= Enable Active Directory account access

:icons: font

:relative\_path: ./authentication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You can use the `security login create` command to enable Active Directory (AD) user or group accounts to access an admin or data SVM. Any user in the AD group can access the SVM with the role that is assigned to the group.

## What you'll need

- The cluster time must be synchronized to within five minutes of the time on the AD domain controller.
- You must be a cluster administrator to perform this task.

## About this task

- You must configure AD domain controller access to the cluster or SVM before the account can access the SVM.

### [Configuring Active Directory domain controller access](#)

You can perform this task before or after you enable account access.

- Beginning with ONTAP 9.11.1, you can use [LDAP fast bind for nsswitch authentication](#) if it is supported by the AD LDAP server.
- If you are unsure of the access control role that you want to assign to the login account, you can use the `security login modify` command to add the role later.

### [Modifying the role assigned to an administrator](#)

AD group account access is supported only with the `SSH` and `ontapi` applications.

## Step

1. Enable AD user or group administrator accounts to access an SVM:

```
security login create -vserver SVM_name -user-or-group-name
user_or_group_name -application application -authmethod domain -role role
-comment comment [-is-ldap-fastbind true]
```

For complete command syntax, see the [worksheet](#).

### Creating or modifying login accounts

The following command enables the AD cluster administrator account `DOMAIN1\guest1` with the predefined `backup` role to access the admin `SVMengCluster`.

```
cluster1::>security login create -vserver engCluster -user-or-group
-name DOMAIN1\guest1 -application ssh -authmethod domain -role
backup
```

The following command enables the SVM administrator accounts in the AD group account `DOMAIN1\adgroup` with the predefined `vsadmin-volume` role to access the `SVMengData`.

```
cluster1::>security login create -vserver engData -user-or-group
-name DOMAIN1\adgroup -application ssh -authmethod domain -role
vsadmin-volume
```

## After you finish

If you have not configured AD domain controller access to the cluster or SVM, you must do so before the account can access the SVM.

### Configuring Active Directory domain controller access

= Enable LDAP or NIS account access

:icons: font

:relative\_path: ./authentication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You can use the `security login create` command to enable LDAP or NIS user accounts to access an admin or data SVM. If you have not configured LDAP or NIS server access to the SVM, you must do so before the account can access the SVM.

## What you'll need

You must be a cluster administrator to perform this task.

## About this task

- Group accounts are not supported.
- You must configure LDAP or NIS server access to the SVM before the account can access the SVM.

## Configuring LDAP or NIS server access

You can perform this task before or after you enable account access.

- If you are unsure of the access control role that you want to assign to the login account, you can use the `security login modify` command to add the role later.

## Modifying the role assigned to an administrator

- Beginning with ONTAP 9.4, multifactor authentication (MFA) is supported for remote users over LDAP or NIS servers.
- Beginning with ONTAP 9.11.1, you can use [LDAP fast bind for nsswitch authentication](#) if it is supported by the LDAP server.
- Because of a known LDAP issue, you should not use the ':' (colon) character in any field of LDAP user account information (for example, `gecos`, `userPassword`, and so on). Otherwise, the lookup operation will fail for that user.

## Steps

1. Enable LDAP or NIS user or group accounts to access an SVM:

```
security login create -vserver SVM_name -user-or-group-name user_name
-application application -authmethod nsswitch -role role -comment comment
-is-ns-switch-group yes|no [-is-ldap-fastbind true]
```

For complete command syntax, see the [worksheet](#).

## Creating or modifying login accounts

The following command enables the LDAP or NIS cluster administrator account `guest2` with the predefined `backup` role to access the `admin SVMengCluster`.

```
cluster1::>security login create -vserver engCluster -user-or-group
-name guest2 -application ssh -authmethod nsswitch -role backup
```

2. Enable MFA login for LDAP or NIS users:

```
security login modify -user-or-group-name rem_usr1 -application ssh
-authentication-method nsswitch -role admin -is-ns-switch-group no -second
-authentication-method publickey
```

The authentication method can be specified as `publickey` and second authentication method as `nsswitch`.

The following example shows the MFA authentication being enabled:

```
cluster-1::*> security login modify -user-or-group-name rem_usr2
-application ssh -authentication-method nsswitch -vserver
cluster-1 -second-authentication-method publickey"
```

## After you finish

If you have not configured LDAP or NIS server access to the SVM, you must do so before the account can access the SVM.

## Configuring LDAP or NIS server access

= Configure SAML authentication

:icons: font

:relative\_path: ./authentication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

Beginning with ONTAP 9.3, you can configure Security Assertion Markup Language (SAML) authentication for web services. When SAML authentication is configured and enabled, users are authenticated by an external Identity Provider (IdP) instead of the directory service providers such as Active Directory and LDAP.

## What you'll need

- You must have configured the IdP for SAML authentication.
- You must have the IdP URI.

## About this task

- SAML authentication applies only to the `http` and `ontapi` applications.

The `http` and `ontapi` applications are used by the following web services: Service Processor Infrastructure, ONTAP APIs, or System Manager.

- SAML authentication is applicable only for accessing the admin SVM.

## Steps

1. Create a SAML configuration so that ONTAP can access the IdP metadata:

```
security saml-sp create -idp-uri idp_uri -sp-host ontap_host_name
```

`idp_uri` is the FTP or HTTP address of the IdP host from where the IdP metadata can be downloaded.

`ontap_host_name` is the host name or IP address of the SAML service provider host, which in this case is the ONTAP system. By default, the IP address of the cluster-management LIF is used.

You can optionally provide the ONTAP server certificate information. By default, the ONTAP web server certificate information is used.

```
cluster_12::> security saml-sp create -idp-uri
https://scspr0235321001.gdl.englab.netapp.com/idp/shibboleth -verify
-metadata-server false
```

Warning: This restarts the web server. Any HTTP/S connections that are active

will be disrupted.

Do you want to continue? {y|n}: y

[Job 179] Job succeeded: Access the SAML SP metadata using the URL:  
https://10.63.56.150/saml-sp/Metadata

Configure the IdP and Data ONTAP users for the same directory server domain to ensure that users are the same for different authentication methods. See the "security login show" command for the Data ONTAP user configuration.

The URL to access the ONTAP host metadata is displayed.

2. From the IdP host, configure the IdP with the ONTAP host metadata.

For more information about configuring the IdP, see the IdP documentation.

3. Enable SAML configuration:

```
security saml-sp modify -is-enabled true
```

Any existing user that accesses the `http` or `ontapi` application is automatically configured for SAML authentication.

4. If you want to create users for the `http` or `ontapi` application after SAML is configured, specify SAML as the authentication method for the new users.

- a. Create a login method for new users with SAML authentication:

```
security login create
-user-or-group-name user_name -application [http | ontapi]
-authentication-method saml -vserver svm_name
```

```
cluster_12::> security login create -user-or-group-name admin1
-application http -authentication-method saml -vserver
cluster_12
```

- b. Verify that the user entry is created:

```
security login show
```

```
cluster_12::> security login show
```

```
Vserver: cluster_12
```

```
Second
```

User/Group	Authentication	Authentication	Acct	
Name	Application	Method	Role Name	Locked
Method				
admin	console	password	admin	no
none				
admin	http	password	admin	no
none				
admin	http	saml	admin	-
none				
admin	ontapi	password	admin	no
none				
admin	ontapi	saml	admin	-
none				
admin	service-processor	password	admin	no
none				
admin	ssh	password	admin	no
none				
admin1	http	password	backup	no
none				
**admin1	http	saml	backup	-
none**				

### Related information

#### [ONTAP 9 Commands](#)

= Manage access-control roles

= Manage access-control roles overview

:icons: font

:relative\_path: ./authentication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

The role assigned to an administrator determines the commands to which the administrator has access. You assign the role when you create the account for the administrator. You can assign a different role or define custom roles as needed.

= Modify the role assigned to an administrator



```
:icons: font
:relative_path: ./authentication/
:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/
```

You can use the `security login modify` command to change the role of a cluster or SVM administrator account. You can assign a predefined or custom role.

### What you'll need

You must be a cluster administrator to perform this task.

### Step

1. Change the role of a cluster or SVM administrator:

```
security login modify -vserver SVM_name -user-or-group-name
user_or_group_name -application application -authmethod
authentication_method -role role -comment comment
```

For complete command syntax, see the [worksheet](#).

### Creating or modifying login accounts

The following command changes the role of the AD cluster administrator account `DOMAIN1\guest1` to the predefined `readonly` role.

```
cluster1::>security login modify -vserver engCluster -user-or-group
-name DOMAIN1\guest1 -application ssh -authmethod domain -role
readonly
```

The following command changes the role of the SVM administrator accounts in the AD group account `DOMAIN1\adgroup` to the custom `vol_role` role.

```
cluster1::>security login modify -vserver engData -user-or-group
-name DOMAIN1\adgroup -application ssh -authmethod domain -role
vol_role
```

= Define custom roles

```
:icons: font
:relative_path: ./authentication/
:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/
```

You can use the `security login role create` command to define a custom role. You can execute the command as many times as necessary to achieve the exact combination of capabilities that you want to associate with the role.

### What you'll need

You must be a cluster administrator to perform this task.

### About this task

- A role, whether predefined or custom, grants or denies access to ONTAP commands or command directories.

A command directory (`volume`, for example) is a group of related commands and command subdirectories. Except as described in this procedure, granting or denying access to a command directory grants or denies access to each command in the directory and its subdirectories.

- Specific command access or subdirectory access overrides parent directory access.

If a role is defined with a command directory, and then is defined again with a different access level for a specific command or for a subdirectory of the parent directory, the access level that is specified for the command or subdirectory overrides that of the parent.

You cannot assign an SVM administrator a role that gives access to a command or command directory that is available only to the `admin` cluster administrator—for example, the `security` command directory.

## Step

1. Define a custom role:

```
security login role create -vserver SVM_name -role role -cmddirname  
command_or_directory_name -access access_level -query query
```

For complete command syntax, see the [worksheet](#).

The following commands grant the `vol_role` role full access to the commands in the `volume` command directory and read-only access to the commands in the `volume snapshot` subdirectory.

```
cluster1::>security login role create -role vol_role -cmddirname  
"volume" -access all
```

```
cluster1::>security login role create -role vol_role -cmddirname  
"volume snapshot" -access readonly
```

The following commands grant the `SVM_storage` role read-only access to the commands in the `storage` command directory, no access to the commands in the `storage encryption` subdirectory, and full access to the `storage aggregate plex offline nonintrinsic` command.

```
cluster1::>security login role create -role SVM_storage -cmddirname  
"storage" -access readonly
```

```
cluster1::>security login role create -role SVM_storage -cmddirname  
"storage encryption" -access none
```

```
cluster1::>security login role create -role SVM_storage -cmddirname  
"storage aggregate plex offline" -access all
```

= Predefined roles for cluster administrators

:icons: font

:relative\_path: ./authentication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

The predefined roles for cluster administrators should meet most of your needs. You can create custom roles as necessary. By default, a cluster administrator is assigned the predefined `admin` role.

The following table lists the predefined roles for cluster administrators:

This role...	Has this level of access...	To the following commands or command directories
--------------	-----------------------------	--

admin	all	All command directories (DEFAULT)
autosupport	all	<ul style="list-style-type: none"> <li>• set</li> <li>• system node autosupport</li> </ul>
	none	All other command directories (DEFAULT)
backup	all	vserver services ndmp
	readonly	volume
	none	All other command directories (DEFAULT)
readonly	all	<ul style="list-style-type: none"> <li>• security login password</li> </ul> <p>For managing own user account local password and key information only</p> <ul style="list-style-type: none"> <li>• set</li> </ul>
	none	security
	readonly	All other command directories (DEFAULT)
none	none	All command directories (DEFAULT)

The `autosupport` role is assigned to the predefined `autosupport` account, which is used by AutoSupport OnDemand. ONTAP prevents you from modifying or deleting the `autosupport` account. ONTAP also prevents you from assigning the `autosupport` role to other user accounts.

= Predefined roles for SVM administrators

:icons: font

:relative\_path: ./authentication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

The predefined roles for SVM administrators should meet most of your needs. You can create custom roles as necessary. By default, an SVM administrator is assigned the predefined `vsadmin` role.

The following table lists the predefined roles for SVM administrators:

Role name	Capabilities
vsadmin	<ul style="list-style-type: none"><li>• Managing own user account local password and key information</li><li>• Managing volumes, except volume moves</li><li>• Managing quotas, qtrees, Snapshot copies, and files</li><li>• Managing LUNs</li><li>• Performing SnapLock operations, except privileged delete</li><li>• Configuring protocols: NFS, SMB, iSCSI, and FC, including FCoE</li><li>• Configuring services: DNS, LDAP, and NIS</li><li>• Monitoring jobs</li><li>• Monitoring network connections and network interface</li><li>• Monitoring the health of the SVM</li></ul>
vsadmin-volume	<ul style="list-style-type: none"><li>• Managing own user account local password and key information</li><li>• Managing volumes, including volume moves</li><li>• Managing quotas, qtrees, Snapshot copies, and files</li><li>• Managing LUNs</li><li>• Configuring protocols: NFS, SMB, iSCSI, and FC, including FCoE</li><li>• Configuring services: DNS, LDAP, and NIS</li><li>• Monitoring network interface</li><li>• Monitoring the health of the SVM</li></ul>

vsadmin-protocol	<ul style="list-style-type: none"> <li>• Managing own user account local password and key information</li> <li>• Configuring protocols: NFS, SMB, iSCSI, and FC, including FCoE</li> <li>• Configuring services: DNS, LDAP, and NIS</li> <li>• Managing LUNs</li> <li>• Monitoring network interface</li> <li>• Monitoring the health of the SVM</li> </ul>
vsadmin-backup	<ul style="list-style-type: none"> <li>• Managing own user account local password and key information</li> <li>• Managing NDMP operations</li> <li>• Making a restored volume read/write</li> <li>• Managing SnapMirror relationships and Snapshot copies</li> <li>• Viewing volumes and network information</li> </ul>
vsadmin-snaplock	<ul style="list-style-type: none"> <li>• Managing own user account local password and key information</li> <li>• Managing volumes, except volume moves</li> <li>• Managing quotas, qtrees, Snapshot copies, and files</li> <li>• Performing SnapLock operations, including privileged delete</li> <li>• Configuring protocols: NFS and SMB</li> <li>• Configuring services: DNS, LDAP, and NIS</li> <li>• Monitoring jobs</li> <li>• Monitoring network connections and network interface</li> </ul>
vsadmin-readonly	<ul style="list-style-type: none"> <li>• Managing own user account local password and key information</li> <li>• Monitoring the health of the SVM</li> <li>• Monitoring network interface</li> <li>• Viewing volumes and LUNs</li> <li>• Viewing services and protocols</li> </ul>

= Manage administrator accounts

= Manage administrator accounts overview

:icons: font

:relative\_path: ./authentication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

Depending on how you have enabled account access, you may need to associate a public key with a local account, install a CA-signed server digital certificate, or configure AD, LDAP, or NIS access. You can perform all of these tasks before or after enabling account access.

= Associate a public key with an administrator account

:icons: font

:relative\_path: ./authentication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

For SSH public key authentication, you must associate the public key with an administrator account before the account can access the SVM. You can use the `security login publickey create` command to associate a key with an administrator account.

### Before you begin

- You must have generated the SSH key.
- You must be a cluster or SVM administrator to perform this task.

### About this task

If you authenticate an account over SSH with both a password and an SSH public key, the account is authenticated first with the public key.

### Step

1. Associate a public key with an administrator account:

```
security login publickey create -vserver SVM_name -username user_name
-index index -publickey certificate -comment comment
```

For complete command syntax, see the [worksheet](#).

### Associating a public key with a user account

The following command associates a public key with the SVM administrator account `svmadmin1` for the SVM `engData1`. The public key is assigned index number 5.

```
cluster1::>security login publickey create -vserver engData1
-username svmadmin1 -index 5 -publickey
"ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAspH64CYbUsDQCdW22JnK6J
/vU9upnKzd2zAk9C1f7YaWRUAFNs2Qe5lUmQ3ldi8AD0Vfbr5T6HZPCixNAIza
FciDy7hgnmdj9eNGedGr/JNrftQbLD1hZybX+72DpQB0tYWBhe6eDJ1oPLob
ZBGfMlPXh8VjeU44i7W4+s0hG0E=tsmith@publickey.example.com"
```

= Generate and install a CA-signed server certificate

= Generate and install a CA-signed server certificate overview

:icons: font

:relative\_path: ./authentication/

```
:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/
```

On production systems, it is a best practice to install a CA-signed digital certificate for use in authenticating the cluster or SVM as an SSL server. You can use the `security certificate generate-csr` command to generate a certificate signing request (CSR), and the `security certificate install` command to install the certificate you receive back from the certificate authority.

= Generate a certificate signing request

```
:icons: font
```

```
:relative_path: ./authentication/
```

```
:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/
```

You can use the `security certificate generate-csr` command to generate a certificate signing request (CSR). After processing your request, the certificate authority (CA) sends you the signed digital certificate.

### What you'll need

You must be a cluster or SVM administrator to perform this task.

### Steps

1. Generate a CSR:

```
security certificate generate-csr -common-name FQDN_or_common_name -size  
512|1024|1536|2048 -country country -state state -locality locality  
-organization organization -unit unit -email-addr email_of_contact -hash  
-function SHA1|SHA256|MD5
```

The following command creates a CSR with a 2048-bit private key generated by the SHA256 hashing function for use by the `Software` group in the IT department of a company whose custom common name is `server1.companyname.com`, located in Sunnyvale, California, USA. The email address of the SVM contact administrator is `web@example.com`. The system displays the CSR and the private key in the output.



```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California
-locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
```

Certificate Signing Request :

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGx1LmNvbTElMAkGA1UEBhMCVVMx
CTAHBgNVBAgTADAEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEPMA0G
CSqGSIB3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApTlnzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3a1woUsb13wfEvQnHVFNCi
2ninsJ8CAwEAAaAAMA0GCSqGSIB3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
```

Private Key :

```
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApTlnzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3a1woUsb13wfEvQnHVFNCi2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgpV+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsferNsZwD8CIQCbz1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----
```

Note: Please keep a copy of your certificate request and private key for future reference.

2. Copy the certificate request from the CSR output, and send it in electronic form (such as email) to a trusted third-party CA for signing.

After processing your request, the CA sends you the signed digital certificate. You should keep a copy of the private key and the CA-signed digital certificate.

= Install a CA-signed server certificate

```
:icons: font
```

```
:relative_path: ./authentication/
```

```
:imagesdir: /tmp/d20221026-17026-1injpo/source/./authentication/./media/
```

You can use the `security certificate install` command to install a CA-signed server certificate on an SVM. ONTAP prompts you for the certificate authority (CA) root and intermediate certificates that form the certificate chain of the server certificate.

**What you'll need**

You must be a cluster or SVM administrator to perform this task.

**Step**

1. Install a CA-signed server certificate: `security certificate install -vserver SVM_name -type certificate_type`

For complete command syntax, see the [worksheet](#).

ONTAP prompts you for the CA root and intermediate certificates that form the certificate chain of the server certificate. The chain starts with the certificate of the CA that issued the server certificate, and can range up to the root certificate of the CA. Any missing intermediate certificates result in the failure of server certificate installation.

+

The following command installs the CA-signed server certificate and intermediate certificates on the SVMengData2.

+

```
cluster1::>security certificate install -vserver engData2 -type server
Please enter Certificate: Press <Enter> when done
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIB8TCCAZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRhc
cHAuY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNV
BAoTAAEJMAcGA1UECzMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNDI2MTk0OTI4
WhcNMTAwNTI2MTk0OTI4WjBfMRMwEQYDVQQDEwpuZXRhcHAuY29tMQswCQYDVQQG
EwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNVBAoTAAEJMAcGA1UECzMA
MQ8wDQYJKoZIhvcNAQkBFgAwXDANBgkqhkiG9w0BAQEFAANLADBIaKEAyXrK2sry
```

```
-----END CERTIFICATE-----
```

```
Please enter Private Key: Press <Enter> when done
```

```
-----BEGIN RSA PRIVATE KEY-----
```

```
MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLycsUdXA7hXhumHNpvF
C61X2G32Sx8VEalth94tx+vOEzq+UaqH1t0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM7OtbUsgPKw+QCCh9dF1jmuQKeDr+wUMWkn1DeGrfhILpzfJGHRlJ
z7UCIQDr8d3gOG71UyX+BbFmo/N0uAKjS2cvUU+Y8a8pDxGLLwIhANqa99SuS18U
DiPvdaKTj6+EcGuXfCXz+G0rfgTZK8uzAiEArlmnrFYC8KwE9k7A0y1RzBLdUwK9
AvuJDn+/z+H1Bd0CIQDD93P/xpaJETNz53Au49VE5Jba/Jugckrbosd/lSd7nQIg
aEMAZt6qHHT4mndi8Bo8sDGedG2SKx6Qbn2IpuNZ7rc=
```

```
-----END RSA PRIVATE KEY-----
```

```
Do you want to continue entering root and/or intermediate certificates
{y|n}: y
```

```
Please enter Intermediate Certificate: Press <Enter> when done
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIE+zCCBGSgAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwwgbsxJDAiBgNVBACGTG1Zh
bG1DZXJ0IFZhbG1kYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIElu
Yy4xNTAzBgNVBAsTTFZhbG1DZXJ0IENsYXNzIDIGUG9saWN5IFZhbG1kYXRpb24g
QXV0aG9yaXR5MSEwHwYDVQQDEwhodHRwOi8vd3d3LnZhbG1jZXJ0LmNvbS8xIDAe
BgkqhkiG9w0BCQEWewluZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDYyMFoX
DTI0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFFRoZSBHbyBE
YWRkeSBHcm91cCwgSW5jLjExMC8GA1UECzM0R28gRGFkZHZkgQ2xhc3MgMiBDZXJ0
```

```
-----END CERTIFICATE-----
```

```
Do you want to continue entering root and/or intermediate certificates
{y|n}: y
```

```

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIC5zCCA1ACAQEwDQYJKoZIhvcNAQEFBQAwbgsxJDAiBgNVBACtG1ZhbG1DZXJ0
IFZhbG1kYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUN1cnQsIEluYy4xNTAz
BgNVBAsTTFZhbG1DZXJ0IENsYXNzIDIgUG9saWN5IFZhbG1kYXRpb24gQXV0aG9y
aXR5MSEwHwYDVQQDEzhodHRwOi8vd3d3LnZhbG1jZXJ0LmNvbS8xIDAeBgkqhkiG
9w0BCQEWEluZm9AdmFsaWN1cnQuY29tMB4XDTE5MDYyNjAwMTk1NFoXDTE5MDYy
NjAwMTk1NFowgbsxJDAiBgNVBACtG1ZhbG1DZXJ0IFZhbG1kYXRpb24gTmV0d29y
azEXMBUGA1UEChMOVmFsaUN1cnQsIEluYy4xNTAzBgNVBAsTTFZhbG1DZXJ0IENs
YXNzIDIgUG9saWN5IFZhbG1kYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDEzhodHRw
-----END CERTIFICATE-----

```

```

Do you want to continue entering root and/or intermediate certificates
{y|n}: n

```

You should keep a copy of the private key and the CA-signed digital certificate for future reference.

= Configure Active Directory domain controller access

= Configure Active Directory domain controller access overview

```
:icons: font
```

```
:relative_path: ./authentication/
```

```
:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/
```

You must configure AD domain controller access to the cluster or SVM before an AD account can access the SVM. If you have already configured a SMB server for a data SVM, you can configure the SVM as a gateway, or *tunnel*, for AD access to the cluster. If you have not configured a SMB server, you can create a computer account for the SVM on the AD domain.

ONTAP supports the following domain controller authentication services:

- Kerberos
- LDAP
- Netlogon
- Local Security Authority (LSA)

ONTAP supports the following session key algorithms for secure Netlogon connections:

Session key algorithm	Available in...
HMAC-SHA256, based on the Advanced Encryption Standard (AES)	ONTAP 9.10.1 and later
DES and HMAC-MD5 (when strong key is set)	All ONTAP 9 releases

If you want to use AES session keys during Netlogon secure channel establishment in ONTAP 9.10.1 and later, you must enable them using the following command:

```
cifs security modify -vserver vs1 -aes-enabled-for-netlogon-channel true
```

The default is `false`.

In ONTAP releases earlier than 9.10.1, if the domain controller enforces AES for secure Netlogon services, the connection fails. The domain controller must be configured to accept strong key connections with ONTAP in these releases.

= Configure an authentication tunnel

:icons: font

:relative\_path: ./authentication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

If you have already configured a SMB server for a data SVM, you can use the `security login domain-tunnel create` command to configure the SVM as a gateway, or *tunnel*, for AD access to the cluster.

#### What you'll need

- You must have configured a SMB server for a data SVM.
- You must have enabled an AD domain user account to access the admin SVM for the cluster.
- You must be a cluster administrator to perform this task.

Beginning with ONTAP 9.10.1, if you have an SVM gateway (domain tunnel) for AD access, you can use Kerberos for admin authentication if you have disabled NTLM in your AD domain. In earlier releases, Kerberos was not supported with admin authentication for SVM gateways. This functionality is available by default; no configuration is required.

#### NOTE

Kerberos authentication is always attempted first. In case of failure, NTLM authentication is then attempted.

#### Step

1. Configure a SMB-enabled data SVM as an authentication tunnel for AD domain controller access to the cluster:

```
security login domain-tunnel create -vserver SVM_name
```

For complete command syntax, see the [worksheet](#).

The SVM must be running for the user to be authenticated.

+

The following command configures the SMB-enabled data SVMengData as an authentication tunnel.

+

```
cluster1::>security login domain-tunnel create -vserver engData
```

= Create an SVM computer account on the domain

:icons: font

:relative\_path: ./authentication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

If you have not configured an SMB server for a data SVM, you can use the `vserver active-directory create` command to create a computer account for the SVM on the domain.

### What you'll need

You must be a cluster or SVM administrator to perform this task.

### About this task

After you enter the `vserver active-directory create` command, you are prompted to provide the credentials for an AD user account with sufficient privileges to add computers to the specified organizational unit in the domain. The password of the account cannot be empty.

### Step

1. Create a computer account for an SVM on the AD domain:

```
vserver active-directory create -vserver SVM_name -account-name  
NetBIOS_account_name -domain domain -ou organizational_unit
```

For complete command syntax, see the [worksheet](#).

The following command creates a computer account named ADSERVER1 on the domain `example.com` for the SVM `engData`. You are prompted to enter the AD user account credentials after you enter the command.

```
cluster1::>vserver active-directory create -vserver engData -account
-name ADSERVER1 -domain example.com
```

In order to create an Active Directory machine account, you must supply the name and password of a Windows account with sufficient privileges to add computers to the "CN=Computers" container within the "example.com" domain.

Enter the user name: Administrator

Enter the password:

= Configure LDAP or NIS server access

= Configure LDAP or NIS server access overview

:icons: font

:relative\_path: ./authentication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You must configure LDAP or NIS server access to an SVM before LDAP or NIS accounts can access the SVM. The switch feature lets you use LDAP or NIS as alternative name service sources.

= Configure LDAP server access

:icons: font

:relative\_path: ./authentication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You must configure LDAP server access to an SVM before LDAP accounts can access the SVM. You can use the `vserver services name-service ldap client create` command to create an LDAP client configuration on the SVM. You can then use the `vserver services name-service ldap create` command to associate the LDAP client configuration with the SVM.

#### What you'll need

- You must have installed a [CA-signed server digital certificate](#) on the SVM.
- You must be a cluster or SVM administrator to perform this task.

#### About this task

Most LDAP servers can use the default schemas provided by ONTAP:

- MS-AD-BIS (the preferred schema for most Windows 2012 and later AD servers)
- AD-IDMU (Windows 2008, Windows 2012 and later AD servers)
- AD-SFU (Windows 2003 and earlier AD servers)
- RFC-2307 (UNIX LDAP servers)

It is best to use the default schemas unless there is a requirement to do otherwise. If so, you can create your own schema by copying a default schema and modifying the copy. For more information, see the following documents.

- [NFS configuration](#)
- [NetApp Technical Report 4835: How to Configure LDAP in ONTAP](#)

### Steps

1. Create an LDAP client configuration on an SVM: `vserver services name-service ldap client create -vserver SVM_name -client-config client_configuration -servers LDAP_server_IPs -schema schema -use-start-tls true|false`

Start TLS is supported for access to data SVMs only. It is not supported for access to admin SVMs.

+

For complete command syntax, see the [worksheet](#).

+

The following command creates an LDAP client configuration named `corp` on the SVM `engData`. The client makes anonymous binds to the LDAP servers with the IP addresses `172.16.0.100` and `172.16.0.101`. The client uses the RFC-2307 schema to make LDAP queries. Communication between the client and server is encrypted using Start TLS.

+

```
cluster1::>vserver services name-service ldap client create
-vserver engData -client-config corp -servers 172.16.0.100,172.16.0.101
-schema RFC-2307 -use-start-tls true
```

+

Beginning with ONTAP 9.2, the field `-ldap-servers` replaces the field `-servers`. This new field can take either a hostname or an IP address for the LDAP server.



1. Associate the LDAP client configuration with the SVM: `vserver services name-service ldap create -vserver SVM_name -client-config client_configuration -client-enabled true|false`

For complete command syntax, see the [worksheet](#).

The following command associates the LDAP client configuration `corp` with the `SVMengData`, and enables the LDAP client on the SVM.

```
cluster1::>vserver services name-service ldap create -vserver  
engData -client-config corp -client-enabled true
```

Beginning with ONTAP 9.2, the `vserver services name-service ldap create` command performs an automatic configuration validation and reports an error message if ONTAP is unable to contact the name server.

1. Validate the status of the name servers by using the `vserver services name-service ldap check` command.

The following command validates LDAP servers on the SVM vs0.

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0 |
| Client Configuration Name: c1 |
| LDAP Status: up |
| LDAP Status Details: Successfully connected to LDAP server |
| "10.11.12.13". |
```

The name service check command is available beginning with ONTAP 9.2.

= Configure NIS server access

:icons: font

:relative\_path: ./authentication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You must configure NIS server access to an SVM before NIS accounts can access the SVM. You can use the `vserver services name-service nis-domain create` command to create an NIS domain configuration on an SVM.

#### What you'll need

- All configured servers must be available and accessible before you configure the NIS domain on the SVM.
- You must be a cluster or SVM administrator to perform this task.

#### About this task

You can create multiple NIS domains. Only one NIS domain can be set to `active` at a time.

#### Step

1. Create an NIS domain configuration on an SVM: `vserver services name-service nis-domain create -vserver SVM_name -domain client_configuration -active true|false -nis-servers NIS_server_IPs`

For complete command syntax, see the [worksheet](#).

Beginning with ONTAP 9.2, the field `-nis-servers` replaces the field `-servers`. This new field can take either a hostname or an IP address for the NIS server.

+

The following command creates an NIS domain configuration on the SVM `engData`. The NIS domain `nisdomain` is active on creation and communicates with an NIS server with the IP address `192.0.2.180`.

+

```
cluster1::>vserver services name-service nis-domain create
-vserver engData -domain nisdomain -active true -nis-servers
192.0.2.180
```

= Create a name service switch

:icons: font

:relative\_path: ./authentication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

The name service switch feature lets you use LDAP or NIS as alternative name service sources. You can use the `vserver services name-service ns-switch modify` command to specify the look-up order for name service sources.

### What you'll need

- You must have configured LDAP and NIS server access.
- You must be a cluster administrator or SVM administrator to perform this task.

### Step

1. Specify the lookup order for name service sources:

```
vserver services name-service ns-switch modify -vserver SVM_name -database
name_service_switch_database -sources name_service_source_order
```

For complete command syntax, see the [worksheet](#).

The following command specifies the lookup order of the LDAP and NIS name service sources for the `passwd` database on the `engDataSVM`.

```
cluster1::>vserver services name-service ns-switch
modify -vserver engData -database passwd -source files ldap,nis
```

= Change an administrator password

:icons: font

:relative\_path: ./authentication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You should change your initial password immediately after logging into the system for the first time. If you are an SVM administrator, you can use the `security login password` command to change your own password. If you are a cluster

administrator, you can use the `security login password` command to change any administrator's password.

#### **What you'll need**

- You must be a cluster or SVM administrator to change your own password.
- You must be a cluster administrator to change another administrator's password.

#### **About this task**

The new password must observe the following rules:

- It cannot contain the user name
- It must be at least eight characters long
- It must contain at least one letter and one number
- It cannot be the same as the last six passwords

You can use the `security login role config modify` command to modify the password rules for accounts associated with a given role. For more information, see the man page `security login role config modify`

## Step

1. Change an administrator password: `security login password -vserver SVM_name -username user_name`

The following command changes the password of the administrator `admin1` for the SVM `vs1.example.com`. You are prompted to enter the current password, then enter and reenter the new password.

```
vs1.example.com::>security login password -vserver engData -username
admin1
Please enter your current password:
Please enter a new password:
Please enter it again:
```

= Lock and unlock an administrator account

:icons: font

:relative\_path: ./authentication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You can use the `security login lock` command to lock an administrator account, and the `security login unlock` command to unlock the account.

## What you'll need

You must be a cluster administrator to perform these tasks.

## Steps

1. Lock an administrator account:

```
security login lock -vserver SVM_name -username user_name
```

The following command locks the administrator account `admin1` for the SVM `vs1.example.com`:

```
cluster1::>security login lock -vserver engData -username admin1
```

2. Unlock an administrator account:

```
security login unlock -vserver SVM_name -username user_name
```

The following command unlocks the administrator account `admin1` for the SVM `vs1.example.com`:

```
cluster1::>security login unlock -vserver engData -username admin1
```

= Manage failed login attempts

:icons: font

```
:relative_path: ./authentication/  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/
```

Repeated failed login attempts sometimes indicate that an intruder is attempting to access the storage system. You can take a number of steps to ensure that an intrusion does not take place.

== How you will know that login attempts have failed

The Event Management System (EMS) notifies you about failed login attempts every hour. You can find a record of failed login attempts in the `audit.log` file.

== What to do if repeated login attempts fail

In the short term, you can take a number of steps to prevent an intrusion:

- Require that passwords be composed of a minimum number of uppercase characters, lowercase characters, special characters, and/or digits
- Impose a delay after a failed login attempt
- Limit the number of allowed failed login attempts, and lock out users after the specified number of failed attempts
- Expire and lock out accounts that are inactive for a specified number of days

You can use the `security login role config modify` command to perform these tasks.

Over the long term, you can take these additional steps:

- Use the `security ssh modify` command to limit the number of failed login attempts for all newly created SVMs.
- Migrate existing MD5-algorithm accounts to the more secure SHA-512 algorithm by requiring users to change their passwords.

= Enforce SHA-2 on administrator account passwords

```
:icons: font  
:relative_path: ./authentication/  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/
```

Administrator accounts created prior to ONTAP 9.0 continue to use MD5 passwords after the upgrade, until the passwords are manually changed. MD5 is less secure than SHA-2. Therefore, after upgrading, you should prompt users of MD5 accounts to change their passwords to use the default SHA-512 hash function.

### **About this task**

The password hash functionality enables you to do the following:

- Display user accounts that match the specified hash function.
- Expire accounts that use a specified hash function (for example, MD5), forcing the users to change their passwords in their next login.
- Lock accounts whose passwords use the specified hash function.

- When reverting to a release earlier than ONTAP 9, reset the cluster administrator's own password for it to be compatible with the hash function (MD5) that is supported by the earlier release.

ONTAP accepts pre-hashed SHA-2 passwords only by using NetApp Manageability SDK (security-login-create and security-login-modify-password).

## Manageability enhancements

### Steps

1. Migrate the MD5 administrator accounts to the SHA-512 password hash function:

- a. Expire all MD5 administrator accounts: `security login expire-password -vserver * -username * -hash-function md5`

Doing so forces MD5 account users to change their passwords upon next login.

- b. Ask users of MD5 accounts to log in through a console or SSH session.

The system detects that the accounts are expired and prompts users to change their passwords. SHA-512 is used by default for the changed passwords.

2. For MD5 accounts whose users do not log in to change their passwords within a period of time, force the account migration:

- a. Lock accounts that still use the MD5 hash function (advanced privilege level): `security login expire-password -vserver * -username * -hash-function md5 -lock-after integer`

After the number of days specified by `-lock-after`, users cannot access their MD5 accounts.

- b. Unlock the accounts when the users are ready to change their passwords: `security login unlock -vserver vserver_name -username user_name`

- c. Have users log in to their accounts through a console or SSH session and change their passwords when the system prompts them to do so.

= Manage multi-admin verification

= Multi-admin verification overview

:icons: font

:relative\_path: ./multi-admin-verify/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

Beginning with ONTAP 9.11.1, you can use multi-admin verification (MAV) to ensure that certain operations, such as deleting volumes or Snapshot copies, can be executed only after approvals from designated administrators. This prevents compromised, malicious, or inexperienced administrators from making undesirable changes or deleting data.

Configuring multi-admin verification consists of:

- [Creating one or more administrator approval groups.](#)
- [Enabling multi-admin verification functionality.](#)

- [Adding or modifying rules.](#)

After initial configuration, these elements can be modified only by administrators in a MAV approval group (MAV administrators).

When multi-admin verification is enabled, the completion of every protected operation requires three steps:

- When a user initiates the operation, a [request is generated](#).
- Before it can be executed, at least one [MAV administrator must approve](#).
- Upon approval, the user completes the operation.

Multi-admin verification is not intended for use with volumes or workflows that involve heavy automation, because each automated task would require approval before the operation could be completed. If you want to use automation and MAV together, it's recommended to use queries for specific MAV operations. For example, you could apply `volume delete` MAV rules only to volumes where automation is not involved, and you could designate those volumes with a particular naming scheme.



If you need to disable multi-admin verification functionality without MAV administrator approval, contact NetApp Support and mention the following Knowledge Base article: [How to disable Multi-Admin Verification if MAV admin is unavailable](#).

== How multi-admin verification works

Multi-admin verification consists of:

- A group of one or more administrators with approval and veto powers.
- A set of protected operations or commands in a *rules table*.
- A *rules engine* to identify and control execution of protected operations.

MAV rules are evaluated after role-based access control (RBAC) rules. Therefore, administrators who execute or approve protected operations must already possess the minimum RBAC privileges for those operations. [Learn more about RBAC](#).

When multi-admin verification is enabled, system-defined rules (also known as *guard-rail* rules) establish a set of MAV operations to contain the risk of circumventing the MAV process itself. These operations cannot be removed from the rules table. Once MAV is enabled, operations designated by an asterisk ( \* ) require approval by one or more administrators before execution, except for **show** commands.

- `security multi-admin-verify modify*`

Controls the configuration of multi-admin verification functionality.

- `security multi-admin-verify approval-group operations*`

Control membership in the set of administrators with multi-admin verification credentials.

- `security multi-admin-verify rule operations*`

Control the set of commands requiring multi-admin verification.

- `security multi-admin-verify request operations`



## Control the approval process.

In addition to the system-defined commands, the following commands are protected by default when multi-admin verification is enabled, but you can modify the rules to remove protection for these commands.

- security login password
- security login unlock
- set

The following commands can be protected in ONTAP 9.11.1.

cluster peer delete	volume snapshot autodelete modify
event config modify	volume snapshot delete
security login create	volume snapshot policy add-schedule
security login delete	volume snapshot policy create
security login modify	volume snapshot policy delete
system node run	volume snapshot policy modify
system node systemshell	volume snapshot policy modify-schedule
volume delete	volume snapshot policy remove-schedule
volume flexcache delete	volume snapshot restore
	vserver peer delete

### == How multi-admin approval works

Any time a protected operation is entered on a MAV-protected cluster, an operation execution request is sent to the designated MAV administrator group.

You can configure:

- The names, contact information, and number of administrators in the MAV group.
  - A MAV administrator should have an RBAC role with cluster administrator privileges.
- The number of MAV administrator groups.
  - A MAV group is assigned for each protected operation rule.
  - For multiple MAV groups, you can configure which MAV group approves a given rule.
- The number of MAV approvals required to execute a protected operation.
- An *approval expiry* period within which a MAV administrator must respond to an approval request.

- An *execution expiry* period within which the requesting administrator must complete the operation.

Once these parameters are configured, MAV approval is required to modify them.

MAV administrators cannot approve their own requests to execute protected operations. Therefore:

- MAV should not be enabled on clusters with only one administrator.
- If there is only one person in the MAV group, that MAV administrator cannot enter protected operations; regular administrators must enter them and the MAV administrator can only approve.
- If you want MAV administrators to be able to execute protected operations, the number of MAV administrators must be one greater than the number of approvals required.  
For example, if two approvals are required for a protected operation, and you want MAV administrators to execute them, there must be three people in the MAV administrators group.

MAV administrators can receive approval requests in email alerts (using EMS) or they can query the request queue. When they receive a request, they can take one of three actions:

- Approve
- Reject (veto)
- Ignore (no action)

Email notifications are sent to all approvers associated with a MAV rule when:

- A request is created.
- A request is approved or vetoed.
- An approved request is executed.

If the requestor is in the same approval group for the operation, they will receive an email when their request is approved.

**Note:** A requestor can't approve their own requests, even if they are in the approval group. But they can get the email notifications. Requestors who are not in approval groups (that is, who are not MAV administrators) don't receive email notifications.

== How protected operation execution works

If execution is approved for a protected operation, the requesting user continues with the operation when prompted. If the operation is vetoed, the requesting user must delete the request before proceeding.

MAV rules are evaluated after RBAC permissions. As a result, a user without sufficient RBAC permissions for operation execution cannot initiate the MAV request process.

= Manage administrator approval groups

:icons: font

:relative\_path: ./multi-admin-verify/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

Before enabling multi-admin verification (MAV), you must create an admin approval group containing one or more administrators to be granted approve or veto authority. Once you have enabled multi-admin verification, any modifications to approval group membership requires approval from one of the existing qualified administrators.

## About this task

You can add existing administrators to a MAV group or create new administrators.



MAV functionality honors existing role-based access control (RBAC) settings. Potential MAV administrators must have sufficient privilege to execute protected operations before they are added to MAV administrator groups. [Learn more about RBAC.](#)

You can configure MAV to alert MAV administrators that approval requests are pending. To do so, you must configure email notifications—in particular, the `Mail From` and `Mail Server` parameters—or you can clear these parameters to disable notification. Without email alerts, MAV administrators must check the approval queue manually.



== System Manager procedure

If you want to create a MAV approval group for the first time, see the System Manager procedure to [enable multi-admin verification.](#)

To modify an existing approval group or create an additional approval group:

1. Identify administrators to receive multi-admin verification.
  - a. Click **Cluster > Settings.**
  - b. Click  next to **Users and Roles.**
  - c. Click  **Add** under **Users.**
  - d. Modify the roster as needed.

For more information, see [Control administrator access.](#)

2. Create or modify the MAV approval group:
  - a. Click **Cluster > Settings.**
  - b. Click  next to **Multi-Admin Approval** in the **Security** section. (You will see the  icon if MAV is not yet configured.)
    - Name: enter a group name.
    - Approvers: select approvers from a list of users.
    - Email address: enter email address(es).
    - Default group: select a group.

MAV approval is required to edit an existing configuration once MAV is enabled.

== CLI procedure

1. Verify that values have been set for the `Mail From` and `Mail Server` parameters. Enter:

```
event config show
```

The display should be similar to the following:

```
cluster01::> event config show
                        Mail From:  admin@localhost
                        Mail Server: localhost
                        Proxy URL:   -
                        Proxy User:  -
                        Publish/Subscribe Messaging Enabled: true
```

To configure these parameters, enter:

```
event config modify -mail-from email_address -mail-server server_name
```

## 2. Identify administrators to receive multi-admin verification

If you want to...	Enter this command
Display current administrators	<code>security login show</code>
Modify credentials of current administrators	<code>security login modify &lt;parameters&gt;</code>
Create new administrator accounts	<code>security login create -user-or-group -name <i>admin_name</i> -application ssh -authentication-method password</code>

## 3. Create the MAV approval group:

```
security multi-admin-verify approval-group create [ -vserver svm_name]
-name group_name -approvers approver1[,approver2...] [-email address1,
address1...]
```

- `-vserver` - Only the admin SVM is supported in this release.
- `-name` - The MAV group name, up to 64 characters.
- `-approvers` - The list of one or more approvers.
- `-email` - One or more email addresses that are notified when a request is created, approved, vetoed, or executed.

**Example:** The following command creates a MAV group with two members and associated email addresses.

```
cluster-1::> security multi-admin-verify approval-group create
-name mav-grp1 -approvers pavan,julia -email
pavan@myfirm.com,julia@myfirm.com
```

## 4. Verify group creation and membership:

```
security multi-admin-verify approval-group show [-instance]
```

**Example:**

```
cluster-1::> security multi-admin-verify approval-group show
-instance
Vserver  Name          Approvers          Email
-----  -
svm-1    mav-grp1      pavan,julia       email
pavan@myfirm.com,julia@myfirm.com
```

Use these commands to modify your initial MAV group configuration.

**Note:** All require MAV administrator approval before execution.

If you want to...	Enter this command
Modify the group characteristics or modify existing member information	<code>security multi-admin-verify approval-group modify [parameters]</code>
Add or remove members	<code>security multi-admin-verify approval-group replace [-vserver svm_name] -name group_name [-approvers-to-add approver1[, approver2...]] [-approvers-to-remove approver1[, approver2...]]</code>
Delete a group	<code>security multi-admin-verify approval-group delete [-vserver svm_name] -name group_name</code>

= Enable and disable multi-admin verification

:icons: font

:relative\_path: ./multi-admin-verify/

:imagesdir: /tmp/d20221026-17026-1injpo/source/./authentication/./media/

Multi-admin verification (MAV) must be enabled explicitly. Once you have enabled multi-admin verification, approval by administrators in a MAV approval group (MAV administrators) is required to delete it.

**About this task**

Once MAV is enabled, modifying or disabling MAV requires MAV administrator approval.



If you need to disable multi-admin verification functionality without MAV administrator approval, contact NetApp Support and mention the following Knowledge Base article: [How to disable Multi-Admin Verification if MAV admin is unavailable](#).

When you enable MAV, you can specify the following parameters globally.

## Approval groups

A list of global approval groups. At least one group is required to enable MAV functionality.

## Required approvers

The number of approvers required to execute a protected operation. The default and minimum number is 1.

**Note:** The required number of approvers must be less than the total number of unique approvers in the default approval groups.

## Approval expiry (hours, minutes, seconds)

The period within which a MAV administrator must respond to an approval request. The default value is one hour (1h), the minimum supported value is one second (1s), and the maximum supported value is 14 days (14d).



## Execution expiry (hours, minutes, seconds)

The period within which the requesting administrator must complete the operation. The default value is one hour (1h), the minimum supported value is one second (1s), and the maximum supported value is 14 days (14d).

You can also override any of these parameters for specific [operation rules](#).



== System Manager procedure

1. Identify administrators to receive multi-admin verification.

- a. Click **Cluster > Settings**.
- b. Click  next to **Users and Roles**.
- c. Click  **Add** under **Users**.
- d. Modify the roster as needed.

For more information, see [Control administrator access](#).

2. Enable multi-admin verification by creating at least one approval group and adding at least one rule.

- a. Click **Cluster > Settings**.
- b. Click  next to **Multi-Admin Approval** in the **Security** section.
- c. Click  **Add** to add at least one approval group.
  - Name – Enter a group name.
  - Approvers – Select approvers from a list of users.
  - Email address – Enter email address(es).
  - Default group – Select a group.
- d. Add at least one rule.
  - Operation – Select a supported command from the list.
  - Query – Enter any desired command options and values.
  - Optional parameters; leave blank to apply global settings, or assign a different value for specific rules to override the global settings.
    - Required number of approvers

- Approval groups

e. Click **Advanced Settings** to view or modify defaults.


- Required number of approvers (default: 1)
- Execution request expiry (default: 1 hour)
- Approval request expiry (default: 1 hour)
- Mail server\*
- From email address\*

\*These update the email settings managed under "Notification Management". You are prompted to set them if they have not yet been configured.


f. Click **Enable** to complete MAV initial configuration.

After initial configuration, the current MAV status is displayed in the **Multi-Admin Approval** tile.

- Status (enabled or not)
- Active operations for which approvals are required
- Number of open requests in pending state

You can display an existing configuration by clicking . MAV approval is required to edit an existing configuration.

To disable multi-admin verification:

1. Click **Cluster > Settings**.
2. Click  next to **Multi-Admin Approval** in the **Security** section.
3. Click the Enabled toggle button.

MAV approval is required to complete this operation.

== CLI procedure

Before enabling MAV functionality at the CLI, at least one **MAV administrator group** must have been created.

If you want to...	Enter this command
Enable MAV functionality	<pre>security multi-admin-verify modify -approval-groups group1[,group2...] [- required-approvers nn ] -enabled true [ -execution-expiry [nnh][nmm][nns]] [ -approval-expiry [nnh][nmm][nns]]</pre> <p><b>Example :</b> the following command enables MAV with 1 approval group, 2 required approvers, and default expiry periods.</p> <pre>cluster-1::&gt; security multi- admin-verify modify -approval -groups mav-grp1 -required -approvers 2 -enabled true</pre> <p>Complete initial configuration by adding at least one <a href="#">operation rule</a>.</p>
Modify a MAV configuration (requires MAV approval)	<pre>security multi-admin-verify approval- group modify [-approval-groups group1[,group2...]] [-required-approvers nn ] [ -execution-expiry [nnh][nmm][ nns]] [ -approval-expiry [nnh][nmm][ nns]]</pre>
Verify MAV functionality	<pre>security multi-admin-verify show</pre> <p><b>Example:</b></p> <pre>cluster-1::&gt; security multi- admin-verify show Is      Required  Execution Approval Approval Enabled Approvers Expiry Expiry  Groups ----- true    2          1h      1h mav-grp1</pre>
Disable MAV functionality (requires MAV approval)	<pre>security multi-admin-verify modify -enabled false</pre>

= Manage protected operation rules



:icons: font  
:relative\_path: ./multi-admin-verify/  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You create multi-admin verification (MAV) rules to designate operations requiring approval. Whenever an operation is initiated, protected operations are intercepted and a request for approval is generated.

Rules can be created before enabling MAV by any administrator with appropriate RBAC capabilities, but once MAV is enabled, any modification to the rule set requires MAV approval.

You can create rules for the following commands in ONTAP 9.11.1.

cluster peer delete	volume snapshot autodelete modify
event config modify	volume snapshot delete
security login create	volume snapshot policy add-schedule
security login delete	volume snapshot policy create
security login modify	volume snapshot policy delete
system node run	volume snapshot policy modify
system node systemshell	volume snapshot policy modify-schedule
volume delete	volume snapshot policy remove-schedule
volume flexcache delete	volume snapshot restore
	vserver peer delete

In addition, the following commands are protected by default when MAV is enabled, but you can modify the rules to remove protection for these commands.

- security login password
- security login unlock
- set

The rules for MAV system-default commands – the security multi-admin-verify commands – cannot be altered.

When you create a rule, you can optionally specify the `-query` option to limit the request to a subset of the command functionality. For example, in the default set command, `-query` is set to `-privilege diag`, meaning that a request is generated for the set command only when `-privilege diag` is specified.

```

smci-vs0120::> security multi-admin-verify rule show
                                     Required  Approval
Vserver Operation                    Approvers Groups
-----
vs01      set                         -         -
          Query: -privilege diagnostic

```

By default, rules specify that a corresponding `security multi-admin-verify request create "protected_operation"` command is generated automatically when a protected operation is entered. You can modify this default to require that the `request create` command be entered separate.



By default, rules inherit the following global MAV settings, although you can specify rule-specific exceptions:

- Required Number of Approvers
- Approval Groups
- Approval Expiry period
- Execution Expiry period

== System Manager procedure

If you want to add a protected operation rule for the first time, see the System Manager procedure to [enable multi-admin verification](#).

To modify the existing rule set:

1. Click **Cluster > Settings**.
2. Click  next to **Multi-Admin Approval** in the **Security** section.
3. Click  **Add** to add at least one rule; you can also modify or delete existing rules.
  - Operation – Select a supported command from the list.
  - Query – Enter any desired command options and values.
  - Optional parameters – Leave blank to apply global settings, or assign a different value for specific rules to override the global settings.
    - Required number of approvers
    - Approval groups

== CLI procedure



All `security multi-admin-verify rule` commands require MAV administrator approval before execution except `security multi-admin-verify rule show`.

If you want to...	Enter this command
Create a rule	<pre>security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [parameters]</pre>
Modify credentials of current administrators	<pre>security login modify &lt;parameters&gt;</pre> <p><b>Example:</b> the following rule requires approval to delete the root volume.</p> <pre>security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"</pre>
Modify a rule	<pre>security multi-admin-verify rule modify -operation "protected_operation" [parameters]</pre>
Delete a rule	<pre>security multi-admin-verify rule delete -operation "protected_operation"</pre>
Show rules	<pre>security multi-admin-verify rule show</pre>

For command syntax details, see the `security multi-admin-verify rule` man pages.

= Request execution of protected operations

:icons: font

:relative\_path: ./multi-admin-verify/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

When you initiate a protected operation or command on a cluster enabled for multi-admin verification (MAV), ONTAP automatically intercepts the operation and asks to generate a request, which must be approved by one or more administrators in a MAV approval group (MAV administrators). Alternatively, you can create a MAV request without the dialog.

If approved, you must then respond to the query to complete the operation within the request expiry period. If vetoed, or if the request or expiry periods are exceeded, you must delete the request and resubmit.

MAV functionality honors existing RBAC settings. That is, your administrator role must have sufficient privilege to execute a protected operation without regard to MAV settings. [Learn more about RBAC.](#)

If you are a MAV administrator, your requests to execute protected operations must also be approved by a MAV administrator.

== System Manager procedure

When a user clicks on a menu item to initiate an operation and the operation is protected, a request for approval is generated and the user receives a notification similar to the following:

```
Approval request to delete the volume was sent.  
Track the request ID 356 from Events & Jobs > Multi-Admin Requests.
```

The **Multi-Admin Requests** window is available when MAV is enabled, showing pending requests based on the user's login ID and MAV role (approver or not). For each pending request, the following fields are displayed:

- Operation
- Index (number)
- Status (Pending, Approved, Rejected, Executed, or Expired)

If a request is rejected by one approver, no further actions are possible.

- Query (any parameters or values for the requested operation)
- Requesting User
- Request Expires On
- (Number of) Pending Approvers
- (Number of) Potential Approvers

When the request is approved, the requesting user can retry the operation within the expiry period.

If the user retries the operation without approval, a notification is displayed similar to the following:

```
Request to perform delete operation is pending approval.  
Retry the operation after request is approved.
```

== CLI procedure

1. Enter the protected operation directly or using the MAV request command.

**Examples – to delete a volume, enter one of the following commands:**

```
° volume delete
```

```
cluster-1::*> volume delete -volume voll -vserver vs0
```

```
Warning: This operation requires multi-admin verification. To  
create a  
verification request use "security multi-admin-verify  
request  
create".
```

```
Would you like to create a request for this operation?  
{y|n}: y
```

```
Error: command failed: The security multi-admin-verify request  
(index 3) is  
auto-generated and requires approval.
```

```
° security multi-admin-verify request create "volume delete"
```

```
Error: command failed: The security multi-admin-verify request  
(index 3)  
requires approval.
```

2. Check the status of the request and respond to the MAV notice.
  - a. If the request is approved, respond to the CLI message to complete the operation.

**Example:**

```
cluster-1::> security multi-admin-verify request show 3
```

```
Request Index: 3
  Operation: volume delete
    Query: -vserver vs0 -volume voll
    State: approved
Required Approvers: 1
Pending Approvers: 0
Approval Expiry: 2/25/2022 14:32:03
Execution Expiry: 2/25/2022 14:35:36
  Approvals: admin2
  User Vetoed: -
  Vserver: cluster-1
User Requested: admin
  Time Created: 2/25/2022 13:32:03
  Time Approved: 2/25/2022 13:35:36
  Comment: -
Users Permitted: -
```

```
cluster-1::*> volume delete -volume voll -vserver vs0
```

```
Info: Volume "voll" in Vserver "vs0" will be marked as deleted
and placed in the volume recovery queue. The space used by the
volume will be recovered only after the retention period of 12
hours has completed. To recover the space immediately, get the
volume name using (privilege:advanced) "volume recovery-queue
show voll_*" and then "volume recovery-queue purge -vserver vs0
-volume <volume_name>" command. To recover the volume use the
(privilege:advanced) "volume recovery-queue recover -vserver vs0
-volume <volume_name>" command.
```

```
Warning: Are you sure you want to delete volume "voll" in Vserver
"vs0" ?
{y|n}: y
```

- b. If the request is vetoed, or the expiry period has passed, delete the request, and either resubmit or contact the MAV administrator.

**Example:**

```
cluster-1::> security multi-admin-verify request show 3
```

```
Request Index: 3
  Operation: volume delete
    Query: -vserver vs0 -volume voll
    State: vetoed
Required Approvers: 1
Pending Approvers: 1
Approval Expiry: 2/25/2022 14:38:47
Execution Expiry: -
  Approvals: -
  User Vetoed: admin2
    Vserver: cluster-1
User Requested: admin
  Time Created: 2/25/2022 13:38:47
  Time Approved: -
    Comment: -
  Users Permitted: -
```

```
cluster-1::*> volume delete -volume voll -vserver vs0
```

```
Error: command failed: The security multi-admin-verify request
(index 3) hasbeen vetoed. You must delete it and create a new
verification request.
To delete, run "security multi-admin-verify request delete 3".
```

= Manage protected operation requests

:icons: font

:relative\_path: ./multi-admin-verify/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

When administrators in a MAV approval group (MAV administrators) are notified of a pending operation execution request, they must respond with an approve or veto message within a fixed time period (approval expiry). If a sufficient number of approvals are not received, the requester must delete the request and make another.

#### **About this task**

Approval requests are identified with index numbers, which are included in email messages and displays of the request queue.

The following information from the request queue can be displayed:

#### **Operation**

The protected operation for which the request is created.

**Query**

The object (or objects) upon which the user wants to apply the operation.

**State**

The current state of the request; pending, approved, rejected, expired, executed. If a request is rejected by one approver, no further actions are possible.

**Required approvers**

The number of MAV administrators that are required to approve the request. A user can set the required-approvers parameter for the operation rule. If a user does not set the required-approvers to the rule, then the required-approvers from the global setting is applied.

**Pending approvers**

The number of MAV administrators that are still required to approve the request for the request to be marked as approved.

**Approval expiry**

The period within which a MAV administrator must respond to an approval request. Any authorized user can set the approval-expiry for an operation rule. If approval-expiry is not set for the rule, then the approval-expiry from the global setting is applied.

**Execution expiry**

The period within which the requesting administrator must complete the operation. Any authorized user can set the execution-expiry for an operation rule. If execution-expiry is not set for the rule, then the execution-expiry from the global setting is applied.

**Users approved**

The MAV administrators who have approved the request.

**User vetoed**

The MAV administrators who have vetoed the request.

**Storage VM (vserver)**

The SVM with which the request is associated with. Only the admin SVM is supported in this release.

**User requested**

The username of the user who created the request.

**Time created**

The time when the request is created.

**Time approved**

The time when the request state changed to approved.

**Comment**

Any comments that are associated with the request.

**Users permitted**

The list of users permitted to perform the protected operation for which the request is approved. If `users-permitted` is empty, then any user with appropriate permissions can perform the operation.

All expired or executed requests are deleted when a limit of 1000 requests is reached, or when the



expired time is greater than 8hrs for expired requests. Vetoed requests are deleted once they are marked as expired.

== System Manager procedure

MAV administrators receive email messages with details of the approval request, request expiry period, and a link to approve or reject the request. They can access an approval dialog by clicking the link in the email or navigate to **Events & Jobs>Requests** in System Manager.

The **Requests** window is available when multi-admin verification is enabled, showing pending requests based on the user's login ID and MAV role (approver or not).

- Operation
- Index (number)
- Status (Pending, Approved, Rejected, Executed, or Expired)

If a request is rejected by one approver, no further actions are possible.

- Query (any parameters or values for the requested operation)
- Requesting User
- Request Expires On
- (Number of) Pending Approvers
- (Number of) Potential Approvers

MAV administrators have additional controls in this window; they can approve, reject, or delete individual operations, or selected groups of operations. However, if the MAV administrator is the Requesting User, they cannot approve, reject or delete their own requests.

== CLI procedure

1. When notified of pending requests by email, note the request's index number and approval expiry period. The index number can also be displayed using the **show** or **show-pending** options mentioned below.
2. Approve or veto the request.

If you want to...	Enter this command
Approve a request	<code>security multi-admin-verify request approve nn</code>
Veto a request	<code>security multi-admin-verify request veto nn</code>

If you want to...	Enter this command
Show all requests, pending requests, or a single request	<pre>security multi-admin-verify request { show   show-pending } [nn] { -fields <i>field1</i> [, <i>field2</i>...]   [- instance ] }</pre> <p>You can show all requests in the queue or only pending requests. If you enter the index number, only information for that is displayed. You can display information about specific fields (by using the <code>-fields</code> parameter) or about all fields (by using the <code>-instance</code> parameter).</p>
Delete a request	<pre>security multi-admin-verify request delete nn</pre>

**Example:**

The following sequence approves a request after the MAV administrator has received the request email with index number 3, which already has one approval.

```

cluster1::> security multi-admin-verify request show-pending
                                Pending
Index Operation      Query State  Approvers Requestor
-----
3 volume delete -    pending 1      julia

cluster-1::> security multi-admin-verify request approve 3

cluster-1::> security multi-admin-verify request show 3

Request Index: 3
  Operation: volume delete
    Query: -
    State: approved
Required Approvers: 2
Pending Approvers: 0
Approval Expiry: 2/25/2022 14:32:03
Execution Expiry: 2/25/2022 14:35:36
Approvals: mav-admin2
User Vetoed: -
Vserver: cluster-1
User Requested: julia
Time Created: 2/25/2022 13:32:03
Time Approved: 2/25/2022 13:35:36
Comment: -
Users Permitted: -

```

**Example:**

The following sequence vetoes a request after the MAV administrator has received the request email with index number 3, which already has one approval.

```

cluster1::> security multi-admin-verify request show-pending
                                Pending
Index Operation      Query State   Approvers Requestor
-----
3 volume delete - pending 1 pavan

cluster-1::> security multi-admin-verify request veto 3

cluster-1::> security multi-admin-verify request show 3

Request Index: 3
  Operation: volume delete
    Query: -
    State: vetoed
Required Approvers: 2
Pending Approvers: 0
Approval Expiry: 2/25/2022 14:32:03
Execution Expiry: 2/25/2022 14:35:36
Approvals: mav-admin1
User Vetoed: mav-admin2
Vserver: cluster-1
User Requested: pavan
Time Created: 2/25/2022 13:32:03
Time Approved: 2/25/2022 13:35:36
Comment: -
Users Permitted: -

```

= Ransomware protection

= Autonomous Ransomware Protection overview

:toc: macro

:hardbreaks:

:toclevels: 1

:icons: font

:linkattrs:

:relative\_path: ./anti-ransomware/

:imagesdir: /tmp/d20221026-17026-1injpo/source/./authentication/./media/

Beginning with ONTAP 9.10.1, the Autonomous Ransomware Protection (ARP) feature uses workload analysis in NAS (NFS and SMB) environments to proactively detect and warn about abnormal activity that might indicate a ransomware attack.

When an attack is suspected, ARP also creates new Snapshot copies, in addition to existing protection from scheduled Snapshot copies.

The ARP feature is enabled with the following licenses.

ONTAP releases	License
ONTAP 9.11.1 and later	Anti_ransomware
ONTAP 9.10.1	MT_EK_MGMT (Multi-Tenant Key Management)

- If you are upgrading to ONTAP 9.11.1 or later and ARP is already configured on your system, you do not need to purchase the new Anti-ransomware license. For new ARP configurations, the new license is required.
- If you are reverting from ONTAP 9.11.1 or later to ONTAP 9.10.1, and you have enabled ARP with the Anti-ransomware license, you will see a warning message and might need to reconfigure ARP. [Learn about reverting ARP](#).

You can configure ARP on a per-volume basis using either ONTAP System Manager or the ONTAP command line interface (CLI).

== ONTAP ransomware protection strategy

An effective ransomware detection strategy should include more than a single layer of protection.

An analogy would be the safety features of a vehicle. You wouldn't want to rely on a single feature, such as a seatbelt, to completely protect you in an accident. Air bags, anti-lock brakes, and forward-collision warning are all additional safety features that will lead to a much better outcome. Ransomware protection should be viewed in the same way.

While ONTAP includes features like FPolicy, Snapshot copies, SnapLock, and Active IQ Digital Advisor to help protect from ransomware, the following information focuses on the ONTAP ARP on-box feature with machine-learning capabilities.

To learn more about ONTAP's other anti-ransomware features, see: [TR-4572: NetApp Solution for Ransomware](#).

== What ONTAP ARP detects

There are two types of ransomware attacks:

1. Denial of service to files by encrypting data.  
The attacker withholds access to this data unless a ransom is paid.
2. Theft of sensitive proprietary data.  
The attacker threatens to release this data to the public domain unless a ransom is paid.

ONTAP ARP addresses the first type, with an anti-ransomware detection mechanism that is based on:

1. Identification of the incoming data as encrypted or plaintext.
2. Analytics, which detects
  - High data *entropy* (an evaluation of the randomness of data in a file)
  - A surge in abnormal volume activity with data encryption
  - An extension that does not conform to the normal extension type



No ransomware detection or prevention system can completely guarantee safety from a ransomware attack. While it's possible an attack might go undetected, NetApp ARP acts as an important additional layer of defense if anti-virus software has failed to detect an intrusion. ARP can detect the spread of most ransomware attacks after only a small number of files are encrypted, take action automatically to protect data, and alert you that a suspected attack is happening.

== How to recover data in ONTAP after a ransomware attack

When an attack is suspected, the system takes a volume Snapshot copy at that point in time and locks that copy. If the attack is confirmed later, the volume can be restored to this proactively taken snapshot, minimizing the data loss.

Locked Snapshot copies cannot be deleted by normal means. However, if you decide later to mark the attack as a false positive, the locked copy will be deleted.

With the knowledge of the affected files and the time of attack, it is possible to selectively recover the affected files from various Snapshot copies, rather than simply reverting the whole volume to one of the snapshots.

ARP thus builds on proven ONTAP data protection and disaster recovery technology to respond to ransomware attacks. See the following topics for more information on recovering data.

- [Recover from Snapshot copies \(System Manager\)](#)
- [Restoring files from Snapshot copies \(CLI\)](#)
- [Smart ransomware recovery](#)

= Autonomous Ransomware Protection use cases and considerations

:toc: macro

:hardbreaks:

:toclevels: 1

:icons: font

:linkattrs:

:relative\_path: ./anti-ransomware/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

## ONTAP platform support:

- The Autonomous Ransomware Protection (ARP) feature is available for all on-premises ONTAP systems beginning with ONTAP 9.10.1.
- It is not available in Cloud Volumes ONTAP environments.

Suitable workloads:

- Databases on NFS storage
- Windows or Linux home directories

Because users could create files with extensions that weren't detected in the learning period, there is greater possibility of false positives in this workload.

- Images and video

For example, health care records and Electronic Design Automation (EDA) data.

#### Unsuitable workloads:

- Workloads with a high frequency of file create or delete (hundreds of thousands of files in few seconds; for example, test/dev workloads)
- ARP depends on the ability to recognize an unusual surge in file create or delete activity. If the application itself is the source of the file activity, it cannot be effectively distinguished from ransomware activity
- Workloads where the application or the host encrypts data  
ARP depends on distinguishing incoming data as encrypted or unencrypted. If the application itself is encrypting the data, then the effectiveness of the feature is reduced. However, the feature can still work based on file activity (create, delete, and overwrite) and file type.

#### Unsupported system configurations:

- SAN environments
- ONTAP S3 environments
- VMDKs on NFS

#### Volume requirements:

- Less than 100% full
- Junction path must be active

#### Unsupported volume types:

- Offline volumes
- Restricted volumes
- SnapLock volumes
- FlexGroup volumes
- FlexCache volumes (the anti-ransomware feature is supported on origin FlexVol volumes but not on cache volumes)
- SAN-only volumes
- Volumes of stopped storage VMs
- Root volumes of storage VMs
- Data protection volumes

== ARP performance and frequency considerations

The ARP feature can have a minimal impact on system performance as measured in throughput and peak IOPS. The impact of the anti-ransomware feature is highly dependent on volume workloads. For most typical or common workloads, the following configuration limits are recommended:

<b>Workload characteristics</b>	<b>Recommended volume limit per node</b>	<b>Performance degradation when per-node volume limit is exceeded *</b>
Read-intensive or the data can be compressed.	150	4% of maximum IOPS

Workload characteristics	Recommended volume limit per node	Performance degradation when per-node volume limit is exceeded *
Write-intensive and the data cannot be compressed.	60	10% of maximum IOPS

\* System performance is not degraded beyond these percentages regardless of the number of volumes added in excess of the recommended limits.

Because ARP analytics are run in a prioritized sequence, as the number of protected volumes increases, analytics are run on each volume less frequently.

== How automatic Snapshot copies work when ransomware is detected

In order to obtain the best possible recovery point, ARP creates an automatic Snapshot copy as soon as it detects abnormal file activity. However, ARP does not immediately flag an alert; rather, analytics need to run and confirm that the suspicious activity matches a ransomware profile before generating an alert. This process could take up to 60 minutes. If the analytics determines the activity is not suspicious, then an alert is not generated, but the automatically created Snapshot copy remains present on the file system for a minimum of two days.

Beginning with ONTAP 9.11.1, you can control the number and retention period for ARP Snapshot copies that are automatically generated in response to suspected ransomware attacks. Learn how to [modify options for automatic Snapshot copies](#).

= Enable Autonomous Ransomware Protection

:toc: macro

:hardbreaks:

:toclevels: 1

:icons: font

:linkattrs:

:relative\_path: ./anti-ransomware/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

Beginning with ONTAP 9.10.1, Autonomous Ransomware Protection (ARP) can be enabled on new or existing volumes. You first enable ARP in learning mode, in which the system analyzes the workload to characterize normal behavior, then you switch to active mode, in which abnormal activity is flagged for your evaluation.

#### What you'll need

- A storage VM enabled for NFS or SMB (or both).
- The correct license is installed for your ONTAP version.

ONTAP releases	License
ONTAP 9.8-9.10.1	MT_EK_MGMT (Multi-Tenant Key Management)
ONTAP 9.11.1 and later	Anti_ransomware

- An NAS workload with clients configured.
- The volume to be protected must have an active junction-path.



- Optional but recommended: The EMS system is configured to send email notifications, which will include notices of ARP activity. For more information, see [Configure EMS events to send email notifications](#).

### About this task

NetApp ARP includes an initial learning period (also known as “dry run”), in which an ONTAP system learns which file extensions are valid and uses the analyzed data to develop alert profiles. After running ARP in learning mode for enough time to assess workload characteristics, you can switch to active mode and start protecting your data. Anti-ransomware continues to collect and analyze data to refine alert profiles.

During the learning period, the system automatically learns the workload characteristics of a configured volume, performing special observations and pattern analysis.

A learning period of 30 days is recommended. Although you can switch from learning to active mode anytime, switching early may lead to too many false positives.

In the ONTAP CLI, you can use the `security anti-ransomware volume workload-behavior show` command to show file extensions detected to date. However, it is recommended that you not use this tool to shorten the learning period.

You can enable ARP on an existing volume, or you can create a new volume and enable ARP from the beginning.



In existing volumes, learning and active modes only apply to newly-written data, not to already existing data in the volume. The existing data is not scanned and analyzed, because the characteristics of earlier normal data traffic are assumed based on the new data after the volume is enabled for ARP.

In the ONTAP CLI, a new command family has been introduced to manage this feature: `security anti-ransomware volume`. You can also use the `volume modify` command with the `-anti-ransomware` parameter to manage the feature.

## System Manager

1. Click **Storage > Volumes** and then select the volume you want to protect.
2. In the **Security** tab of the **Volumes** overview, click **Status** to switch from Disabled to Enabled in learning-mode in the **Anti-ransomware** box.
3. When the learning period is over, switch ARP to active mode.
  - a. Click **Storage > Volumes** and then select the volume that is ready for active mode.
  - b. In the **Security** tab of the **Volumes** overview, click **Switch** to active mode in the Anti-ransomware box.
4. You can always verify the ARP state of the volume in the **Anti-ransomware** box.  
To display ARP status for all volumes: In the **Volumes** pane, click **Show/Hide**, then ensure that **Anti-ransomware** status is checked.

## CLI

1. Modify an existing volume to enable ransomware protection in learning mode:

```
security anti-ransomware volume dry-run -volume vol_name -vserver svm_name
```

You can also enable ransomware with the `volume modify` command:

```
volume modify -volume vol_name -vserver svm_name -anti-ransomware-state dry-run
```

At the CLI, you can also create a new volume with anti-ransomware protection enabled before provisioning data.

```
volume create -volume vol_name -vserver svm_name -aggregate aggr_name -size nn -anti-ransomware-state dry-run -junction-path /path_name
```



You should always enable ARP initially in the dry-run state. Beginning with the active state can lead to excessive false positive reports.

2. When the learning period is over, modify the protected volume to switch to active mode:

```
security anti-ransomware volume enable -volume vol_name -vserver svm_name
```

You can also switch to active mode with the modify volume command:

```
volume modify -volume vol_name -vserver svm_name -anti-ransomware-state active
```

3. Verify the ARP state of the volume.

```
security anti-ransomware volume show
```

= Enable Autonomous Ransomware Protection by default in new volumes

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./anti-ransomware/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

Beginning with ONTAP 9.10.1, you can configure storage VMs (SVMs) such that new volumes are enabled by default for Autonomous Ransomware Protection (ARP) in learning mode.

### What you'll need


- The correct license is installed for your ONTAP version.

ONTAP releases	License
ONTAP 9.11.1 and later	Anti_ransomware
ONTAP 9.8-9.10.1	MT_EK_MGMT (Multi-Tenant Key Management)

### About this task

New volumes are created by default with ARP in disabled mode, but you can change this setting in System Manager and at the CLI. Volumes enabled by default are set to ARP in learning mode.

### System Manager

1. Click **Storage > Storage VMs** and then select the storage VM for default anti-virus.
2. In the **Settings** tab, [in the **Security** section], click  in the **Anti-ransomware** box, then check the box to enable ARP for NAS volumes.

### CLI

1. Modify an existing SVM to enable ARP by default in new volumes:  
`vserver modify -vserver svm_name -anti-ransomware-default-volume-state dry-run`

At the CLI, you can also create a new SVM with ARP enabled by default for new volumes.

```
vserver create -vserver svm_name -anti-ransomware-default-volume-state dry-run  
[other parameters as needed]
```

= Pause Autonomous Ransomware Protection to exclude workload events from analysis

:toc: macro

:hardbreaks:

:toclevels: 1

:icons: font

:linkattrs:

:relative\_path: ./anti-ransomware/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

If you are expecting unusual workload events, you can temporarily suspend and resume Autonomous Ransomware Protection (ARP) analysis at any time.

### What you'll need

- ARP is running in learning or active mode.

### About this task

During an ARP pause, no events are logged nor are any actions for new writes. However, the analytics operation continues for earlier logs in the background.



Do not use the anti-ransomware disable function to pause analytics. Doing so disables ARP on the volume and all the existing information around learned workload behavior is lost. This would require a restart of the learning period.

## System Manager

1. Click **Storage > Volumes** and then select the volume where you want to pause ARP.
2. In the Security tab of the Volumes overview, click **Pause anti-ransomware** in the **Anti-ransomware** box.

## CLI

Pause ARP on a volume:

```
security anti-ransomware volume pause -vserver svm_name -volume vol_name
```

To resume processing, use the `resume` parameter.

```
security anti-ransomware volume resume -vserver svm_name -volume vol_name
```

= Respond to abnormal activity.

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./anti-ransomware/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

When Autonomous Ransomware Protection (ARP) detects abnormal activity in a protected volume, it issues a warning. You should evaluate the notification to determine whether the activity is expected and acceptable, or whether an attack is under way.

### What you'll need

- ARP is running in active mode.

### About this task

ARP displays a list of suspected files when it detects any combination of high data entropy, abnormal volume activity with data encryption, and unusual file extensions.

When the warning is issued, you can respond by marking the file activity in one of two ways:

- False positive

The identified file type is expected in your workload and can be ignored.

- Potential ransomware attack

The identified file type is unexpected in your workload and should be treated as a potential attack.

In both cases, normal monitoring resumes after updating and clearing the notices; ARP records your evaluation, logs are updated with the new file types and using them for future analysis. However, in the case of a suspected attack, you must determine whether it is an attack, respond to it if it is, and restore protected data before clearing the notices. [Learn more about how to recover from a ransomware attack.](#)



There are no notices to clear if you restored an entire volume.

## System Manager

1. When you receive an “abnormal activity” notification, click on the link or navigate to the **Security** tab of the **Volumes** overview.

Warnings are displayed in the Overview pane of the Events window.

2. When a “Detected abnormal volume activity” message is displayed, view the suspect files.

In the **Security** tab, click View **Suspected File Types**.

3. In the **Suspected File Types** dialog box, examine each file type and mark it as either “False Positive” or “Potential Ransomware attack”.

If you selected this value...	Take this action...
False Positive	Click <b>Update</b> and <b>Clear Suspect File Types</b> to record your decision and resume normal anti-ransomware monitoring.
Potential Ransomware Attack	Respond to the attack and restore protected data. Then click <b>Update</b> and <b>Clear Suspect File Types</b> to record your decision and resume normal ARP monitoring. There are no suspect file types to clear if you restored an entire volume.

## CLI

1. When you receive a notification of a suspected ransomware attack, verify the time and severity of the attack:

```
security anti-ransomware volume show -vserver svm_name -volume vol_name
```

Sample output:

```
Vserver Name: vs0
Volume Name: voll
State: enabled
Attack Probability: moderate
Attack Timeline: 9/14/2021 01:03:23
Number of Attacks: 1
```

You can also check EMS messages:

```
event log show -message-name callhome.arw.activity.seen
```

2. Generate an attack report and note the output location:

```
security anti-ransomware volume attack generate-report -volume vol_name -dest -path file_location/
```

Sample output:

```
Report "report_file_vs0_voll_14-09-2021_01-21-08" available at path "vs0:voll/"
```

3. View the report on an admin client system. For example:

```
[root@rhel8 mnt]# cat report_file_vs0_voll_14-09-2021_01-21-08

19 "9/14/2021 01:03:23" test_dir_1/test_file_1.jpg.lckd
20 "9/14/2021 01:03:46" test_dir_2/test_file_2.jpg.lckd
21 "9/14/2021 01:03:46" test_dir_3/test_file_3.png.lckd`
```

4. Take one of the following actions based on your evaluation of the file extensions:

- False positive

Enter the following command to record your decision – adding the new extension to the list of those allowed – and resume normal anti-ransomware monitoring:

```
anti-ransomware volume attack clear-suspect -vserver svm_name -volume vol_name [extension identifiers] -false-positive true
```

Use one of the following parameters to identify the extensions:

`[-seq-no integer]` Sequence number of the file in the suspect list.

`[-extension text, ... ]` File extensions

`[-start-time date_time -end-time date_time]` Starting and ending times for the range of files to be cleared, in the form "MM/DD/YYYY HH:MM:SS".

- Potential ransomware attack

Respond to the attack and restore data. Then enter the following command to record your decision and resume normal ARP monitoring:

```
anti-ransomware volume attack clear-suspect -vserver svm_name -volume vol_name [extension identifiers] -false-positive false
```

Use one of the following parameters to identify the extensions:

`[-seq-no integer]` Sequence number of the file in the suspect list

`[-extension text, ... ]` File extension

`[-start-time date_time -end-time date_time]` Starting and ending times for the range of files to be cleared, in the form "MM/DD/YYYY HH:MM:SS".

There are no suspect file types to clear if you restored an entire volume.

= Restore data after a ransomware attack

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./anti-ransomware/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

Snapshot copies named “Anti\_ransomware\_backup” are created when Autonomous Ransomware Protection (ARP) detects a potential attack. You can restore data from these ARP copies or other Snapshot copies.



If a ransomware attack occurs, see the Knowledge Base article [Ransomware prevention and recovery in ONTAP](#) for additional information on recovery and future mitigation.

#### What you'll need

- ARP enabled
- Reports from potential ransomware attacks

1. Display the Snapshot copies in volumes identified in a potential attack:  
Click **Storage > Volumes**, select the volume, then click the Snapshot Copies tab.
2. Restore the desired copies according to these instructions:  
[Recover from Snapshot copies](#)

## CLI

1. Display the Snapshot copies in volumes identified in a potential attack:  
`volume snapshot show -vserver svm_name -volume vol_name`
2. Restore the desired copies according to these instructions:  
[Restoring files from Snapshot copies](#)



= Modify options for automatic Snapshot copies

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./anti-ransomware/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

Beginning with ONTAP 9.11.1, you can use the CLI to control the number and retention period for Autonomous Ransomware Protection (ARP) Snapshot copies that are automatically generated in response to suspected ransomware attacks.

**Note:** The `vserver options` command is a hidden command. To view the man page, enter `man vserver options` at the ONTAP CLI.

The following options for automatic Snapshot copies can be modified:

#### **arw.snap.max.count**

Specifies the maximum number of ARP Snapshot copies that can exist in a volume at any given time. Older copies are deleted to ensure that the total number of ARP Snapshot copies are within this specified limit.

#### **arw.snap.create.interval.hours**

Specifies the interval (in hours) between ARP Snapshot copies. A new Snapshot copy will be created when an attack is suspected and the copy created previously is older than this specified interval.

#### **arw.snap.normal.retain.interval.hours**

Specifies the duration (in hours) for which an ARP Snapshot copy is retained. When an ARP Snapshot copy becomes this old, any other ARP Snapshot copy created before the latest copy to reach this age is deleted. No ARP Snapshot copy can be older than this duration.

#### **arw.snap.max.retain.interval.days**

Specifies the maximum duration (in days) for which an ARP Snapshot copy can be retained. Any ARP Snapshot copy older than this duration will be deleted if there is no attack reported on the volume.

#### **arw.snap.create.interval.hours.post.max.count**

Specifies the interval (in hours) between ARP Snapshot copies when the volume already contains the maximum number of ARP Snapshot copies. When the maximum number is reached, an ARP Snapshot copy is deleted to make room for a new copy. The new ARP Snapshot copy creation speed can be reduced to retain the older copy using this option. If the volume already contains maximum number of ARP Snapshot copies, then this interval specified in this option is used for next ARP Snapshot copy creation, instead of `arw.snap.create.interval.hours`.

#### **arw.surge.snap.interval.days**

Specifies the interval (in days) between ARP surge Snapshot copies. A new ARP Snapshot surge copy is created when there is a surge in IO traffic and the last created ARP Snapshot copy is older than this specified interval. This option also specifies the duration (in days) for which an ARP surge Snapshot copy is retained.

#### **CLI procedure**

To show all current ARP Snapshot copy settings, enter:

```
vserver options -vserver svm_name arw*
```

To show selected current ARP Snapshot copy settings, enter:

```
vserver options -vserver svm_name -option-name arw_setting_name
```

To modify ARP Snapshot copy settings, enter:

```
vserver options -vserver svm_name -option-name arw_setting_name -option-value arw_setting_value
```

= Antivirus configuration

= Antivirus configuration overview

```
:icons: font
```

```
:relative_path: ./antivirus/
```

```
:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/
```

You can use NetApp virus scanning, called *Vscan*, to protect data from being compromised by viruses or other malicious code. It shows you how to use on-access scanning to check for viruses when clients access files over SMB, and how to use on-demand scanning to check for viruses immediately or on a schedule.

You can work with *Vscan* by using the ONTAP command-line interface (CLI), not System Manager or an automated scripting tool. *Vscan* is not supported by System Manager.

#### Related information

[NetApp Technical Report 4286: Antivirus Solution for Clustered Data ONTAP McAfee](#)

[NetApp Technical Report 4304: Antivirus Solution for Clustered Data ONTAP Symantec](#)

[NetApp Technical Report 4312: Antivirus Solution for Clustered Data ONTAP Trend Micro](#)

= About NetApp antivirus protection

= About NetApp virus scanning

```
:icons: font
```

```
:relative_path: ./antivirus/
```

```
:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/
```

You can use integrated antivirus functionality on NetApp storage systems to protect data from being compromised by viruses or other malicious code. NetApp virus scanning, called *Vscan*, combines best-in-class third-party antivirus software with ONTAP features that give you the flexibility you need to control which files get scanned and when.

== How virus scanning works

Storage systems offload scanning operations to external servers hosting antivirus software from third-party vendors. The ONTAP Antivirus Connector, provided by NetApp and installed on the external server, handles communication between the storage system and the antivirus software.

- You can use *on-access scanning* to check for viruses when clients open, read, rename, or close files

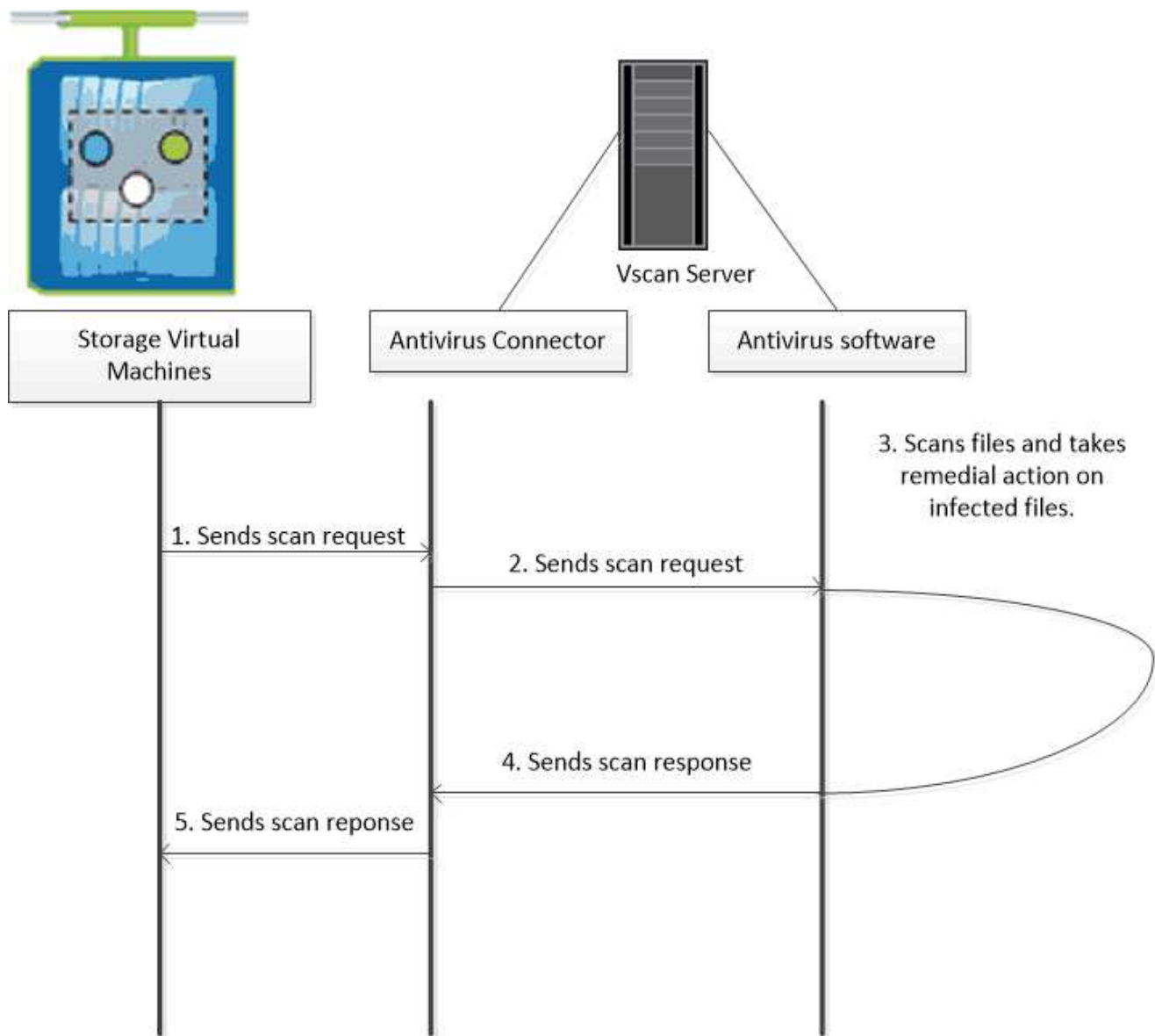
over SMB. File operation is suspended until the external server reports the scan status of the file. If the file has already been scanned, ONTAP allows the file operation. Otherwise, it requests a scan from the server.

On-access scanning is not supported for NFS.

- You can use *on-demand scanning* to check files for viruses immediately or on a schedule. You might want to run scans only in off-peak hours, for example. The external server updates the scan status of the checked files, so that file-access latency for those files (assuming they have not been modified) is typically reduced when they are next accessed over SMB.

You can use on-demand scanning for any path in the SVM namespace, even for volumes that are exported only through NFS.

You typically enable both scanning modes on an SVM. In either mode, the antivirus software takes remedial action on infected files based on your settings in the software.



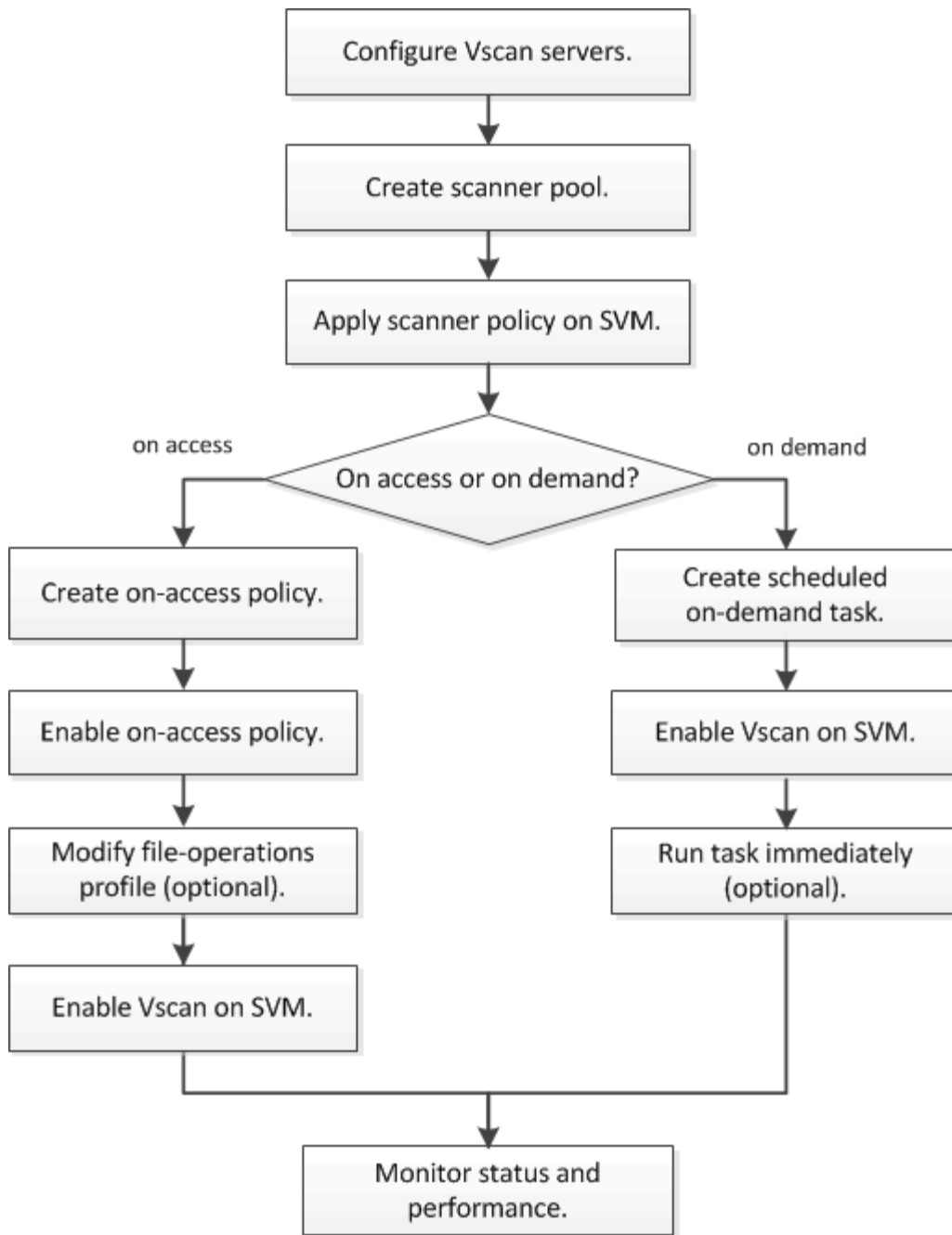
= Virus scanning workflow  
:icons: font

```
:relative_path: ./antivirus/
```

```
:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/
```

You must create a scanner pool and apply a scanner policy before you can enable scanning. You typically enable both on-access and on-demand scanning on an SVM.

You must have completed the CIFS configuration.



= Antivirus architecture

:icons: font

:relative\_path: ./antivirus/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

The NetApp antivirus architecture consists of a Vscan server and a set of ONTAP configurables.

== Vscan server components

You must install the following components on the Vscan server.

- **ONTAP Antivirus Connector**

The ONTAP Antivirus Connector provided by NetApp handles communication between ONTAP and the Vscan server.

- **Antivirus software**

ONTAP-compliant third-party antivirus software scans files for viruses or other malicious code. You specify the remedial actions to be taken on infected files when you configure the software.

== ONTAP configurables

You must configure the following items on the NetApp storage system.

- **Scanner pool**

A scanner pool defines the Vscan servers and privileged users that can connect to SVMs. It also defines a scan request timeout period, after which the scan request is sent to an alternative Vscan server if one is available.

It is a best practice to set the timeout period in the antivirus software on the Vscan server to five seconds less than the scanner-pool request timeout period, to avoid situations in which file access is delayed or denied altogether because the timeout period on the software is greater than the timeout period for the scan request.

- **Privileged user**

A privileged user is a domain user account that a Vscan server uses to connect to the SVM. The account must be included in the list of privileged users defined in the scanner pool.

- **Scanner policy**

A scanner policy determines whether a scanner pool is active. A scanner policy can have one of the following values:

- `Primary` specifies that the scanner pool is active.
  - `Secondary` specifies that the scanner pool is active only if none of the Vscan servers in the primary scanner pool is connected.
  - `Idle` specifies that the scanner pool is inactive.
- Scanner policies are system-defined. You cannot create a custom scanner policy.

- **On-access policy**

An on-access policy defines the scope of an on-access scan. You can specify the maximum size of the files to be scanned, the extensions of the files to be included in the scan, and the extensions and paths of the files to be excluded from the scan.

By default, only read-write volumes are scanned. You can specify filters that enable scanning of read-only volumes or that restrict scanning to files opened with execute access:

- `scan-ro-volume` enables scanning of read-only volumes.
- `scan-execute-access` restricts scanning to files opened with execute access.

“Execute access” is not identical with “execute permission.” A given client will have “execute access” on an executable file only if the file was opened with “execute intent.”

+

You can set the `scan-mandatory` option to off to specify that file access is allowed when no Vscan servers are available for virus scanning.

- **On-demand task**

An on-demand task defines the scope of an on-demand scan. You can specify the maximum size of the files to be scanned, the extensions and paths of the files to be included in the scan, and the extensions and paths of the files to be excluded from the scan. Files in subdirectories are scanned by default.

You use a cron schedule to specify when the task runs. You can use the `vserver vscan on-demand-task run` command to run the task immediately.

- **Vscan file-operations profile (on-access scanning only)**

The `-vscan-fileop-profile` parameter for the `vserver cifs share create` command defines which operations on a SMB share can trigger virus scanning. By default, the parameter is set to `standard`, which is the NetApp best practice.

You can adjust this parameter as necessary when you create or modify a SMB share:

- `no-scan` specifies that virus scans are never triggered for the share.
- `standard` specifies that virus scans can be triggered by open, close, and rename operations.
- `strict` specifies that virus scans can be triggered by open, read, close, and rename operations.

The `strict` profile provides enhanced security for situations in which multiple clients access a file simultaneously. If one client closes a file after writing a virus to it, and the same file remains open on a second client, `strict` ensures that a read operation on the second client triggers a scan before the file is closed.

You should be careful to restrict the `strict` profile to shares containing files that you anticipate will be accessed simultaneously. Because the profile generates more scan requests than the others, it may affect performance adversely.

- `writes-only` specifies that virus scans can be triggered only when a file that has been modified is closed.

If a client application performs a rename operation, the file is closed with the new name and is not scanned. If such operations pose a security concern in your environment, you should use the `standard` or `strict` profile.

+

Because `writes-only` generates fewer scan requests than the other profiles (except `no-scan`), it typically improves performance.

+

Keep in mind, though, that if you use this profile for a share, the scanner must be configured to delete or quarantine an unrepairable infected file, so that it cannot be accessed by clients later. If, for example, a client closes a file after writing a virus to it, and the file is not repaired, deleted, or quarantined, any client that accesses the file *without* writing to it will be infected.

= Vscan server installation and configuration

:icons: font

:relative\_path: ./antivirus/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You must set up one or more Vscan servers to ensure that files on your system are scanned for viruses. Follow the instructions provided by your vendor to install and configure the antivirus software on the server. Follow the instructions in the readme file provided by NetApp to install and configure the ONTAP Antivirus Connector.

For disaster recovery and MetroCluster configurations, you must set up separate Vscan servers for the local and partner clusters.

== Antivirus software requirements

- For information about antivirus software requirements, see the vendor documentation.
- For information about the vendors, software, and versions supported by Vscan, see the NetAppInteroperability Matrix.

[mysupport.netapp.com/matrix](https://mysupport.netapp.com/matrix)

== ONTAP Antivirus Connector requirements

- You can download the ONTAP Antivirus Connector from the Software Download page on the NetApp Support Site. [NetApp Downloads: Software](#)
- For information about the Windows versions supported by the ONTAP Antivirus Connector, see the NetAppInteroperability Matrix.

[mysupport.netapp.com/matrix](https://mysupport.netapp.com/matrix)

You can install different versions of Windows servers for different Vscan servers in a cluster.



- .NET 3.0 or later must be installed on the Windows server.
- SMB 2.0 must be enabled on the Windows server.

= Configure scanner pools

= Configure scanner pools overview

:icons: font

:relative\_path: ./antivirus/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

A scanner pool defines the Vscan servers and privileged users that can connect to SVMs. A scanner policy determines whether a scanner pool is active.

If you use an export policy on a SMB server, you must add each Vscan server to the export policy.

= Create a scanner pool on a single cluster

:icons: font

:relative\_path: ./antivirus/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

A scanner pool defines the Vscan servers and privileged users that can connect to SVMs. You can create a scanner pool for an individual SVM or for all of the SVMs in a cluster.

### What you'll need

- SVMs and Vscan servers must be in the same domain or in trusted domains.
- For scanner pools defined for an individual SVM, you must have configured the ONTAP Antivirus Connector with the SVM management LIF or the SVM data LIF.
- For scanner pools defined for all of the SVMs in a cluster, you must have configured the ONTAP Antivirus Connector with the cluster management LIF.

### About this task

The list of privileged users must include the domain user account the Vscan server uses to connect to the SVM.

### Steps

1. Create a scanner pool:

```
vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM
-scanner-pool scanner_pool -hostnames Vscan_server_hostnames -privileged
-users privileged_users
```

- Specify a data SVM for a pool defined for an individual SVM, and specify a cluster admin SVM for a pool defined for all of the SVMs in a cluster.
- Specify an IP address or FQDN for each Vscan server host name.
- Specify the domain and user name for each privileged user.  
For a complete list of options, see the man page for the command.

The following command creates a scanner pool named *SP* on the *vs1SVM*:

```
cluster1::> vserver vscan scanner-pool create -vserver vs1 -scanner
-pool SP -hostnames 1.1.1.1,vmwin204-27.fsct.nb -privileged-users
cifs\u1,cifs\u2
```

2. Verify that the scanner pool was created: `vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner-pool scanner_pool`

For a complete list of options, see the man page for the command.

The following command displays the details for the *SP* scanner pool:

```

cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner
-pool SP

                Vserver: vs1
                Scanner Pool: SP
                Applied Policy: idle
                Current Status: off
                Cluster on Which Policy Is Applied: -
                Scanner Pool Config Owner: vserver
                List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
                List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
                27.fsct.nb
                List of Privileged Users: cifs\u1, cifs\u2

```

You can also use the `vserver vscan scanner-pool show` command to view all of the scanner pools on an SVM. For complete command syntax, see the man page for the command.

= Create scanner pools in MetroCluster configurations

:icons: font

:relative\_path: ./antivirus/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You must create primary and secondary scanner pools on each cluster in a MetroCluster configuration, corresponding to the primary and secondary SVMs on the cluster.

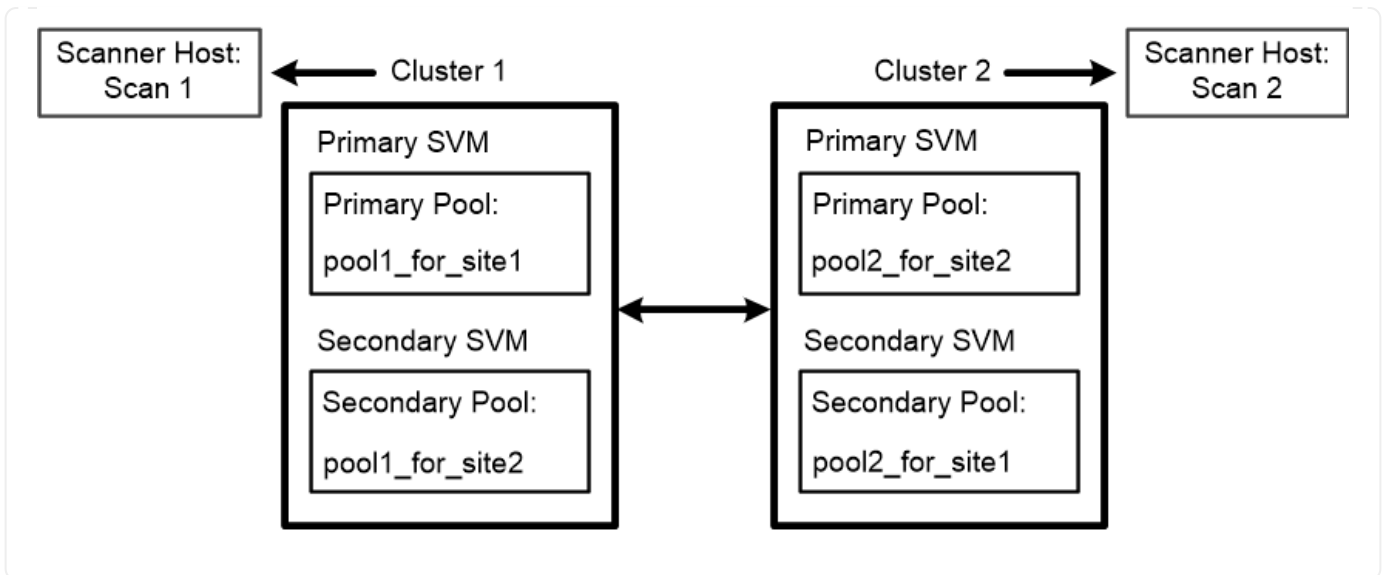
#### What you'll need

- SVMs and Vscan servers must be in the same domain or in trusted domains.
- For scanner pools defined for an individual SVM, you must have configured the ONTAP Antivirus Connector with the SVM management LIF or the SVM data LIF.
- For scanner pools defined for all of the SVMs in a cluster, you must have configured the ONTAP Antivirus Connector with the cluster management LIF.

#### About this task

MetroCluster configurations protect data by implementing two physically separate mirrored clusters. Each cluster synchronously replicates the data and SVM configuration of the other. A primary SVM on the local cluster serves data when the cluster is online. A secondary SVM on the local cluster serves data when the remote cluster is offline.

This means that you must create primary and secondary scanner pools on each cluster in a MetroCluster configuration, corresponding to the primary and secondary SVMs on the cluster. The secondary pool becomes active when the cluster begins serving data from the secondary SVM. The following illustration shows a typical MetroCluster configuration.



The list of privileged users must include the domain user account the Vscan server uses to connect to the SVM.

### Steps

1. Create a scanner pool:

```
vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM
-scanner-pool scanner_pool -hostnames Vscan_server_hostnames -privileged
-users privileged_users
```

- Specify a data SVM for a pool defined for an individual SVM, and specify a cluster admin SVM for a pool defined for all the SVMs in a cluster.
- Specify an IP address or FQDN for each Vscan server host name.
- Specify the domain and user name for each privileged user.

You must create all scanner pools from the cluster containing the primary SVM.

+

For a complete list of options, see the man page for the command.

+

The following commands create primary and secondary scanner pools on each cluster in a MetroCluster configuration:

+

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site1 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2
```

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site2 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2
```

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site1 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2
```

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site2 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2
```

1. Verify that the scanner pools were created: `vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner-pool scanner_pool`

For a complete list of options, see the man page for the command.

The following command displays the details for the scanner pool pool1:

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1
-scanner-pool pool1_for_site1
```

```

                                Vserver: cifssvm1
                                Scanner Pool: pool1_for_site1
                                Applied Policy: idle
                                Current Status: off
                                Cluster on Which Policy Is Applied: -
                                Scanner Pool Config Owner: vserver
                                List of IPs of Allowed Vscan Servers:
                                List of Host Names of Allowed Vscan Servers: scan1
                                List of Privileged Users: cifs\u1,cifs\u2
```

You can also use the `vserver vscan scanner-pool show` command to view all of the scanner pools on an SVM. For complete command syntax, see the man page for the command.

= Apply a scanner policy on a single cluster

:icons: font

:relative\_path: ./antivirus/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

A scanner policy determines whether a scanner pool is active. You must make a scanner pool active before the Vscan servers that are defined in the scanner pool can connect to an SVM.

### About this task

- You can apply only one scanner policy to a scanner pool.
- If you created a scanner pool for all of the SVMs in a cluster, you must apply a scanner policy on each SVM individually.
- For disaster recovery and MetroCluster configurations, you must apply a scanner policy to the scanner pools for the local cluster and partner cluster.

In the policy that you create for the local cluster, you must specify the local cluster in the `cluster` parameter. In the policy that you create for the partner cluster, you must specify the partner cluster in the `cluster` parameter. The partner cluster can then take over virus scanning operations in case of a disaster.

### Steps

1. Apply a scanner policy:

```
vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
scanner_pool -scanner-policy primary|secondary|idle -cluster
cluster_to_apply_policy_on
```

A scanner policy can have one of the following values:

- `Primary` specifies that the scanner pool is active.
- `Secondary` specifies that the scanner pool is active only if none of the Vscan servers in the primary scanner pool are connected.
- `Idle` specifies that the scanner pool is inactive.

The following example shows that the scanner pool named `SP` on the `vs1` SVM is active:

```
cluster1::> vserver vscan scanner-pool apply-policy -vserver vs1
-scanner-pool SP -scanner-policy primary
```

2. Verify that the scanner pool is active:

```
vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM
-scanner-pool scanner_pool
```

For a complete list of options, see the man page for the command.

The following command displays the details for the SP scanner pool:

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner
-pool SP

                Vserver: vs1
                Scanner Pool: SP
                Applied Policy: primary
                Current Status: on
                Cluster on Which Policy Is Applied: cluster1
                Scanner Pool Config Owner: vserver
                List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
                List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
                27.fsct.nb
                List of Privileged Users: cifs\u1, cifs\u2
```

You can use the `vserver vscan scanner-pool show-active` command to view the active scanner pools on an SVM. For the complete command syntax, see the man page for the command.

= Apply scanner policies in MetroCluster configurations

:icons: font

:relative\_path: ./antivirus/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

A scanner policy determines whether a scanner pool is active. You must apply a scanner policy to the primary and secondary scanner pools on each cluster in a MetroCluster configuration.

#### About this task

- You can apply only one scanner policy to a scanner pool.
- If you created a scanner pool for all of the SVMs in a cluster, you must apply a scanner policy on each SVM individually.

#### Steps

1. Apply a scanner policy:

```
vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
scanner_pool -scanner-policy primary|secondary|idle -cluster
cluster_to_apply_policy_on
```

A scanner policy can have one of the following values:

- `Primary` specifies that the scanner pool is active.
- `Secondary` specifies that the scanner pool is active only if none of the Vscan servers in the primary scanner pool is connected.
- `Idle` specifies that the scanner pool is inactive.

You must apply all scanner policies from the cluster containing the primary SVM.



+

The following commands apply scanner policies to the primary and secondary scanner pools on each cluster in a MetroCluster configuration:

+

```
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site1 -scanner-policy primary -cluster cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site1 -scanner-policy secondary -cluster
cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site2 -scanner-policy primary -cluster cluster2

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site2 -scanner-policy secondary -cluster
cluster2
```

#### 1. Verify that the scanner pool is active:

```
vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM
-scanner-pool scanner_pool
```

For a complete list of options, see the man page for the command.

The following command displays the details for the scanner pool pool1:

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1
-scanner-pool pool1_for_site1

                                Vserver: cifssvm1
                                Scanner Pool: pool1_for_site1
                                Applied Policy: primary
                                Current Status: on
                                Cluster on Which Policy Is Applied: cluster1
                                Scanner Pool Config Owner: vserver
                                List of IPs of Allowed Vscan Servers:
                                List of Host Names of Allowed Vscan Servers: scan1
                                List of Privileged Users: cifs\u1,cifs\u2
```

You can use the `vserver vscan scanner-pool show-active` command to view the active scanner pools on an SVM. For complete command syntax, see the man page for the command.

= Commands for managing scanner pools

:icons: font

:relative\_path: ./antivirus/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You can modify and delete scanner pools, and manage privileged users and Vscan servers for a scanner pool. You can view summary and details for a scanner pool.

If you want to...	Enter the following command...
Modify a scanner pool	<code>vserver vscan scanner-pool modify</code>
Delete a scanner pool	<code>vserver vscan scanner-pool delete</code>
Add privileged users to a scanner pool	<code>vserver vscan scanner-pool privileged-users add</code>
Delete privileged users from a scanner pool	<code>vserver vscan scanner-pool privileged-users remove</code>
Add Vscan servers to a scanner pool	<code>vserver vscan scanner-pool servers add</code>
Delete Vscan servers from a scanner pool	<code>vserver vscan scanner-pool servers remove</code>
View summary and details for a scanner pool	<code>vserver vscan scanner-pool show</code>
View privileged users for a scanner pool	<code>vserver vscan scanner-pool privileged-users show</code>
View Vscan servers for all scanner pools	<code>vserver vscan scanner-pool servers show</code>

For more information about these commands, see the man pages.

= Configure on-access scanning

= Create an on-access policy

:icons: font

:relative\_path: ./antivirus/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

An on-access policy defines the scope of an on-access scan. You can specify the maximum size of the files to be scanned, the extensions of the files to be included in the scan, and the extensions and paths of the files to be excluded from the scan. You can create an on-access policy for an individual SVM or for all the SVMs in a cluster.

**About this task**

By default, ONTAP creates an on-access policy named “default\_CIFS” and enables it for all the SVMs in a cluster.

You can set the `scan-mandatory` option to `off` to specify that file access is allowed when no Vscan servers are available for virus scanning. Keep in mind that any file that qualifies for scan exclusion based on the `paths-to-exclude`, `file-ext-to-exclude`, or `max-file-size` parameters is not considered for scanning even if the `scan-mandatory` option is set to `on`.

For potential issues related to the `scan-mandatory` option, see [Potential connectivity issues involving the scan-mandatory option](#).

By default, only read-write volumes are scanned. You can specify filters that enable scanning of read-only volumes or that restrict scanning to files opened with execute access.

## Steps

1. Create an on-access policy:

```
vserver vscan on-access-policy create -vserver data_SVM|cluster_admin_SVM
-policy-name policy_name -protocol CIFS -max-file-size
max_size_of_files_to_scan -filters [scan-ro-volume,][scan-execute-access]
-file-ext-to-include extensions_of_files_to_include -file-ext-to-exclude
extensions_of_files_to_exclude -scan-files-with-no-ext true|false -paths-to
-exclude paths_of_files_to_exclude -scan-mandatory on|off
```

- Specify a data SVM for a policy defined for an individual SVM, a cluster admin SVM for a policy defined for all the SVMs in a cluster.
- The `-file-ext-to-exclude` setting overrides the `-file-ext-to-include` setting.
- Set `-scan-files-with-no-ext` to true to scan files without extensions.

The following command creates an on-access policy named `Policy1` on the `vs1SVM`:

```
cluster1::> vserver vscan on-access-policy create -vserver vs1
-policy-name Policy1 -protocol CIFS -filters scan-ro-volume -max
-file-size 3GB -file-ext-to-include "mp*","tx*" -file-ext-to-exclude
"mp3","txt" -scan-files-with-no-ext false -paths-to-exclude "\vol\a
b\",""\vol\a,b\""
```

2. Verify that the on-access policy has been created: `vserver vscan on-access-policy show -instance data_SVM|cluster_admin_SVM -policy-name policy_name`

For a complete list of options, see the man page for the command.

The following command displays the details for the `Policy1` policy:

```
cluster1::> vserver vscan on-access-policy show -instance vs1
-policy-name Policy1
```

```
                Vserver: vs1
                Policy: Policy1
                Policy Status: off
                Policy Config Owner: vserver
                File-Access Protocol: CIFS
                Filters: scan-ro-volume
                Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
                File Paths Not to Scan: \vol\a b\, \vol\a,b\
                File Extensions Not to Scan: mp3, txt
                File Extensions to Scan: mp*, tx*
                Scan Files with No Extension: false
```

= Enable an on-access policy

:icons: font

:relative\_path: ./antivirus/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You must enable an on-access policy on an SVM before its files can be scanned. If you created an on-access policy for all the SVMs in a cluster, you must enable the policy on each SVM individually. You can enable only one on-access policy on an SVM at a time.

### Steps

1. Enable an on-access policy:

```
vserver vscan on-access-policy enable -vserver data_SVM -policy-name
policy_name
```

The following command enables an on-access policy named `Policy1` on the `vs1` SVM:

```
cluster1::> vserver vscan on-access-policy enable -vserver vs1
-policy-name Policy1
```

2. Verify that the on-access policy is enabled: `vserver vscan on-access-policy show -instance data_SVM -policy-name policy_name`

For a complete list of options, see the man page for the command.

The following command displays the details for the `Policy1` on-access policy:

```
cluster1::> vserver vscan on-access-policy show -instance vs1
-policy-name Policy1
```

```
                Vserver: vs1
                Policy: Policy1
                Policy Status: on
                Policy Config Owner: vserver
                File-Access Protocol: CIFS
                Filters: scan-ro-volume
                Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
                File Paths Not to Scan: \vol\a b\, \vol\a,b\
                File Extensions Not to Scan: mp3, txt
                File Extensions to Scan: mp*, tx*
                Scan Files with No Extension: false
```

= Modify the Vscan file-operations profile for an SMB share

:icons: font

:relative\_path: ./antivirus/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

The Vscan file-operations profile for an SMB share defines which operations on the share can trigger scanning. By default, the parameter is set to `standard`. You can adjust the parameter as necessary when you create or modify an SMB share.

#### About this task

For more information on the available values for a Vscan file-operations profile, see “Vscan file-operations profile.”

[Vscan file-operations profile \(on-access scanning only\)](#)

Virus scanning is not performed on a SMB share for which the `continuously-available` parameter is set to `Yes`.

## Step

1. Modify the value of the Vscan file-operations profile for a SMB share: `vserver cifs share modify -vserver data_SVM -share-name share -path share_path -vscan-fileop-profile no-scan|standard|strict|writes-only`

For a complete list of options, see the man page for the command.

The following command changes the Vscan file operations profile for a SMB share to `strict`:

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name
SALES_SHARE -path /sales -vscan-fileop-profile strict
```

= Commands for managing on-access policies

:icons: font

:relative\_path: ./antivirus/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You can modify, disable, or delete an on-access policy. You can view a summary and details for the policy.

If you want to...	Enter the following command...
Modify an on-access policy	<code>vserver vscan on-access-policy modify</code>
Disable an on-access policy	<code>vserver vscan on-access-policy disable</code>
Delete an on-access policy	<code>vserver vscan on-access-policy delete</code>
View summary and details for an on-access policy	<code>vserver vscan on-access-policy show</code>
Add to the list of paths to exclude	<code>vscan on-access-policy paths-to-exclude add</code>
Delete from the list of paths to exclude	<code>vscan on-access-policy paths-to-exclude remove</code>
View the list of paths to exclude	<code>vscan on-access-policy paths-to-exclude show</code>
Add to the list of file extensions to exclude	<code>vscan on-access-policy file-ext-to-exclude add</code>
Delete from the list of file extensions to exclude	<code>vscan on-access-policy file-ext-to-exclude remove</code>

View the list of file extensions to exclude	<code>vscan on-access-policy file-ext-to-exclude show</code>
Add to the list of file extensions to include	<code>vscan on-access-policy file-ext-to-include add</code>
Delete from the list of file extensions to include	<code>vscan on-access-policy file-ext-to-include remove</code>
View the list of file extensions to include	<code>vscan on-access-policy file-ext-to-include show</code>

For more information about these commands, see the man pages.

= Configure on-demand scanning

= Configure on-demand scanning overview

:icons: font

:relative\_path: ./antivirus/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You can use on-demand scanning to check files for viruses immediately or on a schedule. You might want to run scans only in off-peak hours, for example, or you might want to scan very large files that were excluded from an on-access scan.

You can use a cron schedule to specify when the task runs:

- You can assign a schedule when you create a task.
- You can create a task without assigning a schedule, and use the `vserver vscan on-demand-task schedule` command to assign a schedule.
- You can use the `vserver vscan on-demand-task run` command to run a task immediately, whether or not you have assigned a schedule.

Only one task can be scheduled at a time on an SVM.

On-demand scanning does not support scanning of symbolic links or stream files.



= Create an on-demand task

:icons: font

:relative\_path: ./antivirus/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

An on-demand task defines the scope of an on-demand scan. You can specify the maximum size of the files to be scanned, the extensions and paths of the files to be included in the scan, and the extensions and paths of the files to be excluded from the scan. Files in subdirectories are scanned by default.

### Steps

1. Create an on-demand task:

```
vserver vscan on-demand-task create -vserver data_SVM -task-name task_name
-scan-paths paths_of_files_to_scan -report-directory report_directory_path
-report-expiry-time expiration_time_for_report -schedule cron_schedule -max
-file-size max_size_of_files_to_scan -paths-to-exclude
paths_of_files_to_exclude -file-ext-to-exclude
extensions_of_files_to_exclude -file-ext-to-include
extensions_of_files_to_include -scan-files-with-no-ext true|false
-directory-recursion true|false
```

- The `-file-ext-to-exclude` setting overrides the `-file-ext-to-include` setting.
- Set `-scan-files-with-no-ext` to `true` to scan files without extensions.  
For a complete list of options, see the man page for the command.

The following command creates an on-access task named `Task1` on the `vs1SVM`:

```
cluster1::> vserver vscan on-demand-task create -vserver vs1 -task
-name Task1 -scan-paths "/vol1/", "/vol2/cifs/" -report-directory
"/report" -schedule daily -max-file-size 5GB -paths-to-exclude
"/vol1/cold-files/" -file-ext-to-include "vmdk?", "mp*" -file-ext-to
-exclude "mp3", "mp4" -scan-files-with-no-ext false
[Job 126]: Vscan On-Demand job is queued. Use the "job show -id 126"
command to view the status.
```

You can use the `job show` command to view the status of the job. You can use the `job pause` and `job resume` commands to pause and restart the job, or the `job stop` command to end the job.

1. Verify that the on-demand task has been created: `vserver vscan on-demand-task show -instance data_SVM -task-name task_name`

For a complete list of options, see the man page for the command.

The following command displays the details for the Task1 task:

```
cluster1::> vserver vscan on-demand-task show -instance vs1 -task
-name Task1
```

```

                Vserver: vs1
                Task Name: Task1
                List of Scan Paths: /vol1/, /vol2/cifs/
                Report Directory Path: /report
                Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
                File Paths Not to Scan: /vol1/cold-files/
                File Extensions Not to Scan: mp3, mp4
                File Extensions to Scan: vmdk?, mp*
                Scan Files with No Extension: false
                Request Service Timeout: 5m
                Cross Junction: true
                Directory Recursion: true
                Scan Priority: low
                Report Log Level: info
                Expiration Time for Report: -
```

### After you finish

You must enable scanning on the SVM before the task is scheduled to run.

= Schedule an on-demand task

:icons: font

:relative\_path: ./antivirus/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

If you have created an on-demand task without assigning a schedule, or if you want to assign a different schedule to a task, you can use the `vserver vscan on-demand-task schedule` command to assign a schedule to the task.

### About this task

The schedule assigned with the `vserver vscan on-demand-task schedule` command overrides a schedule already assigned with the `vserver vscan on-demand-task create` command.

### Steps

1. Schedule an on-demand task:

```
vserver vscan on-demand-task schedule -vserver data_SVM -task-name  
task_name -schedule cron_schedule
```

The following command schedules an on-access task named Task2 on the vs2SVM:

```
cluster1::> vserver vscan on-demand-task schedule -vserver vs2 -task  
-name Task2 -schedule daily  
[Job 142]: Vscan On-Demand job is queued. Use the "job show -id 142"  
command to view the status.
```

You can use the `job show` command to view the status of the job. You can use the `job pause` and `job resume` commands to pause and restart the job, or the `job stop` command to end the job.

1. Verify that the on-demand task has been scheduled: `vserver vscan on-demand-task show -instance data_SVM -task-name task_name`

For a complete list of options, see the man page for the command.

The following command displays the details for the Task 2 task:

```
cluster1::> vserver vscan on-demand-task show -instance vs2 -task
-name Task2
```

```

                Vserver: vs2
                Task Name: Task2
                List of Scan Paths: /vol1/, /vol2/cifs/
                Report Directory Path: /report
                Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
                File Paths Not to Scan: /vol1/cold-files/
                File Extensions Not to Scan: mp3, mp4
                File Extensions to Scan: vmdk, mp*
Scan Files with No Extension: false
                Request Service Timeout: 5m
                Cross Junction: true
                Directory Recursion: true
                Scan Priority: low
                Report Log Level: info
```

### After you finish

You must enable scanning on the SVM before the task is scheduled to run.

= Run an on-demand task immediately

:icons: font

:relative\_path: ./antivirus/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You can run an on-demand task immediately, whether or not you have assigned a schedule.

### What you'll need

You must have enabled scanning on the SVM.

### Step

1. Run an on-demand task immediately:

```
vserver vscan on-demand-task run -vserver data_SVM -task-name task_name
```

The following command runs an on-access task named Task1 on the vs1SVM:

```
cluster1::> vserver vscan on-demand-task run -vserver vs1 -task-name
Task1
[Job 161]: Vscan On-Demand job is queued. Use the "job show -id 161"
command to view the status.
```

You can use the `job show` command to view the status of the job. You can use the `job pause` and `job resume` commands to pause and restart the job, or the `job stop` command to end the job.

= Commands for managing on-demand tasks

:icons: font

:relative\_path: ./antivirus/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You can modify, delete, or unschedule an on-demand task. You can view a summary and details for the task, and manage reports for the task.

If you want to...	Enter the following command...
Modify an on-demand task	<code>vserver vscan on-demand-task modify</code>
Delete an on-demand task	<code>vserver vscan on-demand-task delete</code>
Unschedule an on-demand task	<code>vserver vscan on-demand-task unschedule</code>
View summary and details for an on-demand task	<code>vserver vscan on-demand-task show</code>
View on-demand reports	<code>vserver vscan on-demand-task report show</code>
Delete on-demand reports	<code>vserver vscan on-demand-task report delete</code>

For more information about these commands, see the man pages.

= Enable virus scanning on an SVM

:icons: font

:relative\_path: ./antivirus/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You must enable virus scanning on an SVM before an on-access or on-demand scan can run. The Vscan configuration must exist.

### Steps

1. Enable virus scanning on an SVM:

```
vserver vscan enable -vserver data_SVM
```

You can use the `vserver vscan disable` command to disable virus scanning if necessary.

+

The following command enables virus scanning on the vs1SVM:

+

```
cluster1::> vserver vscan enable -vserver vs1
```

1. Verify that virus scanning is enabled on the SVM:

```
vserver vscan show -vserver data_SVM
```

For a complete list of options, see the man page for the command.

The following command displays the Vscan status of the vs1SVM:

```
cluster1::> vserver vscan show -vserver vs1
```

```
          Vserver: vs1
          Vscan Status: on
```

= Reset the status of scanned files

:icons: font

:relative\_path: ./antivirus/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

Occasionally, you might want to reset the scan status of successfully scanned files on an SVM by using the `vserver vscan reset` command to discard the cached information for the files. You might want to use this command to restart the virus scanning processing in case of a misconfigured scan, for example.

#### **About this task**

After you run the `vserver vscan reset` command, all eligible files will be scanned the next time they are accessed.

This command can affect performance adversely, depending on the number and size of the files to be rescanned.

## Step

1. Reset the status of scanned files:

```
vserver vscan reset -vserver data_SVM
```

The following command resets the status of scanned files on the vs1SVM:

```
cluster1::> vserver vscan reset -vserver vs1
```

= View Vscan event log information

:icons: font

:relative\_path: ./antivirus/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You can use the `vserver vscan show-events` command to view event log information about infected files, updates to Vscan servers, and the like. You can view event information for the cluster or for given nodes, SVMs, or Vscan servers.

## What you'll need

Advanced privileges are required for this task.

## Steps

1. Change to advanced privilege level:

```
set -privilege advanced
```

2. View Vscan event log information:

```
vserver vscan show-events
```

For a complete list of options, see the man page for the command.

The following command displays event log information for the cluster `cluster1`:



```
cluster1::*> vserver vscan show-events
```

Vserver Time	Node	Server	Event Type	Event
vs1 9/5/2014 11:37:38	Cluster-01	192.168.1.1	file-infected	
vs1 9/5/2014 11:37:08	Cluster-01	192.168.1.1	scanner-updated	
vs1 9/5/2014 11:34:55	Cluster-01	192.168.1.1	scanner-connected	

3 entries were displayed.

= Troubleshoot connectivity issues

= Potential connectivity issues involving the scan-mandatory option

:icons: font

:relative\_path: ./antivirus/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You can use the `vserver vscan connection-status show` commands to view information about Vscan server connections that you might find helpful in troubleshooting connectivity issues.

By default, the `scan-mandatory` option for on-access scanning denies file access when a Vscan server connection is not available for scanning. Although this option offers important safety features, it can lead to problems in a few situations.

- Before enabling client access, you must ensure that at least one Vscan server is connected to an SVM on each node that has a LIF. If you need to connect servers to SVMs after enabling client access, you must turn off the `scan-mandatory` option on the SVM to ensure that file access is not denied because a Vscan server connection is not available. You can turn the option back on after the server has been connected.
- If a target LIF hosts all the Vscan server connections for an SVM, the connection between the server and the SVM will be lost if the LIF is migrated. To ensure that file access is not denied because a Vscan server connection is not available, you must turn off the `scan-mandatory` option before migrating the LIF. You can turn the option back on after the LIF has been migrated.

Each SVM should have at least two Vscan servers assigned to it. It is a best practice to connect Vscan servers to the storage system over a different network from the one used for client access.

= Commands for viewing Vscan server connection status

:icons: font

:relative\_path: ./antivirus/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You can use the `vserver vscan connection-status show` commands to view

summary and detailed information about Vscan server connection status.

If you want to...	Enter the following command...
View a summary of Vscan server connections	<code>vserver vscan connection-status show</code>
View details for Vscan server connections	<code>vserver vscan connection-status show-all</code>
View details for connected Vscan servers	<code>vserver vscan connection-status show-connected</code>
View details for available Vscan servers that are not connected	<code>vserver vscan connection-status show-not-connected</code>

For more information about these commands, see the man pages.

= NAS auditing and security tracing

= SMB and NFS auditing and security tracing overview

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You can use the file access auditing features available for the SMB and NFS protocols with ONTAP, such as native auditing and file policy management using FPolicy.

You should design and implement auditing of SMB and NFS file access events under the following circumstances:

- Basic SMB and NFS protocol file access has been configured.
- You want to create and maintain an auditing configuration using one of the following methods:
  - Native ONTAP functionality
  - External FPolicy servers

= Audit NAS events on SVMs

= Audit NAS events on SVMs overview

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

Auditing for NAS events is a security measure that enables you to track and log certain SMB and NFS events on storage virtual machines (SVMs). This helps you track potential security problems and provides evidence of any security breaches. You can also stage and audit Active Directory central access policies to see what the result of implementing them would be.

## == SMB events

You can audit the following events:

- SMB file and folder access events

You can audit SMB file and folder access events on objects stored on FlexVol volumes belonging to the auditing-enabled SVMs.

- SMB logon and logoff events

You can audit SMB logon and logoff events for SMB servers on SVMs.

- Central access policy staging events

You can audit the effective access of objects on SMB servers using permissions applied through proposed central access policies. Auditing through the staging of central access policies enables you to see what the effects are of central access policies before they are deployed.

Auditing of central access policy staging is set up using Active Directory GPOs; however, the SVM auditing configuration must be configured to audit central access policy staging events.

Although you can enable central access policy staging in the auditing configuration without enabling Dynamic Access Control on the SMB server, central access policy staging events are generated only if Dynamic Access Control is enabled. Dynamic Access Control is enabled through a SMB server option. It is not enabled by default.

## == NFS events

You can audit file and directory NFSv4 access events on objects stored on SVMs.

### = How auditing works

#### = Basic auditing concepts

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

To understand auditing in ONTAP, you should be aware of some basic auditing concepts.

- **Staging files**

The intermediate binary files on individual nodes where audit records are stored prior to consolidation and conversion. Staging files are contained in staging volumes.

- **Staging volume**

A dedicated volume created by ONTAP to store staging files. There is one staging volume per aggregate. Staging volumes are shared by all audit-enabled storage virtual machines (SVMs) to store audit records of data access for data volumes in that particular aggregate. Each SVM's audit records are stored in a separate directory within the staging volume.

Cluster administrators can view information about staging volumes, but most other volume operations are not permitted. Only ONTAP can create staging volumes. ONTAP automatically assigns a name to

staging volumes. All staging volume names begin with `MDV_aud_` followed by the UUID of the aggregate containing that staging volume (for example: `MDV_aud_1d0131843d4811e296fc123478563412.`)

- **System volumes**

A FlexVol volume that contains special metadata, such as metadata for file services audit logs. The admin SVM owns system volumes, which are visible across the cluster. Staging volumes are a type of system volume.

- **Consolidation task**

A task that gets created when auditing is enabled. This long-running task on each SVM takes the audit records from staging files across the member nodes of the SVM. This task merges the audit records in sorted chronological order, and then converts them to a user-readable event log format specified in the auditing configuration—either the EVT<sub>X</sub> or XML file format. The converted event logs are stored in the audit event log directory that is specified in the SVM auditing configuration.

= How the ONTAP auditing process works

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

The ONTAP auditing process is different from the Microsoft auditing process. Before you configure auditing, you should understand how the ONTAP auditing process works.

Audit records are initially stored in binary staging files on individual nodes. If auditing is enabled on an SVM, every member node maintains staging files for that SVM. Periodically, they are consolidated and converted to user-readable event logs, which are stored in the audit event log directory for the SVM.

== Process when auditing is enabled on an SVM

Auditing can only be enabled on SVMs. When the storage administrator enables auditing on the SVM, the auditing subsystem checks whether staging volumes are present. A staging volume must exist for each aggregate that contains data volumes owned by the SVM. The auditing subsystem creates any needed staging volumes if they do not exist.

The auditing subsystem also completes other prerequisite tasks before auditing is enabled:

- The auditing subsystem verifies that the log directory path is available and does not contain symlinks.

The log directory must already exist as a path within the SVM's namespace. It is recommended to create a new volume or qtree to hold the audit log files. The auditing subsystem does not assign a default log file location. If the log directory path specified in the auditing configuration is not a valid path, auditing configuration creation fails with the error `The specified path "/path" does not exist in the namespace belonging to Vserver "Vserver_name" error.`

Configuration creation fails if the directory exists but contains symlinks.

- Auditing schedules the consolidation task.

After this task is scheduled, auditing is enabled. The SVM auditing configuration and the log files persist across a reboot or if the NFS or SMB servers are stopped or restarted.

#### == Event log consolidation

Log consolidation is a scheduled task that runs on a routine basis until auditing is disabled. When auditing is disabled, the consolidation task verifies that all of the remaining logs are consolidated.

#### == Guaranteed auditing

By default, auditing is guaranteed. ONTAP guarantees that all auditable file access events (as specified by configured audit policy ACLs) are recorded, even if a node is unavailable. A requested file operation cannot be completed until the audit record for that operation is saved to the staging volume on persistent storage. If audit records cannot be committed to the disk in the staging files, either because of insufficient space or because of other issues, client operations are denied.

An administrator, or account user with privilege level access, can bypass the file audit logging operation by using NetApp Manageability SDK or REST APIs. You can determine if any file actions have been taken using NetApp Manageability SDK or REST APIs by reviewing the command history logs stored in the `audit.log` file.

For more information about command history audit logs, see the "Managing audit logging for management activities" section in [System administration](#).

## == Consolidation process when a node is unavailable

If a node containing volumes belonging to an SVM with auditing enabled is unavailable, the behavior of the auditing consolidation task depends on whether the node's storage failover (SFO) partner (or the HA partner in the case of a two-node cluster) is available:

- If the staging volume is available through the SFO partner, the staging volumes last reported from the node are scanned, and consolidation proceeds normally.
- If the SFO partner is not available, the task creates a partial log file.

When a node is not reachable, the consolidation task consolidates the audit records from the other available nodes of that SVM. To identify that it is not complete, the task adds the suffix `.partial` to the consolidated file name.

- After the unavailable node is available, the audit records in that node are consolidated with the audit records from the other nodes at that time.
- All audit records are preserved.

## == Event log rotation

Audit event log files are rotated when they reach a configured threshold log size or on a configured schedule. When an event log file is rotated, the scheduled consolidation task first renames the active converted file to a time-stamped archive file, and then creates a new active converted event log file.

## == Process when auditing is disabled on the SVM

When auditing is disabled on the SVM, the consolidation task is triggered one final time. All outstanding, recorded audit records are logged in a user-readable format. Existing event logs stored in the event log directory are not deleted when auditing is disabled on the SVM and are available for viewing.

After all existing staging files for that SVM are consolidated, the consolidation task is removed from the schedule. Disabling the auditing configuration for the SVM does not remove the auditing configuration. A storage administrator can reenabling auditing at any time.

The auditing consolidation job, which gets created when auditing is enabled, monitors the consolidation task and re-creates it if the consolidation task exits because of an error. Previously, users could delete the auditing consolidation job by using job manager commands such as `job delete`. Users are no longer allowed to delete the auditing consolidation job.

## = Auditing requirements and considerations

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

Before you configure and enable auditing on your storage virtual machine (SVM), you need to be aware of certain requirements and considerations.

- The maximum number of auditing-enabled SVMs supported in a cluster is 50.
- Auditing is not tied to SMB or NFS licensing.

You can configure and enable auditing even if SMB and NFS licenses are not installed on the cluster.

- NFS auditing supports security ACEs (type U).
- For NFS auditing, there is no mapping between mode bits and auditing ACEs.

When converting ACLs to mode bits, auditing ACEs are skipped. When converting mode bits to ACLs, auditing ACEs are not generated.

- The directory specified in the auditing configuration must exist.

If it does not exist, the command to create the auditing configuration fails.

- The directory specified in the auditing configuration must meet the following requirements:
  - The directory must not contain symbolic links.

If the directory specified in the auditing configuration contains symbolic links, the command to create the auditing configuration fails.

- You must specify the directory by using an absolute path.

You should not specify a relative path, for example, `/vs1/././`.

- Auditing is dependent on having available space in the staging volumes.

You must be aware of and have a plan for ensuring that there is sufficient space for the staging volumes in aggregates that contain audited volumes.

- Auditing is dependent on having available space in the volume containing the directory where converted event logs are stored.

You must be aware of and have a plan for ensuring that there is sufficient space in the volumes used to store event logs. You can specify the number of event logs to retain in the auditing directory by using the `-rotate-limit` parameter when creating an auditing configuration, which can help to ensure that there is enough available space for the event logs in the volume.

- Although you can enable central access policy staging in the auditing configuration without enabling Dynamic Access Control on the SMB server, Dynamic Access Control must be enabled to generate central access policy staging events.

Dynamic Access Control is not enabled by default.

#### == Aggregate space considerations when enabling auditing

When an auditing configuration is created and auditing is enabled on at least one storage virtual machine (SVM) in the cluster, the auditing subsystem creates staging volumes on all existing aggregates and on all new aggregates that are created. You need to be aware of certain aggregate space considerations when you enable auditing on the cluster.

Staging volume creation might fail due to non-availability of space in an aggregate. This might happen if you create an auditing configuration and existing aggregates do not have enough space to contain the staging volume.

You should ensure that there is enough space on existing aggregates for the staging volumes before enabling auditing on an SVM.

#### = Limitations for the size of audit records on staging files

```
:icons: font
:relative_path: ./nas-audit/
:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/
```

The size of an audit record on a staging file cannot be greater than 32 KB.

== When large audit records can occur

Large audit records might occur during management auditing in one of the following scenarios:

- Adding or deleting users to or from groups with a large number of users.
- Adding or deleting a file-share access control list (ACL) on a file-share with a large number of file-share users.
- Other scenarios.

Disable management auditing to avoid this issue. To do this, modify the audit configuration and remove the following from the list of audit event types:

- file-share
- user-account
- security-group
- authorization-policy-change

After removal, they will not be audited by the file services auditing subsystem.

== The effects of audit records that are too large

- If the size of an audit record is too large (over 32 KB), the audit record is not created and the auditing subsystem generates an event management system (EMS) message similar to the following:

```
File Services Auditing subsystem failed the operation or truncated an audit
record because it was greater than max_audit_record_size value. Vserver
UUID=%s, event_id=%u, size=%u
```

If auditing is guaranteed, the file operation fails because its audit record cannot be created.

- If the size of the audit record is more than 9,999 bytes, the same EMS message as above is displayed. A partial audit record is created with the larger key value missing.
- If the audit record exceeds 2,000 characters, the following error message shows instead of the actual value:

```
The value of this field was too long to display.
```

= What the supported audit event log formats are

```
:icons: font
:relative_path: ./nas-audit/
:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/
```

Supported file formats for the converted audit event logs are `EVTX` and `XML` file formats.



You can specify the type of file format when you create the auditing configuration. By default, ONTAP converts the binary logs to the `EVTX` file format.

= View audit event logs

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You can use audit event logs to determine whether you have adequate file security and whether there have been improper file and folder access attempts. You can view and process audit event logs saved in the `EVTX` or `XML` file formats.

- `EVTX` file format

You can open the converted `EVTX` audit event logs as saved files using Microsoft Event Viewer.

There are two options that you can use when viewing event logs using Event Viewer:

- General view

Information that is common to all events is displayed for the event record. In this version of ONTAP, the event-specific data for the event record is not displayed. You can use the detailed view to display event-specific data.

- Detailed view

A friendly view and an XML view are available. The friendly view and the XML view display both the information that is common to all events and the event-specific data for the event record.

- `XML` file format

You can view and process `XML` audit event logs on third-party applications that support the `XML` file format. `XML` viewing tools can be used to view the audit logs provided you have the `XML` schema and information about definitions for the `XML` fields. For more information about the `XML` schema and definitions, see the [ONTAP Auditing Schema Reference](#).

== How active audit logs are viewed using Event Viewer

If the audit consolidation process is running on the cluster, the consolidation process appends new records to the active audit log file for audit-enabled storage virtual machines (SVMs). This active audit log can be accessed and opened over an SMB share in Microsoft Event Viewer.

In addition to viewing existing audit records, Event Viewer has a refresh option that enables you to refresh the content in the console window. Whether the newly appended logs are viewable in Event Viewer depends on whether oplocks are enabled on the share used to access the active audit log.

Oplocks setting on the share	Behavior
Enabled	Event Viewer opens the log that contains events written to it up to that point in time. The refresh operation does not refresh the log with new events appended by the consolidation process.

Disabled	Event Viewer opens the log that contains events written to it up to that point in time. The refresh operation refreshes the log with new events appended by the consolidation process.
----------	--

This information is applicable only for `EVTX` event logs. `XML` event logs can be viewed through `SMB` in a browser or through `NFS` using any `XML` editor or viewer.

= SMB events that can be audited

= SMB events that can be audited overview

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

ONTAP can audit certain SMB events, including certain file and folder access events, certain logon and logoff events, and central access policy staging events. Knowing which access events can be audited is helpful when interpreting results from the event logs.

The following additional SMB events can be audited in ONTAP 9.2 and later:

Event ID (EVT/EVTX)	Event	Description	Category
4670	Object permissions were changed	OBJECT ACCESS: Permissions changed.	File Access
4907	Object auditing settings were changed	OBJECT ACCESS: Audit settings changed.	File Access
4913	Object Central Access Policy was changed	OBJECT ACCESS: CAP changed.	File Access

The following SMB events can be audited in ONTAP 9.0 and later:

Event ID (EVT/EVTX)	Event	Description	Category
540/4624	An account was successfully logged on	LOGON/LOGOFF: Network (SMB) logon.	Logon and Logoff
529/4625	An account failed to log on	LOGON/LOGOFF: Unknown user name or bad password.	Logon and Logoff
530/4625	An account failed to log on	LOGON/LOGOFF: Account logon time restriction.	Logon and Logoff
531/4625	An account failed to log on	LOGON/LOGOFF: Account currently disabled.	Logon and Logoff
532/4625	An account failed to log on	LOGON/LOGOFF: User account has expired.	Logon and Logoff
533/4625	An account failed to log on	LOGON/LOGOFF: User cannot log on to this computer.	Logon and Logoff

534/4625	An account failed to log on	LOGON/LOGOFF: User not granted logon type here.	Logon and Logoff
535/4625	An account failed to log on	LOGON/LOGOFF: User's password has expired.	Logon and Logoff
537/4625	An account failed to log on	LOGON/LOGOFF: Logon failed for reasons other than above.	Logon and Logoff
539/4625	An account failed to log on	LOGON/LOGOFF: Account locked out.	Logon and Logoff
538/4634	An account was logged off	LOGON/LOGOFF: Local or network user logoff.	Logon and Logoff
560/4656	Open Object/Create Object	OBJECT ACCESS: Object (file or directory) open.	File Access
563/4659	Open Object with the Intent to Delete	OBJECT ACCESS: A handle to an object (file or directory) was requested with the Intent to Delete.	File Access
564/4660	Delete Object	OBJECT ACCESS: Delete Object (file or directory). ONTAP generates this event when a Windows client attempts to delete the object (file or directory).	File Access
567/4663	Read Object/Write Object/Get Object Attributes/Set Object Attributes	OBJECT ACCESS: Object access attempt (read, write, get attribute, set attribute).  <b>Note:</b> For this event, ONTAP audits only the first SMB read and first SMB write operation (success or failure) on an object. This prevents ONTAP from creating excessive log entries when a single client opens an object and performs many successive read or write operations to the same object.	File Access
NA/4664	Hard link	OBJECT ACCESS: An attempt was made to create a hard link.	File Access

NA/4818	Proposed central access policy does not grant the same access permissions as the current central access policy	OBJECT ACCESS: Central Access Policy Staging.	File Access
NA/NA Data ONTAP Event ID 9999	Rename Object	OBJECT ACCESS: Object renamed. This is an ONTAP event. It is not currently supported by Windows as a single event.	File Access
NA/NA Data ONTAP Event ID 9998	Unlink Object	OBJECT ACCESS: Object unlinked. This is an ONTAP event. It is not currently supported by Windows as a single event.	File Access

== Additional information about Event 4656

The `HandleID` tag in the audit XML event contains the handle of the object (file or directory) accessed. The `HandleID` tag for the EVTX 4656 event contains different information depending on whether the open event is for creating a new object or for opening an existing object:

- If the open event is an open request to create a new object (file or directory), the `HandleID` tag in the audit XML event shows an empty `HandleID` (for example: `<Data Name="HandleID">0000000000000000;00;00000000;00000000</Data>` ).

The `HandleID` is empty because the OPEN (for creating a new object) request gets audited before the actual object creation happens and before a handle exists. Subsequent audited events for the same object have the right object handle in the `HandleID` tag.

- If the open event is an open request to open an existing object, the audit event will have the assigned handle of that object in the `HandleID` tag (for example: `<Data Name="HandleID">000000000000401;00;000000ea;00123ed4</Data>` ).

= Determine what the complete path to the audited object is

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

The object path printed in the `<ObjectName>` tag for an audit record contains the name of the volume (in parentheses) and the relative path from the root of the containing volume. If you want to determine the complete path of the audited object, including the junction path, there are certain steps you must take.

### Steps

1. Determine what the volume name and relative path to audited object is by looking at the `<ObjectName>` tag in the audit event.

In this example, the volume name is "data1" and the relative path to the file is `/dir1/file.txt`:

```
<Data Name="ObjectName"> (data1);/dir1/file.txt </Data>
```

- Using the volume name determined in the previous step, determine what the junction path is for the volume containing the audited object:

In this example, the volume name is "data1" and the junction path for the volume containing the audited object is /data/data1:

```
volume show -junction -volume data1
```

Vserver Source	Volume	Language	Junction Active	Junction Path	Junction Path
vs1	data1	en_US.UTF-8	true	/data/data1	
RW_volume					

- Determine the full path to the audited object by appending the relative path found in the <ObjectName> tag to the junction path for the volume.

In this example, the junction path for the volume:

```
/data/data1/dir1/file.txt
```

= Considerations when auditing symlinks and hard links

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

There are certain considerations you must keep in mind when auditing symlinks and hard links.

An audit record contains information about the object being audited including the path to the audited object, which is identified in the `ObjectName` tag. You should be aware of how paths for symlinks and hard links are recorded in the `ObjectName` tag.

== Symlinks

A symlink is a file with a separate inode that contains a pointer to the location of a destination object, known as the target. When accessing an object through a symlink, ONTAP automatically interprets the symlink and follows the actual canonical protocol agnostic path to the target object in the volume.

In the following example output, there are two symlinks, both pointing to a file named `target.txt`. One of the symlinks is a relative symlink and one is an absolute symlink. If either of the symlinks are audited, the `ObjectName` tag in the audit event contains the path to the file `target.txt`:

```
[root@host1 audit]# ls -l
total 0
lrwxrwxrwx 1 user1 group1 37 Apr  2 10:09 softlink_fullpath.txt ->
/data/audit/target.txt
lrwxrwxrwx 1 user1 group1 10 Apr  2 09:54 softlink.txt -> target.txt
-rwxrwxrwx 1 user1 group1 16 Apr  2 10:05 target.txt
```

## == Hard links

A hard link is a directory entry that associates a name with an existing file on a file system. The hard link points to the inode location of the original file. Similar to how ONTAP interprets symlinks, ONTAP interprets the hard link and follows the actual canonical path to the target object in the volume. When access to a hard link object is audited, the audit event records this absolute canonical path in the `ObjectName` tag rather than the hard link path.

= Considerations when auditing alternate NTFS data streams

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

There are certain considerations you must keep in mind when auditing files with NTFS alternate data streams.

The location of an object being audited is recorded in an event record using two tags, the `ObjectName` tag (the path) and the `HandleID` tag (the handle). To properly identify which stream requests are being logged, you must be aware of what ONTAP records in these fields for NTFS alternate data streams:

- EVTX ID: 4656 events (open and create audit events)
  - The path of the alternate data stream is recorded in the `ObjectName` tag.
  - The handle of the alternate data stream is recorded in the `HandleID` tag.
- EVTX ID: 4663 events (all other audit events, such as read, write, getattr, and so on)
  - The path of the base file, not the alternate data stream, is recorded in the `ObjectName` tag.
  - The handle of the alternate data stream is recorded in the `HandleID` tag.

## Example

The following example illustrates how to identify EVTX ID: 4663 events for alternate data streams using the `HandleID` tag. Even though the `ObjectName` tag (path) recorded in the read audit event is to the base file path, the `HandleID` tag can be used to identify the event as an audit record for the alternate data stream.

Stream file names take the form `base_file_name:stream_name`. In this example, the `dir1` directory contains a base file with an alternate data stream having the following paths:

```
/dir1/file1.txt
/dir1/file1.txt:stream1
```

The output in the following event example is truncated as indicated; the output does not display all of the available output tags for the events.



For an EVTX ID 4656 (open audit event), the audit record output for the alternate data stream records the alternate data stream name in the `ObjectName` tag:

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4656</EventID>
  <EventName>Open Object</EventName>
  [...]
</System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt:stream1</Data\>
  **
  [...]
</EventData>
</Event>
- <Event>
```

For an EVTX ID 4663 (read audit event), the audit record output for the same alternate data stream records the base file name in the `ObjectName` tag; however, the handle in the `HandleID` tag is the alternative data stream's handle and can be used to correlate this event with the alternative data stream:

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4663</EventID>
  <EventName>Read Object</EventName>
  [...]
</System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt</Data\> **
  [...]
</EventData>
</Event>
- <Event>
```

= NFS file and directory access events that can be audited  
:icons: font

```
:relative_path: ./nas-audit/  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/
```

ONTAP can audit certain NFS file and directory access events. Knowing what access events can be audited is helpful when interpreting results from the converted audit event logs.

You can audit the following NFS file and directory access events:

- READ
- OPEN
- CLOSE
- REaddir
- WRITE
- SETATTR
- CREATE
- LINK
- OPENATTR
- REMOVE
- GETATTR
- VERIFY
- NVERIFY
- RENAME

To reliably audit NFS RENAME events, you should set audit ACEs on directories instead of files because file permissions are not checked for a RENAME operation if the directory permissions are sufficient.

= Plan the auditing configuration

```
:icons: font  
:relative_path: ./nas-audit/  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/
```

Before you configure auditing on storage virtual machines (SVMs), you must understand which configuration options are available and plan the values that you want to set for each option. This information can help you configure the auditing configuration that meets your business needs.

There are certain configuration parameters that are common to all auditing configurations.

Additionally, there are certain parameters that you can use to specify which methods are used when rotating the consolidated and converted audit logs. You can specify one of the three following methods when you configure auditing:

- Rotate logs based on log size

This is the default method used to rotate logs.

- Rotate logs based on a schedule
- Rotate logs based on log size and schedule (whichever event occurs first)

At least one of the methods for log rotation should always be set.

== Parameters common to all auditing configurations

There are two required parameters that you must specify when you create the auditing configuration. There are also three optional parameters that you can specify:

Type of information	Option	Required	Include	Your values
<p><i>SVM name</i></p> <p>Name of the SVM on which to create the auditing configuration. The SVM must already exist.</p>	<code>-vserver vserver_name</code>	Yes	Yes	
<p><i>Log destination path</i></p> <p>Specifies the directory where the converted audit logs are stored, typically a dedicated volume or qtree. The path must already exist in the SVM namespace.</p> <p>The path can be up to 864 characters in length and must have read-write permissions.</p> <p>If the path is not valid, the audit configuration command fails.</p> <p>If the SVM is an SVM disaster recovery source, the log destination path cannot be on the root volume. This is because root volume content is not replicated to the disaster recovery destination.</p> <p>You cannot use a FlexCache volume as a log destination (ONTAP 9.7 and later).</p>	<code>-destination text</code>	Yes	Yes	

<p><i>Categories of events to audit</i></p> <p>Specifies the categories of events to audit. The following event categories can be audited:</p> <ul style="list-style-type: none"> <li>• File access events (both SMB and NFSv4)</li> <li>• SMB logon and logoff events</li> <li>• Central access policy staging events</li> </ul> <p>Central access policy staging events are a new advanced auditing event available beginning with Windows 2012 Active Directory domains. Central access policy staging events log information about changes to central access policies configured in Active Directory.</p> <ul style="list-style-type: none"> <li>• File share category events</li> <li>• Audit policy change events</li> <li>• Local user account management events</li> <li>• Security group management events</li> <li>• Authorization policy change events</li> </ul> <p>The default is to audit file access and SMB logon and logoff events.</p> <p><b>Note:</b> Before you can specify <code>cap-staging</code> as an event category, a SMB server must exist on the SVM. Although you can enable central access policy staging in the auditing configuration without enabling Dynamic Access Control on the SMB server, central access policy staging events are generated only if Dynamic Access Control is enabled. Dynamic Access Control is enabled through a SMB server option. It is not enabled by default.</p>	<pre>-events {file-ops cifs- logon-logoff cap- staging file-share  audit-policy-change  user-account security- group authorization- policy-change}</pre>	No		
<p><i>Log file output format</i></p> <p>Determines the output format of the audit logs. The output format can be either ONTAP-specific XML or Microsoft Windows EVTX log format. By default, the output format is EVTX.</p>	<pre>-format {xml evtx}</pre>	No		

<p><b>Log files rotation limit</b></p> <p>Determines how many audit log files to retain before rotating the oldest log file out. For example, if you enter a value of 5, the last five log files are retained.</p> <p>A value of 0 indicates that all the log files are retained. The default value is 0.</p>	<code>-rotate-limit integer</code>	No		
---	------------------------------------	----	--	--

== Parameters used for determining when to rotate audit event logs

### Rotate logs based on log size

The default is to rotate audit logs based on size.

- The default log size is 100 MB
- If you want to use the default log rotation method and the default log size, you do not need to configure any specific parameters for log rotation.
- If you want to rotate the audit logs based on a log size alone, use the following command to unset the `-rotate-schedule-minute` parameter: `vserver audit modify -vserver vs0 -destination / -rotate-schedule-minute -`

If you do not want to use the default log size, you can configure the `-rotate-size` parameter to specify a custom log size:

Type of information	Option	Required	Include	Your values
<p><b>Log file size limit</b></p> <p>Determines the audit log file size limit.</p>	<code>-rotate-size { integer[KB MB GB TB PB]}</code>	No		

### Rotate logs based on a schedule

If you choose to rotate the audit logs based on a schedule, you can schedule log rotation by using the time-based rotation parameters in any combination.

- If you use time-based rotation, the `-rotate-schedule-minute` parameter is mandatory.
- All other time-based rotation parameters are optional.
- The rotation schedule is calculated by using all the time-related values.

For example, if you specify only the `-rotate-schedule-minute` parameter, the audit log files are rotated based on the minutes specified on all days of the week, during all hours on all months of the year.

- If you specify only one or two time-based rotation parameters (for example, `-rotate-schedule-month` and `-rotate-schedule-minutes`), the log files are rotated based on the minute values that you specified on all days of the week, during all hours, but only during the specified months.

For example, you can specify that the audit log is to be rotated during the months January, March, and August on all Mondays, Wednesdays, and Saturdays at 10:30 a.m.

- If you specify values for both `-rotate-schedule-dayofweek` and `-rotate-schedule-day`, they are considered independently.

For example, if you specify `-rotate-schedule-dayofweek` as `Friday` and `-rotate-schedule-day` as `13`, then the audit logs would be rotated on every Friday and on the 13th day of the specified month, not just on every Friday the 13th.

- If you want to rotate the audit logs based on a schedule alone, use the following command to unset the `-rotate-size` parameter: `vserver audit modify -vserver vs0 -destination / -rotate-size -`

You can use the following list of available auditing parameters to determine what values to use for configuring a schedule for audit event log rotations:

Type of information	Option	Required	Include	Your values
<p><i>Log rotation schedule: Month</i></p> <p>Determines the monthly schedule for rotating audit logs.</p> <p>Valid values are <code>January</code> through <code>December</code>, and <code>all</code>. For example, you can specify that the audit log is to be rotated during the months January, March, and August.</p>	<p><code>-rotate-schedule-month</code> <code>chron_month</code></p>	No		
<p><i>Log rotation schedule: Day of week</i></p> <p>Determines the daily (day of week) schedule for rotating audit logs.</p> <p>Valid values are <code>Sunday</code> through <code>Saturday</code>, and <code>all</code>. For example, you can specify that the audit log is to be rotated on Tuesdays and Fridays, or during all the days of a week.</p>	<p><code>-rotate-schedule-dayofweek</code> <code>chron_dayofweek</code></p>	No		
<p><i>Log rotation schedule: Day</i></p> <p>Determines the day of the month schedule for rotating the audit log.</p> <p>Valid values range from 1 through 31. For example, you can specify that the audit log is to be rotated on the 10th and 20th days of a month, or all days of a month.</p>	<p><code>-rotate-schedule-day</code> <code>chron_dayofmonth</code></p>	No		

<p><i>Log rotation schedule: Hour</i></p> <p>Determines the hourly schedule for rotating the audit log.</p> <p>Valid values range from 0 (midnight) to 23 (11:00 p.m.). Specifying <code>all</code> rotates the audit logs every hour. For example, you can specify that the audit log is to be rotated at 6 (6 a.m.) and 18 (6 p.m.).</p>	<pre>-rotate-schedule-hour chron_hour</pre>	No		
<p><i>Log rotation schedule: Minute</i></p> <p>Determines the minute schedule for rotating the audit log.</p> <p>Valid values range from 0 to 59. For example, you can specify that the audit log is to be rotated at the 30th minute.</p>	<pre>-rotate-schedule -minute chron_minute</pre>	Yes, if configuring schedule-based log rotation; otherwise, no.		

### Rotate logs based on log size and schedule

You can choose to rotate the log files based on log size and a schedule by setting both the `-rotate-size` parameter and the time-based rotation parameters in any combination. For example: if `-rotate-size` is set to 10 MB and `-rotate-schedule-minute` is set to 15, the log files rotate when the log file size reaches 10 MB or on the 15th minute of every hour (whichever event occurs first).

= Create a file and directory auditing configuration on SVMs

= Create the auditing configuration

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

Creating a file and directory auditing configuration on your storage virtual machine (SVM) includes understanding the available configuration options, planning the configuration, and then configuring and enabling the configuration. You can then display information about the auditing configuration to confirm that the resultant configuration is the desired configuration.

Before you can begin auditing file and directory events, you must create an auditing configuration on the storage virtual machine (SVM).

#### Before you begin

If you plan on creating an auditing configuration for central access policy staging, a SMB server must exist on the SVM.

- Although you can enable central access policy staging in the auditing configuration without enabling Dynamic Access Control on the SMB server, central access policy staging events are generated only if Dynamic Access Control is enabled.



Dynamic Access Control is enabled through a SMB server option. It is not enabled by default.

- If the arguments of a field in a command is invalid, for example, invalid entries for fields, duplicate entries, and non-existent entries, then the command fails before the audit phase.

Such failures do not generate an audit record.

### About this task

If the SVM is an SVM disaster recovery source, the destination path cannot be on the root volume.

### Step

1. Using the information in the planning worksheet, create the auditing configuration to rotate audit logs based on log size or a schedule:

If you want to rotate audit logs by...	Enter...
Log size	<pre>vserver audit create -vserver vserver_name -destination path -events [{file-ops cifs-logon- logoff cap-staging file-share audit-policy- change user-account security-group authorization- policy-change}] [-format {xml evtx}] [-rotate-limit integer] [-rotate-size {integer[KB MB GB TB PB]}]</pre>
A schedule	<pre>vserver audit create -vserver vserver_name -destination path -events [{file-ops cifs-logon- logoff cap-staging}] [-format {xml evtx}] [-rotate- limit integer] [-rotate-schedule-month chron_month] [-rotate-schedule-dayofweek chron_dayofweek] [- rotate-schedule-day chron_dayofmonth] [-rotate- schedule-hour chron_hour] -rotate-schedule-minute chron_minute</pre>

The `-rotate-schedule-minute` parameter is required if you are configuring time-based audit log rotation.



## .Examples

The following example creates an auditing configuration that audits file operations and SMB logon and logoff events (the default) using size-based rotation. The log format is `EVTX` (the default). The logs are stored in the `/audit_log` directory. The log file size limit is 200 MB. The logs are rotated when they reach 200 MB in size:

```
----  
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -rotate-size 200MB  
----
```

The following example creates an auditing configuration that audits file operations and SMB logon and logoff events (the default) using size-based rotation. The log format is `EVTX` (the default). The log file size limit is 100 MB (the default), and the log rotation limit is 5:

```
----  
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -rotate-limit 5  
----
```

The following example creates an auditing configuration that audits file operations, CIFS logon and logoff events, and central access policy staging events using time-based rotation. The log format is `EVTX` (the default). The audit logs are rotated monthly, at 12:30 p.m. on all days of the week. The log rotation limit is 5:

```
----  
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -events file-ops,cifs-logon-logoff,file-  
share,audit-policy-change,user-account,security-group,authorization-policy-change,cap-staging -rotate  
-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour 12 -rotate-schedule-minute 30  
-rotate-limit 5  
----
```

= Enable auditing on the SVM

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

[.lead]

After you finish setting up the auditing configuration, you must enable auditing on the storage virtual machine (SVM).

.What you'll need

The SVM audit configuration must already exist.

.About this task

When an SVM disaster recovery ID discard configuration is first started (after the SnapMirror initialization is complete) and the SVM has an auditing configuration, ONTAP automatically disables the auditing configuration. Auditing is disabled on the read-only SVM to prevent the staging volumes from filling up. You can enable auditing only after the SnapMirror relationship is broken and the SVM is read-write.

h| If you want to.... h| Do the following

a|

Set up auditing for a new user or group

a|

- a. Click **Add**.
- b. In the Enter the object name to select box, type the name of the user or group that you want to add.
- c. Click **OK**.

a|

Remove auditing from a user or group

a|

- a. In the Enter the object name to select box, select the user or group that you want to remove.
- b. Click **Remove**.
- c. Click **OK**.
- d. Skip the rest of this procedure.

a|

Change auditing for a user or group

a|

- a. In the Enter the object name to select box, select the user or group that you want to change.
- b. Click **Edit**.
- c. Click **OK**.

If you are setting up auditing on a user or group or changing auditing on an existing user or group, the Auditing Entry for <object> box opens.

. In the **Apply to** box, select how you want to apply this auditing entry.

+

You can select one of the following:

**This folder, subfolders and files**

**This folder and subfolders**

**This folder only**

**This folder and files**

**Subfolders and files only**

**Subfolders only**

**\* \*Files only**

If you are setting up auditing on a single file, the **Apply to** box is not active. The **Apply to** box setting defaults to **This object only**.

+

[NOTE]

Because auditing takes SVM resources, select only the minimal level that provides the auditing events that meet your security requirements.

1. In the **Access** box, select what you want audited and whether you want to audit successful events, failure events, or both.

- To audit successful events, select the Success box.
- To audit failure events, select the Failure box.

Select only the actions that you need to monitor to meet your security requirements. For more information about these auditable events, see your Windows documentation. You can audit the following events:

- **Full control**
- **Traverse folder / execute file**
- **List folder / read data**
- **Read attributes**
- **Read extended attributes**
- **Create files / write data**
- **Create folders / append data**
- **Write attributes**
- **Write extended attributes**
- **Delete subfolders and files**
- **Delete**
- **Read permissions**
- **Change permissions**
- **Take ownership**

2. If you do not want the auditing setting to propagate to subsequent files and folders of the original container, select the **Apply these auditing entries to objects and/or containers within this container only** box.

3. Click **Apply**.

4. After you finish adding, removing, or editing auditing entries, click **OK**.

The Auditing Entry for <object> box closes.

5. In the **Auditing** box, select the inheritance settings for this folder.

Select only the minimal level that provides the auditing events that meet your security requirements. You can choose one of the following:

- Select the Include inheritable auditing entries from this object's parent box.
- Select the Replace all existing inheritable auditing entries on all descendants with inheritable auditing entries from this object box.
- Select both boxes.
- Select neither box.

If you are setting SACLs on a single file, the Replace all existing inheritable auditing entries on all descendants with inheritable auditing entries from this object box is not present in the Auditing box.

## 6. Click **OK**.

The Auditing box closes.

== Configure NTFS audit policies using the ONTAP CLI

You can configure audit policies on files and folders using the ONTAP CLI. This enables you to configure NTFS audit policies without needing to connect to the data using an SMB share on a Windows client.

You can configure NTFS audit policies by using the `vserver security file-directory` command family.

You can only configure NTFS SACLs using the CLI. Configuring NFSv4 SACLs is not supported with this ONTAP command family. See the man pages for more information about using these commands to configure and add NTFS SACLs to files and folders.

= Configure auditing for UNIX security style files and directories

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You configure auditing for UNIX security style files and directories by adding audit ACEs to NFSv4.x ACLs. This allows you to monitor certain NFS file and directory access events for security purposes.

### **About this task**

For NFSv4.x, both discretionary and system ACEs are stored in the same ACL. They are not stored in separate DACLs and SACLs. Therefore, you must exercise caution when adding audit ACEs to an existing ACL to avoid overwriting and losing an existing ACL. The order in which you add the audit ACEs to an existing ACL does not matter.

### **Steps**

1. Retrieve the existing ACL for the file or directory by using the `nfs4_getfacl` or equivalent command.

For more information about manipulating ACLs, see the man pages of your NFS client.

2. Append the desired audit ACEs.
3. Apply the updated ACL to the file or directory by using the `nfs4_setfacl` or equivalent command.

= Display information about audit policies applied to files and directories

= Display information about audit policies using the Windows Security tab

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You can display information about audit policies that have been applied to files and directories by using the Security tab in the Windows Properties window. This is the same method used for data residing on a Windows server, which enables customers to use the same GUI interface that they are accustomed to using.

### About this task

Displaying information about audit policies applied to files and directories enables you to verify that you have the appropriate system access control lists (SACLs) set on specified files and folders.

To display information about SACLs that have been applied to NTFS files and folders, complete the following steps on a Windows host.

### Steps

1. From the **Tools** menu in Windows Explorer, select **Map network drive**.
2. Complete the **Map Network Drive** dialog box:
  - a. Select a **Drive** letter.
  - b. In the **Folder** box, type the IP address or SMB server name of the storage virtual machine (SVM) containing the share that holds both the data you would like to audit and the name of the share.

If your SMB server name is "SMB\_SERVER" and your share is named "share1", you should enter \\SMB\_SERVER\share1.

You can specify the IP address of the data interface for the SMB server instead of the SMB server name.

a. Click **Finish**.

The drive you selected is mounted and ready with the Windows Explorer window displaying files and folders contained within the share.

- . Select the file or directory for which you display auditing information.
- . Right-click on the file or directory, and select **Properties**.
- . Select the **Security** tab.
- . Click **Advanced**.
- . Select the **Auditing** tab.
- . Click **Continue**.

+

The Auditing box opens. The **Auditing entries** box displays a summary of users and groups that have SACLs applied to them.

1. In the **Auditing entries** box select the user or group whose SACL entries you want displayed.
2. Click **Edit**.

The Auditing entry for <object> box opens.

3. In the **Access** box, view the current SACLs that are applied to the selected object.
4. Click **Cancel** to close the **Auditing entry for <object>** box.
5. Click **Cancel** to close the **Auditing** box.

= Display information about NTFS audit policies on FlexVol volumes using the CLI

```
:icons: font
```

```
:relative_path: ./nas-audit/
```

```
:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/
```

You can display information about NTFS audit policies on FlexVol volumes, including what the security styles and effective security styles are, what permissions are applied, and information about system access control lists. You can use the information to validate your security configuration or to troubleshoot auditing issues.

#### About this task

Displaying information about audit policies applied to files and directories enables you to verify that you have the appropriate system access control lists (SACLs) set on specified files and folders.

You must provide the name of the storage virtual machine (SVM) and the path to the files or folders whose audit information you want to display. You can display the output in summary form or as a detailed list.

- NTFS security-style volumes and qtrees use only NTFS system access control lists (SACLs) for audit policies.
- Files and folders in a mixed security-style volume with NTFS effective security can have NTFS audit policies applied to them.

Mixed security-style volumes and qtrees can contain some files and directories that use UNIX file permissions, either mode bits or NFSv4 ACLs, and some files and directories that use NTFS file permissions.



- The top level of a mixed security-style volume can have either UNIX or NTFS effective security and might or might not contain NTFS SACLs.
- Because Storage-Level Access Guard security can be configured on a mixed security-style volume or qtree even if the effective security style of the volume root or qtree is UNIX, the output for a volume or qtree path where Storage-Level Access Guard is configured might display both regular file and folder NFSv4 SACLs and Storage-Level Access Guard NTFS SACLs.
- If the path that is entered in the command is to data with NTFS effective security, the output also displays information about Dynamic Access Control ACEs if Dynamic Access Control is configured for the given file or directory path.
- When displaying security information about files and folders with NTFS effective security, UNIX-related output fields contain display-only UNIX file permission information.

NTFS security-style files and folders use only NTFS file permissions and Windows users and groups when determining file access rights.

- ACL output is displayed only for files and folders with NTFS or NFSv4 security.

This field is empty for files and folders using UNIX security that have only mode bit permissions applied (no NFSv4 ACLs).

- The owner and group output fields in the ACL output apply only in the case of NTFS security descriptors.

### Step

1. Display file and directory audit policy settings with the desired level of detail:

If you want to display information...	Enter the following command...
In summary form	<pre>vserver security file-directory show -vserver vserver_name -path path</pre>
As a detailed list	<pre>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</pre>

### Examples

The following example displays the audit policy information for the path `/corp` in SVM `vs1`. The path has NTFS effective security. The NTFS security descriptor contains both a SUCCESS and a SUCCESS/FAIL SACL entry.

```

cluster::> vserver security file-directory show -vserver vs1 -path
/corp

          Vserver: vs1
          File Path: /corp
File Inode Number: 357
          Security Style: ntfs
          Effective Style: ntfs
          DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
          Unix User Id: 0
          Unix Group Id: 0
          Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
          ACLs: NTFS Security Descriptor
          Control:0x8014
          Owner:DOMAIN\Administrator
          Group:BUILTIN\Administrators
          SACL - ACEs
              ALL-DOMAIN\Administrator-0x100081-
OI|CI|SA|FA
              SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
          DACL - ACEs
              ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
              ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
              ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
              ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI

```

The following example displays the audit policy information for the path /datavol1 in SVM vs1. The path contains both regular file and folder SACLs and Storage-Level Access Guard SACLs.

```
cluster::> vserver security file-directory show -vserver vs1 -path /datavol1
```

```
      Vserver: vs1
      File Path: /datavol1
      File Inode Number: 77
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0xaa14
            Owner: BUILTIN\Administrators
            Group: BUILTIN\Administrators
            SACL - ACEs
              AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
            DACL - ACEs
              ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
              ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

      Storage-Level Access Guard security
      SACL (Applies to Directories):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Directories):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
      SACL (Applies to Files):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Files):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

= Ways to display information about file security and audit policies

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You can use the wildcard character (\*) to display information about file security and audit policies of all files and directories under a given path or a root volume.

The wildcard character (\*) can be used as the last subcomponent of a given directory path below which you want to display information of all files and directories.

If you want to display information of a particular file or directory named as "\*", then you need to provide the complete path inside double quotes (" ").

### **Example**

The following command with the wildcard character displays the information about all files and directories below the path /1/ of SVM vs1:

```

cluster::> vserver security file-directory show -vserver vs1 -path /1/*

      Vserver: vs1
      File Path: /1/1
      Security Style: mixed
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8514
            Owner: BUILTIN\Administrators
            Group: BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

      Vserver: vs1
      File Path: /1/1/abc
      Security Style: mixed
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8404
            Owner: BUILTIN\Administrators
            Group: BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

```

The following command displays the information of a file named as "\*" under the path /vol1/a of SVM vs1. The path is enclosed within double quotes (" ").

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/voll/a/*"
```

```
          Vserver: vs1
          File Path: "/voll/a/*"
          Security Style: mixed
          Effective Style: unix
          DOS Attributes: 10
          DOS Attributes in Text: ----D---
          Expanded Dos Attributes: -
            Unix User Id: 1002
            Unix Group Id: 65533
            Unix Mode Bits: 755
          Unix Mode Bits in Text: rwxr-xr-x
          ACLs: NFSV4 Security Descriptor
            Control:0x8014
            SACL - ACEs
              AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
            DACL - ACEs
              ALLOW-EVERYONE@-0x1f00a9-FI|DI
              ALLOW-OWNER@-0x1f01ff-FI|DI
              ALLOW-GROUP@-0x1200a9-IG
```

= CLI change events that can be audited

= CLI change events that can be audited overview

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

ONTAP can audit certain CLI change events, including certain SMB-share events, certain audit policy events, certain local security group events, local user group events, and authorization policy events. Understanding which change events can be audited is helpful when interpreting results from the event logs.

You can manage storage virtual machine (SVM) auditing CLI change events by manually rotating the audit logs, enabling or disabling auditing, displaying information about auditing change events, modifying auditing change events, and deleting auditing change events.

As an administrator, if you execute any command to change configuration related to the SMB-share, local user-group, local security-group, authorization-policy, and audit-policy events, a record generates and the corresponding event gets audited:

Auditing Category	Events	Event IDs	Run this command...
-------------------	--------	-----------	---------------------

Mhost Auditing	policy-change	[4719] Audit configuration changed	vserver audit disable enable modify
	file-share	[5142] Network share was added	vserver cifs share create
		[5143] Network share was modified	vserver cifs share modify vserver cifs share create modify delete vserver cifs share add remove
		[5144] Network share deleted	vserver cifs share delete

Auditing



	Rename	users-and-groups local-user rename
security-group	[4731] Local Security Group created	vserver cifs users-and-groups local-group create vserver services name-service unix- group create
	[4734] Local Security Group deleted	vserver cifs users-and-groups local-group delete vserver services name-service unix- group delete
	[4735] Local Security Group Modified	vserver cifs users-and-groups local-group rename modify vserver services name-service unix- group modify
	[4732] User added to Local Group	vserver cifs users-and-groups local-group add- members vserver services name- service unix-group adduser
	[4733] User Removed from Local Group	vserver cifs users-and-groups local-group remove-members vserver services name-service unix- group deluser
authorization-policy- change	[4704] User Rights Assigned	vserver cifs users-and-groups privilege add- privilege
	[4705] User Rights Removed	vserver cifs users-and-groups privilege remove- privilege reset- privilege

= Manage file-share event

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

When a file-share event is configured for a storage virtual machine (SVM) and an audit is enabled, audit events are generated. The file-share events are generated when the SMB network share is modified using `vserver cifs share` related commands.

The file-share events with the event-ids 5142, 5143, and 5144 are generated when a SMB network share is added, modified, or deleted for the SVM. The SMB network share configuration is modified using the `cifs share access control create|modify|delete` commands.

The following example displays a file-share event with the ID 5143 is generated, when a share object called 'audit\_dest' is created:

```
netapp-clus1::*> cifs share create -share-name audit_dest -path
/audit_dest
- System
  - Provider
    [ Name]   NetApp-Security-Auditing
    [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
    EventID  5142
    EventName Share Object Added
    ...
    ...
    ShareName audit_dest
    SharePath /audit_dest
    ShareProperties oplocks;browsable;changenotify;show-previous-
versions;
    SD O:BAG:S-1-5-21-2447422786-1297661003-4197201688-513D:(A;;FA;;;WD)
```

= Manage audit-policy-change event

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

When an audit-policy-change event is configured for a storage virtual machine (SVM) and an audit is enabled, audit events are generated. The audit-policy-change events are generated when an audit policy is modified using `vserver audit` related commands.

The audit-policy-change event with the event-id 4719 is generated whenever an audit policy is disabled, enabled, or modified and helps to identify when a user attempts to disable auditing to cover the tracks. It is configured by default and requires diagnostic privilege to disable.

The following example displays an audit-policy change event with the ID 4719 generated, when an audit

is disabled:

```
netapp-clus1::*> vserver audit disable -vserver vserver_1
- System
- Provider
  [ Name]  NetApp-Security-Auditing
  [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
EventID 4719
EventName Audit Disabled
...
...
SubjectUserName admin
SubjectUserSid 65533-1001
SubjectDomainName ~
SubjectIP console
SubjectPort
```

= Manage user-account event

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

When a user-account event is configured for a storage virtual machine (SVM) and an audit is enabled, audit events are generated.

The user-account events with event-ids 4720, 4722, 4724, 4725, 4726, 4738, and 4781 are generated when a local SMB or NFS user is created or deleted from the system, local user account is enabled, disabled or modified, and local SMB user password is reset or changed. The user-account events are generated when a user account is modified using `vserver cifs users-and-groups <local user>` and `vserver services name-service <unix user>` commands.

The following example displays a user account event with the ID 4720 generated, when a local SMB user is created:

```

netapp-clus1::~*> vserver cifs users-and-groups local-user create -user
-name testuser -is-account-disabled false -vserver vserver_1
Enter the password:
Confirm the password:

- System
  - Provider
    [ Name] NetApp-Security-Auditing
    [ Guid] {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
    EventID 4720
    EventName Local Cifs User Created
    ...
    ...
    TargetUserName testuser
    TargetDomainName NETAPP-CLUS1
    TargetSid S-1-5-21-2447422786-1297661003-4197201688-1003
    TargetType CIFS
    DisplayName testuser
    PasswordLastSet 1472662216
    AccountExpires NO
    PrimaryGroupId 513
    UserAccountControl %%0200
    SidHistory ~
    PrivilegeList ~

```

The following example displays a user account event with the ID 4781 generated, when the local SMB user created in the preceding example is renamed:

```
netapp-clus1::*> vserver cifs users-and-groups local-user rename -user
-name testuser -new-user-name testuser1
- System
- Provider
  [ Name]  NetApp-Security-Auditing
  [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
  EventID 4781
  EventName Local Cifs User Renamed
  ...
  ...
  OldTargetUserName testuser
  NewTargetUserName testuser1
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1000
  TargetType CIFS
  SidHistory ~
  PrivilegeList ~
```

= Manage security-group event

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

When a security-group event is configured for a storage virtual machine (SVM) and an audit is enabled, audit events are generated.

The security-group events with event-ids 4731, 4732, 4733, 4734, and 4735 are generated when a local SMB or NFS group is created or deleted from the system, and local user is added or removed from the group. The security-group-events are generated when a user account is modified using `vserver cifs users-and-groups <local-group>` and `vserver services name-service <unix-group>` commands.

The following example displays a security group event with the ID 4731 generated, when a local UNIX security group is created:

```

netapp-clus1::*> vserver services name-service unix-group create -name
testunixgroup -id 20
- System
- Provider
  [ Name]  NetApp-Security-Auditing
  [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
  EventID 4731
  EventName Local Unix Security Group Created
  ...
  ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
  TargetUserName testunixgroup
  TargetDomainName
  TargetGid 20
  TargetType NFS
  PrivilegeList ~
  GidHistory ~

```

= Manage authorization-policy-change event

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

When authorization-policy-change event is configured for a storage virtual machine (SVM) and an audit is enabled, audit events are generated.

The authorization-policy-change events with the event-ids 4704 and 4705 are generated whenever the authorization rights are granted or revoked for an SMB user and SMB group. The authorization-policy-change events are generated when the authorization rights are assigned or revoked using `vserver cifs users-and-groups privilege` related commands.

The following example displays an authorization policy event with the ID 4704 generated, when the authorization rights for a SMB user group are assigned:

```

netapp-clus1::*> vserver cifs users-and-groups privilege add-privilege
-user-or-group-name testcifslocalgroup -privileges *
- System
- Provider
  [ Name] NetApp-Security-Auditing
  [ Guid] {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
  EventID 4704
  EventName User Right Assigned
  ...
  ...
  TargetUserOrGroupName testcifslocalgroup
  TargetUserOrGroupDomainName NETAPP-CLUS1
  TargetUserOrGroupSid S-1-5-21-2447422786-1297661003-4197201688-1004;
  PrivilegeList
  SeTcbPrivilege;SeBackupPrivilege;SeRestorePrivilege;SeTakeOwnershipPriv
ilege;SeSecurityPrivilege;SeChangeNotifyPrivilege;
  TargetType CIFS

```

= Manage auditing configurations

= Manually rotate the audit event logs

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

Before you can view the audit event logs, the logs must be converted to user-readable formats. If you want to view the event logs for a specific storage virtual machine (SVM) before ONTAP automatically rotates the log, you can manually rotate the audit event logs on an SVM.

### Step

1. Rotate the audit event logs by using the `vserver audit rotate-log` command.

```
vserver audit rotate-log -vserver vs1
```

The audit event log is saved in the SVM audit event log directory with the format specified by the auditing configuration (XML or EVTX), and can be viewed by using the appropriate application.

= Enable and disable auditing on SVMs

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You can enable or disable auditing on storage virtual machines (SVMs). You might want to temporarily stop file and directory auditing by disabling auditing. You can enable auditing at any time (if an auditing configuration exists).

## What you'll need

Before you can enable auditing on the SVM, the SVM's auditing configuration must already exist.

## About this task

Disabling auditing does not delete the auditing configuration.

## Steps

1. Perform the appropriate command:

If you want auditing to be...	Enter the command...
Enabled	<code>vserver audit enable -vserver vserver_name</code>
Disabled	<code>vserver audit disable -vserver vserver_name</code>

2. Verify that auditing is in the desired state:

```
vserver audit show -vserver vserver_name
```

## Examples

The following example enables auditing for SVM vs1:

```
cluster1::> vserver audit enable -vserver vs1

cluster1::> vserver audit show -vserver vs1

                Vserver: vs1
                Auditing state: true
                Log Destination Path: /audit_log
                Categories of Events to Audit: file-ops, cifs-logon-logoff
                Log Format: evtX
                Log File Size Limit: 100MB
                Log Rotation Schedule: Month: -
                Log Rotation Schedule: Day of Week: -
                Log Rotation Schedule: Day: -
                Log Rotation Schedule: Hour: -
                Log Rotation Schedule: Minute: -
                Rotation Schedules: -
                Log Files Rotation Limit: 10
```

The following example disables auditing for SVM vs1:



```

cluster1::> vserver audit disable -vserver vs1

                Vserver: vs1
                Auditing state: false
                Log Destination Path: /audit_log
                Categories of Events to Audit: file-ops, cifs-logon-logoff
                Log Format: evtX
                Log File Size Limit: 100MB
                Log Rotation Schedule: Month: -
                Log Rotation Schedule: Day of Week: -
                Log Rotation Schedule: Day: -
                Log Rotation Schedule: Hour: -
                Log Rotation Schedule: Minute: -
                Rotation Schedules: -
                Log Files Rotation Limit: 10

```

= Display information about auditing configurations

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You can display information about auditing configurations. The information can help you determine whether the configuration is what you want in place for each SVM. The displayed information also enables you to verify whether an auditing configuration is enabled.

#### About this task

You can display detailed information about auditing configurations on all SVMs or you can customize what information is displayed in the output by specifying optional parameters. If you do not specify any of the optional parameters, the following is displayed:

- SVM name to which the auditing configuration applies
- The audit state, which can be `true` or `false`

If the audit state is `true`, auditing is enabled. If the audit state is `false`, auditing is disabled.

- The categories of events to audit
- The audit log format
- The target directory where the auditing subsystem stores consolidated and converted audit logs

#### Step

1. Display information about the auditing configuration by using the `vserver audit show` command.

For more information about using the command, see the man pages.

#### Examples

The following example displays a summary of the auditing configuration for all SVMs:

```
cluster1::> vserver audit show

Vserver      State  Event Types  Log Format  Target Directory
-----
vs1          false  file-ops     evtX       /audit_log
```

The following example displays, in list form, all auditing configuration information for all SVMs:

```
cluster1::> vserver audit show -instance

                Vserver: vs1
                Auditing state: true
                Log Destination Path: /audit_log
                Categories of Events to Audit: file-ops
                Log Format: evtX
                Log File Size Limit: 100MB
                Log Rotation Schedule: Month: -
                Log Rotation Schedule: Day of Week: -
                Log Rotation Schedule: Day: -
                Log Rotation Schedule: Hour: -
                Log Rotation Schedule: Minute: -
                Rotation Schedules: -
                Log Files Rotation Limit: 0
```

= Commands for modifying auditing configurations


:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

If you want to change an auditing setting, you can modify the current configuration at any time, including modifying the log path destination and log format, modifying the categories of events to audit, how to automatically save log files, and specify the maximum number of log files to save.

If you want to...	Use this command...
Modify the log destination path	<code>vserver audit modify</code> with the <code>-destination</code> parameter

Modify the category of events to audit	<pre>vserver audit modify with the -events parameter</pre> <div style="display: flex; align-items: center; margin-top: 10px;">  <p>To audit central access policy staging events, the Dynamic Access Control (DAC) SMB server option must be enabled on the storage virtual machine (SVM).</p> </div>
Modify the log format	<pre>vserver audit modify with the -format parameter</pre>
Enabling automatic saves based on internal log file size	<pre>vserver audit modify with the -rotate -size parameter</pre>
Enabling automatic saves based on a time interval	<pre>vserver audit modify with the -rotate -schedule-month, -rotate-schedule -dayofweek, -rotate-schedule-day, -rotate-schedule-hour, and -rotate -schedule-minute parameters</pre>
Specifying the maximum number of saved log files	<pre>vserver audit modify with the -rotate -limit parameter</pre>

= Delete an auditing configuration

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

In you no longer want to audit file and directory events on the storage virtual machine (SVM) and do not want to maintain an auditing configuration on the SVM, you can delete the auditing configuration.

### Steps

1. Disable the auditing configuration:

```
vserver audit disable -vserver vserver_name
```

```
vserver audit disable -vserver vs1
```

2. Delete the auditing configuration:

```
vserver audit delete -vserver vserver_name
```

```
vserver audit delete -vserver vs1
```

= What the process is when reverting

:icons: font

```
:relative_path: ./nas-audit/  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/
```

If you plan to revert the cluster, you should be aware of the revert process ONTAP follows when there are auditing-enabled storage virtual machines (SVMs) in the cluster. You must take certain actions before reverting.

== Reverting to a version of ONTAP that does not support the auditing of SMB logon and logoff events and central access policy staging events

Support for auditing of SMB logon and logoff events and for central access policy staging events starts with clustered Data ONTAP 8.3. If you are reverting to a version of ONTAP that does not support these event types and you have auditing configurations that monitor these event types, you must change the auditing configuration for those audit-enabled SVMs before reverting. You must modify the configuration so that only file-op events are audited.

= Troubleshoot auditing and staging volume space issues

```
:icons: font
```

```
:relative_path: ./nas-audit/
```

```
:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/
```

Issues can arise when there is insufficient space on either the staging volumes or on the volume containing the audit event logs. If there is insufficient space, new audit records cannot be created, which prevents clients from accessing data, and access requests fail. You should know how to troubleshoot and resolve these volume space issues.

== Troubleshoot space issues related to the event log volumes

If volumes containing event log files run out of space, auditing cannot convert log records into log files. This results in client access failures. You must know how to troubleshoot space issues related to event log volumes.

- storage virtual machine (SVM) and cluster administrators can determine whether there is insufficient volume space by displaying information about volume and aggregate usage and configuration.
- If there is insufficient space in the volumes containing event logs, SVM and cluster administrators can resolve the space issues by either removing some of the event log files or by increasing the size of the volume.

If the aggregate that contains the event log volume is full, then the size of the aggregate must be increased before you can increase the size of the volume. Only a cluster administrator can increase the size of an aggregate.

- The destination path for the event log files can be changed to a directory on another volume by modifying the auditing configuration.

Data access is denied in the following cases:

- If the destination directory is deleted.

- If the file limit on a volume, which hosts the destination directory, reaches to its maximum level.

For more information about how to view information about volumes and increasing volume size, see the [Logical storage management](#)

For more information about how to view information about aggregates and managing aggregates, see [Disks and aggregates management](#).

== Troubleshoot space issues related to the staging volumes

If any of the volumes containing staging files for your storage virtual machine (SVM) runs out of space, auditing cannot write log records into staging files. This results in client access failures. To troubleshoot this issue, you need to determine whether any of the staging volumes used in the SVM are full by displaying information about volume usage.

If the volume containing the consolidated event log files has sufficient space but there are still client access failures due to insufficient space, then the staging volumes might be out of space. The SVM administrator must contact you to determine whether the staging volumes that contain staging files for the SVM have insufficient space. The auditing subsystem generates an EMS event if auditing events cannot be generated due to insufficient space in a staging volume. The following message is displayed: `No space left on device`. Only you can view information about staging volumes; SVM administrators cannot.

All staging volume names begin with `MDV_aud_` followed by the UUID of the aggregate containing that staging volume. The following example shows four system volumes on the admin SVM, which were automatically created when a file services auditing configuration was created for a data SVM in the cluster:

```
cluster1::> volume show -vserver cluster1
Vserver   Volume                Aggregate      State      Type      Size
Available Used%
-----
cluster1  MDV_aud_1d0131843d4811e296fc123478563412
          aggr0                online        RW         2GB
1.90GB    5%
cluster1  MDV_aud_8be27f813d7311e296fc123478563412
          root_vs0             online        RW         2GB
1.90GB    5%
cluster1  MDV_aud_9dc4ad503d7311e296fc123478563412
          aggr1                online        RW         2GB
1.90GB    5%
cluster1  MDV_aud_a4b887ac3d7311e296fc123478563412
          aggr2                online        RW         2GB
1.90GB    5%
4 entries were displayed.
```

If there is insufficient space in the staging volumes, you can resolve the space issues by increasing the size of the volume.

If the aggregate that contains the staging volume is full, then the size of the aggregate must be increased before you can increase the size of the volume. Only you can increase the size of an aggregate; SVM administrators cannot.

If one or more aggregates have an available space of less than 2 GB, the SVM audit creation fails. When the SVM audit creation fails, the staging volumes that were created are deleted.

### Related information

[ONTAP concepts](#)

[Logical storage management](#)

[Disks and aggregates management](#)

= Use FPolicy for file monitoring and management on SVMs

= How FPolicy works

= What the two parts of the FPolicy solution are

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

FPolicy is a file access notification framework that is used to monitor and manage file access events on storage virtual machines (SVMs).

There are two parts to an FPolicy solution. The ONTAP FPolicy framework manages activities on the cluster and sends notifications to external FPolicy servers. External FPolicy servers process notifications sent by ONTAP FPolicy.

The ONTAP framework creates and maintains the FPolicy configuration, monitors file events, and sends notifications to external FPolicy servers. ONTAP FPolicy provides the infrastructure that allows communication between external FPolicy servers and storage virtual machine (SVM) nodes.

The FPolicy framework connects to external FPolicy servers and sends notifications for certain file system events to the FPolicy servers when these events occur as a result of client access. The external FPolicy servers process the notifications and send responses back to the node. What happens as a result of the notification processing depends on the application and whether the communication between the node and the external servers is asynchronous or synchronous.

= What synchronous and asynchronous notifications are

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

FPolicy sends notifications to external FPolicy servers via the FPolicy interface. The notifications are sent either in synchronous or asynchronous mode. The notification mode determines what ONTAP does after sending notifications to FPolicy servers.

- **Asynchronous notifications**

With asynchronous notifications, the node does not wait for a response from the FPolicy server, which enhances overall throughput of the system. This type of notification is suitable for applications where the FPolicy server does not require that any action be taken as a result of notification evaluation. For example, asynchronous notifications are used when the storage virtual machine (SVM) administrator wants to monitor and audit file access activity.

If an FPolicy server operating in asynchronous mode experiences a network outage, FPolicy notifications generated during the outage are stored on the storage node. When the FPolicy server



comes back online, it is alerted of the stored notifications and can fetch them from the storage node. The length of time the notifications can be stored during an outage is configurable up to 10 minutes.

- **Synchronous notifications**

When configured to run in synchronous mode, the FPolicy server must acknowledge every notification before the client operation is allowed to continue. This type of notification is used when an action is required based on the results of notification evaluation. For example, synchronous notifications are used when the SVM administrator wants to either allow or deny requests based on criteria specified on the external FPolicy server.

== Synchronous and asynchronous applications

There are many possible uses for FPolicy applications, both asynchronous and synchronous.

Asynchronous applications are ones where the external FPolicy server does not alter access to files or directories or modify data on the storage virtual machine (SVM). For example:

- File access and audit logging
- Storage resource management

Synchronous applications are ones where data access is altered or data is modified by the external FPolicy server. For example:

- Quota management
- File access blocking
- File archiving and hierarchical storage management
- Encryption and decryption services
- Compression and decompression services

You can use the SDK for FPolicy to identify and implement other applications as well.

= Roles that cluster components play with FPolicy implementation

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

The cluster, the contained storage virtual machines (SVMs), and data LIFs all play a role in an FPolicy implementation.

- **cluster**

The cluster contains the FPolicy management framework and maintains and manages information about all FPolicy configurations in the cluster.

- **SVM**

An FPolicy configuration is defined at the SVM level. The scope of the configuration is the SVM, and it only operates on SVM resources. One SVM configuration cannot monitor and send notifications for file access requests that are made for data residing on another SVM.

FPolicy configurations can be defined on the admin SVM. After configurations are defined on the

admin SVM, they can be seen and used in all SVMs.

- **data LIFs**

Connections to the FPolicy servers are made through data LIFs belonging to the SVM with the FPolicy configuration. The data LIFs used for these connections can fail over in the same manner as data LIFs used for normal client access.

= How FPolicy works with external FPolicy servers

= How FPolicy works with external FPolicy servers overview

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

After FPolicy is configured and enabled on the storage virtual machine (SVM), FPolicy runs on every node on which the SVM participates. FPolicy is responsible for establishing and maintaining connections with external FPolicy servers (FPolicy servers), for notification processing, and for managing notification messages to and from FPolicy servers.

Additionally, as part of connection management, FPolicy has the following responsibilities:

- Ensures that file notification flows through the correct LIF to the FPolicy server.
- Ensures that when multiple FPolicy servers are associated with a policy, load balancing is done when sending notifications to the FPolicy servers.
- Attempts to reestablish the connection when a connection to an FPolicy server is broken.
- Sends the notifications to FPolicy servers over an authenticated session.
- Manages the passthrough-read data connection established by the FPolicy server for servicing client requests when passthrough-read is enabled.

= How control channels are used for FPolicy communication

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

FPolicy initiates a control channel connection to an external FPolicy server from the data LIFs of each node participating on a storage virtual machine (SVM). FPolicy uses control channels for transmitting file notifications; therefore, an FPolicy server might see multiple control channel connections based on SVM topology.

= How privileged data access channels are used for synchronous communication

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

With synchronous use cases, the FPolicy server accesses data residing on the storage virtual machine (SVM) through a privileged data access path. Access through the privileged path exposes the complete file system to the FPolicy server. It can access data files to collect information, to scan files, read files, or write into files.

Because the external FPolicy server can access the entire file system from the root of the SVM through the privileged data channel, the privileged data channel connection must be secure.

= How FPolicy connection credentials are used with privileged data access channels

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

The FPolicy server makes privileged data access connections to cluster nodes by using a specific Windows user credential that is saved with the FPolicy configuration. SMB is the only supported protocol for making a privileged data access channel connection.

If the FPolicy server requires privileged data access, the following conditions must be met:

- A SMB license must be enabled on the cluster.
- The FPolicy server must run under the credentials configured in the FPolicy configuration.

When making a data channel connection, FPolicy uses the credential for the specified Windows user name. Data access is made over the admin share ONTAP\_ADMIN\$.

= What granting super user credentials for privileged data access means

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

ONTAP uses the combination of the IP address and the user credential configured in the FPolicy configuration to grant super user credentials to the FPolicy server.

Super user status grants the following privileges when the FPolicy server accesses data:

- Avoid permission checks

The user avoids checks on files and directory access.

- Special locking privileges

ONTAP allows read, write, or modify access to any file regardless of existing locks. If the FPolicy server takes byte range locks on the file, it results in immediate removal of existing locks on the file.

- Bypass any FPolicy checks

Access does not generate any FPolicy notifications.

= How FPolicy manages policy processing

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

There might be multiple FPolicy policies assigned to your storage virtual machine (SVM); each with a different priority. To create an appropriate FPolicy configuration on the SVM, it is important to understand how FPolicy manages policy processing.

Each file access request is initially evaluated to determine which policies are monitoring this event. If it is a monitored event, information about the monitored event along with interested policies is passed to FPolicy where it is evaluated. Each policy is evaluated in order of the assigned priority.

You should consider the following recommendations when configuring policies:

- When you want a policy to always be evaluated before other policies, configure that policy with a higher priority.
- If the success of requested file access operation on a monitored event is a prerequisite for a file request that is evaluated against another policy, give the policy that controls the success or failure of the first file operation a higher priority.

For example, if one policy manages FPolicy file archiving and restore functionality and a second policy manages file access operations on the online file, the policy that manages file restoration must have a higher priority so that the file is restored before the operation managed by the second policy can be allowed.

- If you want all policies that might apply to a file access operation to be evaluated, give synchronous policies a lower priority.

You can reorder policy priorities for existing policies by modifying the policy sequence number. However, to have FPolicy evaluate policies based on the modified priority order, you must disable and reenble the policy with the modified sequence number.

= What the node-to-external FPolicy server communication process is

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

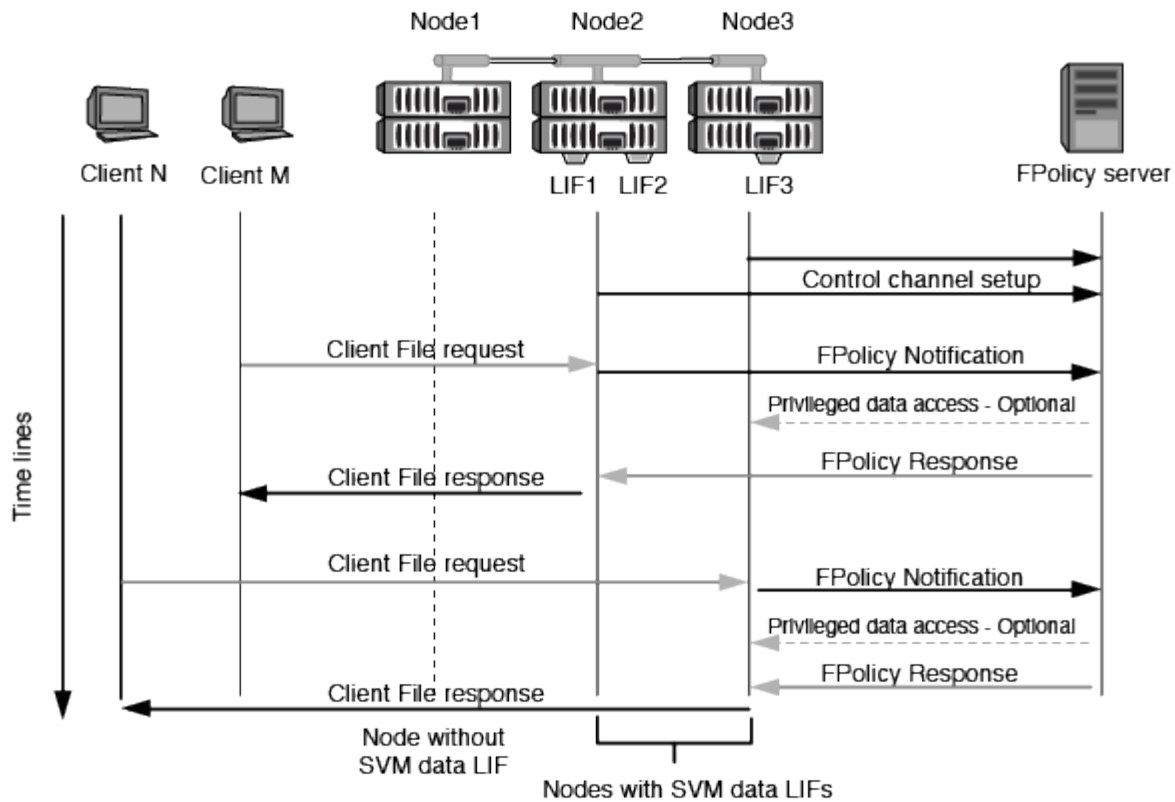
To properly plan your FPolicy configuration, you should understand what the node-to-external FPolicy server communication process is.

Every node that participates on each storage virtual machine (SVM) initiates a connection to an external FPolicy server (FPolicy server) using TCP/IP. Connections to the FPolicy servers are set up using node data LIFs; therefore, a participating node can set up a connection only if the node has an operational data LIF for the SVM.

Each FPolicy process on participating nodes attempts to establish a connection with the FPolicy server when the policy is enabled. It uses the IP address and port of the FPolicy external engine specified in the policy configuration.

The connection establishes a control channel from each of the nodes participating on each SVM to the FPolicy server through the data LIF. In addition, if IPv4 and IPv6 data LIF addresses are present on the same participating node, FPolicy attempts to establish connections for both IPv4 and IPv6. Therefore, in a scenario where the SVM extends over multiple nodes or if both IPv4 and IPv6 addresses are present, the FPolicy server must be ready for multiple control channel setup requests from the cluster after the FPolicy policy is enabled on the SVM.

For example, if a cluster has three nodes—Node1, Node2, and Node3—and SVM data LIFs are spread across only Node2 and Node3, control channels are initiated only from Node2 and Node3, irrespective of the distribution of data volumes. Say that Node2 has two data LIFs—LIF1 and LIF2—that belong to the SVM and that the initial connection is from LIF1. If LIF1 fails, FPolicy attempts to establish a control channel from LIF2.



== How FPolicy manages external communication during LIF migration or failover

Data LIFs can be migrated to data ports in the same node or to data ports on a remote node.

When a data LIF fails over or is migrated, a new control channel connection is made to the FPolicy server. FPolicy can then retry SMB and NFS client requests that timed out, with the result that new notifications are sent to the external FPolicy servers. The node rejects FPolicy server responses to original, timed-out SMB and NFS requests.

== How FPolicy manages external communication during node failover

If the cluster node that hosts the data ports used for FPolicy communication fails, ONTAP breaks the connection between the FPolicy server and the node.

The impact of cluster failover to the FPolicy server can be mitigated by configuring the LIF manager to migrate the data port used in FPolicy communication to another active node. After the migration is complete, a new connection is established using the new data port.

If the LIF manager is not configured to migrate the data port, the FPolicy server must wait for the failed node to come up. After the node is up, a new connection is initiated from that node with a new Session ID.

The FPolicy server detects broken connections with the keep-alive protocol message. The timeout for purging the session ID is determined when configuring FPolicy. The default keep-alive timeout is two minutes.

= How FPolicy services work across SVM namespaces

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

ONTAP provides a unified storage virtual machine (SVM) namespace. Volumes across the cluster are joined together by junctions to provide a single, logical file system. The FPolicy server is aware of the namespace topology and provides FPolicy services across the namespace.

The namespace is specific to and contained within the SVM; therefore, you can see the namespace only from the SVM context. Namespaces have the following characteristics:

- A single namespace exists in each SVM, with the root of the namespace being the root volume, represented in the namespace as slash (/).
- All other volumes have junction points below the root (/).
- Volume junctions are transparent to clients.
- A single NFS export can provide access to the complete namespace; otherwise, export policies can export specific volumes.
- SMB shares can be created on the volume or on qtrees within the volume, or on any directory within the namespace.
- The namespace architecture is flexible.

Examples of typical namespace architectures are as follows:

- A namespace with a single branch off of the root
- A namespace with multiple branches off of the root
- A namespace with multiple unbranched volumes off of the root

= FPolicy configuration types

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

There are two basic FPolicy configuration types. One configuration uses external FPolicy servers to process and act upon notifications. The other configuration does not use external FPolicy servers; instead, it uses the ONTAP internal, native FPolicy server for simple file blocking based on extensions.

- **External FPolicy server configuration**

The notification is sent to the FPolicy server, which screens the request and applies rules to determine whether the node should allow the requested file operation. For synchronous policies, the FPolicy server then sends a response to the node to either allow or block the requested file operation.

- **Native FPolicy server configuration**

The notification is screened internally. The request is allowed or denied based on file extension settings configured in the FPolicy scope.

## == When to create a native FPolicy configuration

Native FPolicy configurations use the ONTAP internal FPolicy engine to monitor and block file operations based on the file's extension. This solution does not require external FPolicy servers (FPolicy servers). Using a native file blocking configuration is appropriate when this simple solution is all that is needed.

Native file blocking enables you to monitor any file operations that match configured operation and filtering events and then deny access to files with particular extensions. This is the default configuration.

This configuration provides a means to block file access based only on the file's extension. For example, to block files that contain `mp3` extensions, you configure a policy to provide notifications for certain operations with target file extensions of `mp3`. The policy is configured to deny `mp3` file requests for operations that generate notifications.

The following applies to native FPolicy configurations:

- The same set of filters and protocols that are supported by FPolicy server-based file screening are also supported for native file blocking.
- Native file blocking and FPolicy server-based file screening applications can be configured at the same time.

To do so, you can configure two separate FPolicy policies for the storage virtual machine (SVM), with one configured for native file blocking and one configured for FPolicy server-based file screening.

- The native file blocking feature only screens files based on the extensions and not on the content of the file.
- In the case of symbolic links, native file blocking uses the file extension of the root file.

## == When to create a configuration that uses external FPolicy servers

FPolicy configurations that use external FPolicy servers to process and manage notifications provide robust solutions for use cases where more than simple file blocking based on file extension is needed.

You should create a configuration that uses external FPolicy servers when you want to do such things as monitor and record file access events, provide quota services, perform file blocking based on criteria other than simple file extensions, provide data migration services using hierarchical storage management applications, or provide a fine-grained set of policies that monitor only a subset of data in the storage virtual machine (SVM).

= How FPolicy passthrough-read enhances usability for hierarchical storage management

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injpo/source/./authentication/./media/

Passthrough-read enables the FPolicy server (functioning as the hierarchical storage management (HSM) server) to provide read access to offline files without having to recall the file from the secondary storage system to the primary storage system.

When an FPolicy server is configured to provide HSM to files residing on a SMB server, policy-based file migration occurs where the files are stored offline on secondary storage and only a stub file remains on primary storage. Even though a stub file appears as a normal file to clients, it is actually a sparse file that is the same size of the original file. The sparse file has the SMB offline bit set and points to the actual file that has been migrated to secondary storage.

Typically when a read request for an offline file is received, the requested content must be recalled back to primary storage and then accessed through primary storage. The need to recall data back to primary storage has several undesirable effects. Among the undesirable effects is the increased latency to client requests caused by the need to recall the content before responding to the request and the increased space consumption needed for recalled files on the primary storage.

FPolicy passthrough-read allows the HSM server (the FPolicy server) to provide read access to migrated, offline files without having to recall the file from the secondary storage system to the primary storage system. Instead of recalling the files back to primary storage, read requests can be serviced directly from secondary storage.

Copy Offload (ODX) is not supported with FPolicy passthrough-read operation.



Passthrough-read enhances usability by providing the following benefits:

- Read requests can be serviced even if the primary storage does not have sufficient space to recall requested data back to primary storage.
- Better capacity and performance management when a surge of data recall might occur, such as if a script or a backup solution needs to access many offline files.
- Read requests for offline files in Snapshot copies can be serviced.

Because Snapshot copies are read-only, the FPolicy server cannot restore the original file if the stub file is located in a Snapshot copy. Using passthrough-read eliminates this problem.

- Policies can be set up that control when read requests are serviced through access to the file on secondary storage and when the offline file should be recalled to primary storage.

For example, a policy can be created on the HSM server that specifies the number of times the offline file can be accessed in a specified period of time before the file is migrated back to primary storage. This type of policy avoids recalling files that are rarely accessed.

== How read requests are managed when FPolicy passthrough-read is enabled

You should understand how read requests are managed when FPolicy passthrough-read is enabled so that you can optimally configure connectivity between the storage virtual machine (SVM) and the FPolicy servers.

When FPolicy passthrough-read is enabled and the SVM receives a request for an offline file, FPolicy sends a notification to the FPolicy server (HSM server) through the standard connection channel.

After receiving the notification, the FPolicy server reads the data from the file path sent in the notification and sends the requested data to the SVM through the passthrough-read privileged data connection that is established between the SVM and the FPolicy server.

After the data is sent, the FPolicy server then responds to the read request as an ALLOW or DENY. Based on whether the read request is allowed or denied, ONTAP either sends the requested information or sends an error message to the client.

= Requirements, considerations, and best practices for configuring FPolicy

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

Before you create and configure FPolicy configurations on your storage virtual machines (SVMs), you need to be aware of certain requirements, considerations, and best practices for configuring FPolicy.

== Ways to configure FPolicy

FPolicy features are configured either through the command line interface (CLI) or through APIs. This guide uses the CLI to create, manage, and monitor an FPolicy configuration on the cluster.

== Requirements for setting up FPolicy

Before you configure and enable FPolicy on your storage virtual machine (SVM), you need to be aware of

certain requirements.

- All nodes in the cluster must be running a version of ONTAP that supports FPolicy.
- If you are not using the ONTAP native FPolicy engine, you must have external FPolicy servers (FPolicy servers) installed.
- The FPolicy servers must be installed on a server accessible from the data LIFs of the SVM where FPolicy policies are enabled.
- The IP address of the FPolicy server must be configured as a primary or secondary server in the FPolicy policy external engine configuration.
- If the FPolicy servers access data over a privileged data channel, the following additional requirements must be met:
  - SMB must be licensed on the cluster.

Privileged data access is accomplished using SMB connections.

- A user credential must be configured for accessing files over the privileged data channel.
- The FPolicy server must run under the credentials configured in the FPolicy configuration.
- All data LIFs used to communicate with the FPolicy servers must be configured to have `cifs` as one of the allowed protocols.

This includes the LIFs used for passthrough-read connections.

== Best practices and recommendations when setting up FPolicy

When setting up FPolicy on storage virtual machines (SVMs), you need to be familiar with configuration best practices and recommendations to ensure that your FPolicy configuration provides robust monitoring performance and results that meet your requirements.

- External FPolicy servers (FPolicy servers) should be placed in close proximity to the cluster with high-bandwidth connectivity to provide minimal latency and high-bandwidth connectivity.
- The FPolicy external engine should be configured with more than one FPolicy server to provide resiliency and high availability of FPolicy server notification processing, especially if policies are configured for synchronous screening.
- It is recommended that you disable the FPolicy policy before making any configuration changes.

For example, if you want to add or modify an IP address in the FPolicy external engine configured for the enabled policy, you should first disable the policy.

- The cluster node-to-FPolicy server ratio should be optimized to ensure that FPolicy servers are not overloaded, which can introduce latencies when the SVM responds to client requests.

The optimal ratio depends on the application for which the FPolicy server is being used.

== Passthrough-read upgrade and revert considerations

There are certain upgrade and revert considerations that you must know about before upgrading to an ONTAP release that supports passthrough-read or before reverting to a release that does not support passthrough-read.

=== Upgrading

After all nodes are upgraded to a version of ONTAP that supports FPolicy passthrough-read, the cluster is capable of using the passthrough-read functionality; however, passthrough-read is disabled by default on existing FPolicy configurations. To use passthrough-read on existing FPolicy configurations, you must disable the FPolicy policy and modify the configuration, and then reenables the configuration.

=== Reverting

Before reverting to a version of ONTAP that does not support FPolicy passthrough-read, the following conditions must be met:

- All the policies using passthrough-read must be disabled, and then the affected configurations must be modified so that they do not use passthrough-read.
- FPolicy functionality must be disabled on the cluster by disabling every FPolicy policy on the cluster.

= What the steps for setting up an FPolicy configuration are

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

Before FPolicy can monitor file access, an FPolicy configuration must be created and enabled on the storage virtual machine (SVM) for which FPolicy services are required.

The steps for setting up and enabling an FPolicy configuration on the SVM are as follows:

1. Create an FPolicy external engine.

The FPolicy external engine identifies the external FPolicy servers (FPolicy servers) that are associated with a specific FPolicy configuration. If the internal “native” FPolicy engine is used to create a native file-blocking configuration, you do not need to create an FPolicy external engine.

2. Create an FPolicy event.

An FPolicy event describes what the FPolicy policy should monitor. Events consist of the protocols and file operations to monitor, and can contain a list of filters. Events use filters to narrow the list of monitored events for which the FPolicy external engine must send notifications. Events also specify whether the policy monitors volume operations.

3. Create an FPolicy policy.

The FPolicy policy is responsible for associating, with the appropriate scope, the set of events that need to be monitored and for which of the monitored events notifications must be sent to the designated FPolicy server (or to the native engine if no FPolicy servers are configured). The policy also defines whether the FPolicy server is allowed privileged access to the data for which it receives notifications. An FPolicy server needs privileged access if the server needs to access the data. Typical use cases where privileged access is needed include file blocking, quota management, and hierarchical storage management. The policy is where you specify whether the configuration for this policy uses an FPolicy server or the internal “native” FPolicy server.

A policy specifies whether screening is mandatory. If screening is mandatory and all FPolicy servers are down or no response is received from the FPolicy servers within a defined timeout period, then file access is denied.

A policy’s boundaries are the SVM. A policy cannot apply to more than one SVM. However, a specific

SVM can have multiple FPolicy policies, each with the same or different combination of scope, event, and external server configurations.

4. Configure the policy scope.

The FPolicy scope determines which volumes, shares, or export-policies the policy acts on or excludes from monitoring. A scope also determines which file extensions should be included or excluded from FPolicy monitoring.

Exclude lists take precedence over include lists.

1. Enable the FPolicy policy.

When the policy is enabled, the control channels and, optionally, the privileged data channels are connected. The FPolicy process on the nodes on which the SVM participates begin monitoring file and folder access and, for events that match configured criteria, sends notifications to the FPolicy servers (or to the native engine if no FPolicy servers are configured).

If the policy uses native file blocking, an external engine is not configured or associated with the policy.

= Plan the FPolicy configuration

= Plan the FPolicy external engine configuration

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

Before you configure the FPolicy external engine (external engine), you must understand what it means to create an external engine and which configuration parameters are available. This information helps you to determine which values to set for each parameter.

== Information that is defined when creating the FPolicy external engine

The external engine configuration defines the information that FPolicy needs to make and manage connections to the external FPolicy servers (FPolicy servers), including the following information:

- SVM name
- Engine name
- The IP addresses of the primary and secondary FPolicy servers and the TCP port number to use when making the connection to the FPolicy servers
- Whether the engine type is asynchronous or synchronous
- How to authenticate the connection between the node and the FPolicy server

If you choose to configure mutual SSL authentication, then you must also configure parameters that provide SSL certificate information.

- How to manage the connection using various advanced privilege settings

This includes parameters that define such things as timeout values, retry values, keep-alive values, maximum request values, sent and receive buffer size values, and session timeout values.

The `vserver fpolicy policy external-engine create` command is used to create an FPolicy external engine.

== What the basic external engine parameters are

You can use the following table of basic FPolicy configuration parameters to help you plan your configuration:

Type of information	Option
---------------------	--------

### *SVM*

Specifies the SVM name that you want to associate with this external engine.

Each FPolicy configuration is defined within a single SVM. The external engine, policy event, policy scope, and policy that combine together to create an FPolicy policy configuration must all be associated with the same SVM.

`-vserver vserver_name`

The name should be up to 200 characters long if configuring the external engine name in a MetroCluster or SVM disaster recovery configuration.

The name can contain any combination of the following ASCII-range characters:

- a through z
- A through Z
- 0 through 9
- “\_”, “-”, and “.”

a|

-engine-name engine\_name

a|

*Primary FPolicy servers*

Specifies the primary FPolicy servers to which the node sends notifications for a given FPolicy policy. The value is specified as a comma-delimited list of IP addresses.

If more than one primary server IP address is specified, every node on which the SVM participates creates a control connection to every specified primary FPolicy server at the time the policy is enabled. If you configure multiple primary FPolicy servers, notifications are sent to the FPolicy servers in a round-robin fashion.

If the external engine is used in a MetroCluster or SVM disaster recovery configuration, you should specify the IP addresses of the FPolicy servers at the source site as primary servers. The IP addresses of the FPolicy servers at the destination site should be specified as secondary servers.

a|

-primary-servers IP\_address,...

a|

*Port number*

Specifies the port number of the FPolicy service.

a|

-port integer

a|

*Secondary FPolicy servers*

Specifies the secondary FPolicy servers to which to send file access events for a given FPolicy policy. The value is specified as a comma-delimited list of IP addresses.

Secondary servers are used only when none of the primary servers are reachable. Connections to secondary servers are established when the policy is enabled, but notifications are sent to secondary servers only if none of the primary servers are reachable. If you configure multiple secondary servers, notifications are sent to the FPolicy servers in a round-robin fashion.

a|

-secondary-servers IP\_address,...

a|

*External engine type*

Specifies whether the external engine operates in synchronous or asynchronous mode. By default, FPolicy operates in synchronous mode.

When set to `synchronous`, file request processing sends a notification to the FPolicy server, but then does not continue until after receiving a response from the FPolicy server. At that point, request flow either continues or processing results in denial, depending on whether the response from the FPolicy server permits the requested action.

When set to `asynchronous`, file request processing sends a notification to the FPolicy server, and then continues.

a|

`-extern-engine-type external_engine_type` The value for this parameter can be one of the following:

- `synchronous`
- `asynchronous`

a|

*SSL option for communication with FPolicy server*

Specifies the SSL option for communication with the FPolicy server. This is a required parameter. You can choose one of the options based on the following information:

- When set to `no-auth`, no authentication takes place.

The communication link is established over TCP.

- When set to `server-auth`, the SVM authenticates the FPolicy server using SSL server authentication.
- When set to `mutual-auth`, mutual authentication takes place between the SVM and the FPolicy server; the SVM authenticates the FPolicy server, and the FPolicy server authenticates the SVM.

If you choose to configure mutual SSL authentication, then you must also configure the `-certificate-common-name`, `-certificate-serial`, and `-certificate-ca` parameters.

a|

`-ssl-option {no-auth|server-auth|mutual-auth}`

a|

*Certificate FQDN or custom common name*

Specifies the certificate name used if SSL authentication between the SVM and the FPolicy server is configured. You can specify the certificate name as an FQDN or as a custom common name.

If you specify `mutual-auth` for the `-ssl-option` parameter, you must specify a value for the `-certificate-common-name` parameter.

a|

`-certificate-common-name text`

a|

*Certificate serial number*

Specifies the serial number of the certificate used for authentication if SSL authentication between the SVM and the FPolicy server is configured.



If you specify `mutual-auth` for the `-ssl-option` parameter, you must specify a value for the `-certificate-serial` parameter.

```
a|  
-certificate-serial text
```

```
a|  
Certificate authority
```

Specifies the CA name of the certificate used for authentication if SSL authentication between the SVM and the FPolicy server is configured.

If you specify `mutual-auth` for the `-ssl-option` parameter, you must specify a value for the `-certificate-ca` parameter.

```
a|  
-certificate-ca text
```

== What the advanced external engine options are

You can use the following table of advanced FPolicy configuration parameters as you plan whether to customize your configuration with advanced parameters. You use these parameters to modify communication behavior between the cluster nodes and the FPolicy servers:

```
[cols="70,30"]
```

h  Type of information	h  Option
------------------------	-----------

a	<i>Timeout for canceling a request</i>
---	--

Specifies the time interval in hours (h), minutes (m), or seconds (s) that the node waits for a response from the FPolicy server.

If the timeout interval passes, the node sends a cancel request to the FPolicy server. The node then sends the notification to an alternate FPolicy server. This timeout helps in handling an FPolicy server that is not responding, which can improve SMB/NFS client response. Also, canceling requests after a timeout period can help in releasing system resources because the notification request is moved from a down/bad FPolicy server to an alternate FPolicy server.

The range for this value is 0 through 100. If the value is set to 0, the option is disabled and cancel request messages are not sent to the FPolicy server. The default is 20s.

a	<code>-reqs-cancel-timeout integer[h m s]</code>
---	--

a	<i>Timeout for aborting a request</i>
---	---------------------------------------

Specifies the timeout in hours (h), minutes (m), or seconds (s) for aborting a request.

The range for this value is 0 through 200.

a	<code>-reqs-abort-timeout ` `integer[h m s]</code>
---	--

a	
---	--

### *Interval for sending status requests*

Specifies the interval in hours (h), minutes (m), or seconds (s) after which a status request is sent to the FPolicy server.

The range for this value is 0 through 50. If the value is set to 0, the option is disabled and status request messages are not sent to the FPolicy server. The default is 10s.

a|  
-status-req-interval integer[h|m|s]

### *Maximum outstanding requests on the FPolicy server*

Specifies the maximum number of outstanding requests that can be queued on the FPolicy server.

The range for this value is 1 through 10000. The default is 50.

a|  
-max-server-reqs integer

### *Timeout for disconnecting a nonresponsive FPolicy server*

Specifies the time interval in hours (h), minutes (m), or seconds (s) after which the connection to the FPolicy server is terminated.

The connection is terminated after the timeout period only if the FPolicy server's queue contains the maximum allowed requests and no response is received within the timeout period. The maximum allowed number of requests is either 50 (the default) or the number specified by the `max-server-reqs` parameter.

The range for this value is 1 through 100. The default is 60s.

a|  
-server-progress-timeout integer[h|m|s]

### *Interval for sending keep-alive messages to the FPolicy server*

Specifies the time interval in hours (h), minutes (m), or seconds (s) at which keep-alive messages are sent to the FPolicy server.

Keep-alive messages detect half-open connections.

The range for this value is 10 through 600. If the value is set to 0, the option is disabled and keep-alive messages are prevented from being sent to the FPolicy servers. The default is 120s.

a|  
-keep-alive-interval- integer[h|m|s]

### *Maximum reconnect attempts*

Specifies the maximum number of times the SVM attempts to reconnect to the FPolicy server after the connection has been broken.

The range for this value is 0 through 20. The default is 5.

a|  
-max-connection-retries integer

a|  
*Receive buffer size*

Specifies the receive buffer size of the connected socket for the FPolicy server.

The default value is set to 256 kilobytes (Kb). When the value is set to 0, the size of the receive buffer is set to a value defined by the system.

For example, if the default receive buffer size of the socket is 65536 bytes, by setting the tunable value to 0, the socket buffer size is set to 65536 bytes. You can use any non-default value to set the size (in bytes) of the receive buffer.

a|  
-recv-buffer-size integer

a|  
*Send buffer size*

Specifies the send buffer size of the connected socket for the FPolicy server.

The default value is set to 256 kilobytes (Kb). When the value is set to 0, the size of the send buffer is set to a value defined by the system.

For example, if the default send buffer size of the socket is set to 65536 bytes, by setting the tunable value to 0, the socket buffer size is set to 65536 bytes. You can use any non-default value to set the size (in bytes) of the send buffer.

a|  
-send-buffer-size integer

a|  
*Timeout for purging a session ID during reconnection*

Specifies the interval in hours (h), minutes (m), or seconds (s) after which a new session ID is sent to the FPolicy server during reconnection attempts.

If the connection between the storage controller and the FPolicy server is terminated and reconnection is made within the `-session-timeout` interval, the old session ID is sent to FPolicy server so that it can send responses for old notifications.

The default value is set to 10 seconds.

a|  
-session-timeout [integerh][integerm][integer s]

:leveloffset: +1

= Additional information about configuring FPolicy external engines to use SSL authenticated connections

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

[.lead]

You need to know some additional information if you want to configure the FPolicy external engine to use SSL when connecting to FPolicy servers.

== SSL server authentication

If you choose to configure the FPolicy external engine for SSL server authentication, before creating the external engine, you must install the public certificate of the certificate authority (CA) that signed the FPolicy server certificate.

== Mutual authentication

If you configure FPolicy external engines to use SSL mutual authentication when connecting storage virtual machine (SVM) data LIFs to external FPolicy servers, before creating the external engine, you must install the public certificate of the CA that signed the FPolicy server certificate along with the public certificate and key file for authentication of the SVM. You must not delete this certificate while any FPolicy policies are using the installed certificate.

If the certificate is deleted while FPolicy is using it for mutual authentication when connecting to an external FPolicy server, you cannot reenab a disabled FPolicy policy that uses that certificate. The FPolicy policy cannot be reenabled in this situation even if a new certificate with the same settings is created and installed on the SVM.

If the certificate has been deleted, you need to install a new certificate, create new FPolicy external engines that use the new certificate, and associate the new external engines with the FPolicy policy that you want to reenab by modifying the FPolicy policy.

== Install certificates for SSL

The public certificate of the CA that is used to sign the FPolicy server certificate is installed by using the `security certificate install` command with the `-type` parameter set to `client_ca`. The private key and public certificate required for authentication of the SVM is installed by using the `security certificate install` command with the `-type` parameter set to `server`.

= Certificates do not replicate in SVM disaster recovery relationships with a non-ID-preserve configuration

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

[.lead]

h| Configuration h| Permitted?

a|

MetroCluster or SVM disaster recovery and a cluster-scoped FPolicy external engine with no authentication (SSL is not configured)

a|

Yes

a|

MetroCluster or SVM disaster recovery and a cluster-scoped FPolicy external engine with SSL server or SSL mutual authentication

a|

No

\* If a cluster-scoped FPolicy external engine with SSL authentication exists and you want to create a MetroCluster or SVM disaster recovery configuration, you must modify this external engine to use no authentication or remove the external engine before you can create the MetroCluster or SVM disaster recovery configuration.

\* If the MetroCluster or SVM disaster recovery configuration already exists, ONTAP prevents you from creating a cluster-scoped FPolicy external engine with SSL authentication.

= Complete the FPolicy external engine configuration worksheet

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

[.lead]

You can use this worksheet to record the values that you need during the FPolicy external engine configuration process. If a parameter value is required, you need to determine what value to use for those parameters before you configure the external engine.

== Information for a basic external engine configuration

You should record whether you want to include each parameter setting in the external engine configuration and then record the value for the parameters that you want to include.

[cols="40,20,20,20"]

h| Type of information h| Required h| Include h| Your values

a|

Storage virtual machine (SVM) name

a|

Yes

a|

Yes

a|

a|

Engine name

a|

Yes

a|

Yes

a|

a|

Primary FPolicy servers

a|

Yes

a|

Yes

a|

a|

Port number

a|

Yes

a|

Yes

a|

a|

Secondary FPolicy servers

a|

No

a|

a|

a|

External engine type

a|

No

a|

a|

a|

SSL option for communication with external FPolicy server

a|

Yes

a|

Yes

a|

a|

Certificate FQDN or custom common name

a|

No

a|

a|

a|

Certificate serial number

a|  
No  
a|  
  
a|  
  
a|  
Certificate authority  
a|  
No  
a|  
  
a|

== Information for advanced external engine parameters

To configure an external engine with advanced parameters, you must enter the configuration command while in advanced privilege mode.

[cols="40,20,20,20"]

h| Type of information h| Required h| Include h| Your values

a|  
Timeout for canceling a request  
a|  
No  
a|

a|

a|  
Timeout for aborting a request  
a|  
No  
a|

a|

a|  
Interval for sending status requests  
a|  
No  
a|

a|

a|  
Maximum outstanding requests on the FPolicy server  
a|  
No  
a|

a|

a|  
Timeout for disconnecting a nonresponsive FPolicy server

a|  
No  
a|

a|

a|  
Interval for sending keep-alive messages to the FPolicy server

a|  
No  
a|

a|

a|  
Maximum reconnect attempts

a|  
No  
a|

a|

a|  
Receive buffer size

a|  
No  
a|

a|

a|  
Send buffer size

a|  
No  
a|

a|

a|  
Timeout for purging a session ID during reconnection

a|  
No  
a|

a|



:leveloffset: -1

= Plan the FPolicy event configuration

:leveloffset: +1

= Plan the FPolicy event configuration overview

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injpo/source/./authentication/./media/

[.lead]

Before you configure FPolicy events, you must understand what it means to create an FPolicy event. You must determine which protocols you want the event to monitor, which events to monitor, and which event filters to use. This information helps you plan the values that you want to set.

== What it means to create an FPolicy event

Creating the FPolicy event means defining information that the FPolicy process needs to determine what file access operations to monitor and for which of the monitored events notifications should be sent to the external FPolicy server. The FPolicy event configuration defines the following configuration information:

\* Storage virtual machine (SVM) name

\* Event name

\* Which protocols to monitor

+

FPolicy can monitor SMB, NFSv3, and NFSv4 file access operations.

\* Which file operations to monitor

+

Not all file operations are valid for each protocol.

\* Which file filters to configure

+

Only certain combinations of file operations and filters are valid. Each protocol has its own set of supported combinations.

\* Whether to monitor volume mount and unmount operations

[NOTE]

There is a dependency with three of the parameters (`-protocol`, `-file-operations`, `-filters`). The following combinations are valid for the three parameters:

- You can specify the `-protocol` and `-file-operations` parameters.
- You can specify all three of the parameters.
- You can specify none of the parameters.

== What the FPolicy event configuration contains

You can use the following list of available FPolicy event configuration parameters to help you plan your configuration:

Type of information	Option
<p><b>SVM</b></p> <p>Specifies the SVM name that you want to associate with this FPolicy event.</p> <p>Each FPolicy configuration is defined within a single SVM. The external engine, policy event, policy scope, and policy that combine together to create an FPolicy policy configuration must all be associated with the same SVM.</p>	<p><code>-vserver vserver_name</code></p>

The name should be up to 200 characters long if configuring the event in a MetroCluster or SVM disaster recovery configuration.

The name can contain any combination of the following ASCII-range characters:

- a through z
- A through Z
- 0 through 9
- " \_ ", "-", and "."

a|  
-event-name event\_name  
a|  
*Protocol*

Specifies which protocol to configure for the FPolicy event. The list for `-protocol` can include one of the following values:

- `cifs`
- `nfsv3`
- `nfsv4`

If you specify `-protocol`, then you must specify a valid value in the `-file-operations` parameter. As the protocol version changes, the valid values might change.

```
a|
-protocol protocol
```

```
a|
File operations
```

Specifies the list of file operations for the FPolicy event.

The event checks the operations specified in this list from all client requests using the protocol specified in the `-protocol` parameter. You can list one or more file operations by using a comma-delimited list. The list for `-file-operations` can include one or more of the following values:

- `close` for file close operations
- `create` for file create operations
- `create-dir` for directory create operations
- `delete` for file delete operations
- `delete_dir` for directory delete operations
- `getattr` for get attribute operations
- `link` for link operations
- `lookup` for lookup operations
- `open` for file open operations
- `read` for file read operations
- `write` for file write operations
- `rename` for file rename operations
- `rename_dir` for directory rename operations
- `setattr` for set attribute operations
- `symlink` for symbolic link operations

If you specify `-file-operations`, then you must specify a valid protocol in the `-protocol` parameter.

```
a|
-file-operations file_operations,...
```

```
a|
Filters
```

Specifies the list of filters for a given file operation for the specified protocol. The values in the `-filters` parameter are used to filter client requests. The list can include one or more of the following:

If you specify the `-filters` parameter, then you must also specify valid values for the `-file-operations` and `-protocol` parameters.

- `monitor-ads` option to filter the client request for alternate data stream.
- `close-with-modification` option to filter the client request for close with modification.
- `close-without-modification` option to filter the client request for close without modification.
- `first-read` option to filter the client request for first read.
- `first-write` option to filter the client request for first write.
- `offline-bit` option to filter the client request for offline bit set.

Setting this filter results in the FPolicy server receiving notification only when offline files are accessed.

- `open-with-delete-intent` option to filter the client request for open with delete intent.

Setting this filter results in the FPolicy server receiving notification only when an attempt is made to open a file with the intent to delete it. This is used by file systems when the `FILE_DELETE_ON_CLOSE` flag is specified.

- `open-with-write-intent` option to filter client request for open with write intent.

Setting this filter results in the FPolicy server receiving notification only when an attempt is made to open a file with the intent to write something in it.

- `write-with-size-change` option to filter the client request for write with size change.

```
a|
-filters filter, ...
```

```
a|
Filters continued
```

- `setattr-with-owner-change` option to filter the client setattr requests for changing owner of a file or a directory.
- `setattr-with-group-change` option to filter the client setattr requests for changing the group of a file or a directory.
- `setattr-with-sacl-change` option to filter the client setattr requests for changing the SAACL on a file or a directory.

This filter is available only for the SMB and NFSv4 protocols.

- `setattr-with-dacl-change` option to filter the client setattr requests for changing the DACL on a file or a directory.

This filter is available only for the SMB and NFSv4 protocols.

- `setattr-with-modify-time-change` option to filter the client setattr requests for changing the modification time of a file or a directory.
- `setattr-with-access-time-change` option to filter the client setattr requests for changing the access time of a file or a directory.
- `setattr-with-creation-time-change` option to filter the client setattr requests for changing the creation time of a file or a directory.

This option is available only for the SMB protocol.

- `setattr-with-mode-change` option to filter the client setattr requests for changing the mode bits on a file or a directory.
- `setattr-with-size-change` option to filter the client setattr requests for changing the size of a file.
- `setattr-with-allocation-size-change` option to filter the client setattr requests for changing the allocation size of a file.

This option is available only for the SMB protocol.

- `exclude-directory` option to filter the client requests for directory operations.

When this filter is specified, the directory operations are not monitored.

```
a|
-filters filter, ...
a|
Is volume operation required
```

Specifies whether monitoring is required for volume mount and unmount operations. The default is `false`.

```
a|
-volume-operation {true|false}
```

= List of supported file operation and filter combinations that FPolicy can monitor for SMB

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injpo/source/./authentication/./media/

[.lead]

When you configure your FPolicy event, you need to be aware that only certain combinations of file operations and filters are supported for monitoring SMB file access operations.

The list of supported file operation and filter combinations for FPolicy monitoring of SMB file access events is provided in the following table:

[cols="30,70"]

h  Supported file operations	h  Supported filters
------------------------------	----------------------

a  close	
a  monitor-ads, offline-bit, close-with-modification, close-without-modification, close-with-read, exclude-directory	
a  create	
a  monitor-ads, offline-bit	

a|  
create\_dir  
a|  
Currently no filter is supported for this file operation.  
a|  
delete  
a|  
monitor-ads, offline-bit  
a|  
delete\_dir  
a|  
Currently no filter is supported for this file operation.  
a|  
getattr  
a|  
offline-bit, exclude-dir  
a|  
open  
a|  
monitor-ads, offline-bit, open-with-delete-intent, open-with-write-intent, exclude-dir  
a|  
read  
a|  
monitor-ads, offline-bit, first-read  
a|  
write  
a|  
monitor-ads, offline-bit, first-write, write-with-size-change  
a|  
rename  
a|  
monitor-ads, offline-bit  
a|  
rename\_dir  
a|  
Currently no filter is supported for this file operation.  
a|  
setattr  
a|  
monitor-ads, offline-bit, setattr\_with\_owner\_change, setattr\_with\_group\_change,  
setattr\_with\_mode\_change, setattr\_with\_sacl\_change, setattr\_with\_dacl\_change,  
setattr\_with\_modify\_time\_change, setattr\_with\_access\_time\_change,  
setattr\_with\_creation\_time\_change, setattr\_with\_size\_change, setattr\_with\_allocation\_size\_change,  
exclude\_directory

= Supported file operation and filter combinations that FPolicy can monitor for NFSv3

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

[.lead]

When you configure your FPolicy event, you need to be aware that only certain combinations of file operations and filters are supported for monitoring NFSv3 file access operations.

The list of supported file operation and filter combinations for FPolicy monitoring of NFSv3 file access events is provided in the following table:

[cols="30,70"]

h| Supported file operations h| Supported filters

a|

create

a|

offline-bit

a|

create\_dir

a|

Currently no filter is supported for this file operation.

a|

delete

a|

offline-bit

a|

delete\_dir

a|

Currently no filter is supported for this file operation.

a|

link

a|

offline-bit

a|

lookup

a|

offline-bit, exclude-dir

a|

read

a|

offline-bit, first-read

a|

write

a|

offline-bit, first-write, write-with-size-change

a|

rename

a|

offline-bit

a|

rename\_dir

a|

Currently no filter is supported for this file operation.

a|

setattr

a|

offline-bit, setattr\_with\_owner\_change, setattr\_with\_group\_change, setattr\_with\_mode\_change, setattr\_with\_modify\_time\_change, setattr\_with\_access\_time\_change, setattr\_with\_size\_change, exclude\_directory

a|

symlink

a|

offline-bit

= Supported file operation and filter combinations that FPolicy can monitor for NFSv4

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

[.lead]

When you configure your FPolicy event, you need to be aware that only certain combinations of file operations and filters are supported for monitoring NFSv4 file access operations.

The list of supported file operation and filter combinations for FPolicy monitoring of NFSv4 file access events is provided in the following table:

[cols="30,70"]

h| Supported file operations h| Supported filters

a|

close

a|

offline-bit, exclude-directory

a|

create

a|

offline-bit

a|

create\_dir

a|

Currently no filter is supported for this file operation.

a|

delete

a|

offline-bit

a|

delete\_dir

a|

Currently no filter is supported for this file operation.

a|

getattr

a|



offline-bit, exclude-directory  
a|  
link  
a|  
offline-bit  
a|  
lookup  
a|  
offline-bit, exclude-directory  
a|  
open  
a|  
offline-bit, exclude-directory  
a|  
read  
a|  
offline-bit, first-read  
a|  
write  
a|  
offline-bit, first-write, write-with-size-change  
a|  
rename  
a|  
offline-bit  
a|  
rename\_dir  
a|  
Currently no filter is supported for this file operation.  
a|  
setattr  
a|  
offline-bit, setattr\_with\_owner\_change, setattr\_with\_group\_change, setattr\_with\_mode\_change,  
setattr\_with\_sacl\_change, setattr\_with\_dacl\_change, setattr\_with\_modify\_time\_change,  
setattr\_with\_access\_time\_change, setattr\_with\_size\_change, exclude\_directory  
a|  
symlink  
a|  
offline-bit

= Complete the FPolicy event configuration worksheet

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

[.lead]

You can use this worksheet to record the values that you need during the FPolicy event configuration process. If a parameter value is required, you need to determine what value to use for those parameters before you configure the FPolicy event.

You should record whether you want to include each parameter setting in the FPolicy event configuration and then record the value for the parameters that you want to include.

[cols="40,20,20,20"]

h  Type of information	h  Required	h  Include	h  Your values
------------------------	-------------	------------	----------------

a  Storage virtual machine (SVM) name			
---------------------------------------	--	--	--

a  Yes			
--------	--	--	--

a  Yes			
--------	--	--	--

a			
---	--	--	--

a  Event name			
---------------	--	--	--

a  Yes			
--------	--	--	--

a  Yes			
--------	--	--	--

a			
---	--	--	--

a  Protocol			
-------------	--	--	--

a  No			
-------	--	--	--

a			
---	--	--	--

a			
---	--	--	--

a  File operations			
--------------------	--	--	--

a  No			
-------	--	--	--

a			
---	--	--	--

a			
---	--	--	--

a  Filters			
------------	--	--	--

a  No			
-------	--	--	--

a|

a|

a|

Volume operation

a|

No

a|

a|

:leveloffset: -1

= Plan the FPolicy policy configuration

:leveloffset: +1

= Plan the FPolicy policy configuration overview

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injpo/source/./authentication/./media/

[.lead]

Before you configure the FPolicy policy, you must understand which parameters are required when creating the policy as well as why you might want to configure certain optional parameters. This information helps you to determine which values to set for each parameter.

When creating an FPolicy policy you associate the policy with the following:

- \* The storage virtual machine (SVM)
- \* One or more FPolicy events
- \* An FPolicy external engine

You can also configure several optional policy settings.

== What the FPolicy policy configuration contains

You can use the following list of available FPolicy policy required and optional parameters to help you plan your configuration:

[cols="40,20,20,20"]

h| Type of information h| Option h| Required h| Default

a|

*SVM name*

Specifies the name of the SVM on which you want to create an FPolicy policy.

a|

```
-vserver vserver_name
```

```
a|
```

```
Yes
```

```
a|
```

```
None
```

```
a|
```

```
Policy name
```

Specifies the name of the FPolicy policy.

The name can be up to 256 characters long.

The name should be up to 200 characters long if configuring the policy in a MetroCluster or SVM disaster recovery configuration.

The name can contain any combination of the following ASCII-range characters:

- a through z
- A through Z
- 0 through 9
- “\_”, “-”, and “.”

```
a|  
-policy-name policy_name  
a|  
Yes  
a|  
None  
a|  
Event names
```

Specifies a comma-delimited list of events to associate with the FPolicy policy.

- You can associate more than one event to a policy.
- An event is specific to a protocol.
- You can use a single policy to monitor file access events for more than one protocol by creating an event for each protocol that you want the policy to monitor, and then associating the events to the policy.
- The events must already exist.

```
a|  
-events event_name, ...  
a|  
Yes  
a|  
None  
a|  
External engine name
```

Specifies the name of the external engine to associate with the FPolicy policy.

- An external engine contains information required by the node to send notifications to an FPolicy server.
- You can configure FPolicy to use the ONTAP native external engine for simple file blocking or to use an external engine that is configured to use external FPolicy servers (FPolicy servers) for more sophisticated file blocking and file management.
- If you want to use the native external engine, you can either not specify a value for this parameter or you can specify `native` as the value.
- If you want to use FPolicy servers, the configuration for the external engine must already exist.

```
a|  
-engine engine_name  
a|  
Yes (unless the policy uses the internal ONTAP native engine)
```

a|

native

a|

*Is mandatory screening required*

Specifies whether mandatory file access screening is required.

- The mandatory screening setting determines what action is taken on a file access event in a case when all primary and secondary servers are down or no response is received from the FPolicy servers within a given timeout period.
- When set to `true`, file access events are denied.
- When set to `false`, file access events are allowed.

a|

`-is-mandatory {true|false}`

a|

No

a|

`true`

a|

*Allow privileged access*

Specifies whether you want the FPolicy server to have privileged access to the monitored files and folders by using a privileged data connection.

If configured, FPolicy servers can access files from the root of the SVM containing the monitored data using the privileged data connection.

For privileged data access, SMB must be licensed on the cluster and all the data LIFs used to connect to the FPolicy servers must be configured to have `cifs` as one of the allowed protocols.

If you want to configure the policy to allow privileged access, you must also specify the user name for the account that you want the FPolicy server to use for privileged access.

a|

`-allow-privileged-access {yes|no}`

a|

No (unless passthrough-read is enabled)

a|

`no`

a|

*Privileged user name*

Specifies the user name of the account the FPolicy servers use for privileged data access.

- The value for this parameter should use the “domain\user name” format.
- If `-allow-privileged-access` is set to `no`, any value set for this parameter is ignored.

a|

`-privileged-user-name user_name`

a|

No (unless privileged access is enabled)

a|

None

a|

*Allow passthrough-read*

Specifies whether the FPolicy servers can provide passthrough-read services for files that have been archived to secondary storage (offline files) by the FPolicy servers:

- Passthrough-read is a way to read data for offline files without restoring the data to the primary storage.

Passthrough-read reduces response latencies because there is no need to recall files back to primary storage before responding to the read request. Additionally, passthrough-read optimizes storage efficiency by eliminating the need to consume primary storage space with files that are recalled solely to satisfy read requests.

- When enabled, the FPolicy servers provide the data for the file over a separate privileged data channel opened specifically for passthrough-reads.
- If you want to configure passthrough-read, the policy must also be configured to allow privileged access.

a|

`-is-passthrough-read-enabled {true|false}`

a|

No

a|

false

= Requirement for FPolicy scope configurations if the FPolicy policy uses the native engine

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

[.lead]

If you configure the FPolicy policy to use the native engine, there is a specific requirement for how you define the FPolicy scope configured for the policy.

The FPolicy scope defines the boundaries on which the FPolicy policy applies, for example whether the FPolicy applies to specified volumes or shares. There are a number of parameters that further restrict the scope to which the FPolicy policy applies. One of these parameters, `-is-file-extension-check-on-directories-enabled`, specifies whether to check file extensions on directories. The default value is `false`, which means that file extensions on directories are not checked.

When an FPolicy policy that uses the native engine is enabled on a share or volume and the `-is-file-extension-check-on-directories-enabled` parameter is set to `false` for the scope of the policy, directory access is denied. With this configuration, because the file extensions are not checked for directories, any directory operation is denied if it falls under the scope of the policy.

To ensure that directory access succeeds when using the native engine, you must set the `-is-file-extension-check-on-directories-enabled` parameter to `true` when creating the scope.

With this parameter set to `true`, extension checks happen for directory operations and the decision whether to allow or deny access is taken based on the extensions included or excluded in the FPolicy scope configuration.

= Complete the FPolicy policy worksheet

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

[.lead]

You can use this worksheet to record the values that you need during the FPolicy policy configuration process. You should record whether you want to include each parameter setting in the FPolicy policy configuration and then record the value for the parameters that you want to include.

[cols="50,25,25"]

h  Type of information	h  Include	h  Your values
a		
Storage virtual machine (SVM) name		
a		
Yes		
a		
a		
Policy name		
a		



Yes

a|

a|

Event names

a|

Yes

a|

a|

External engine name

a|

a|

a|

Is mandatory screening required?

a|

a|

a|

Allow privileged access

a|

a|

a|

Privileged user name

a|

a|

a|

Is passthrough-read enabled?

a|

a|

:leveloffset: -1

= Plan the FPolicy scope configuration

:leveloffset: +1

= Plan the FPolicy scope configuration overview

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

[.lead]

Before you configure the FPolicy scope, you must understand what it means to create a scope. You must understand what the scope configuration contains. You also need to understand what the scope rules of precedence are. This information can help you plan the values that you want to set.

== What it means to create an FPolicy scope

Creating the FPolicy scope means defining the boundaries on which the FPolicy policy applies. The storage virtual machine (SVM) is the basic boundary. When you create a scope for an FPolicy policy, you must define the FPolicy policy to which it will apply, and you must designate to which SVM you want to apply the scope.

There are a number of parameters that further restrict the scope within the specified SVM. You can restrict the scope by specifying what to include in the scope or by specifying what to exclude from the scope. After you apply a scope to an enabled policy, policy event checks get applied to the scope defined by this command.

Notifications are generated for file access events where matches are found in the “include” options. Notifications are not generated for file access events where matches are found in the “exclude” options.

The FPolicy scope configuration defines the following configuration information:

- \* SVM name
- \* Policy name
- \* The shares to include or exclude from what gets monitored
- \* The export policies to include or exclude from what gets monitored
- \* The volumes to include or exclude from what gets monitored
- \* The file extensions to include or exclude from what gets monitored
- \* Whether to do file extension checks on directory objects

[NOTE]

There are special considerations for the scope for a cluster FPolicy policy. The cluster FPolicy policy is a policy that the cluster administrator creates for the admin SVM. If the cluster administrator also creates the scope for that cluster FPolicy policy, the SVM administrator cannot create a scope for that same policy. However, if the cluster administrator does not create a scope for the cluster FPolicy policy, then any SVM administrator can create the scope for that cluster policy. If the SVM administrator creates a scope for that cluster FPolicy policy, the cluster administrator cannot subsequently create a cluster scope for that same cluster policy. This is because the cluster administrator cannot override the scope for the same cluster policy.

== What the scope rules of precedence are

The following rules of precedence apply to scope configurations:

- When a share is included in the `-shares-to-include` parameter and the parent volume of the share is included in the `-volumes-to-exclude` parameter, `-volumes-to-exclude` has precedence over `-shares-to-include`.
- When an export policy is included in the `-export-policies-to-include` parameter and the parent volume of the export policy is included in the `-volumes-to-exclude` parameter, `-volumes-to-exclude` has precedence over `-export-policies-to-include`.
- An administrator can specify both `-file-extensions-to-include` and `-file-extensions-to-exclude` lists.

The `-file-extensions-to-exclude` parameter is checked before the `-file-extensions-to-include` parameter is checked.

== What the FPolicy scope configuration contains

You can use the following list of available FPolicy scope configuration parameters to help you plan your configuration:

When configuring what shares, export policies, volumes, and file extensions to include or exclude from the scope, the include and exclude parameters can contain regular expressions and can include metacharacters such as “?” and “\*”.

Type of information	Option
<p><b>SVM</b></p> <p>Specifies the SVM name on which you want to create an FPolicy scope.</p> <p>Each FPolicy configuration is defined within a single SVM. The external engine, policy event, policy scope, and policy that combine together to create an FPolicy policy configuration must all be associated with the same SVM.</p>	<p><code>-vserver vserver_name</code></p>
<p><b>Policy name</b></p> <p>Specifies the name of the FPolicy policy to which you want to attach the scope. The FPolicy policy must already exist.</p>	<p><code>-policy-name policy_name</code></p>
<p><b>Shares to include</b></p> <p>Specifies a comma-delimited list of shares to monitor for the FPolicy policy to which the scope is applied.</p>	<p><code>-shares-to-include share_name, ...</code></p>
<p><b>Shares to exclude</b></p> <p>Specifies a comma-delimited list of shares to exclude from monitoring for the FPolicy policy to which the scope is applied.</p>	<p><code>-shares-to-exclude share_name, ...</code></p>
<p><b>Volumes to include</b> Specifies a comma-delimited list of volumes to monitor for the FPolicy policy to which the scope is applied.</p>	<p><code>-volumes-to-include volume_name, ...</code></p>
<p><b>Volumes to exclude</b></p> <p>Specifies a comma-delimited list of volumes to exclude from monitoring for the FPolicy policy to which the scope is applied.</p>	<p><code>-volumes-to-exclude volume_name, ...</code></p>
<p><b>Export policies to include</b></p> <p>Specifies a comma-delimited list of export policies to monitor for the FPolicy policy to which the scope is applied.</p>	<p><code>-export-policies-to -include export_policy_name, ...</code></p>
<p><b>Export policies to exclude</b></p> <p>Specifies a comma-delimited list of export policies to exclude from monitoring for the FPolicy policy to which the scope is applied.</p>	<p><code>-export-policies-to -exclude export_policy_name, ...</code></p>
<p><b>File extensions to include</b></p> <p>Specifies a comma-delimited list of file extensions to monitor for the FPolicy policy to which the scope is applied.</p>	<p><code>-file-extensions-to -include file_extensions, ...</code></p>

<p><i>File extension to exclude</i></p> <p>Specifies a comma-delimited list of file extensions to exclude from monitoring for the FPolicy policy to which the scope is applied.</p>	<pre>-file-extensions-to-exclude file_extensions,...</pre>
<p><i>Is file extension check on directory enabled ?</i></p> <p>Specifies whether the file name extension checks apply to directory objects as well. If this parameter is set to <code>true</code>, the directory objects are subjected to the same extension checks as regular files. If this parameter is set to <code>false</code>, the directory names are not matched for extensions and notifications are sent for directories even if their name extensions do not match.</p> <p>If the FPolicy policy to which the scope is assigned is configured to use the native engine, this parameter must be set to <code>true</code>.</p>	<pre>-is-file-extension-check-on-directories-enabled {true  false}</pre>

= Complete the FPolicy scope worksheet

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You can use this worksheet to record the values that you need during the FPolicy scope configuration process. If a parameter value is required, you need to determine what value to use for those parameters before you configure the FPolicy scope.

You should record whether you want to include each parameter setting in the FPolicy scope configuration and then record the value for the parameters that you want to include.

Type of information	Required	Include	Your values
Storage virtual machine (SVM) name	Yes	Yes	
Policy name	Yes	Yes	
Shares to include	No		
Shares to exclude	No		
Volumes to include	No		
Volumes to exclude	No		
Export policies to include	No		
Export policies to exclude	No		
File extensions to include	No		

File extension to exclude	No		
Is file extension check on directory enabled?	No		

= Create the FPolicy configuration

= Create the FPolicy external engine

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You must create an external engine to start creating an FPolicy configuration. The external engine defines how FPolicy makes and manages connections to external FPolicy servers. If your configuration uses the internal ONTAP engine (the native external engine) for simple file blocking, you do not need to configure a separate FPolicy external engine and do not need to perform this step.

### What you'll need

The [external engine](#) worksheet should be completed.

### About this task

If the external engine is used in a MetroCluster configuration, you should specify the IP addresses of the FPolicy servers at the source site as primary servers. The IP addresses of the FPolicy servers at the destination site should be specified as secondary servers.

### Steps

1. Create the FPolicy external engine by using the `vserver fpolicy policy external-engine create` command.

The following command creates an external engine on storage virtual machine (SVM) `vs1.example.com`. No authentication is required for external communications with the FPolicy server.

```
vserver fpolicy policy external-engine create -vserver-name vs1.example.com
-engine-name engine1 -primary-servers 10.1.1.2,10.1.1.3 -port 6789 -ssl
-option no-auth
```

2. Verify the FPolicy external engine configuration by using the `vserver fpolicy policy external-engine show` command.

The following command display information about all external engines configured on SVM `vs1.example.com`:

```
vserver fpolicy policy external-engine show -vserver vs1.example.com
```

External Vserver	Engine	Primary Servers	Secondary Servers	Port
vs1.example.com	engine1	10.1.1.2, 10.1.1.3	-	6789

The following command displays detailed information about the external engine named “engine1” on SVM vs1.example.com:

```
vserver fpolicy policy external-engine show -vserver vs1.example.com
-engine-name engine1
```

```

Vserver: vs1.example.com
Engine: engine1
Primary FPolicy Servers: 10.1.1.2, 10.1.1.3
Port Number of FPolicy Service: 6789
Secondary FPolicy Servers: -
External Engine Type: synchronous
SSL Option for External Communication: no-auth
FQDN or Custom Common Name: -
Serial Number of Certificate: -
Certificate Authority: -

```

= Create the FPolicy event

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

As part of creating an FPolicy policy configuration, you need to create an FPolicy event. You associate the event with the FPolicy policy when it is created. An event defines which protocol to monitor and which file access events to monitor and filter.

### Before you begin

You should complete the FPolicy event worksheet.

### Steps

1. Create the FPolicy event by using the `vserver fpolicy policy event create` command.

```
vserver fpolicy policy event create -vserver-name vs1.example.com -event
-name event1 -protocol cifs -file-operations open,close,read,write
```

2. Verify the FPolicy event configuration by using the `vserver fpolicy policy event show`

command.

```
vserver fpolicy policy event show -vserver vs1.example.com
```

Volume	Event	File	Is		
Vserver	Name	Protocols	Operations	Filters	
Operation					
vs1.example.com	event1	cifs	open, close, read, write	-	false

= Create the FPolicy policy

```
:icons: font
```

```
:relative_path: ./nas-audit/
```

```
:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/
```

When you create the FPolicy policy, you associate an external engine and one or more events to the policy. The policy also specifies whether mandatory screening is required, whether the FPolicy servers have privileged access to data on the storage virtual machine (SVM), and whether passthrough-read for offline files is enabled.

#### What you'll need

- The FPolicy policy worksheet should be completed.
- If you plan on configuring the policy to use FPolicy servers, the external engine must exist.
- At least one FPolicy event that you plan on associating with the FPolicy policy must exist.
- If you want to configure privileged data access, a SMB server must exist on the SVM.

#### Steps

1. Create the FPolicy policy:

```
vserver fpolicy policy create -vserver-name vserver_name -policy-name  
policy_name -engine engine_name -events event_name,... [-is-mandatory  
{true|false}] [-allow-privileged-access {yes|no}] [-privileged-user-name  
domain\user_name] [-is-passthrough-read-enabled {true|false}]
```

- You can add one or more events to the FPolicy policy.
- By default, mandatory screening is enabled.
- If you want to allow privileged access by setting the `-allow-privileged-access` parameter to `yes`, you must also configure a privileged user name for privileged access.
- If you want to configure passthrough-read by setting the `-is-passthrough-read-enabled` parameter to `true`, you must also configure privileged data access.

The following command creates a policy named “policy1” that has the event named “event1” and the external engine named “engine1” associated with it. This policy uses default values in the



policy configuration:

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name policy1 -events event1 -engine engine1
```

The following command creates a policy named “policy2” that has the event named “event2” and the external engine named “engine2” associated with it. This policy is configured to use privileged access using the specified user name. Passthrough-read is enabled:

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name policy2 -events event2 -engine engine2 -allow-privileged-access yes -privileged-user-name example\archive_acct -is-passthrough-read-enabled true
```

The following command creates a policy named “native1” that has the event named “event3” associated with it. This policy uses the native engine and uses default values in the policy configuration:

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name native1 -events event3 -engine native
```

## 2. Verify the FPolicy policy configuration by using the `vserver fpolicy policy show` command.

The following command displays information about the three configured FPolicy policies, including the following information:

- The SVM associated with the policy
- The external engine associated with the policy
- The events associated with the policy
- Whether mandatory screening is required
- Whether privileged access is required

```
vserver fpolicy policy show
```

Vserver	Policy	Events	Engine	Is Mandatory	Access
Privileged	Name				
vs1.example.com	policy1	event1	engine1	true	no
vs1.example.com	policy2	event2	engine2	true	yes
vs1.example.com	native1	event3	native	true	no

= Create the FPolicy scope

```
:icons: font
```

```
:relative_path: ./nas-audit/
```

```
:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/
```

After creating the FPolicy policy, you need to create an FPolicy scope. When creating the scope, you associate the scope with an FPolicy policy. A scope defines the

boundaries on which the FPolicy policy applies. Scopes can include or exclude files based on shares, export policies, volumes, and file extensions.

### What you'll need

The FPolicy scope worksheet must be completed. The FPolicy policy must exist with an associated external engine (if the policy is configured to use external FPolicy servers) and must have at least one associated FPolicy event.

### Steps

1. Create the FPolicy scope by using the `vserver fpolicy policy scope create` command.

```
vserver fpolicy policy scope create -vserver-name vs1.example.com -policy
-name policy1 -volumes-to-include datavol1,datavol2
```

2. Verify the FPolicy scope configuration by using the `vserver fpolicy policy scope show` command.

```
vserver fpolicy policy scope show -vserver vs1.example.com -instance
```

```
Vserver: vs1.example.com
Policy: policy1
Shares to Include: -
Shares to Exclude: -
Volumes to Include: datavol1, datavol2
Volumes to Exclude: -
Export Policies to Include: -
Export Policies to Exclude: -
File Extensions to Include: -
File Extensions to Exclude: -
```

= Enable the FPolicy policy

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injpo/source/./authentication/./media/

After you are through configuring an FPolicy policy configuration, you enable the FPolicy policy. Enabling the policy sets its priority and starts file access monitoring for the policy.

### What you'll need

The FPolicy policy must exist with an associated external engine (if the policy is configured to use external FPolicy servers) and must have at least one associated FPolicy event. The FPolicy policy scope must exist and must be assigned to the FPolicy policy.

### About this task

The priority is used when multiple policies are enabled on the storage virtual machine (SVM) and more than one policy has subscribed to the same file access event. Policies that use the native engine configuration have a higher priority than policies for any other engine, regardless of the sequence number

assigned to them when enabling the policy.

A policy cannot be enabled on the admin SVM.

## Steps

1. Enable the FPolicy policy by using the `vserver fpolicy enable` command.

```
vserver fpolicy enable -vserver-name vs1.example.com -policy-name policy1
-sequence-number 1
```

2. Verify that the FPolicy policy is enabled by using the `vserver fpolicy show` command.

```
vserver fpolicy show -vserver vs1.example.com
```

Vserver	Policy Name	Sequence Number	Status	Engine
vs1.example.com	policy1	1	on	engine1

= Modify FPolicy configurations

= Commands for modifying FPolicy configurations

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You can modify FPolicy configurations by modifying the elements that make up the configuration. You can modify external engines, FPolicy events, FPolicy scopes, and FPolicy policies. You can also enable or disable FPolicy policies. When you disable the FPolicy policy, file monitoring is discontinued for that policy.

It is recommended to disable the FPolicy policy before modifying the configuration.

If you want to modify...	Use this command...
External engines	<code>vserver fpolicy policy external-engine modify</code>
Events	<code>vserver fpolicy policy event modify</code>
Scopes	<code>vserver fpolicy policy scope modify</code>
Policies	<code>vserver fpolicy policy modify</code>

See the man pages for the commands for more information.

= Enable or disable FPolicy policies

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

You can enable FPolicy policies after the configuration is complete. Enabling the policy sets its priority and starts file access monitoring for the policy. You can disable FPolicy policies if you want to stop file access monitoring for the policy.

### What you'll need

Before enabling FPolicy policies, the FPolicy configuration must be completed.

### About this task

- The priority is used when multiple policies are enabled on the storage virtual machine (SVM) and more than one policy has subscribed to the same file access event.
- Policies that use the native engine configuration have a higher priority than policies for any other engine, regardless of the sequence number assigned to them when enabling the policy.
- If you want to change the priority of an FPolicy policy, you must disable the policy and then reenabling it using the new sequence number.

### Step

1. Perform the appropriate action:

If you want to...	Enter the following command...
Enable an FPolicy policy	<pre>vserver fpolicy enable -vserver-name vserver_name -policy-name policy_name -sequence -number integer</pre>
Disable an FPolicy policy	<pre>vserver fpolicy disable -vserver-name vserver_name -policy-name policy_name</pre>

= Display information about FPolicy configurations

= How the show commands work

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./authentication/./media/

It is helpful when displaying information about the FPolicy configuration to understand how the `show` commands work.

A `show` command without additional parameters displays information in a summary form. Additionally, every `show` command has the same two mutually exclusive optional parameters, `-instance` and `-fields`.

When you use the `-instance` parameter with a `show` command, the command output displays detailed information in a list format. In some cases, the detailed output can be lengthy and include more information than you need. You can use the `-fields fieldname[,fieldname...]` parameter to customize the output so that it displays information only for the fields you specify. You can identify which fields that you can specify by entering `?` after the `-fields` parameter.

The output of a `show` command with the `-fields` parameter might display other relevant and necessary fields

related to the requested fields.

Every `show` command has one or more optional parameters that filter that output and enable you to narrow the scope of information displayed in command output. You can identify which optional parameters are available for a command by entering `?` after the `show` command.

The `show` command supports UNIX-style patterns and wildcards to enable you to match multiple values in command-parameters arguments. For example, you can use the wildcard operator (`*`), the NOT operator (`!`), the OR operator (`|`), the range operator (integer...integer), the less-than operator (`<`), the greater-than operator (`>`), the less-than or equal to operator (`<=`), and the greater-than or equal to operator (`>=`) when specifying values.

For more information about using UNIX-style patterns and wildcards, see the [Using the ONTAP command-line interface](#).

= Commands for displaying information about FPolicy configurations

You use the `fpolicy show` commands to display information about the FPolicy configuration, including information about FPolicy external engines, events, scopes, and policies.

If you want to display information about FPolicy...	Use this command...
External engines	<code>vserver fpolicy policy external-engine show</code>
Events	<code>vserver fpolicy policy event show</code>
Scopes	<code>vserver fpolicy policy scope show</code>
Policies	<code>vserver fpolicy policy show</code>

See the man pages for the commands for more information.

= Display information about FPolicy policy status

You can display information about the status for FPolicy policies to determine whether a policy is enabled, what external engine it is configured to use, what the sequence number is for the policy, and to which storage virtual machine (SVM) the FPolicy policy is associated.

#### About this task

If you do not specify any parameters, the command displays the following information:

- SVM name
- Policy name
- Policy sequence number
- Policy status

In addition to displaying information about policy status for FPolicy policies configured on the cluster or a

specific SVM, you can use command parameters to filter the command's output by other criteria.

You can specify the `-instance` parameter to display detailed information about listed policies. Alternatively, you can use the `-fields` parameter to display only the indicated fields in the command output, or `-fields ?` to determine what fields you can use.

### Step

1. Display filtered information about FPolicy policy status by using the appropriate command:

If you want to display status information about policies...	Enter the command...
On the cluster	<code>vserver fpolicy show</code>
That have the specified status	<code>vserver fpolicy show -status {on off}</code>
On a specified SVM	<code>vserver fpolicy show -vserver vserver_name</code>
With the specified policy name	<code>vserver fpolicy show -policy-name policy_name</code>
That use the specified external engine	<code>vserver fpolicy show -engine engine_name</code>

### Example

The following example displays the information about FPolicy policies on the cluster:

```
cluster1::> vserver fpolicy show
```

Vserver	Policy Name	Sequence Number	Status	Engine
FPolicy	cserver_policy	-	off	eng1
vs1.example.com	v1p1	-	off	eng2
vs1.example.com	v1p2	-	off	native
vs1.example.com	v1p3	-	off	native
vs1.example.com	cserver_policy	-	off	eng1
vs2.example.com	v1p1	3	on	native
vs2.example.com	v1p2	1	on	eng3
vs2.example.com	cserver_policy	2	on	eng1

= Display information about enabled FPolicy policies

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

You can display information about enabled FPolicy policies to determine what FPolicy external engine it is configured to use, what the priority is for the policy, and to which



storage virtual machine (SVM) the FPolicy policy is associated.

### About this task

If you do not specify any parameters, the command displays the following information:

- SVM name
- Policy name
- Policy priority

You can use command parameters to filter the command's output by specified criteria.

### Step

1. Display information about enabled FPolicy policies by using the appropriate command:

If you want to display information about enabled policies...	Enter the command...
On the cluster	<code>vserver fpolicy show-enabled</code>
On a specified SVM	<code>vserver fpolicy show-enabled -vserver vserver_name</code>
With the specified policy name	<code>vserver fpolicy show-enabled -policy-name policy_name</code>
With the specified sequence number	<code>vserver fpolicy show-enabled -priority integer</code>

### Example

The following example displays the information about enabled FPolicy policies on the cluster:

```
cluster1::> vserver fpolicy show-enabled
Vserver                Policy Name                Priority
-----
vs1.example.com        pol_native                 native
vs1.example.com        pol_native2                native
vs1.example.com        pol1                       2
vs1.example.com        pol2                       4
```

= Manage FPolicy server connections

= Connect to external FPolicy servers

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injpo/source/./nas-audit/./media/

To enable file processing, you might need to manually connect to an external FPolicy server if the connection has previously been terminated. A connection is terminated after the server timeout is reached or due to some error. Alternatively, the administrator might manually terminate a connection.

#### About this task

If a fatal error occurs, the connection to the FPolicy server can be terminated. After resolving the issue that caused the fatal error, you must manually reconnect to the FPolicy server.

#### Steps

1. Connect to the external FPolicy server by using the `vserver fpolicy engine-connect` command.

For more information about the command, see the man pages.

2. Verify that the external FPolicy server is connected by using the `vserver fpolicy show-engine` command.

For more information about the command, see the man pages.

= Disconnect from external FPolicy servers

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

You might need to manually disconnect from an external FPolicy server. This might be desirable if the FPolicy server has issues with notification request processing or if you need to perform maintenance on the FPolicy server.

#### Steps

1. Disconnect from the external FPolicy server by using the `vserver fpolicy engine-disconnect` command.

For more information about the command, see the man pages.

2. Verify that the external FPolicy server is disconnected by using the `vserver fpolicy show-engine` command.

For more information about the command, see the man pages.

= Display information about connections to external FPolicy servers

You can display status information about connections to external FPolicy servers (FPolicy servers) for the cluster or for a specified storage virtual machine (SVM). This information can help you determine which FPolicy servers are connected.

#### About this task

If you do not specify any parameters, the command displays the following information:

- SVM name

- Node name
- FPolicy policy name
- FPolicy server IP address
- FPolicy server status
- FPolicy server type

In addition to displaying information about FPolicy connections on the cluster or a specific SVM, you can use command parameters to filter the command's output by other criteria.

You can specify the `-instance` parameter to display detailed information about listed policies. Alternatively, you can use the `-fields` parameter to display only the indicated fields in the command output. You can enter `?` after the `-fields` parameter to find out which fields you can use.

### Step

1. Display filtered information about connection status between the node and the FPolicy server by using the appropriate command:

If you want to display connection status information about FPolicy servers...	Enter...
That you specify	<code>vserver fpolicy show-engine -server IP_address</code>
For a specified SVM	<code>vserver fpolicy show-engine -vserver vserver_name</code>
That are attached with a specified policy	<code>vserver fpolicy show-engine -policy-name policy_name</code>
With the server status that you specify	<p><code>vserver fpolicy show-engine -server-status status</code></p> <p>The server status can be one of the following:</p> <ul style="list-style-type: none"> <li>• <code>connected</code></li> <li>• <code>disconnected</code></li> <li>• <code>connecting</code></li> <li>• <code>disconnecting</code></li> </ul>
With the specified type	<p><code>vserver fpolicy show-engine -server-type type</code></p> <p>The FPolicy server type can be one of the following:</p> <ul style="list-style-type: none"> <li>• <code>primary</code></li> <li>• <code>secondary</code></li> </ul>

That were disconnected with the specified reason

```
vserver fpolicy show-engine -disconnect-reason text
```

Disconnect can be due to multiple reasons. The following are common reasons for disconnect:

- Disconnect command received from CLI.
- Error encountered while parsing notification response from FPolicy server.
- FPolicy Handshake failed.
- SSL handshake failed.
- TCP Connection to FPolicy server failed.
- The screen response message received from the FPolicy server is not valid.

### Example

This example displays information about external engine connections to FPolicy servers on SVM vs1.example.com:

```
cluster1::> vserver fpolicy show-engine -vserver vs1.example.com
FPolicy
Server-
Server-
Vserver          Policy      Node          Server          status          type
-----
vs1.example.com policy1    node1         10.1.1.2        connected
primary
vs1.example.com policy1    node1         10.1.1.3        disconnected
primary
vs1.example.com policy1    node2         10.1.1.2        connected
primary
vs1.example.com policy1    node2         10.1.1.3        disconnected
primary
```

This example displays information only about connected FPolicy servers:

```
cluster1::> vserver fpolicy show-engine -fields server -server-status
connected
node          vserver          policy-name    server
-----
node1         vs1.example.com  policy1        10.1.1.2
node2         vs1.example.com  policy1        10.1.1.2
```

= Display information about the FPolicy passthrough-read connection status

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

You can display information about FPolicy passthrough-read connection status to external FPolicy servers (FPolicy servers) for the cluster or for a specified storage virtual machine (SVM). This information can help you determine which FPolicy servers have passthrough-read data connections and for which FPolicy servers the passthrough-read connection is disconnected.

### About this task

If you do not specify any parameter, the command displays the following information:

- SVM name
- FPolicy policy name
- Node name
- FPolicy server IP address
- FPolicy passthrough-read connection status

In addition to displaying information about FPolicy connections on the cluster or a specific SVM, you can use command parameters to filter the command's output by other criteria.

You can specify the `-instance` parameter to display detailed information about listed policies.

Alternatively, you can use the `-fields` parameter to display only the indicated fields in the command output. You can enter `?` after the `-fields` parameter to find out which fields you can use.

### Step

1. Display filtered information about connection status between the node and the FPolicy server by using the appropriate command:

If you want to display connection status information about...	Enter the command...
FPolicy passthrough-read connection status for the cluster	<code>vserver fpolicy show-passthrough-read-connection</code>
FPolicy passthrough-read connection status for a specified SVM	<code>vserver fpolicy show-passthrough-read-connection -vserver vserver_name</code>
FPolicy passthrough-read connection status for a specified policy	<code>vserver fpolicy show-passthrough-read-connection -policy-name policy_name</code>
Detailed FPolicy passthrough-read connection status for a specified policy	<code>vserver fpolicy show-passthrough-read-connection -policy-name policy_name -instance</code>

FPolicy passthrough-read connection status for the status that you specify

```
vserver fpolicy show-passthrough-read-connection -policy-name policy_name -server -status status
```

The server status can be one of the following:

- connected
- disconnected

### Example

The following command displays information about passthrough-read connections from all FPolicy servers on the cluster:

```
cluster1::> vserver fpolicy show-passthrough-read-connection
```

Vserver	Policy Name	Node	FPolicy Server	Server Status
vs2.example.com	pol_cifs_2	FPolicy-01	2.2.2.2	disconnected
vs1.example.com	pol_cifs_1	FPolicy-01	1.1.1.1	connected

The following command displays detailed information about passthrough-read connections from FPolicy servers configured in the “pol\_cifs\_1” policy:

```
cluster1::> vserver fpolicy show-passthrough-read-connection -policy -name pol_cifs_1 -instance
```

Node: FPolicy-01  
Vserver: vs1.example.com  
Policy: pol\_cifs\_1  
Server: 1.1.1.1  
Session ID of the Control Channel: 8cef052e-2502-11e3-88d4-123478563412  
Server Status: connected  
Time Passthrough Read Channel was Connected: 9/24/2013 10:17:45  
Time Passthrough Read Channel was Disconnected: -  
Reason for Passthrough Read Channel Disconnection: none

= Use security tracing to verify or troubleshoot file and directory access

= How security traces work

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

You can add permission tracing filters to instruct ONTAP to log information about why the SMB and NFS servers on a storage virtual machine (SVM) allows or denies a client or user's request to perform an operation. This can be useful when you want to verify that your file access security scheme is appropriate or when you want to troubleshoot file access issues.

Security traces allow you to configure a filter that detects client operations over SMB and NFS on the SVM, and trace all access checks matching that filter. You can then view the trace results, which provides a convenient summary of the reason that access was allowed or denied.

When you want to verify the security settings for SMB or NFS access on files and folders on your SVM or if you are faced with an access problem, you can quickly add a filter to turn on permission tracing.

The following list outlines important facts about how security traces works:

- ONTAP applies security traces at the SVM level.
- Each incoming request is screened to see if it matches filtering criteria of any enabled security traces.
- Traces are performed for both file and folder access requests.
- Traces can filter based on the following criteria:
  - Client IP
  - SMB or NFS path
  - Windows name
  - UNIX name
- Requests are screened for *Allowed* and *Denied* access response results.
- Each request matching filtering criteria of enabled traces is recorded in the trace results log.
- The storage administrator can configure a timeout on a filter to automatically disable it.
- If a request matches multiple filters, the results from the filter with the highest index number is recorded.
- The storage administrator can print results from the trace results log to determine why an access request was allowed or denied.

= Types of access checks security traces monitor

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

Access checks for a file or folder are done based on multiple criteria. Security traces monitor operations on all these criteria.

The types of access checks that security traces monitor include the following:

- Volume and qtree security style
- Effective security of the file system containing the files and folders on which operations are requested
- User mapping
- Share-level permissions
- Export-level permissions

- File-level permissions
- Storage-Level Access Guard security

= Considerations when creating security traces

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

You should keep several considerations in mind when you create security traces on storage virtual machines (SVMs). For example, you need to know on which protocols you can create a trace, which security-styles are supported, and what the maximum number of active traces is.

- You can only create security traces on SVMs.
- Each security trace filter entry is SVM specific.

You must specify the SVM on which you want to run the trace.

- You can add permission tracing filters for SMB and NFS requests.
- You must set up the SMB or NFS server on the SVM on which you want to create trace filters.
- You can create security traces for files and folders residing on NTFS, UNIX, and mixed security-style volumes and qtrees.
- You can add a maximum of 10 permission tracing filters per SVM.
- You must specify a filter index number when creating or modifying a filter.

Filters are considered in order of the index number. The criteria in a filter with a higher index number is considered before the criteria with a lower index number. If the request being traced matches criteria in multiple enabled filters, only the filter with the highest index number is triggered.

- After you have created and enabled a security trace filter, you must perform some file or folder requests on a client system to generate activity that the trace filter can capture and log in the trace results log.
- You should add permission tracing filters for file access verification or troubleshooting purposes only.

Adding permission tracing filters has a minor effect on controller performance.

When you are done with verification or troubleshooting activity, you should disable or remove all permission tracing filters. Furthermore, the filtering criteria you select should be as specific as possible so that ONTAP does not send a large number of trace results to the log.

= Perform security traces

= Perform security traces overview

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

Performing a security trace involves creating a security trace filter, verifying the filter criteria, generating access requests on an SMB or NFS client that match filter criteria, and viewing the results.



After you are finished using a security filter to capture trace information, you can modify the filter and reuse it, or disable it if you no longer need it. After viewing and analyzing the filter trace results, you can then delete them if they are no longer needed.

= Create security trace filters

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

You can create security trace filters that detect SMB and NFS client operations on storage virtual machines (SVMs) and trace all access checks matching the filter. You can use the results from security traces to validate your configuration or to troubleshoot access issues.

### About this task

There are two required parameters for the vservers security trace filter create command:

Required parameters	Description
<code>-vservers vservers_name</code>	<i>SVM name</i>  The name of the SVM that contains the files or folders on which you want to apply the security trace filter.
<code>-index index_number</code>	<i>Filter index number</i>  The index number you want to apply to the filter. You are limited to a maximum of 10 trace filters per SVM. The allowed values for this parameter are 1 through 10.

A number of optional filter parameters enable you to customize the security trace filter so that you can narrow down the results produced by the security trace:

Filter parameter	Description
<code>-client-ip IP_Address</code>	This filter specifies the IP address from which the user is accessing the SVM.
<code>-path path</code>	This filter specifies the path on which to apply the permission trace filter. The value for <code>-path</code> can use either of the following formats: <ul style="list-style-type: none"><li>• The complete path, starting from the root of the share or export</li><li>• A partial path, relative to the root of the share</li></ul> You must use NFS style directory UNIX-style directory separators in the path value.

```
-windows-name  
win_user_name or -unix  
-name ``unix_user_name
```

You can specify either the Windows user name or UNIX user name whose access requests you want to trace. The user name variable is case insensitive. You cannot specify both a Windows user name and a UNIX user name in the same filter.

Even though you can trace SMB and NFS access events, the mapped UNIX user and the mapped UNIX users' groups might be used when performing access checks on mixed or UNIX security-style data.

a|

`-trace-allow {yes|no}`

a|

Tracing for deny events is always enabled for a security trace filter. You can optionally trace allow events. To trace allow events, you set this parameter to `yes`.

a|

`-enabled {enabled|disabled}`

a|

You can enable or disable the security trace filter. By default, the security trace filter is enabled.

a|

`-time-enabled integer`

a|

You can specify a timeout for the filter, after which it is disabled.

## .Steps

. Create a security trace filter:

+

```
vserver security trace filter create -vserver vserver_name -index  
index_numberfilter_parameters
```

+

filter\_parameters is a list of optional filter parameters.

+

For more information, see the man pages for the command.

. Verify the security trace filter entry:

+

```
vserver security trace filter show -vserver vserver_name -index index_number
```

## .Examples

The following command creates a security trace filter for any user accessing a file with a share path `\\server\share1\dir1\dir2\file.txt` from the IP address 10.10.10.7. The filter uses a complete path for the `-path` option. The client's IP address used to access data is 10.10.10.7. The filter times out after 30 minutes:

----

```
cluster1::> vserver security trace filter create -vserver vs1 -index 1 -path /dir1/dir2/file.txt -time-enabled  
30 -client-ip 10.10.10.7
```

```
cluster1::> vserver security trace filter show -index 1
```

```
Vserver Index Client-IP Path Trace-Allow Windows-Name
```

```
-----
```

```
vs1 1 10.10.10.7 /dir1/dir2/file.txt no -
```

----

The following command creates a security trace filter using a relative path for the `-path` option. The filter traces access for a Windows user named "joe". Joe is accessing a file with a share path `\\server\share1\dir1\dir2\file.txt`. The filter traces allow and deny events:

----

```
cluster1::> vserver security trace filter create -vserver vs1 -index 2 -path /dir1/dir2/file.txt -trace-allow yes  
-windows-name mydomain\joe
```

```
cluster1::> vserver security trace filter show -vserver vs1 -index 2
```

```
Vserver: vs1
```

```
Filter Index: 2
```

```
Client IP Address to Match: -
```

```
Path: /dir1/dir2/file.txt
```

```
Windows User Name: mydomain\joe
```

```
UNIX User Name: -
```

```
Trace Allow Events: yes
```

```
Filter Enabled: enabled
```

```
Minutes Filter is Enabled: 60
```

----

h| If the filter is configured... h| Then...

a|

With a UNIX user name

a|

The security trace result displays the UNIX user name.

a|

With a Windows user name

a|

The security trace result displays the Windows user name.

a|

Without a user name

a|

The security trace result displays the Windows user name.

You can customize the output by using optional parameters. Some of the optional parameters that you can use to narrow the results returned in the command output include the following:

```
[cols="35,65"]
```

h| Optional parameter h| Description

a|

```
-fields field_name, ...
```

a|

Displays output on the fields you choose. You can use this parameter either alone or in combination with other optional parameters.

a|

```
-instance
```

a|

Displays detailed information about security trace events. Use this parameter with other optional parameters to display detailed information about specific filter results.

a|

```
-node node_name
```

a|

Displays information only about events on the specified node.

a|

```
-vserver vservice_name
```

a|

Displays information only about events on the specified SVM.

a|

```
-index integer
```

a|

Displays information about the events that occurred as a result of the filter corresponding to the specified index number.

a|

```
-client-ip IP_address
```

a|

Displays information about the events that occurred as a result of file access from the specified client IP address.

a|

```
-path path
```

a|

Displays information about the events that occurred as a result of file access to the specified path.

a|

-user-name user\_name

a|

Displays information about the events that occurred as a result of file access by the specified Windows or UNIX user.

a|

-security-style security\_style

a|

Displays information about the events that occurred on file systems with the specified security style.

See the man page for information about other optional parameters that you can use with the command.

### .Step

. Display security trace filter results by using the `vserver security trace trace-result show` command.

```
+  
vserver security trace trace-result show -user-name domain\user
```

```
+  
----
```

Vserver: vs1

#### Node Index Filter Details Reason

```
-----  
node1 3 User:domain\user Access denied by explicit ACE  
Security Style:mixed  
Path:/dir1/dir2/
```

```
node1 5 User:domain\user Access denied by explicit ACE  
Security Style:unix  
Path:/dir1/
```

```
----
```

= Modify security trace filters

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

[.lead]

If you want to change the optional filter parameters used to determine which access events are traced, you can modify existing security trace filters.

### .About this task

You must identify which security trace filter you want to modify by specifying the storage virtual machine (SVM) name on which the filter is applied and the index number of the filter. You can modify all the optional filter parameters.

### .Steps

. Modify a security trace filter:

```
+  
vserver security trace filter modify -vserver vserver_name -index  
index_numberfilter_parameters
```

```
+  

```

**vserver\_name** is the name of the SVM on which you want to apply a security trace filter.

**index\_number** is the index number that you want to apply to the filter. The allowed values for this parameter are 1 through 10.

\*\* **filter\_parameters** is a list of optional filter parameters.

. Verify the security trace filter entry:

```
+  

```

Each storage virtual machine (SVM) can store a maximum of 128 trace records. If the maximum is reached on the SVM, the oldest trace records are automatically deleted as new ones are added. If you do not want to manually delete trace records on this SVM, you can let ONTAP automatically delete the oldest trace results after the maximum is reached to make room for new results.



## Steps

1. Identify the sequence number of the record you want to delete:

```
vserver security trace trace-result show -vserver vserver_name -instance
```

2. Delete the security trace record:

```
vserver security trace trace-result delete -node node_name -vserver  
vserver_name -seqnum integer
```

```
vserver security trace trace-result delete -vserver vs1 -node node1 -seqnum  
999
```

- `-node node_name` is the name of the cluster node on which the permission tracing event that you want to delete occurred.

This is a required parameter.

- `-vserver vserver_name` is the name of the SVM on which the permission tracing event that you want to delete occurred.

This is a required parameter.

- `-seqnum integer` is the sequence number of the log event that you want to delete.

This is a required parameter.

= Delete all security trace records

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

If you do not want to keep any of the existing security trace records, you can delete all of the records on a node with a single command.

## Step

1. Delete all security trace records:

```
vserver security trace trace-result delete -node node_name -vserver  
vserver_name *
```

- `-node node_name` is the name of the cluster node on which the permission tracing event that you want to delete occurred.

- `-vserver vserver_name` is the name of the storage virtual machine (SVM) on which the permission tracing event that you want to delete occurred.

= Interpret security trace results

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

Security trace results provide the reason that a request was allowed or denied. Output displays the result as a combination of the reason for allowing or denying access and the location within the access checking pathway where access is either allowed or denied. You can use the results to isolate and identify why actions are or are not allowed.

== Finding information about the lists of result types and filter details

You can find the lists of result types and filter details that can be included in the security trace results in the man pages for the `vserver security trace trace-result show` command.

#### **Example of output from the `Reason` field in an `Allow` result type**

The following is an example of the output from the `Reason` field that appears in the trace results log in an `Allow` result type:

```
Access is allowed because SMB implicit permission grants requested
access while opening existing file or directory.
```

```
Access is allowed because NFS implicit permission grants requested
access while opening existing file or directory.
```

#### **Example of output from the `Reason` field in an `Allow` result type**

The following is an example of the output from the `Reason` field that appears in the trace results log in a `Deny` result type:

```
Access is denied. The requested permissions are not granted by the
ACE while checking for child-delete access on the parent.
```

#### **Example of output from the `Filter details` field**

The following is an example of the output from the `Filter details` field in the trace results log, which list the effective security style of the file system containing files and folders that match the filter criteria:

```
Security Style: MIXED and ACL
```

= Where to find additional information

:icons: font

:relative\_path: ./nas-audit/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

After you have successfully tested SMB client access, you can perform advanced SMB configuration or add SAN access. After you have successfully tested NFS client access, you can perform advanced NFS configuration or add SAN access. When protocol access is complete, you should protect the root volume of SVM.

## == SMB configuration

You can further configure SMB access using the following:

- [SMB management](#)

Describes how to configure and manage file access using the SMB protocol.

- [NetApp Technical Report 4191: Best Practices Guide for Clustered Data ONTAP 8.2 Windows File Services](#)

Provides a brief overview of SMB implementation and other Windows File Services features with recommendations and basic troubleshooting information for ONTAP.

- [NetApp Technical Report 3740: SMB 2 Next-Generation CIFS Protocol in Data ONTAP](#)

Describes SMB 2 features, configuration details, and its implementation in ONTAP.

## == NFS configuration

You can further configure NFS access using the following:

- [NFS management](#)

Describes how to configure and manage file access using the NFS protocol.

- [NetApp Technical Report 4067: NFS Best Practice and Implementation Guide](#)

Serves as an NFSv3 and NFSv4 operational guide and provides an overview of ONTAP operating system with a focus on NFSv4.

- [NetApp Technical Report 4668: Name Services Best Practices Guide](#)

Provides a comprehensive list of best practices, limits, recommendations, and considerations when configuring LDAP, NIS, DNS, and local user and group files for authentication purposes.

- [NetApp Technical Report 4616: NFS Kerberos in ONTAP with Microsoft Active Directory](#)

- [NetApp Technical Report 4835: How to Configure LDAP in ONTAP](#)

- [NetApp Technical Report 3580: NFSv4 Enhancements and Best Practices Guide Data ONTAP Implementation](#)

Describes the best practices that should be followed while implementing NFSv4 components on AIX, Linux, or Solaris clients attached to systems running ONTAP.

## == Root volume protection

After configuring protocols on the SVM, you should ensure that its root volume is protected:

- [Data protection](#)

Describes how to create a load-sharing mirror to protect the SVM root volume, which is a NetApp best practice for NAS-enabled SVMs. Also describes how to quickly recover from volume failures or losses by promoting the SVM root volume from a load-sharing mirror.

= Manage encryption with System Manager

= Encrypt stored data using software-based encryption

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./



:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

Use volume encryption to ensure that volume data cannot be read if the underlying device is repurposed, returned, misplaced, or stolen. Volume encryption does not require special disks; it works with all HDDs and SSDs.

Volume encryption requires a key manager. You can configure the Onboard Key Manager using System Manager. You can also use an external key manager, but you need to first set it up using the ONTAP CLI.

After the key manager is configured, new volumes are encrypted by default.

### Steps

1. Click **Cluster > Settings**.
2. Under **Encryption**, click  to configure the Onboard Key Manager for the first time.
3. To encrypt existing volumes, click **Storage > Volumes**.
4. On the desired volume, click  and then click **Edit**.
5. Select **Enable encryption**.

= Encrypt stored data using self-encrypting drives

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./



:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

Use disk encryption to ensure that all data in a local tier cannot be read if the underlying device is repurposed, returned, misplaced, or stolen. Disk encryption requires special self-encrypting HDDs or SSDs.

Disk encryption requires a key manager. You can configure the onboard key manager using System Manager. You can also use an external key manager, but you need to first set it up using the ONTAP CLI.

If ONTAP detects self-encrypting disks, it prompts you to configure the onboard key manager when you create the local tier.

### Steps

1. Under **Encryption**, click  to configure the onboard key manager.
2. If you see a message that disks need to be rekeyed, click , and then click **Rekey Disks**.

= Manage encryption with the CLI

= NetApp Encryption overview with the CLI

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

NetApp offers both software- and hardware-based encryption technologies for ensuring that data at rest cannot be read if the storage medium is repurposed, returned, misplaced, or stolen.

- Software-based encryption supports data encryption one volume at a time.
- Hardware-based encryption supports full-disk encryption (FDE) of data as it is written.

You can work with encryption if the following apply:

- You want to use best practices, not explore every available option.
- You want to use the ONTAP command-line interface (CLI), not System Manager or an automated scripting tool.

= Configure NetApp Volume Encryption

= Configure NetApp Volume Encryption overview

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

NetApp Volume Encryption (NVE) is a software-based technology for encrypting data at rest one volume at a time. An encryption key accessible only to the storage system ensures that volume data cannot be read if the underlying device is repurposed, returned, misplaced, or stolen.

== Understanding NVE

Both data, including Snapshot copies, and metadata are encrypted. Access to the data is given by a unique XTS-AES-256 key, one per volume. An external key management server or Onboard Key Manager serves keys to nodes:

- The external key management server is a third-party system in your storage environment that serves keys to nodes using the Key Management Interoperability Protocol (KMIP). It is a best practice to configure external key management servers on a different storage system from your data.
- The Onboard Key Manager is a built-in tool that serves keys to nodes from the same storage system as your data.

Beginning with ONTAP 9.7, aggregate and volume encryption is enabled by default if you have a volume encryption (VE) license and use an onboard or external key manager. Whenever an external or onboard key manager is configured there is a change in how the encryption of data at rest is configured for brand new aggregates and brand new volumes. Brand new aggregates will have NetApp Aggregate Encryption (NAE) enabled by default. Brand new volumes that are not part of an NAE aggregate will have NetApp Volume Encryption (NVE) enabled by default. If a data storage virtual machine (SVM) is configured with its own key-manager using multi-tenant key management, then the volume created for that SVM is automatically configured with NVE.

You can enable encryption on a new or existing volume. NVE supports the full range of storage efficiency

features, including deduplication and compression.

If you are using SnapLock, you can enable encryption only on new, empty SnapLock volumes. You cannot enable encryption on an existing SnapLock volume.

You can use NVE on any type of aggregate (HDD, SSD, hybrid, array LUN), with any RAID type, and in any supported ONTAP implementation, including ONTAP Select. You can also use NVE with hardware-based encryption to “double encrypt” data on self-encrypting drives.

AFF A220, AFF A800, FAS2720, FAS2750, and later systems store core dumps on their boot device. When NVE is enabled on these systems, the core dump is also encrypted.

## == Aggregate-level encryption

Ordinarily, every encrypted volume is assigned a unique key. When the volume is deleted, the key is deleted with it.

Beginning with ONTAP 9.6, you can use *NetApp Aggregate Encryption (NAE)* to assign keys to the containing aggregate for the volumes to be encrypted. When an encrypted volume is deleted, the keys for the aggregate are preserved. The keys are deleted if the entire aggregate is deleted.

You must use aggregate-level encryption if you plan to perform inline or background aggregate-level deduplication. Aggregate-level deduplication is otherwise not supported by NVE.

Beginning with ONTAP 9.7, aggregate and volume encryption is enabled by default if you have a volume encryption (VE) license and use an onboard or external key manager.

NVE and NAE volumes can coexist on the same aggregate. Volumes encrypted under aggregate-level encryption are NAE volumes by default. You can override the default when you encrypt the volume.

You can use the `volume move` command to convert an NVE volume to an NAE volume, and vice versa. You can replicate an NAE volume to an NVE volume.

You cannot use `secure purge` commands on an NAE volume.

## == When to use external key management servers

Although it is less expensive and typically more convenient to use the onboard key manager, you should set up KMIP servers if any of the following are true:

- Your encryption key management solution must comply with Federal Information Processing Standards (FIPS) 140-2 or the OASIS KMIP standard.
- You need a multi-cluster solution, with centralized management of encryption keys.
- Your business requires the added security of storing authentication keys on a system or in a location different from the data.

## == Scope of external key management

The scope of external key management determines whether key management servers secure all the SVMs in the cluster or selected SVMs only:

- You can use a *cluster scope* to configure external key management for all the SVMs in the cluster. The cluster administrator has access to every key stored on the servers.
- Beginning with ONTAP 9.6, you can use an *SVM scope* to configure external key management for a named SVM in the cluster. That's best for multitenant environments in which each tenant uses a different SVM (or set of SVMs) to serve data. Only the SVM administrator for a given tenant has access to the keys for that tenant.
- Beginning with ONTAP 9.10.1, you can use [Azure Key Vault](#) and [Google Cloud KMS](#) to protect NVE keys only for data vservers.

You can use both scopes in the same cluster. If key management servers have been configured for an SVM, ONTAP uses only those servers to secure keys. Otherwise, ONTAP secures keys with the key management servers configured for the cluster.

A list of validated external key managers is available in the [NetApp Interoperability Matrix Tool \(IMT\)](#). You can find this list by entering the term "key managers" into the IMT's search feature.

== Support details

The following table shows NVE support details:

Resource or feature	Support details
Platforms	AES-NI offload capability required. See the Hardware Universe (HWU) to verify that NVE and NAE are supported for your platform.
Encryption	<p>Beginning with ONTAP 9.7, newly created aggregates and volumes are encrypted by default when you add a volume encryption (VE) license and have an onboard or external key manager configured. If you need to create an unencrypted aggregate, use the following command:</p> <pre>storage aggregate create -encrypt-with-aggr-key false</pre> <p>If you need to create a plain text volume, use the following command:</p> <pre>volume create -encrypt false</pre> <p>Encryption is not enabled by default when:</p> <ul style="list-style-type: none"> <li>• VE license is not installed.</li> <li>• Key manager is not configured.</li> <li>• Platform or software does not support encryption.</li> <li>• Hardware encryption is enabled.</li> </ul>
ONTAP	All ONTAP implementations. Support for ONTAP Cloud is available in ONTAP 9.5 and later.
Devices	HDD, SSD, hybrid, array LUN.
RAID	RAID0, RAID4, RAID-DP, RAID-TEC.
Volumes	Data volumes and existing root volumes. You cannot encrypt data on an SVM root volume or MetroCluster metadata volumes.
Aggregate-level encryption	<p>Beginning with ONTAP 9.6, NVE supports aggregate-level encryption (NAE):</p> <ul style="list-style-type: none"> <li>• You must use aggregate-level encryption if you plan to perform inline or background aggregate-level deduplication.</li> <li>• You cannot rekey an aggregate-level encryption volume.</li> <li>• Secure-purge is not supported on aggregate-level encryption volumes.</li> <li>• In addition to data volumes, NAE supports encryption of SVM root volumes and the MetroCluster metadata volume. NAE does not support encryption of the root volume.</li> </ul>



SVM scope	Beginning with ONTAP 9.6, NVE supports SVM scope for external key management only, not for Onboard Key Manager. MetroCluster is supported beginning with ONTAP 9.8.
Storage efficiency	Deduplication, compression, compaction, FlexClone. Clones use the same key as the parent, even after splitting the clone from the parent. You are warned to rekey the split clone.
Replication	<ul style="list-style-type: none"> <li>• For volume replication, the destination volume must have been enabled for encryption. Encryption can be configured for the source and unconfigured for the destination, and vice versa.</li> <li>• For SVM replication, the destination volume is automatically encrypted, unless the destination does not contain a node that supports volume encryption, in which case replication succeeds, but the destination volume is not encrypted.</li> <li>• For MetroCluster configurations, each cluster pulls external key management keys from its configured key servers. OKM keys are replicated to the partner site by the configuration replication service.</li> </ul>
Compliance	Beginning with ONTAP 9.2, SnapLock is supported in both Compliance and Enterprise modes, for new volumes only. You cannot enable encryption on an existing SnapLock volume.
FlexGroups	Beginning with ONTAP 9.2, FlexGroups are supported. Destination aggregates must be of the same type as source aggregates, either volume-level or aggregate-level. Beginning with ONTAP 9.5, in-place rekey of FlexGroup volumes is supported.
7-Mode transition	Beginning with 7-Mode Transition Tool 3.3, you can use the 7-Mode Transition Tool CLI to perform copy-based transition to NVE-enabled destination volumes on the clustered system.

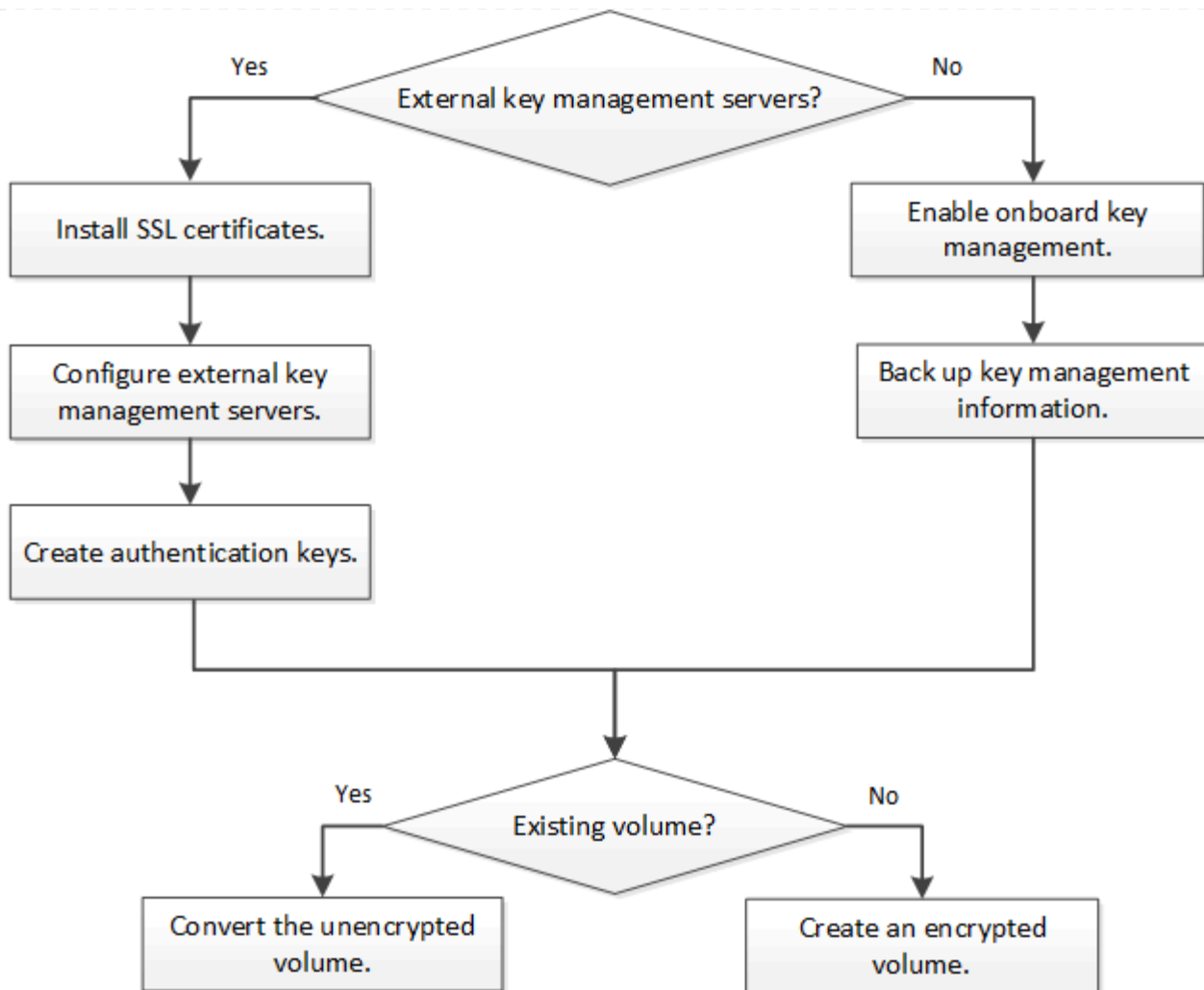
= NetApp Volume Encryption workflow

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

You must configure key management services before you can enable volume encryption. You can enable encryption on a new volume or on an existing volume.



You must install the VE license and configure key management services before you can encrypt data with NVE. Before installing the license, you should [determine whether your ONTAP version supports NVE](#).

= Configure NVE

= Determine whether your cluster version supports NVE

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

You should determine whether your cluster version supports NVE before you install the license. You can use the `version` command to determine the cluster version.

### About this task

The cluster version is the lowest version of ONTAP running on any node in the cluster.

### Step

1. Determine whether your cluster version supports NVE:

```
version -v
```

NVE is not supported if the command output displays the text “1Ono-DARE” (for “no Data At Rest Encryption”), or if you are using a platform that is not listed in [Support details](#).

The following command determines whether NVE is supported on `cluster1`.

```
cluster1::> version -v
NetApp Release 9.1.0: Tue May 10 19:30:23 UTC 2016 <1Ono-DARE>
```

The text “1Ono-DARE” in the command output indicates that NVE is not supported on your cluster version.

= Install the license

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

A VE license entitles you to use the feature on all nodes in the cluster. You must install the license before you can encrypt data with NVE.

### What you'll need

You must be a cluster administrator to perform this task.

### About this task

You should have received the VE license key from your sales representative.

### Steps

1. Install the VE license for a node:

```
system license add -license-code license_key
```

The following command installs the license with the key `AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA`.

```
cluster1::> system license add -license-code
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

2. Verify that the license is installed by displaying all the licenses on the cluster:

```
system license show
```

For complete command syntax, see the man page for the command.

The following command displays all the licenses on `cluster1`:

```
cluster1::> system license show
```

The VE license package name is “VE”.

= Configure external key management

= Configure external key management overview

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

You can use one or more external key management servers to secure the keys that the cluster uses to access encrypted data. An external key management server is a third-party system in your storage environment that serves keys to nodes using the Key Management Interoperability Protocol (KMIP).



For ONTAP 9.1 and earlier versions, node management LIFs must be assigned to ports that are configured with the node management role before you can use the external key manager.

NetApp Volume Encryption (NVE) supports Onboard Key Manager in ONTAP 9.1 and later. Beginning in ONTAP 9.3, NVE supports external key management (KMIP) and Onboard Key Manager. Beginning in ONTAP 9.10.1, you can use [Azure Key Vault](#) or [Google Cloud Key Manager Service](#) to protect your NVE keys. Beginning in ONTAP 9.11.1, you can configure multiple external key managers in a cluster. See [Configure clustered key servers](#).

= Install SSL certificates on the cluster

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

The cluster and KMIP server use KMIP SSL certificates to verify each other's identity and establish an SSL connection. Before configuring the SSL connection with the KMIP server, you must install the KMIP client SSL certificates for the cluster, and the SSL public certificate for the root certificate authority (CA) of the KMIP server.

#### What you'll need

- The time must be synchronized on the server creating the certificates, the KMIP server, and the cluster.
- You must have obtained the public SSL KMIP client certificate for the cluster.
- You must have obtained the private key associated with the SSL KMIP client certificate for the cluster.

The SSL KMIP client certificate must not be password-protected.

- You must have obtained the SSL public certificate for the root certificate authority (CA) of the KMIP server.

You can install the client and server certificates on the KMIP server before or after installing the certificates on the cluster.

## About this task

In an HA pair, both nodes must use the same public and private KMIP SSL certificates. If you connect multiple HA pairs to the same KMIP server, all nodes in the HA pairs must use the same public and private KMIP SSL certificates.

## Steps

1. Install the SSL KMIP client certificates for the cluster:

```
security certificate install -vserver admin_svm_name -type client
```

You are prompted to enter the SSL KMIP public and private certificates.

```
cluster1::> security certificate install -vserver cluster1 -type client
```

2. Install the SSL public certificate for the root certificate authority (CA) of the KMIP server:

```
security certificate install -vserver admin_svm_name -type server-ca
```

```
cluster1::> security certificate install -vserver cluster1 -type server-ca
```

= Enable external key management in ONTAP 9.6 and later (NVE)

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

You can use one or more KMIP servers to secure the keys the cluster uses to access encrypted data. Beginning with ONTAP 9.6, you can use one or more KMIP servers to secure the keys a given SVM uses to access encrypted data.

Beginning in ONTAP 9.11.1, you can add up to 3 secondary key servers per primary key server to create a clustered key server. For more information, see [Configure clustered external key servers](#).

## Before you begin

- The KMIP SSL client and server certificates must have been installed.
- You must be a cluster or SVM administrator to perform this task.
- If you want to enable external key management for a MetroCluster environment, MetroCluster must be fully configured before enabling external key management.

## About this task

You can connect up to four KMIP servers to a cluster or SVM. A minimum of two servers is recommended for redundancy and disaster recovery.

The scope of external key management determines whether key management servers secure all the SVMs in the cluster or selected SVMs only:

- You can use a *cluster scope* to configure external key management for all the SVMs in the cluster. The cluster administrator has access to every key stored on the servers.
- Beginning with ONTAP 9.6, you can use an *SVM scope* to configure external key management for a data SVM in the cluster. That's best for multitenant environments in which each tenant uses a different SVM (or set of SVMs) to serve data. Only the SVM administrator for a given tenant has access to the

keys for that tenant.

- For multitenant environments, install a license for *MT\_EK\_MGMT* by using the following command:

```
system license add -license-code <MT_EK_MGMT license code>
```

For complete command syntax, see the man page for the command.

You can use both scopes in the same cluster. If key management servers have been configured for an SVM, ONTAP uses only those servers to secure keys. Otherwise, ONTAP secures keys with the key management servers configured for the cluster.

You can configure onboard key management at the cluster scope and external key management at the SVM scope. You can use the `security key-manager key migrate` command to migrate keys from onboard key management at the cluster scope to external key managers at the SVM scope.

### Steps

1. Configure key manager connectivity for the cluster:

```
security key-manager external enable -vserver admin_SVM -key-servers  
host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert  
server_CA_certificates
```

The `security key-manager external enable` command replaces the `security key-manager setup` command. If you run the command at the cluster login prompt, *admin\_SVM* defaults to the admin SVM of the current cluster. You must be the cluster administrator to configure cluster scope. You can run the `security key-manager external modify` command to change the external key management configuration.

+

The following command enables external key management for `cluster1` with three external key servers. The first key server is specified using its hostname and port, the second is specified using an IP address and the default port, and the third is specified using an IPv6 address and port:

+

```
cluster1::> security key-manager external enable -vserver cluster1 -key  
-servers  
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:123  
4 -client-cert AdminVserverClientCert -server-ca-certs  
AdminVserverServerCaCert
```

1. Configure a key manager an SVM:

```
security key-manager external enable -vserver SVM -key-servers  
host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert  
server_CA_certificates
```

If you run the command at the SVM login prompt, SVM defaults to the current SVM. You must be a cluster or SVM administrator to configure SVM scope. You can run the `security key-manager external modify` command to change the external key management configuration.

+

The following command enables external key management for `svm1` with a single key server listening on the default port 5696:

+

```
svm11::> security key-manager external enable -vserver svm1 -key
-servers keyserver.svm1.com -client-cert SVM1ClientCert -server-ca
-certs SVM1ServerCaCert
```

1. Repeat the last step for any additional SVMs.

You can also use the `security key-manager external add-servers` command to configure additional SVMs. The `security key-manager external add-servers` command replaces the `security key-manager add` command. For complete command syntax, see the man page.

1. Verify that all configured KMIP servers are connected:

```
security key-manager external show-status -node node_name
```

The `security key-manager external show-status` command replaces the `security key-manager show -status` command. For complete command syntax, see the man page.

+

```
cluster1::> security key-manager external show-status
```

Node	Vserver	Key Server	Status
-----			
-----			
node1			
	svm1	keyserver.svm1.com:5696	available
	cluster1	10.0.0.10:5696	available
		fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234	available
		ks1.local:15696	available
node2			
	svm1	keyserver.svm1.com:5696	available
	cluster1	10.0.0.10:5696	available
		fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234	available
		ks1.local:15696	available

```
8 entries were displayed.
```

= Enable external key management in ONTAP 9.5 and earlier

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

You can use one or more KMIP servers to secure the keys the cluster uses to access encrypted data. You can connect up to four KMIP servers to a node. A minimum of two servers is recommended for redundancy and disaster recovery.

### What you'll need

- The KMIP SSL client and server certificates must have been installed.
- You must be a cluster administrator to perform this task.
- You must configure the MetroCluster environment before you configure an external key manager.

### About this task

ONTAP configures KMIP server connectivity for all nodes in the cluster.

### Steps

1. Configure key manager connectivity for cluster nodes:

```
security key-manager setup
```



The key manager setup starts.

2. Enter the appropriate response at each prompt.
3. Add a KMIP server:

```
security key-manager add -address key_management_server_ipaddress
```

```
cluster1::> security key-manager add -address 20.1.1.1
```

4. Add an additional KMIP server for redundancy:

```
security key-manager add -address key_management_server_ipaddress
```

```
cluster1::> security key-manager add -address 20.1.1.2
```

5. Verify that all configured KMIP servers are connected:

```
security key-manager show -status
```

For complete command syntax, see the man page.

```
cluster1::> security key-manager show -status
```

Node	Port	Registered Key Manager	Status
cluster1-01	5696	20.1.1.1	available
cluster1-01	5696	20.1.1.2	available
cluster1-02	5696	20.1.1.1	available
cluster1-02	5696	20.1.1.2	available

= Manage keys with Azure Key Vault or Google Cloud KMS

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

:hardbreaks-option:

Beginning in ONTAP 9.10.1, you can use [Azure Key Vault \(AKV\)](#) and [Google Cloud Platform's Key Management Service \(Cloud KMS\)](#) to protect your ONTAP encryption keys in a Azure- or Google Cloud Platform-deployed application.

AKV and Cloud KMS can be used to protect [NetApp Volume Encryption \(NVE\) keys](#) only for data SVMs.

Key management with AKV or Cloud KMS can be enabled with the CLI or the ONTAP REST API.

When using AKV or Cloud KMS, be aware that by default a data SVM LIF is used to communicate with the cloud key management endpoint. A node management network is used to communicate with the cloud provider's authentication services (login.microsoftonline.com for Azure; oauth2.googleapis.com for

Cloud KMS). If the cluster network is not configured correctly, the cluster will not properly utilize the key management service.

### Prerequisites

- The ONTAP cluster's nodes must support NVE
- Volume Encryption (VE) license installed
- Multi-tenant Encryption Key Management (MTEKM) license installed
- You must be a cluster or SVM administrator

### Limitations

- AKV and Cloud KMS are not available for NSE and NAE. [External KMIPs](#) can be used instead
- AKV and Cloud KMS are not available for MetroCluster configurations.
- AKV and Cloud KMS can only be configured on a data SVM

== Enable external key management with the CLI

Enabling external key management depends on the specific key manager you use. If you are enabling AKV in a Cloud Volumes ONTAP, note that there is a separate procedure. Choose the tab of the key manager and environment that suits your needs:

## Azure

### Enable Azure Key Vault for ONTAP

1. Before you begin, you need to obtain the appropriate authentication credentials from your Azure account, either a client secret or certificate.  
You must also ensure all nodes in the cluster are healthy. You can check this with the command `cluster show`.

2. Set privileged level to advanced  
`set -priv advanced`

3. Enable AKV on the SVM  
`security key-manager external azure enable -client-id client_id -tenant-id tenant_id -name -key-id key_id -authentication-method {certificate|client-secret}`  
When prompted, enter either the client certificate or client secret from your Azure account.

4. Verify AKV is enabled correctly:  
`security key-manager external azure show vservers SVM_name`  
If the service reachability is not OK, establish the connectivity to the AKV key management service via data SVM LIF.

## Google Cloud

### Enable Cloud KMS with the CLI for ONTAP

1. Before you begin, you need to obtain the private key for the Google Cloud KMS account key file in a JSON format. This can be found in your GCP account.  
You must also ensure all nodes in the cluster are healthy. You can check this with the command `cluster show`.
2. Set privileged level to advanced  
`set -priv advanced`

### 3. Enable Cloud KMS on the SVM

```
security key-manager external gcp enable -vserver data_svm_name -project-id  
project_id-key-ring-name key_ring_name -key-ring-location key_ring_location  
-key-name key_name
```

When prompted, enter the contents of the JSON file with the Service Account Private Key

### 4. Verify that Cloud KMS is configured with the correct parameters:

```
security key-manager external gcp show vserver SVM_name
```

The status of `kms_wrapped_key_status` will be "UNKNOWN" if no encrypted volumes have been created.

If the service reachability is not OK, establish the connectivity to the GCP key management service via data SVM LIF.

If one or more encrypted volumes is already configured for a data SVM and the corresponding NVE keys are managed by the admin SVM onboard key manager, those keys should be migrated to the external key management service. To do this with the CLI, run the command:

```
security key-manager key migrate -from-Vserver admin_SVM -to-Vserver data_SVM
```

New encrypted volumes cannot be created for the tenant's data vserver until all NVE keys of the data SVM are successfully migrated.

= Enable onboard key management in ONTAP 9.6 and later (NVE)

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

You can use the Onboard Key Manager to secure the keys that the cluster uses to access encrypted data. You must enable Onboard Key Manager on each cluster that accesses an encrypted volume or a self-encrypting disk.

### What you'll need

- You must be a cluster administrator to perform this task.
- You must configure the MetroCluster environment before you configure an external key manager.

### About this task

You must run the `security key-manager onboard sync` command each time you add a node to the cluster.

If you have a MetroCluster configuration you must run `security key-manager onboard enable` on the local cluster first, then run `security key-manager onboard sync` on the remote cluster, using the same passphrase on each.

By default, you are not required to enter the key manager passphrase when a node is rebooted. You can use the `cc-mode-enabled=yes` option to require that users enter the passphrase after a reboot.

For NVE, if you set `cc-mode-enabled=yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted. For `volume create`, you need not specify `-encrypt true`. For `volume move start`, you need not specify `-encrypt-destination true`.

When configuring ONTAP data at rest encryption, to meet the requirements for Commercial Solutions for Classified (CSfC) you must use NSE with NVE and ensure the Onboard Key Manager is enabled in Common Criteria mode. Refer to the [CSfC Solution Brief](#) for more information on CSfC.

When the Onboard Key Manager is enabled in Common Criteria mode (`cc-mode-enabled=yes`), system behavior is changed in the following ways:

- The system monitors for consecutive failed cluster passphrase attempts when operating in Common Criteria mode.

If you fail to enter the correct cluster passphrase at boot, encrypted volumes are not mounted. To correct this, you must reboot the node and enter the correct cluster passphrase. Once booted, the system allows up to 5 consecutive attempts to correctly enter the cluster passphrase in a 24-hour period for any command that requires the cluster passphrase as a parameter. If the limit is reached (for example, you have failed to correctly enter the cluster passphrase 5 times in a row) then you must either wait for the 24-

hour timeout period to elapse, or you must reboot the node, in order to reset the limit.

- System image updates use the NetApp RSA-3072 code signing certificate together with SHA-384 code signed digests to check the image integrity instead of the usual NetApp RSA-2048 code signing certificate and SHA-256 code signed digests.

The upgrade command verifies that the image contents have not been altered or corrupted by checking various digital signatures. The image update process proceeds to the next step if validation succeeds; otherwise, the image update fails. See the “cluster image” man page for information concerning system updates.



The Onboard Key Manager stores keys in volatile memory. Volatile memory contents are cleared when the system is rebooted or halted. Under normal operating conditions, volatile memory contents will be cleared within 30s when a system is halted.

### Steps

1. Start the key manager setup:

```
security key-manager onboard enable -cc-mode-enabled yes|no
```

Set `cc-mode-enabled=yes` to require that users enter the key manager passphrase after a reboot. For NVE, if you set `cc-mode-enabled=yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted. The `-cc-mode-enabled` option is not supported in MetroCluster configurations. The `security key-manager onboard enable` command replaces the `security key-manager setup` command.

+

The following example starts the key manager setup command on cluster1 without requiring that the passphrase be entered after every reboot:

+

```
cluster1::> security key-manager onboard enable
```

```
Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1":> <32..256 ASCII characters long text>
Reenter the cluster-wide passphrase: <32..256 ASCII characters long
text>
```

1. At the passphrase prompt, enter a passphrase between 32 and 256 characters, or for “cc-mode”, a passphrase between 64 and 256 characters.

If the specified “cc-mode” passphrase is less than 64 characters, there is a five-second delay before the key manager setup operation displays the passphrase prompt again.

1. At the passphrase confirmation prompt, reenter the passphrase.
2. Verify that the authentication keys have been created:

```
security key-manager key query -key-type NSE-AK
```

The `security key-manager key query` command replaces the `security key-manager query key` command. For complete command syntax, see the man page.

+

The following example verifies that authentication keys have been created for cluster1:

+

```

cluster1::> security key-manager key query -key-type NSE-AK
  Vserver: cluster1
  Key Manager: onboard
  Node: node1

Key Tag                                Key Type  Restored
-----                                -
node1                                  NSE-AK    yes
  Key ID:
000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e0000000
000000000
node1                                  NSE-AK    yes
  Key ID:
000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf7970000000
000000000

  Vserver: svm1
  Key Manager: onboard
  Node: node1
  Key Server: keyserver.svm1.com:5965

Key Tag                                Key Type  Restored
-----                                -
eb9f8311-e8d8-487e-9663-7642d7788a75  VEK       yes
  Key ID:
000000000000000000002000000000004001cb18336f7c8223743d3e75c6a7726e0000000
000000000
9d09cbbf-0da9-4696-87a1-8e083d8261bb  VEK       yes
  Key ID:
000000000000000000002000000000004064f2e1533356a470385274a9c3ffb9770000000
000000000

  Vserver: cluster1
  Key Manager: onboard
  Node: node2

Key Tag                                Key Type  Restored
-----                                -
node1                                  NSE-AK    yes
  Key ID:

```

```

000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e0000000
000000000
node1                               NSE-AK      yes
  Key ID:
000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf7970000000
000000000

  Vserver: svm1
  Key Manager: onboard
    Node: node2
  Key Server: keyserver.svm1.com:5965

Key Tag                               Key Type  Restored
-----
eb9f8311-e8d8-487e-9663-7642d7788a75  VEK      yes
  Key ID:
0000000000000000000020000000000004001cb18336f7c8223743d3e75c6a7726e0000000
000000000
9d09cbbf-0da9-4696-87a1-8e083d8261bb  VEK      yes
  Key ID:
0000000000000000000020000000000004064f2e1533356a470385274a9c3ffb9770000000
000000000

```

### After you finish

Copy the passphrase to a secure location outside the storage system for future use.

All key management information is automatically backed up to the replicated database (RDB) for the cluster. You should also back up the information manually for use in case of a disaster.

= Enable onboard key management in ONTAP 9.5 and earlier (NVE)

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

You can use the Onboard Key Manager to secure the keys that the cluster uses to access encrypted data. You must enable Onboard Key Manager on each cluster that accesses an encrypted volume or a self-encrypting disk.

### What you'll need

- If you are using NSE with an external key management (KMIP) server, you must have deleted the external key manager database.

[Transitioning to onboard key management from external key management](#)

- You must be a cluster administrator to perform this task.
- You must configure the MetroCluster environment before you configure the Onboard Key Manager.

### About this task



You must run the `security key-manager setup` command each time you add a node to the cluster.

If you have a MetroCluster configuration, review these guidelines:

- In ONTAP 9.5, you must run `security key-manager setup` on the local cluster and `security key-manager setup -sync-metrocluster-config yes` on the remote cluster, using the same passphrase on each.
- Prior to ONTAP 9.5, you must run `security key-manager setup` on the local cluster, wait approximately 20 seconds, and then run `security key-manager setup` on the remote cluster, using the same passphrase on each.

By default, you are not required to enter the key manager passphrase when a node is rebooted. Beginning with ONTAP 9.4, you can use the `-enable-cc-mode yes` option to require that users enter the passphrase after a reboot.

For NVE, if you set `-enable-cc-mode yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted. For `volume create`, you need not specify `-encrypt true`. For `volume move start`, you need not specify `-encrypt-destination true`.

After a failed passphrase attempt, you must reboot the node again.

### Steps

1. Start the key manager setup:

```
security key-manager setup -enable-cc-mode yes|no
```

Beginning with ONTAP 9.4, you can use the `-enable-cc-mode yes` option to require that users enter the key manager passphrase after a reboot. For NVE, if you set `-enable-cc-mode yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted.

+

The following example starts setting up the key manager on cluster1 without requiring that the passphrase be entered after every reboot:

+

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase:  <32..256 ASCII characters long
text>
```

1. Enter `yes` at the prompt to configure onboard key management.
2. At the passphrase prompt, enter a passphrase between 32 and 256 characters, or for “cc-mode”, a passphrase between 64 and 256 characters.

If the specified “cc-mode” passphrase is less than 64 characters, there is a five-second delay before the key manager setup operation displays the passphrase prompt again.

1. At the passphrase confirmation prompt, reenter the passphrase.
2. Verify that keys are configured for all nodes:

```
security key-manager key show
```

For the complete command syntax, see the man page.

```
cluster1::> security key-manager key show

Node: node1
Key Store: onboard
Key ID
Used By
-----
-----
0000000000000000000020000000000010059851742AF2703FC91369B7DB47C4722
NSE-AK
000000000000000000002000000000001008C07CC0AF1EF49E0105300EFC83004BF
NSE-AK

Node: node2
Key Store: onboard
Key ID
Used By
-----
-----
0000000000000000000020000000000010059851742AF2703FC91369B7DB47C4722
NSE-AK
000000000000000000002000000000001008C07CC0AF1EF49E0105300EFC83004BF
NSE-AK
```

### After you finish

Copy the passphrase to a secure location outside the storage system for future use.

All key management information is automatically backed up to the replicated database (RDB) for the cluster.

Whenever you configure the Onboard Key Manager passphrase, you should also back up the information manually to a secure location outside the storage system for use in case of a disaster. See [Back up onboard key management information manually](#).

= Enable onboard key management in newly added nodes

```
:icons: font
```

```
:relative_path: ./encryption-at-rest/
```

```
:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/
```

You can use the Onboard Key Manager to secure the keys that the cluster uses to

access encrypted data. You must enable Onboard Key Manager on each cluster that accesses an encrypted volume or a self-encrypting disk.

For ONTAP 9.5 and earlier, you must run the `security key-manager setup` command each time you add a node to the cluster.

For ONTAP 9.6 and later, you must run the `security key-manager sync` command each time you add a node to the cluster.

If you add a node to a cluster that has onboard key management configured, you will run this command to refresh the missing keys.

If you have a MetroCluster configuration, review these guidelines:

- Beginning with ONTAP 9.6, you must run `security key-manager onboard enable` on the local cluster first, then run `security key-manager onboard sync` on the remote cluster, using the same passphrase on each.
- In ONTAP 9.5, you must run `security key-manager setup` on the local cluster and `security key-manager setup -sync-metrocluster-config yes` on the remote cluster, using the same passphrase on each.
- Prior to ONTAP 9.5, you must run `security key-manager setup` on the local cluster, wait approximately 20 seconds, and then run `security key-manager setup` on the remote cluster, using the same passphrase on each.

By default, you are not required to enter the key manager passphrase when a node is rebooted. Beginning with ONTAP 9.4, you can use the `-enable-cc-mode yes` option to require that users enter the passphrase after a reboot.

For NVE, if you set `-enable-cc-mode yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted. For `volume create`, you need not specify `-encrypt true`. For `volume move start`, you need not specify `-encrypt-destination true`.

After a failed passphrase attempt, you must reboot the node again.

= Encrypt volume data with NVE

= Encrypt volume data with NVE overview

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

Beginning with ONTAP 9.7, aggregate and volume encryption is enabled by default when you have the VE license and onboard or external key management. For ONTAP 9.6 and earlier, you can enable encryption on a new volume or on an existing volume. You must have installed the VE license and enabled key management before you can enable volume encryption. NVE is FIPS-140-2 level 1 compliant.

= Enable aggregate-level encryption with VE license

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

Beginning with ONTAP 9.7, newly created aggregates and volumes are encrypted by default when you have the VE license and onboard or external key management. Beginning with ONTAP 9.6, you can use aggregate-level encryption to assign keys to the containing aggregate for the volumes to be encrypted. Volumes you create in the aggregate are encrypted by default. You can override the default when you encrypt the volume.

### What you'll need

You must be a cluster administrator to perform this task.

### About this task

You must use aggregate-level encryption if you plan to perform inline or background aggregate-level deduplication. Aggregate-level deduplication is otherwise not supported by NVE.

An aggregate enabled for aggregate-level encryption is called an *NAE aggregate* (for NetApp Aggregate Encryption). Plain text volumes are not supported in NAE aggregates.

### Steps

1. Enable or disable aggregate-level encryption:

To...	Use this command...
Create an NAE aggregate with ONTAP 9.7 or later	<code>storage aggregate create -aggregate aggregate_name -node node_name</code>
Create an NAE aggregate with ONTAP 9.6	<code>storage aggregate create -aggregate aggregate_name -node node_name -encrypt-with -aggr-key true</code>

Convert a non-NAE aggregate to an NAE aggregate	<code>storage aggregate modify -aggregate aggregate_name -node node_name -encrypt-with -aggr-key true</code>
Convert an NAE aggregate to a non-NAE aggregate	<code>storage aggregate modify -aggregate aggregate_name -node node_name -encrypt-with -aggr-key false</code>

For complete command syntax, see the man pages.

The following command enables aggregate-level encryption on `aggr1`:

- ONTAP 9.7 or later:

```
cluster1::> storage aggregate create -aggregate aggr1
```

- ONTAP 9.6 or earlier:

```
cluster1::> storage aggregate create -aggregate aggr1 -encrypt
-with-aggr-key true
```

## 2. Verify that the aggregate is enabled for encryption:

```
storage aggregate show -fields encrypt-with-aggr-key
```

For complete command syntax, see the man page.

The following command verifies that `aggr1` is enabled for encryption:

```
cluster1::> storage aggregate show -fields encrypt-with-aggr-key
aggregate          encrypt-aggr-key
-----
aggr0_vsim4        false
aggr1               true
2 entries were displayed.
```

### After you finish

Run the `volume create` command to create the encrypted volumes.

If you are using a KMIP server to store the encryption keys for a node, ONTAP automatically “pushes” an encryption key to the server when you encrypt a volume.

= Enable encryption on a new volume

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

You can use the `volume create` command to enable encryption on a new volume.

### About this task

Beginning with ONTAP 9.2, you can enable encryption on a SnapLock volume.

Beginning with ONTAP 9.4, if you enable “cc-mode” when you set up the Onboard Key Manager, volumes you create with the `volume create` command are automatically encrypted, whether or not you specify `-encrypt true`.

Beginning with ONTAP 9.6, you can use aggregate-level encryption to assign keys to the containing aggregate for the volumes to be encrypted. Volumes you create in the aggregate are encrypted by default. You can use the `-encrypt` option to override the default when you create the volume.

Beginning with ONTAP 9.7, newly created volumes are encrypted by default when you have the VE license and onboard or external key management.

A volume encrypted with a unique key is called an *NVE volume*. A volume encrypted with an aggregate-level key is called an *NAE aggregate* (for NetApp Aggregate Encryption). Plaintext volumes are not supported in NAE aggregates.

### Steps

1. Create a new volume and specify whether encryption is enabled on the volume:

To create...	Use this command...
An ONTAP 9.7 or later NAE volume	<code>volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name</code>
An ONTAP 9.6 NAE volume (assuming aggregate-level encryption is enabled)	<code>volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name</code>
An ONTAP 9.7 or later NVE volume	<code>volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name</code>
An ONTAP 9.6 or earlier NVE volume	<code>volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name -encrypt true</code>
A plain text volume	<code>volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name -encrypt false</code>

For complete command syntax, see the man page for the command.

Beginning with ONTAP 9.7 or later, the following command creates an NAE volume named `vol1` on `aggr1`:

```
cluster1::> volume create -vserver vs1 -volume vol1 -aggregate agr1
```

Using ONTAP 9.6, assuming aggregate-level encryption is enabled, the following command creates an NAE volume named `vol1` on `agr1`:

```
cluster1::> volume create -vserver vs1 -volume vol1 -aggregate agr1
```

Beginning with ONTAP 9.7 or later, the following command creates an NVE volume named `vol2` on `agr1`:

```
cluster1::> volume create -vserver vs1 -volume vol2 -aggregate agr1
```

Using ONTAP 9.6 or earlier, the following command creates an NVE volume named `vol2` on `agr1`:

```
cluster1::> volume create -vserver vs1 -volume vol2 -aggregate agr1
-encrypt true
```

The following command creates a plaintext volume named `vol3` on `agr1`:

```
cluster1::> volume create -vserver vs1 -volume vol3 -aggregate agr1
-encrypt false
```

## 2. Verify that volumes are enabled for encryption:

```
volume show -is-encrypted true
```

For complete command syntax, see the man page for the command.

The following command displays the encrypted volumes on `cluster2`:

```
cluster2::> volume show -is-encrypted true
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used
vs1	vol1	agr2	online	RW	200GB	160.0GB	20%

### Result

If you are using a KMIP server to store the encryption keys for a node, ONTAP automatically “pushes” an encryption key to the server when you encrypt a volume.

= Enable encryption on an existing volume with the volume encryption conversion start command



```
:icons: font  
:relative_path: ./encryption-at-rest/  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/
```

Beginning with ONTAP 9.3, you can use the `volume encryption conversion start` command to enable encryption of an existing volume "in place," without having to move the volume to a different location.

**About this task**

Once you start a conversion operation, it must complete. If you encounter a performance issue during the operation, you can run the `volume encryption conversion pause` command to pause the operation, and the `volume encryption conversion resume` command to resume the operation.

You cannot use `volume encryption conversion start` to convert a SnapLock volume.

## Steps

1. Enable encryption on an existing volume:

```
volume encryption conversion start -vserver SVM_name -volume volume_name
```

For complete command syntax, see the man page for the command.

The following command enables encryption on the existing volume `vol1`:

```
cluster1::> volume encryption conversion start -vserver vs1 -volume
vol1
```

The system creates an encryption key for the volume. The data on the volume is encrypted.

2. Verify the status of the conversion operation:

```
volume encryption conversion show
```

For complete command syntax, see the man page for the command.

The following command displays the status of the conversion operation:

```
cluster1::> volume encryption conversion show
```

Vserver	Volume	Start Time	Status
vs1	vol1	9/18/2017 17:51:41	Phase 2 of 2 is in progress.

3. When the conversion operation is complete, verify that the volume is enabled for encryption:

```
volume show -is-encrypted true
```

For complete command syntax, see the man page for the command.

The following command displays the encrypted volumes on `cluster1`:

```
cluster1::> volume show -is-encrypted true
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used
vs1	vol1	aggr2	online	RW	200GB	160.0GB	20%

## Result

If you are using a KMIP server to store the encryption keys for a node, ONTAP automatically “pushes” an encryption key to the server when you encrypt a volume.

= Enable encryption on an existing volume with the volume move start command

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

You can use the `volume move start` command to enable encryption by moving an existing volume. You must use `volume move start` in ONTAP 9.2 and earlier. You can use the same aggregate or a different aggregate.

### What you'll need

You must be a cluster administrator to perform this task, or an SVM administrator to whom the cluster administrator has delegated authority.

### Delegating authority to run the volume move command

### About this task

Beginning with ONTAP 9.8, you can use `volume move start` to enable encryption on a SnapLock or FlexGroup volume.

Beginning with ONTAP 9.4, if you enable “cc-mode” when you set up the Onboard Key Manager, volumes you create with the `volume move start` command are automatically encrypted. You need not specify `-encrypt-destination true`.

Beginning with ONTAP 9.6, you can use aggregate-level encryption to assign keys to the containing aggregate for the volumes to be moved. A volume encrypted with a unique key is called an *NVE volume*. A volume encrypted with an aggregate-level key is called an *NAE volume* (for NetApp Aggregate Encryption). Plaintext volumes are not supported in NAE aggregates.

### Steps

1. Move an existing volume and specify whether encryption is enabled on the volume:

To convert...	Use this command...
A plaintext volume to an NVE volume	<code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination true</code>
An NVE or plaintext volume to an NAE volume (assuming aggregate-level encryption is enabled on the destination)	<code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key true</code>
An NAE volume to an NVE volume	<code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key false</code>
An NAE volume to a plaintext volume	<code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false -encrypt-with-aggr-key false</code>

An NVE volume to a plaintext volume

```
volume move start -vserver SVM_name -volume
volume_name -destination-aggregate
aggregate_name -encrypt-destination false
```

For complete command syntax, see the man page for the command.

The following command converts a plaintext volume named `vol1` to an NVE volume:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-destination true
```

Assuming aggregate-level encryption is enabled on the destination, the following command converts an NVE or plaintext volume named `vol1` to an NAE volume:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-with-aggr-key true
```

The following command converts an NAE volume named `vol2` to an NVE volume:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-with-aggr-key false
```

The following command converts an NAE volume named `vol2` to a plaintext volume:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false -encrypt-with-aggr-key
false
```

The following command converts an NVE volume named `vol2` to a plaintext volume:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false
```

## 2. View the encryption type of cluster volumes:

```
volume show -fields encryption-type none|volume|aggregate
```

The `encryption-type` field is available in ONTAP 9.6 and later.

For complete command syntax, see the man page for the command.

The following command displays the encryption type of volumes in `cluster2`:

```
cluster2::> volume show -fields encryption-type
```

```
vserver  volume  encryption-type
-----  -
vs1      vol11    none
vs2      vol12    volume
vs3      vol13    aggregate
```

### 3. Verify that volumes are enabled for encryption:

```
volume show -is-encrypted true
```

For complete command syntax, see the man page for the command.

The following command displays the encrypted volumes on `cluster2`:

```
cluster2::> volume show -is-encrypted true
```

```
Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-----  -
vs1      vol11   aggr2      online  RW   200GB  160.0GB   20%
```

## Result

If you are using a KMIP server to store the encryption keys for a node, ONTAP automatically “pushes” an encryption key to the server when you encrypt a volume.

= Enable node root volume encryption

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

Beginning with ONTAP 9.8, you can use NetApp Volume Encryption to protect the root volume of your node.

### What you'll need

- Your system must be using an HA configuration.

Root volume encryption is not supported on single node configurations.

- Your node root volume must already be created.
- Your system must have an onboard key manager or an external key management server using the Key Management Interoperability Protocol (KMIP).

This procedure applies to the node root volume. It does not apply to SVM root volumes. SVM root volumes can be protected through aggregate-level encryption.

Once root volume encryption begins, it must complete. You cannot pause the operation. Once encryption is complete, you cannot assign a new key to the root volume and you cannot perform a secure-purge operation.

### Steps

1. Encrypt the root volume:

```
volume encryption conversion start -vserver SVM_name -volume root_vol_name
```

2. Verify the status of the conversion operation:

```
volume encryption conversion show
```

3. When the conversion operation is complete, verify that the volume is encrypted:

```
volume show -fields
```

The following shows example output for an encrypted volume.

```
::> volume show -vserver xyz -volume vol0 -fields is-encrypted
vserver      volume is-encrypted
-----
xyz          vol0    true
```

= Configure NetApp hardware-based encryption

= Configure NetApp hardware-based encryption overview

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

NetApp hardware-based encryption supports full-disk encryption (FDE) of data as it is written. The data cannot be read without an encryption key stored on the firmware. The encryption key, in turn, is accessible only to an authenticated node.

== Understanding NetApp hardware-based encryption

A node authenticates itself to a self-encrypting drive using an authentication key retrieved from an external key management server or Onboard Key Manager:

- The external key management server is a third-party system in your storage environment that serves keys to nodes using the Key Management Interoperability Protocol (KMIP). It is a best practice to configure external key management servers on a different storage system from your data.
- The Onboard Key Manager is a built-in tool that serves authentication keys to nodes from the same storage system as your data.

You can use NetApp Volume Encryption with hardware-based encryption to “double encrypt” data on self-encrypting drives.

AFF A220, AFF A800, FAS2720, FAS2750, and later systems store core dumps on their boot device.

When self-encrypting drives are enabled on these systems, the core dump is also encrypted.



If an HA pair is using encrypting SAS or NVMe drives (SED, NSE, FIPS), you must follow the instructions in the topic [Returning a FIPS drive or SED to unprotected mode](#) for all drives within the HA pair prior to initializing the system (boot options 4 or 9). Failure to do this may result in future data loss if the drives are repurposed.

== Supported self-encrypting drive types

Two types of self-encrypting drives are supported:

- Self-encrypting FIPS-certified SAS or NVMe drives are supported on all FAS and AFF systems. These drives, called *FIPS drives*, conform to the requirements of Federal Information Processing Standard Publication 140-2, level 2. The certified capabilities enable protections in addition to encryption, such as preventing denial-of-service attacks on the drive. FIPS drives cannot be mixed with other types of drives on the same node or HA pair.
- Beginning with ONTAP 9.6, self-encrypting NVMe drives that have not undergone FIPS testing are supported on AFF A800, A320, and later systems. These drives, called *SEDs*, offer the same encryption capabilities as FIPS drives, but can be mixed with non-encrypting drives on the same node or HA pair.
- All FIPS validated drives use a firmware cryptographic module that has been through FIPS validation. The FIPS drive cryptographic module does not use any keys that are generated outside of the drive (the authentication passphrase that is input to the drive is used by the drive's firmware cryptographic module to obtain a key encryption key).



Non-encrypting drives are drives that are not SEDs or FIPS drives.

== When to use external key management

Although it is less expensive and typically more convenient to use the onboard key manager, you should use external key management if any of the following are true:

- Your organization's policy requires a key management solution that uses a FIPS 140-2 Level 2 (or higher) cryptographic module.
- You need a multi-cluster solution, with centralized management of encryption keys.
- Your business requires the added security of storing authentication keys on a system or in a location different from the data.

== Support details

The following table shows important hardware encryption support details. See the Interoperability Matrix for the latest information about supported KMIP servers, storage systems, and disk shelves.

Resource or feature	Support details
Non-homogeneous disk sets	<ul style="list-style-type: none"><li>• FIPS drives cannot be mixed with other types of drives on the same node or HA pair. Conforming HA pairs can coexist with non-conforming HA pairs in the same cluster.</li><li>• SEDs can be mixed with non-encrypting drives on the same node or HA pair.</li></ul>

Drive type	<ul style="list-style-type: none"> <li>• FIPS drives can be SAS or NVMe drives.</li> <li>• SEDs must be NVMe drives.</li> </ul>
10 Gb network interfaces	Beginning with ONTAP 9.3, KMIP key management configurations support 10 Gb network interfaces for communications with external key management servers.
Ports for communication with the key management server	Beginning with ONTAP 9.3, you can use any storage controller port for communication with the key management server. Otherwise, you should use port e0M for communication with key management servers. Depending on the storage controller model, certain network interfaces might not be available during the boot process for communication with key management servers.
MetroCluster (MCC)	<ul style="list-style-type: none"> <li>• NVMe drives support MCC.</li> <li>• SAS drives do not support MCC.</li> </ul>

### Related information

[NetApp Hardware Universe](#)

= Hardware-based encryption workflow

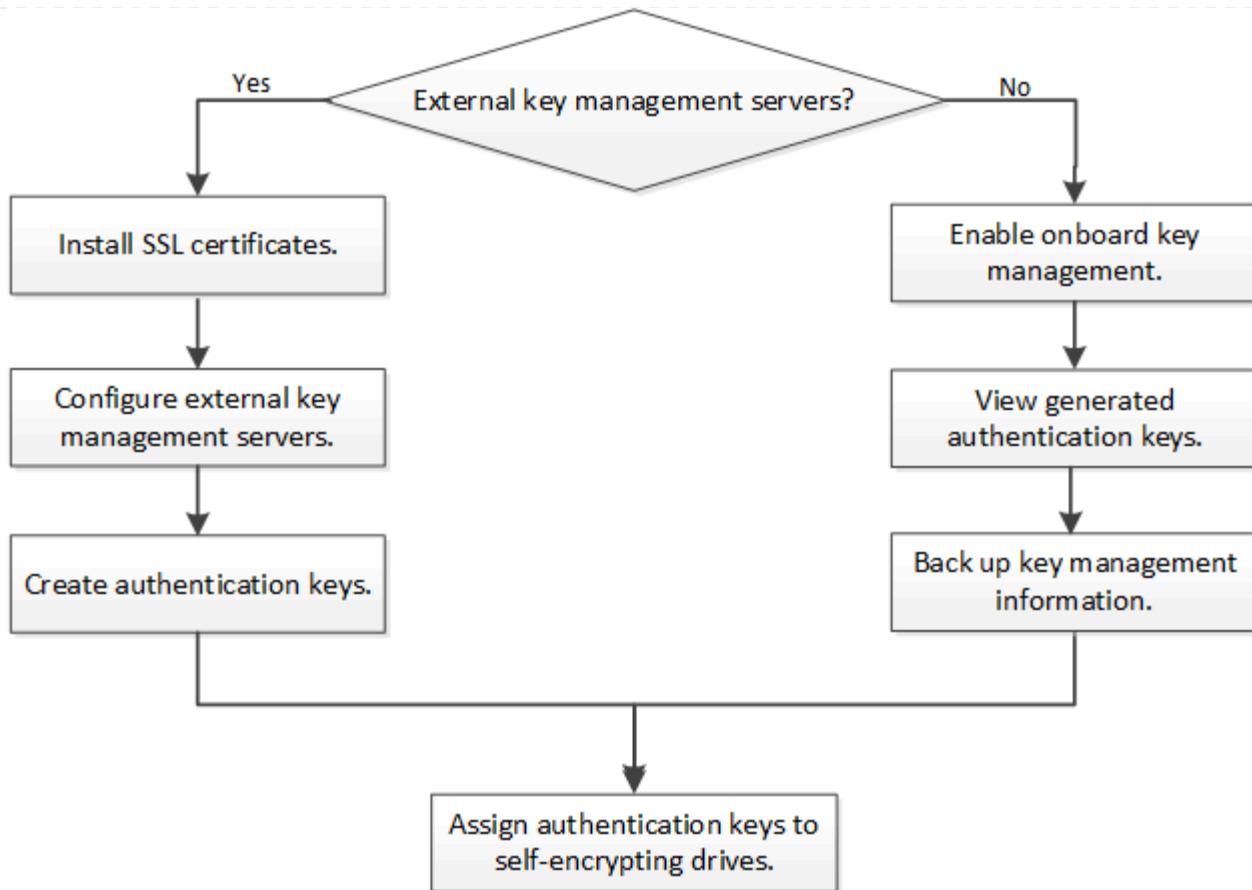
:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

You must configure key management services before the cluster can authenticate itself to the self-encrypting drive. You can use an external key management server or an onboard key manager.





= Configure external key management

= Configure external key management overview

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

You can use one or more external key management servers to secure the keys that the cluster uses to access encrypted data. An external key management server is a third-party system in your storage environment that serves keys to nodes using the Key Management Interoperability Protocol (KMIP).

For ONTAP 9.1 and earlier versions, node management LIFs must be assigned to ports that are configured with the node management role before you can use the external key manager.

NetApp Volume Encryption (NVE) can be implemented with Onboard Key Manager in ONTAP 9.1 and later. In ONTAP 9.3 and later, NVE can be implemented with external key management (KMIP) and Onboard Key Manager. Beginning in ONTAP 9.11.1, you can configure multiple external key managers in a cluster. See [Configure clustered key servers](#).

= Collect network information in ONTAP 9.2 and earlier

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

If you are using ONTAP 9.2 or earlier, you should fill out the network configuration

worksheet before enabling external key management.

Beginning with ONTAP 9.3, the system discovers all needed network information automatically.

Item	Notes	Value
Key management network interface name		
Key management network interface IP address	IP address of node management LIF, in IPv4 or IPv6 format	
Key management network interface IPv6 network prefix length	If you are using IPv6, the IPv6 network prefix length	
Key management network interface subnet mask		
Key management network interface gateway IP address		
IPv6 address for the cluster network interface	Required only if you are using IPv6 for the key management network interface	
Port number for each KMIP server	Optional. The port number must be the same for all KMIP servers. If you do not provide a port number, it defaults to port 5696, which is the Internet Assigned Numbers Authority (IANA) assigned port for KMIP.	
Key tag name	Optional. The key tag name is used to identify all keys belonging to a node. The default key tag name is the node name.	

### Related information

[NetApp Technical Report 3954: NetApp Storage Encryption Preinstallation Requirements and Procedures for IBM Tivoli Lifetime Key Manager](#)

[NetApp Technical Report 4074: NetApp Storage Encryption Preinstallation Requirements and Procedures for SafeNet KeySecure](#)

= Install SSL certificates on the cluster

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

The cluster and KMIP server use KMIP SSL certificates to verify each other's identity and establish an SSL connection. Before configuring the SSL connection with the KMIP server, you must install the KMIP client SSL certificates for the cluster, and the

## SSL public certificate for the root certificate authority (CA) of the KMIP server.

### What you'll need

- The time must be synchronized on the server creating the certificates, the KMIP server, and the cluster.
- You must have obtained the public SSL KMIP client certificate for the cluster.
- You must have obtained the private key associated with the SSL KMIP client certificate for the cluster.

The SSL KMIP client certificate must not be password-protected.

- You must have obtained the SSL public certificate for the root certificate authority (CA) of the KMIP server.

You can install the client and server certificates on the KMIP server before or after installing the certificates on the cluster.

## About this task

In an HA pair, both nodes must use the same public and private KMIP SSL certificates. If you connect multiple HA pairs to the same KMIP server, all nodes in the HA pairs must use the same public and private KMIP SSL certificates.

## Steps

1. Install the SSL KMIP client certificates for the cluster:

```
security certificate install -vserver admin_svm_name -type client
```

You are prompted to enter the SSL KMIP public and private certificates.

```
cluster1::> security certificate install -vserver cluster1 -type client
```

2. Install the SSL public certificate for the root certificate authority (CA) of the KMIP server:

```
security certificate install -vserver admin_svm_name -type server-ca
```

```
cluster1::> security certificate install -vserver cluster1 -type server-ca
```

= Enable external key management in ONTAP 9.6 and later (HW-based)

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

You can use one or more KMIP servers to secure the keys the cluster uses to access encrypted data. You can connect up to four KMIP servers to a node. A minimum of two servers is recommended for redundancy and disaster recovery.

Beginning in ONTAP 9.11.1, you can add up to 3 secondary key servers per primary key server to create a clustered key server. For more information, see [Configure clustered external key servers](#).

## Before you begin

- The KMIP SSL client and server certificates must have been installed.
- You must be a cluster administrator to perform this task.
- You must configure the MetroCluster environment before you configure an external key manager.

## Steps

1. Configure key manager connectivity for the cluster:

```
security key-manager external enable -vserver admin_SVM -key-servers  
host_name|IP_address:port,... -client-cert client_certificate -server-ca  
-cert server_CA_certificates
```

The `security key-manager external enable` command replaces the `security key-manager setup` command. You can run the `security key-manager external modify` command to change the external key management configuration. For complete command syntax, see the man pages.

+

The following command enables external key management for `cluster1` with three external key servers. The first key server is specified using its hostname and port, the second is specified using an IP address and the default port, and the third is specified using an IPv6 address and port:

+

```
cluster1::> security key-manager external enable -key-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:123
4 -client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

1. Verify that all configured KMIP servers are connected:

```
security key-manager external show-status -node node_name -vserver SVM -key
-server host_name|IP_address:port -key-server-status available|not-
responding|unknown
```

The `security key-manager external show-status` command replaces the `security key-manager show -status` command. For complete command syntax, see the man page.

+

```
cluster1::> security key-manager external show-status

Node  Vserver  Key Server                                     Status
----  -
node1
  cluster1
    10.0.0.10:5696                             available
    fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234 available
    ks1.local:15696                             available
node2
  cluster1
    10.0.0.10:5696                             available
    fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234 available
    ks1.local:15696                             available

6 entries were displayed.
```

= Enable external key management in ONTAP 9.5 and earlier

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

You can use one or more KMIP servers to secure the keys the cluster uses to access encrypted data. You can connect up to four KMIP servers to a node. A minimum of two servers is recommended for redundancy and disaster recovery.

### What you'll need

- The KMIP SSL client and server certificates must have been installed.
- You must be a cluster administrator to perform this task.
- You must configure the MetroCluster environment before you configure an external key manager.

### About this task

ONTAP configures KMIP server connectivity for all nodes in the cluster.

### Steps

1. Configure key manager connectivity for cluster nodes:

```
security key-manager setup
```

The key manager setup starts.

2. Enter the appropriate response at each prompt.
3. Add a KMIP server:

```
security key-manager add -address key_management_server_ipaddress
```

```
cluster1::> security key-manager add -address 20.1.1.1
```

4. Add an additional KMIP server for redundancy:

```
security key-manager add -address key_management_server_ipaddress
```

```
cluster1::> security key-manager add -address 20.1.1.2
```

5. Verify that all configured KMIP servers are connected:

```
security key-manager show -status
```

For complete command syntax, see the man page.

```
cluster1::> security key-manager show -status
```

Node	Port	Registered Key Manager	Status
cluster1-01	5696	20.1.1.1	available
cluster1-01	5696	20.1.1.2	available
cluster1-02	5696	20.1.1.1	available
cluster1-02	5696	20.1.1.2	available

= Configure clustered external key servers

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

Beginning in ONTAP 9.11.1, you can configure connectivity to clustered external key management servers on an SVM. With clustered key servers, you can designate primary and secondary key servers on a SVM. When registering keys, ONTAP will first attempt to access a primary key server before sequentially attempting to access secondary servers until the operation completes successfully, preventing duplication of keys.

External key servers can be used for NSE, NVE, NAE, and SED keys. An SVM can support up to four primary external KMIP servers. Each primary server can support up to three secondary key servers.

== Before you begin

\* [KMIP key management is already enabled for the SVM.](#)

\* This process only supports key servers that use KMIP. For a list of supported key servers, check the [NetApp Interoperability Matrix Tool](#).



\* All nodes in the cluster must be running ONTAP 9.11.1 or later.

\* The order of servers list arguments in the `-secondary-key-servers` parameter reflects the access order of the external key management (KMIP) servers.

== Create a clustered key server

The configuration procedure depends on whether or not you have configured a primary key server.

### Add primary and secondary key servers to an SVM

1. Confirm that no key management has been enabled for the cluster:

```
security key-manager external show -vserver vserver_name
```

If the SVM already has the maximum of four primary key servers enabled, you must remove one of the existing primary key servers before adding a new one.

2. Enable the primary key manager:

```
security key-manager external enable -vserver vserver_name -key-servers  
server_ip -client-cert client_cert_name -server-ca-certs server_ca_cert_names
```

3. Modify the primary key server to add secondary key servers. The `-secondary-key-servers` parameter accepts a comma-separated list of up to three key servers.

```
security key-manager external modify-server -vserver vserver_name -key-servers  
primary_key_server -secondary-key-servers list_of_key_servers
```

### Add secondary key servers to an existing primary key server

1. Modify the primary key server to add secondary key servers. The `-secondary-key-servers` parameter accepts a comma-separated list of up to three key servers.

```
security key-manager external modify-server -vserver vserver_name -key-servers  
primary_key_server -secondary-key-servers list_of_key_servers
```

For more information about secondary key servers, see [\[mod-secondary\]](#).

## == Modify clustered key servers

You can modify external key servers clusters by changing the status (primary or secondary) of particular key servers, add and removing secondary key servers, or by changing the access order of secondary key servers.

### === Converting primary and secondary key servers

To convert a primary key server into a secondary key server, you must first remove it from the SVM with the `security key-manager external remove-servers` command.

To convert a secondary key server into a primary key server, you must first remove the secondary key server from its existing primary key server. See [\[mod-secondary\]](#). If you convert a secondary key server to a primary server while removing an existing key, attempting to add a new server before completing the removal and conversion can result in the the duplication of keys.

### === Modifying secondary key servers

Secondary key servers are managed with the `-secondary-key-servers` parameter of the `security key-manager external modify-server` command. The `-secondary-key-servers` parameter accepts a comma-separated list. The specified order of the secondary key servers in the list determines the access sequence for the secondary key servers. The access order can be modified by running the command `security key-manager external modify-server` with the secondary key servers entered in a different sequence.

To remove a secondary key server, the `-secondary-key-servers` arguments should include the key servers you want to keep while omitting the one to be removed. To remove all secondary key servers, use the argument `-`, signifying none.

For additional information, refer to the `security key-manager external` page in the [ONTAP command reference](#).

## = Create authentication keys in ONTAP 9.6 and later

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

You can use the `security key-manager key create` command to create the authentication keys for a node and store them on the configured KMIP servers.

### What you'll need

You must be a cluster administrator to perform this task.

### About this task

If your security setup requires you to use different keys for data authentication and FIPS 140-2 authentication, you should create a separate key for each. If that is not the case, you can use the same authentication key for FIPS compliance that you use for data access.

ONTAP creates authentication keys for all nodes in the cluster.

- This command is not supported when Onboard Key Manager is enabled. However, two authentication keys are created automatically when Onboard Key Manager is enabled. The keys can be viewed with the following command:

```
security key-manager key query -key-type NSE-AK
```

- You receive a warning if the configured key management servers are already storing more than 128 authentication keys.

You can use the `security key-manager key delete` command to delete any unused keys. The `security key-manager key delete` command fails if the given key is currently in use by ONTAP. (You must have privileges greater than “admin” to use this command.)

### Steps

1. Create the authentication keys for cluster nodes:

```
security key-manager key create -key-tag passphrase_label -prompt-for-key true|false
```

Setting `prompt-for-key=true` causes the system to prompt the cluster administrator for the passphrase to use when authenticating encrypted drives. Otherwise, the system automatically generates a 32-byte passphrase. The `security key-manager key create` command replaces the `security key-manager create-key` command. For complete command syntax, see the man page.

+

The following example creates the authentication keys for `cluster1`, automatically generating a 32-byte passphrase:

+

```
cluster1::> security key-manager key create
Key ID:
000000000000000000002000000000001006268333f870860128fbe17d393e5083b0000000
000000000
```

1. Verify that the authentication keys have been created:

```
security key-manager key query -node node
```

The `security key-manager key query` command replaces the `security key-manager query key` command. For complete command syntax, see the man page. The key ID displayed in the output is an identifier used to refer to the authentication key. It is not the actual authentication key or the data encryption key.

+

The following example verifies that authentication keys have been created for cluster1:

+

```

cluster1::> security key-manager key query
      Vserver: cluster1
      Key Manager: external
      Node: node1

Key Tag                                Key Type  Restored
-----                                -
node1                                   NSE-AK    yes
  Key ID:
000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e0000000
000000000
node1                                   NSE-AK    yes
  Key ID:
000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf7970000000
000000000

      Vserver: cluster1
      Key Manager: external
      Node: node2

Key Tag                                Key Type  Restored
-----                                -
node2                                   NSE-AK    yes
  Key ID:
000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e0000000
000000000
node2                                   NSE-AK    yes
  Key ID:
000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf7970000000
000000000

```

= Create authentication keys in ONTAP 9.5 and earlier

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./nas-audit/./media/

You can use the `security key-manager create-key` command to create the authentication keys for a node and store them on the configured KMIP servers.

**What you'll need**

You must be a cluster administrator to perform this task.

### About this task

If your security setup requires you to use different keys for data authentication and FIPS 140-2 authentication, you should create a separate key for each. If that is not the case, you can use the same authentication key for FIPS compliance that you use for data access.

ONTAP creates authentication keys for all nodes in the cluster.

- This command is not supported when onboard key management is enabled.
- You receive a warning if the configured key management servers are already storing more than 128 authentication keys.

You can use the key management server software to delete any unused keys, then run the command again.

### Steps

1. Create the authentication keys for cluster nodes:

```
security key-manager create-key
```

For complete command syntax, see the man page for the command.

The key ID displayed in the output is an identifier used to refer to the authentication key. It is not the actual authentication key or the data encryption key.

+

The following example creates the authentication keys for `cluster1`:

+

```
cluster1::> security key-manager create-key
  (security key-manager create-key)
Verifying requirements...

Node: cluster1-01
Creating authentication key...
Authentication key creation successful.
Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

Node: cluster1-01
Key manager restore operation initialized.
Successfully restored key information.

Node: cluster1-02
Key manager restore operation initialized.
Successfully restored key information.
```

1. Verify that the authentication keys have been created:

```
security key-manager query
```

For complete command syntax, see the man page.

The following example verifies that authentication keys have been created for `cluster1`:

```

cluster1::> security key-manager query

(security key-manager query)

      Node: cluster1-01
    Key Manager: 20.1.1.1
  Server Status: available

Key Tag          Key Type  Restored
-----          -
cluster1-01     NSE-AK   yes
      Key ID:
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C

      Node: cluster1-02
    Key Manager: 20.1.1.1
  Server Status: available

Key Tag          Key Type  Restored
-----          -
cluster1-02     NSE-AK   yes
      Key ID:
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C

```

= Assign a data authentication key to a FIPS drive or SED (external key management)

You can use the `storage encryption disk modify` command to assign a data authentication key to a FIPS drive or SED. Cluster nodes use this key to lock or unlock encrypted data on the drive.

### What you'll need

You must be a cluster administrator to perform this task.

### About this task

A self-encrypting drive is protected from unauthorized access only if its authentication key ID is set to a non-default value. The manufacturer secure ID (MSID), which has key ID 0x0, is the standard default value for SAS drives. For NVMe drives, the standard default value is a null key, represented as a blank key ID. When you assign the key ID to a self-encrypting drive, the system changes its authentication key ID to a non-default value.

### Steps

1. Assign a data authentication key to a FIPS drive or SED:

```
storage encryption disk modify -disk disk_ID -data-key-id key_ID
```

For complete command syntax, see the man page for the command.

You can use the `security key-manager query -key-type NSE-AK` command to view key IDs.



+

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
```

Info: Starting modify on 14 disks.  
View the status of the operation by using the  
storage encryption disk show-status command.

#### 1. Verify that the authentication keys have been assigned:

```
storage encryption disk show
```

For complete command syntax, see the man page.

```
cluster1::> storage encryption disk show
Disk      Mode Data Key ID
-----  ----
-----
0.0.0     data
F1CB30AFF1CB30B001010000000000A68B167F92DD54196297159B5968923C
0.0.1     data
F1CB30AFF1CB30B001010000000000A68B167F92DD54196297159B5968923C
[...]
```

= Configure onboard key management

= Enable onboard key management in ONTAP 9.6 and later

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the Onboard Key Manager to authenticate cluster nodes to a FIPS drive or SED. The Onboard Key Manager is a built-in tool that serves authentication keys to nodes from the same storage system as your data. The Onboard Key Manager is FIPS-140-2 level 1 compliant.

You can use the Onboard Key Manager to secure the keys that the cluster uses to access encrypted data. You must enable Onboard Key Manager on each cluster that accesses an encrypted volume or a self-encrypting disk.

#### What you'll need

- If you are using NSE with an external key management (KMIP) server, you must have deleted the external key manager database.

[Transitioning to onboard key management from external key management](#)

- You must be a cluster administrator to perform this task.
- You must configure the MetroCluster environment before the Onboard key manager is configured.

### About this task

You must run the `security key-manager onboard enable` command each time you add a node to the cluster. In MetroCluster configurations, you must run `security key-manager onboard enable` on the local cluster first, then run `security key-manager onboard sync` on the remote cluster, using the same passphrase on each.

By default, you are not required to enter the key manager passphrase when a node is rebooted. Except in MetroCluster, you can use the `cc-mode-enabled=yes` option to require that users enter the passphrase after a reboot.

When the Onboard Key Manager is enabled in Common Criteria mode (`cc-mode-enabled=yes`), system behavior is changed in the following ways:

- The system monitors for consecutive failed cluster passphrase attempts when operating in Common Criteria mode.

If NetApp Storage Encryption (NSE) is enabled and you fail to enter the correct cluster passphrase at boot, the system cannot authenticate to its drives and automatically reboots. To correct this, you must enter the correct cluster passphrase at the boot prompt. Once booted, the system allows up to 5 consecutive attempts to correctly enter the cluster passphrase in a 24-hour period for any command that requires the cluster passphrase as a parameter. If the limit is reached (for example, you have failed to correctly enter the cluster passphrase 5 times in a row) then you must either wait for the 24-hour timeout period to elapse, or you must reboot the node, in order to reset the limit.

- System image updates use the NetApp RSA-3072 code signing certificate together with SHA-384 code signed digests to check the image integrity instead of the usual NetApp RSA-2048 code signing certificate and SHA-256 code signed digests.

The upgrade command verifies that the image contents have not been altered or corrupted by checking various digital signatures. The image update process proceeds to the next step if validation succeeds; otherwise, the image update fails. See the “cluster image” man page for information concerning system updates.

The Onboard Key Manager stores keys in volatile memory. Volatile memory contents are cleared when the system is rebooted or halted. Under normal operating conditions, volatile memory contents will be cleared within 30s when a system is halted.

### Steps

1. Start the key manager setup command:

```
security key-manager onboard enable -cc-mode-enabled yes|no
```

Set `cc-mode-enabled=yes` to require that users enter the key manager passphrase after a reboot. The `-cc-mode-enabled` option is not supported in MetroCluster configurations. The `security key-manager onboard enable` command replaces the `security key-manager setup` command.

+

The following example starts the key manager setup command on cluster1 without requiring that the passphrase be entered after every reboot:

+

```
cluster1::> security key-manager onboard enable
```

```
Enter the cluster-wide passphrase for onboard key management in Vserver  
"cluster1"::: <32..256 ASCII characters long text>  
Reenter the cluster-wide passphrase: <32..256 ASCII characters long  
text>
```

1. At the passphrase prompt, enter a passphrase between 32 and 256 characters, or for “cc-mode”, a passphrase between 64 and 256 characters.

If the specified “cc-mode” passphrase is less than 64 characters, there is a five-second delay before the key manager setup operation displays the passphrase prompt again.

1. At the passphrase confirmation prompt, reenter the passphrase.
2. Verify that the authentication keys have been created:

```
security key-manager key query -node node
```

The `security key-manager key query` command replaces the `security key-manager query key` command. For complete command syntax, see the man page.

+

The following example verifies that authentication keys have been created for cluster1:

+

```

cluster1::> security key-manager key query
      Vserver: cluster1
      Key Manager: onboard
      Node: node1

Key Tag                                Key Type  Restored
-----                                -
node1                                  NSE-AK    yes
  Key ID:
000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e0000000
000000000
node1                                  NSE-AK    yes
  Key ID:
000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf7970000000
000000000

      Vserver: cluster1
      Key Manager: onboard
      Node: node2

Key Tag                                Key Type  Restored
-----                                -
node1                                  NSE-AK    yes
  Key ID:
000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e0000000
000000000
node2                                  NSE-AK    yes
  Key ID:
000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf7970000000
000000000

```

**After you finish**

Copy the passphrase to a secure location outside the storage system for future use.

All key management information is automatically backed up to the replicated database (RDB) for the cluster. You should also back up the information manually for use in case of a disaster.

= Enable onboard key management in ONTAP 9.5 and earlier

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the Onboard Key Manager to authenticate cluster nodes to a FIPS drive or SED. The Onboard Key Manager is a built-in tool that serves authentication keys to nodes from the same storage system as your data. The Onboard Key Manager is FIPS-140-2 level 1 compliant.

You can use the Onboard Key Manager to secure the keys that the cluster uses to access encrypted data. You must enable Onboard Key Manager on each cluster that accesses an encrypted volume or a self-encrypting disk.

### What you'll need

- If you are using NSE with an external key management (KMIP) server, you must have deleted the external key manager database.

#### [Transitioning to onboard key management from external key management](#)

- You must be a cluster administrator to perform this task.
- You must configure the MetroCluster environment before the Onboard Key Manager is configured.

### About this task

You must run the `security key-manager setup` command each time you add a node to the cluster.

If you have a MetroCluster configuration, review these guidelines:

- In ONTAP 9.5, you must run `security key-manager setup` on the local cluster and `security key-manager setup -sync-metrocluster-config yes` on the remote cluster, using the same passphrase on each.
- Prior to ONTAP 9.5, you must run `security key-manager setup` on the local cluster, wait approximately 20 seconds, and then run `security key-manager setup` on the remote cluster, using the same passphrase on each.

By default, you are not required to enter the key manager passphrase when a node is rebooted. Beginning with ONTAP 9.4, you can use the `-enable-cc-mode yes` option to require that users enter the passphrase after a reboot.

For NVE, if you set `-enable-cc-mode yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted. For `volume create`, you need not specify `-encrypt true`. For `volume move start`, you need not specify `-encrypt-destination true`.

After a failed passphrase attempt, you must reboot the node again.

### Steps

1. Start the key manager setup:

```
security key-manager setup -enable-cc-mode yes|no
```

Beginning with ONTAP 9.4, you can use the `-enable-cc-mode yes` option to require that users enter the key manager passphrase after a reboot. For NVE, if you set `-enable-cc-mode yes`, volumes you create

with the `volume create` and `volume move start` commands are automatically encrypted.

+

The following example starts setting up the key manager on cluster1 without requiring that the passphrase be entered after every reboot:

+

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase:  <32..256 ASCII characters long
text>
```

1. Enter `yes` at the prompt to configure onboard key management.
2. At the passphrase prompt, enter a passphrase between 32 and 256 characters, or for “cc-mode”, a passphrase between 64 and 256 characters.

If the specified “cc-mode” passphrase is less than 64 characters, there is a five-second delay before the key manager setup operation displays the passphrase prompt again.

1. At the passphrase confirmation prompt, reenter the passphrase.
2. Verify that keys are configured for all nodes:

```
security key-manager key show
```

For the complete command syntax, see the man page.

```
cluster1::> security key-manager key show

Node: node1
Key Store: onboard
Key ID
Used By
-----
-----
0000000000000000000020000000000010059851742AF2703FC91369B7DB47C4722
NSE-AK
000000000000000000002000000000001008C07CC0AF1EF49E0105300EFC83004BF
NSE-AK

Node: node2
Key Store: onboard
Key ID
Used By
-----
-----
0000000000000000000020000000000010059851742AF2703FC91369B7DB47C4722
NSE-AK
000000000000000000002000000000001008C07CC0AF1EF49E0105300EFC83004BF
NSE-AK
```

### After you finish

All key management information is automatically backed up to the replicated database (RDB) for the cluster.

Whenever you configure the Onboard Key Manager passphrase, you should also back up the information manually to a secure location outside the storage system for use in case of a disaster. See [Back up onboard key management information manually](#).

= Assign a data authentication key to a FIPS drive or SED (onboard key management)

```
:icons: font
```

```
:relative_path: ./encryption-at-rest/
```

```
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/
```

You can use the `storage encryption disk modify` command to assign a data authentication key to a FIPS drive or SED. Cluster nodes use this key to access data

on the drive.

### What you'll need

You must be a cluster administrator to perform this task.

### About this task

A self-encrypting drive is protected from unauthorized access only if its authentication key ID is set to a non-default value. The manufacturer secure ID (MSID), which has key ID 0x0, is the standard default value for SAS drives. For NVMe drives, the standard default value is a null key, represented as a blank key ID. When you assign the key ID to a self-encrypting drive, the system changes its authentication key ID to a non-default value.

### Steps

1. Assign a data authentication key to a FIPS drive or SED:

```
storage encryption disk modify -disk disk_ID -data-key-id key_ID
```

For complete command syntax, see the man page for the command.

You can use the `security key-manager key query -key-type NSE-AK` command to view key IDs.



+

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id  
0000000000000000020000000000010019215b9738bc7b43d4698c80246db1f4
```

Info: Starting modify on 14 disks.  
View the status of the operation by using the  
storage encryption disk show-status command.

#### 1. Verify that the authentication keys have been assigned:

```
storage encryption disk show
```

For complete command syntax, see the man page.

```
cluster1::> storage encryption disk show  
Disk      Mode Data Key ID  
-----  
-----  
0.0.0     data  
0000000000000000020000000000010019215b9738bc7b43d4698c80246db1f4  
0.0.1     data  
0000000000000000020000000000010059851742AF2703FC91369B7DB47C4722  
[...]
```

= Assign a FIPS 140-2 authentication key to a FIPS drive

You can use the `storage encryption disk modify` command with the `-fips -key-id` option to assign a FIPS 140-2 authentication key to a FIPS drive. Cluster nodes use this key for drive operations other than data access, such as preventing denial-of-service attacks on the drive.

#### What you'll need

The drive firmware must support FIPS 140-2 compliance. The [NetApp Interoperability Matrix Tool](#) contains information about supported drive firmware versions.

#### About this task

Your security setup may require you to use different keys for data authentication and FIPS 140-2 authentication. If that is not the case, you can use the same authentication key for FIPS compliance that you use for data access.

#### Steps

1. You must first ensure you have assigned a data authentication key. This can be done with using an [external key manager](#) or an [onboard key manager](#). Verify the key is assigned with the command `storage encryption disk show`.

## 2. Assign a FIPS 140-2 authentication key to SEDs:

```
storage encryption disk modify -disk disk_id -fips-key-id  
fips_authentication_key_id
```

You can use the `security key-manager query` command to view key IDs.

```
cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id  
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
```

```
Info: Starting modify on 14 disks.  
View the status of the operation by using the  
storage encryption disk show-status command.
```

## 3. Verify that the authentication key has been assigned:

```
storage encryption disk show -fips
```

For complete command syntax, see the man page.

```
cluster1::> storage encryption disk show -fips  
Disk      Mode FIPS-Compliance Key ID  
-----  ----  
-----  
2.10.0    full  
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A  
2.10.1    full  
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A  
[...]
```

= Enable cluster-wide FIPS-compliant mode for KMIP server connections

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the `security config modify` command with the `-is-fips-enabled` option to enable cluster-wide FIPS-compliant mode for data in flight. Doing so forces the cluster to use OpenSSL in FIPS mode when connecting to KMIP servers.

### Before you begin

- The storage controller must be configured in FIPS-compliant mode.
- All KMIP servers must support TLSv1.2. The system requires TLSv1.2 to complete the connection to the KMIP server when cluster-wide FIPS-compliant mode is enabled.

### About this task

When you enable cluster-wide FIPS-compliant mode, the cluster will automatically use only TLS1.2 and FIPS-validated cipher suites. Cluster-wide FIPS-compliant mode is disabled by default.

You must reboot cluster nodes manually after modifying the cluster-wide security configuration.

### Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Verify that TLSv1.2 is supported:

```
security config show -supported-protocols
```

For complete command syntax, see the man page.

```
cluster1::> security config show
      Cluster
Cluster Security
Interface FIPS Mode  Supported Protocols      Supported Ciphers
Config Ready
-----
-----
SSL             false      TLSv1.2, TLSv1.1, TLSv1  ALL:!LOW:
                                     !aNULL:!EXP:
                                     !eNULL
                                     yes
```

3. Enable cluster-wide FIPS-compliant mode:

```
security config modify -is-fips-enabled true -interface SSL
```

For complete command syntax, see the man page.

4. Reboot cluster nodes manually.
5. Verify that cluster-wide FIPS-compliant mode is enabled:

```
security config show
```

```

cluster1::> security config show
          Cluster
Cluster Security
Interface FIPS Mode   Supported Protocols   Supported Ciphers
Config Ready
-----
-----
SSL           true           TLSv1.2, TLSv1.1     ALL:!LOW:           yes
                  !aNULL:!EXP:
                  !eNULL:!RC4

```

= Manage NetApp encryption

= Unencrypt volume data

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the `volume move start` command to move and unencrypt volume data.

### What you'll need

You must be a cluster administrator to perform this task, or an SVM administrator to whom the cluster administrator has delegated authority.

### Delegating authority to run the volume move command

### Steps

1. Move an existing encrypted volume and unencrypt the data on the volume:

```

volume move start -vserver SVM_name -volume volume_name -destination
-aggregate aggregate_name -encrypt-destination false

```

For complete command syntax, see the man page for the command.

The following command moves an existing volume named `vol1` to the destination aggregate `aggr3` and unencrypts the data on the volume:

```

cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr3 -encrypt-destination false

```

The system deletes the encryption key for the volume. The data on the volume is unencrypted.

2. Verify that the volume is disabled for encryption:

```

volume show -encryption

```

For complete command syntax, see the man page for the command.

The following command displays whether volumes on `cluster1` are encrypted:

```
cluster1::> volume show -encryption
```

Vserver	Volume	Aggregate	State	Encryption State
-----	-----	-----	-----	-----
vs1	vol1	aggr1	online	none

= Move an encrypted volume

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the `volume move start` command to move an encrypted volume. The moved volume can reside on the same aggregate or a different aggregate.

### What you'll need

You must be a cluster administrator to perform this task, or an SVM administrator to whom the cluster administrator has delegated authority.

### [Delegating authority to run the volume move command](#)

### About this task

The move will fail if the destination node or destination volume does not support volume encryption.

The `-encrypt-destination` option for `volume move start` defaults to `true` for encrypted volumes. Requiring you to specify explicitly that you do not want the destination volume to be encrypted ensures that you do not inadvertently unencrypt the data on the volume.

### Steps

1. Move an existing encrypted volume and leave the data on the volume encrypted:

```
volume move start -vserver SVM_name -volume volume_name -destination  
-aggregate aggregate_name
```

For complete command syntax, see the man page for the command.

The following command moves an existing volume named `vol1` to the destination aggregate `aggr3` and leaves the data on the volume encrypted:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination  
-aggr3 aggr3
```

2. Verify that the volume is enabled for encryption:

```
volume show -is-encrypted true
```

For complete command syntax, see the man page for the command.

The following command displays the encrypted volumes on `cluster1`:

```
cluster1::> volume show -is-encrypted true
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used
vs1	vol1	aggr3	online	RW	200GB	160.0GB	20%

= Delegate authority to run the volume move command

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the `volume move` command to encrypt an existing volume, move an encrypted volume, or unencrypt a volume. Cluster administrators can run `volume move` command themselves, or they can delegate the authority to run the command to SVM administrators.

#### About this task

By default, SVM administrators are assigned the `vsadmin` role, which does not include the authority to move volumes. You must assign the `vsadmin-volume` role to SVM administrators to enable them to run the `volume move` command.

#### Step

1. Delegate authority to run the `volume move` command:

```
security login modify -vserver SVM_name -user-or-group-name  
user_or_group_name -application application -authmethod  
authentication_method -role vsadmin-volume
```

For complete command syntax, see the man page for the command.

The following command grants the SVM administrator authority to run the `volume move` command.

```
cluster1::>security login modify -vserver engData -user-or-group  
-name SVM-admin -application ssh -authmethod domain -role vsadmin-  
volume
```

= Change the encryption key for a volume with the `volume encryption rekey start` command

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

It is a security best practice to change the encryption key for a volume periodically. Beginning with ONTAP 9.3, you can use the `volume encryption rekey start` command to change the encryption key.

**About this task**

Once you start a rekey operation, it must complete. There is no returning to the old key. If you encounter a performance issue during the operation, you can run the `volume encryption rekey pause` command to pause the operation, and the `volume encryption rekey resume` command to resume the operation.

Until the rekey operation finishes, the volume will have two keys. New writes and their corresponding reads will use the new key. Otherwise, reads will use the old key.

You cannot use `volume encryption rekey start` to rekey a SnapLock volume.

## Steps

1. Change an encryption key:

```
volume encryption rekey start -vserver SVM_name -volume volume_name
```

The following command changes the encryption key for `vol1` on `SVMvs1`:

```
cluster1::> volume encryption rekey start -vserver vs1 -volume vol1
```

2. Verify the status of the rekey operation:

```
volume encryption rekey show
```

For complete command syntax, see the man page for the command.

The following command displays the status of the rekey operation:

```
cluster1::> volume encryption rekey show
```

Vserver	Volume	Start Time	Status
vs1	vol1	9/18/2017 17:51:41	Phase 2 of 2 is in progress.

3. When the rekey operation is complete, verify that the volume is enabled for encryption:

```
volume show -is-encrypted true
```

For complete command syntax, see the man page for the command.

The following command displays the encrypted volumes on `cluster1`:

```
cluster1::> volume show -is-encrypted true
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used
vs1	vol1	aggr2	online	RW	200GB	160.0GB	20%

= Change the encryption key for a volume with the volume move start command

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

It is a security best practice to change the encryption key for a volume periodically. You can use the `volume move start` command to change the encryption key. You must use `volume move start` in ONTAP 9.2 and earlier. The moved volume can



reside on the same aggregate or a different aggregate.

### What you'll need

You must be a cluster administrator to perform this task, or an SVM administrator to whom the cluster administrator has delegated authority.

### Delegating authority to run the volume move command

### About this task

You cannot use `volume move start` to rekey a SnapLock or FlexGroup volume.

### Steps

1. Move an existing volume and change the encryption key:

```
volume move start -vserver SVM_name -volume volume_name -destination  
-aggregate aggregate_name -generate-destination-key true
```

For complete command syntax, see the man page for the command.

The following command moves an existing volume named **vol1** to the destination aggregate **aggr2** and changes the encryption key:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination  
-aggregate aggr2 -generate-destination-key true
```

A new encryption key is created for the volume. The data on the volume remains encrypted.

2. Verify that the volume is enabled for encryption:

```
volume show -is-encrypted true
```

For complete command syntax, see the man page for the command.

The following command displays the encrypted volumes on `cluster1`:

```
cluster1::> volume show -is-encrypted true
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used
-----	-----	-----	-----	-----	-----	-----	-----
vs1	vol1	aggr2	online	RW	200GB	160.0GB	20%

= Rotate authentication keys for NetApp Storage Encryption

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can rotate authentication keys when using NetApp Storage Encryption (NSE).

### About this task

Rotating authentication keys in an NSE environment is supported if you are using External Key Manager (KMIP).

Rotating authentication keys in an NSE environment is not supported for Onboard Key Manager (OKM).

## Steps

1. Use the `security key-manager create-key` command to generate new authentication keys.

You need to generate new authentication keys before you can change the authentication keys.

2. Use the `storage encryption disk modify -disk * -data-key-id` command to change the authentication keys.

= Delete an encrypted volume

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the `volume delete` command to delete an encrypted volume.

## What you'll need

- You must be a cluster administrator to perform this task, or an SVM administrator to whom the cluster administrator has delegated authority.

[Delegating authority to run the volume move command](#)

- The volume must be offline.

## Step

1. Delete an encrypted volume:

```
volume delete -vserver SVM_name -volume volume_name
```

For complete command syntax, see the man page for the command.

The following command deletes an encrypted volume named `vol1`:

```
cluster1::> volume delete -vserver vs1 -volume vol1
```

Enter `yes` when you are prompted to confirm deletion.

The system deletes the encryption key for the volume after 24 hours.

Use `volume delete` with the `-force true` option to delete a volume and destroy the corresponding encryption key immediately. This command requires advanced privileges. For more information, see the man page.

## After you finish

You can use the `volume recovery-queue` command to recover a deleted volume during the retention period after issuing the `volume delete` command:

```
volume recovery-queue SVM_name -volume volume_name
```

[How to use the Volume Recovery feature](#)

= Securely purge data on an encrypted volume

= Securely purge data on an encrypted volume overview

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.4, you can use secure purge to non-disruptively scrub data on NVE-enabled volumes. Scrubbing data on an encrypted volume ensures that it cannot be recovered from the physical media, for example, in cases of “spillage,” where data traces may have been left behind when blocks were overwritten, or for securely deleting a vacating tenant’s data.

Secure purge works only for previously deleted files on NVE-enabled volumes. You cannot scrub an unencrypted volume. You must use KMIP servers to serve keys, not the onboard key manager.

== Considerations for using secure purge

\* Volumes created in an aggregate enabled for NetApp Aggregate Encryption (NAE) do not support secure purge.

\* Secure purge works only for previously deleted files on NVE-enabled volumes.

\* You cannot scrub an unencrypted volume.

\* You must use KMIP servers to serve keys, not the onboard key manager.

Secure purge functions differently depending upon your version of ONTAP.

### ONTAP 9.8 and later

- Secure purge is supported by MetroCluster and FlexGroup.
- If the volume being purged is the source of a SnapMirror relationship, you do not have to break the SnapMirror relationship to perform a secure purge.
- The re-encryption method is different for volumes using SnapMirror data protection versus volumes not using SnapMirror data protection (DP) or those using SnapMirror extended data protection..
  - By default, volumes using SnapMirror data protection (DP) mode re-encrypt data using the volume move re-encryption method.
  - By default, volumes not using SnapMirror data protection or volumes using SnapMirror extended data protection (XDP) mode use the in-place re-encryption method.
  - These defaults can be changed using the `secure purge re-encryption-method [volume-move|in-place-rekey]` command.
- By default, all Snapshot copies in FlexVol volumes are automatically deleted during the secure purge operation. By default, Snapshots in FlexGroup volumes and volumes using SnapMirror data protection are not automatically deleted during the secure purge operation. These defaults can be changed using the `secure purge delete-all-snapshots [true|false]` command.

### ONTAP 9.7 and earlier:

- Secure purge does not support the following:
  - FlexClone
  - SnapVault
  - FabricPool

- If the volume being purged is the source of a SnapMirror relationship, you must break the SnapMirror relationship before you can purge the volume.

If there are busy Snapshot copies in the volume, you must release the Snapshot copies before you can purge the volume. For example, you may need to split a FlexClone volume from its parent.

- Successfully invoking the secure-purge feature triggers a volume move that re-encrypts the remaining, unpurged data with a new key.

The moved volume remains on the current aggregate. The old key is automatically destroyed, ensuring that purged data cannot be recovered from the storage media.

= Securely purge data on an encrypted volume without a SnapMirror relationship

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.4, you can use secure-purge to non-disruptively “scrub” data on NVE-enabled volumes.

#### What you’ll need

- You must be a cluster administrator to perform this task.
- Advanced privileges are required for this task.

#### About this task

Secure-purge may take from several minutes to many hours to complete, depending on the amount of data in the deleted files. You can use the `volume encryption secure-purge show` command to view the status of the operation. You can use the `volume encryption secure-purge abort` command to terminate the operation.

In order to do a secure purge on a SAN host, you must delete the entire LUN containing the files you want to purge, or you must be able to punch holes in the LUN for the blocks that belong to the files you want purge. If you cannot delete the LUN or your host operating system does not support punching holes in the LUN, you cannot perform a secure purge.

## Steps

1. Delete the files or the LUN you want to securely purge.
  - On a NAS client, delete the files you want to securely purge.
  - On a SAN host, delete the LUN you want to securely purge or punch holes in the LUN for the blocks that belong to the files you want to purge.
2. On the storage system, change to advanced privilege level:

```
set -privilege advanced
```

3. If the files you want to securely purge are in snapshots, delete the snapshots:

```
snapshot delete -vserver SVM_name -volume vol_name -snapshot
```

4. Securely purge the deleted files:

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name
```

The following command securely purges the deleted files on vol1 on SVMvs1:

```
cluster1::> volume encryption secure-purge start -vserver vs1  
-volume vol1
```

5. Verify the status of the secure-purge operation:

```
volume encryption secure-purge show
```

= Securely purge data on an encrypted volume with an Asynchronous SnapMirror relationship

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.8, you can use a secure purge to non-disruptively “scrub” data on NVE-enabled volumes with an Asynchronous SnapMirror relationship.

### What you’ll need

- You must be a cluster administrator to perform this task.
- Advanced privileges are required for this task.

### About this task

Secure-purge may take from several minutes to many hours to complete, depending on the amount of data in the deleted files. You can use the `volume encryption secure-purge show` command to view the status of the operation. You can use the `volume encryption secure-purge abort` command to terminate the operation.

In order to do a secure purge on a SAN host, you must delete the entire LUN containing the files you want to purge, or you must be able to punch holes in the LUN for the blocks that belong to the files you want to purge. If you cannot delete the LUN or your host operating system does not support punching holes in the LUN, you

cannot perform a secure purge.

## Steps

1. On the storage system, change to advanced privilege level:

```
set -privilege advanced
```

2. Delete the files or the LUN you want to securely purge.
  - On a NAS client, delete the files you want to securely purge.
  - On a SAN host, delete the LUN you want to securely purge or punch holes in the LUN for the blocks that belong to the files you want to purge.
3. Prepare the destination volume in the Asynchronous relationship to be securely purged:

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name  
-prepare true
```

Repeat this step on each volume in your Asynchronous SnapMirror relationship.

4. If the files you want to securely purge are in Snapshot copies, delete the Snapshot copies:

```
snapshot delete -vserver SVM_name -volume vol_name -snapshot
```

5. If the files you want to securely purge are in the base Snapshot copies, do the following:
  - a. Create a Snapshot copy on the destination volume in the Asynchronous SnapMirror relationship:

```
volume snapshot create -snapshot snapshot_name -vserver SVM_name -volume  
vol_name
```

- b. Update SnapMirror to move the base Snapshot copy forward:

```
snapmirror update -source-snapshot snapshot_name -destination-path  
destination_path
```

Repeat this step for each volume in the Asynchronous SnapMirror relationship.

- c. Repeat steps (a) and (b) equal to the number of base Snapshot copies plus one.

For example, if you have two base Snapshot copies, you should repeat steps (a) and (b) three times.

- d. Verify that the base Snapshot copy is present:

```
snapshot show -vserver SVM_name -volume vol_name`
```

- e. Delete the base Snapshot copy:

```
snapshot delete -vserver SVM_name -volume vol_name -snapshot snapshot
```

6. Securely purge the deleted files:

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name
```

Repeat this step on each volume in the Asynchronous SnapMirror relationship.



The following command securely purges the deleted files on “vol1” on SVM “vs1”:

```
cluster1::> volume encryption secure-purge start -vserver vs1
-volume vol1
```

7. Verify the status of the secure purge operation:

```
volume encryption secure-purge show
```

= Scrub data on an encrypted volume with a Synchronous SnapMirror relationship

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.8, you can use a secure purge to non-disruptively “scrub” data on NVE-enabled volumes with a Synchronous SnapMirror relationship.

#### What you’ll need

- You must be a cluster administrator to perform this task.
- Advanced privileges are required for this task.

#### About this task

A secure purge might take from several minutes to many hours to complete, depending on the amount of data in the deleted files. You can use the `volume encryption secure-purge show` command to view the status of the operation. You can use the `volume encryption secure-purge abort` command to terminate the operation.

In order to do a secure purge on a SAN host, you must delete the entire LUN containing the files you want to purge, or you must be able to punch holes in the LUN for the blocks that belong to the files you want purge. If you cannot delete the LUN or your host operating system does not support punching holes in the LUN, you cannot perform a secure purge.

## Steps

1. On the storage system, change to advanced privilege level:

```
set -privilege advanced
```

2. Delete the files or the LUN you want to securely purge.
  - On a NAS client, delete the files you want to securely purge.
  - On a SAN host, delete the LUN you want to securely purge or punch holes in the LUN for the blocks that belong to the files you want to purge.
3. Prepare the destination volume in the Asynchronous relationship to be securely purged:

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name  
-prepare true
```

Repeat this step for the other volume in your Synchronous SnapMirror relationship.

4. If the files you want to securely purge are in Snapshot copies, delete the Snapshot copies:

```
snapshot delete -vserver SVM_name -volume vol_A -snapshot snapshot
```

5. If the secure purge file is in the base or common Snapshot copies, update the SnapMirror to move the common Snapshot copy forward:

```
snapmirror update -source-snapshot snapshot_name -destination-path  
destination_path
```

There are two common Snapshot copies, so this command must be issued twice.

6. If the secure purge file is in the application-consistent Snapshot copy, delete the Snapshot copy on both volumes in the Synchronous SnapMirror relationship:

```
snapshot delete -vserver SVM_name -volume vol_name -snapshot snapshot
```

Perform this step on both volumes.

7. Securely purge the deleted files:

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name
```

Repeat this step on each volume in the synchronous SnapMirror relationship.

The following command securely purges the deleted files on “vol1” on SMV “vs1”.

```
cluster1::> volume encryption secure-purge start -vserver vs1  
-volume vol1
```

8. Verify the status of the secure purge operation:

```
volume encryption secure-purge show
```

= Change the onboard key management passphrase

It is a security best practice to change the onboard key management passphrase periodically. You should copy the new onboard key management passphrase to a secure location outside the storage system for future use.

### What you'll need

- You must be a cluster or SVM administrator to perform this task.
- Advanced privileges are required for this task.

### Steps

1. Change to advanced privilege level:

```
set -privilege advanced
```

2. Change the onboard key management passphrase:

For this ONTAP version...	Use this command...
ONTAP 9.6 and later	<code>security key-manager onboard update-passphrase</code>
ONTAP 9.5 and earlier	<code>security key-manager update-passphrase</code>

For complete command syntax, see the man pages.

The following ONTAP 9.6 command lets you change the onboard key management passphrase for `cluster1`:

```
cluster1::> security key-manager onboard update-passphrase
Warning: This command will reconfigure the cluster passphrase for
onboard key management for Vserver "cluster1".
Do you want to continue? {y|n}: y
Enter current passphrase:
Enter new passphrase:
```

3. Enter `y` at the prompt to change the onboard key management passphrase.
4. Enter the current passphrase at the current passphrase prompt.
5. At the new passphrase prompt, enter a passphrase between 32 and 256 characters, or for “cc-mode”, a passphrase between 64 and 256 characters.

If the specified “cc-mode” passphrase is less than 64 characters, there is a five-second delay before the key manager setup operation displays the passphrase prompt again.

6. At the passphrase confirmation prompt, reenter the passphrase.

### After you finish

In a MetroCluster environment, you must update the passphrase on the partner cluster:

- In ONTAP 9.5 and earlier, you must run `security key-manager update-passphrase` with the same passphrase on the partner cluster.
- In ONTAP 9.6 and later, you are prompted to run `security key-manager onboard sync` with the same passphrase on the partner cluster.

You should copy the onboard key management passphrase to a secure location outside the storage system for future use.

You should back up key management information manually whenever you change the onboard key management passphrase.

### Backing up onboard key management information manually

= Back up onboard key management information manually

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You should copy onboard key management information to a secure location outside the storage system whenever you configure the Onboard Key Manager passphrase.

#### What you'll need

- You must be a cluster administrator to perform this task.
- Advanced privileges are required for this task.

#### About this task

All key management information is automatically backed up to the replicated database (RDB) for the cluster. You should also back up key management information manually for use in case of a disaster.

#### Steps

1. Change to advanced privilege level:

```
set -privilege advanced
```

2. Display the key management backup information for the cluster:

For this ONTAP version...	Use this command...
ONTAP 9.6 and later	<code>security key-manager onboard show-backup</code>
ONTAP 9.5 and earlier	<code>security key-manager backup show</code>

For complete command syntax, see the man pages.

+

The following 9.6 command displays the key management backup information for `cluster1`:

+



- If you are using NSE with an external key management (KMIP) server, you must have deleted the external key manager database.

### Transitioning to onboard key management from external key management

- You must be a cluster administrator to perform this task.

== Steps for ONTAP 9.6 and later

1. Verify that the key needs to be restored:

```
security key-manager key query -node node
```

2. If you are running ONTAP 9.8 and later, and your root volume is encrypted, complete [\[root\\_volume\\_encrypted\]](#).

If you are running ONTAP 9.6 or 9.7, or if you are running ONTAP 9.8 or later and your root volume is not encrypted, skip this step.

3. Restore the key:

```
security key-manager onboard sync
```

For complete command syntax, see the man pages.

The following ONTAP 9.6 command synchronize the keys in the onboard key hierarchy:

```
cluster1::> security key-manager onboard sync
```

```
Enter the cluster-wide passphrase for onboard key management in
Vserver "cluster1":: <32..256 ASCII characters long text>
```

4. At the passphrase prompt, enter the onboard key management passphrase for the cluster.

== Steps for ONTAP 9.5 and earlier

1. Verify that the key needs to be restored:

```
security key-manager key show
```

2. If you are running ONTAP 9.8 and later, and your root volume is encrypted, complete these steps:

If you are running ONTAP 9.6 or 9.7, or if you are running ONTAP 9.8 or later and your root volume is not encrypted, skip this step.

3. Restore the key:

```
security key-manager setup -node node
```

For complete command syntax, see the man pages.

4. At the passphrase prompt, enter the onboard key management passphrase for the cluster.

== Steps if the root volume is encrypted

If you are running ONTAP 9.8 and later, and your root volume is encrypted, you must set an onboard key management recovery passphrase with the boot menu. This process is also necessary if you do a boot

media replacement.

1. Boot the node to the boot menu and select option (10) Set onboard key management recovery secrets.
2. Enter `y` to use this option.
3. At the prompt, enter the onboard key management passphrase for the cluster.
4. At the prompt, enter the backup key data.

The node returns to the boot menu.

5. From the boot menu, select option (1) Normal Boot.

= Restore external key management encryption keys

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can manually restore external key management encryption keys and “push” them to a different node. You might want to do this if you are restarting a node that was down temporarily when you created the keys for the cluster.

### What you'll need

You must be a cluster or SVM administrator to perform this task.

### About this task

In ONTAP 9.6 and later, you can use the `security key-manager key query -node node_name` command to verify if your key needs to be restored.

In ONTAP 9.5 and earlier, you can use the `security key-manager key show` command to verify if your key needs to be restored.

### Steps

1. If you are running ONTAP 9.8 or later and your root volume is encrypted, do the following:

If you are running ONTAP 9.7 or earlier, or if you are running ONTAP 9.8 or later and your root volume is not encrypted, skip this step.

- a. Set the bootargs:

```
setenv kmip.init.ipaddr <ip-address>
```

```
setenv kmip.init.netmask <netmask>
```

```
setenv kmip.init.gateway <gateway>
```

```
setenv kmip.init.interface e0M
```

```
boot_ontap
```

- b. Boot the node to the boot menu and select option (11) Configure node for external key management.

c. Follow prompts to enter management certificate.

After all management certificate information is entered, the system returns to the boot menu.

d. From the boot menu, select option (1) Normal Boot.

2. Restore the key:

For this ONTAP version...	Use this command...
ONTAP 9.6 and later	<pre>security key-manager external restore -vserver SVM -node node -key-server host_name IP_address:port -key-id key_id -key -tag key_tag</pre>
ONTAP 9.5 and earlier	<pre>security key-manager restore -node node -address IP_address -key-id key_id -key-tag key_tag</pre>

node defaults to all nodes. For complete command syntax, see the man pages. This command is not supported when onboard key management is enabled.



+

The following ONTAP 9.6 command restores external key management authentication keys to all nodes in cluster1:

+

```
cluster1::> security key-manager external restore
```

= Replace SSL certificates

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

All SSL certificates have an expiration date. You must update your certificates before they expire to prevent loss of access to authentication keys.

### Before you begin

- You must have obtained the replacement public certificate and private key for the cluster (KMIP client certificate).
- You must have obtained the replacement public certificate for the KMIP server (KMIP server-ca certificate).
- You must be a cluster or SVM administrator to perform this task.



You can install the replacement client and server certificates on the KMIP server before or after installing the certificates on the cluster.

### Steps

1. Install the new KMIP server-ca certificate:

```
security certificate install -type server-ca -vserver <>
```

2. Install the new KMIP client certificate:

```
security certificate install -type client -vserver <>
```

3. Update the key manager configuration to use the newly installed certificates:

```
security key-manager external modify -vserver <> -client-cert <> -server-ca -certs <>
```



Updating the key manager configuration to use the newly installed certificates will return an error if the public/private keys of the new client certificate are different from the keys previously installed. See the Knowledge Base article [The new client certificate public or private keys are different from the existing client certificate](#) for instructions on how to override this error.

= Replace a FIPS drive or SED

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can replace a FIPS drive or SED the same way you replace an ordinary disk. Make sure to assign new data authentication keys to the replacement drive. For a FIPS drive, you may also want to assign a new FIPS 140-2 authentication key.



If an HA pair is using [encrypting SAS or NVMe drives \(SED, NSE, FIPS\)](#), you must follow the instructions in the topic [Returning a FIPS drive or SED to unprotected mode](#) for all drives within the HA pair prior to initializing the system (boot options 4 or 9). Failure to do this may result in future data loss if the drives are repurposed.

### What you'll need

- You must know the key ID for the authentication key used by the drive.
- You must be a cluster administrator to perform this task.

### Steps

1. Ensure that the disk has been marked as failed:

```
storage disk show -broken
```

For complete command syntax, see the man page.

```
cluster1::> storage disk show -broken
Original Owner: cluster1-01
Checksum Compatibility: block

Usable Physical
Disk   Outage Reason HA Shelf Bay Chan  Pool  Type  RPM
Size   Size
-----
0.0.0  admin   failed  0b    1    0    A    Pool0 FCAL  10000
132.8GB 133.9GB
0.0.7  admin   removed 0b    2    6    A    Pool1 FCAL  10000
132.8GB 134.2GB
[...]
```

2. Remove the failed disk and replace it with a new FIPS drive or SED, following the instructions in the hardware guide for your disk shelf model.
3. Assign ownership of the newly replaced disk:

```
storage disk assign -disk disk_name -owner node
```

For complete command syntax, see the man page.

```
cluster1::> storage disk assign -disk 2.1.1 -owner cluster1-01
```

4. Confirm that the new disk has been assigned:

```
storage encryption disk show
```

For complete command syntax, see the man page.

```
cluster1::> storage encryption disk show
Disk      Mode Data Key ID
-----  ----
-----
0.0.0     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
1.10.0    data
F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
1.10.1    data
F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
2.1.1     open 0x0
[...]
```

5. Assign the data authentication keys to the FIPS drive or SED.

[Assigning a data authentication key to a FIPS drive or SED \(external key management\)](#)

6. If necessary, assign a FIPS 140-2 authentication key to the FIPS drive.

[Assigning a FIPS 140-2 authentication key to a FIPS drive](#)

= Make data on a FIPS drive or SED inaccessible

= Make data on a FIPS drive or SED inaccessible overview

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

If you want to make data on a FIPS drive or SED permanently inaccessible, but keep the drive's unused space available for new data, you can sanitize the disk. If you want to make data permanently inaccessible and you do not need to reuse the drive, you can destroy it.

- Disk sanitization

When you sanitize a self-encrypting drive, the system changes the disk encryption key to a new random value, resets the power-on lock state to false, and sets the key ID to a default value, either the manufacturer secure ID 0x0 (SAS drives) or a null key (NVMe drives). Doing so renders the data

on the disk inaccessible and impossible to retrieve. You can reuse sanitized disks as non-zeroed spare disks.

- Disk destroy

When you destroy a FIPS drive or SED, the system sets the disk encryption key to an unknown random value and locks the disk irreversibly. Doing so renders the disk permanently unusable and the data on it permanently inaccessible.

You can sanitize or destroy individual self-encrypting drives, or all the self-encrypting drives for a node.

= Sanitize a FIPS drive or SED

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

If you want to make data on a FIPS drive or SED permanently inaccessible, and use the drive for new data, you can use the `storage encryption disk sanitize` command to sanitize the drive.

### What you'll need

You must be a cluster administrator to perform this task.

### About this task

When you sanitize a self-encrypting drive, the system changes the disk encryption key to a new random value, resets the power-on lock state to false, and sets the key ID to a default value, either the manufacturer secure ID 0x0 (SAS drives) or a null key (NVMe drives). Doing so renders the data on the disk inaccessible and impossible to retrieve. You can reuse sanitized disks as non-zeroed spare disks.

### Steps

1. Migrate any data that needs to be preserved to an aggregate on another disk.
2. Delete the aggregate on the FIPS drive or SED to be sanitized:

```
storage aggregate delete -aggregate aggregate_name
```

For complete command syntax, see the man page.

```
cluster1::> storage aggregate delete -aggregate aggr1
```

3. Identify the disk ID for the FIPS drive or SED to be sanitized:

```
storage encryption disk show -fields data-key-id,fips-key-id,owner
```

For complete command syntax, see the man page.

```

cluster1::> storage encryption disk show
Disk      Mode Data Key ID
-----  ----
-----
0.0.0    data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1    data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
1.10.2   data
F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
[...]

```

4. If a FIPS drive is running in FIPS-compliance mode, set the FIPS authentication key ID for the node back to the default MSID 0x0:

```
storage encryption disk modify -disk disk_id -fips-key-id 0x0
```

You can use the `security key-manager query` command to view key IDs.

```
cluster1::> storage encryption disk modify -disk 1.10.2 -fips-key-id
0x0
```

```

Info: Starting modify on 1 disk.
      View the status of the operation by using the
      storage encryption disk show-status command.

```

5. Sanitize the drive:

```
storage encryption disk sanitize -disk disk_id
```

You can use this command to sanitize hot spare or broken disks only. To sanitize all disks regardless of type, use the `-force-all-state` option. For complete command syntax, see the man page.

You are prompted to enter a confirmation phrase before continuing. Enter the phrase exactly as shown on the screen.

+

```
cluster1::> storage encryption disk sanitize -disk 1.10.2
```

```
Warning: This operation will cryptographically sanitize 1 spare or  
broken self-encrypting disk on 1 node.
```

```
    To continue, enter sanitize disk: sanitize disk
```

```
Info: Starting sanitize on 1 disk.
```

```
    View the status of the operation using the  
    storage encryption disk show-status command.
```

= Destroy a FIPS drive or SED

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

If you want to make data on a FIPS drive or SED permanently inaccessible and you do not need to reuse the drive, you can use the `storage encryption disk destroy` command to destroy the disk.

#### What you'll need

You must be a cluster administrator to perform this task.

#### About this task

When you destroy a FIPS drive or SED, the system sets the disk encryption key to an unknown random value and locks the drive irreversibly. Doing so renders the disk virtually unusable and the data on it permanently inaccessible. However, you can reset the disk to its factory-configured settings using the physical secure ID (PSID) printed on the disk's label. For more information, see [Returning a FIPS drive or SED to service when authentication keys are lost](#).

You should not destroy a FIPS drive or SED unless you have the Non-Returnable Disk Plus service (NRD Plus). Destroying a disk voids its warranty.

## Steps

1. Migrate any data that needs to be preserved to an aggregate on another different disk.
2. Delete the aggregate on the FIPS drive or SED to be destroyed:

```
storage aggregate delete -aggregate aggregate_name
```

For complete command syntax, see the man page.

```
cluster1::> storage aggregate delete -aggregate aggr1
```

3. Identify the disk ID for the FIPS drive or SED to be destroyed:

```
storage encryption disk show
```

For complete command syntax, see the man page.

```
cluster1::> storage encryption disk show
Disk      Mode Data Key ID
-----  ----
-----
0.0.0     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
1.10.2    data
F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
[...]
```

4. Destroy the disk:

```
storage encryption disk destroy -disk disk_id
```

For complete command syntax, see the man page.

You are prompted to enter a confirmation phrase before continuing. Enter the phrase exactly as shown on the screen.

+

```
cluster1::> storage encryption disk destroy -disk 1.10.2
```

Warning: This operation will cryptographically destroy 1 spare or broken

self-encrypting disks on 1 node.

You cannot reuse destroyed disks unless you revert them to their original state using the PSID value.

To continue, enter

```
destroy disk
```

```
:destroy disk
```

Info: Starting destroy on 1 disk.

View the status of the operation by using the "storage encryption disk show-status" command.

= Emergency shredding of data on a FIPS drive or SED

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

In case of a security emergency, you can instantly prevent access to a FIPS drive or SED, even if power is not available to the storage system or the KMIP server.

#### What you'll need

- If you are using a KMIP server that has no available power, the KMIP server must be configured with an easily destroyed authentication item (for example, a smart card or USB drive).
- You must be a cluster administrator to perform this task.

#### Step

1. Perform emergency shredding of data on a FIPS drive or SED:

If...	Then...
-------	---------



Power is available to the storage system and you have time to take the storage system offline gracefully

a. If the storage system is configured as an HA pair, disable takeover.

b. Take all aggregates offline and delete them.

c. Set the privilege level to advanced:

```
set -privilege advanced
```

d. If the drive is in FIPS-compliance mode, set the FIPS authentication key ID for the node back to the default MSID:

```
storage encryption disk modify -disk * -fips  
-key-id 0x0
```

e. Halt the storage system.

f. Boot into maintenance mode.

g. Sanitize or destroy the disks:

- If you want to make the data on the disks inaccessible and still be able to reuse the disks, sanitize the disks:

```
disk encrypt sanitize -all
```

- If you want to make the data on the disks inaccessible and you do not need to save the disks, destroy the disks:

```
disk encrypt destroy disk_id1 disk_id2 ...
```

The `disk encrypt sanitize` and `disk encrypt destroy` commands are reserved for maintenance mode only. These commands must be run on each HA node, and are not available for broken disks.

a. Repeat these steps for the partner node.

This leaves the storage system in a permanently disabled state with all data erased. To use the system again, you must reconfigure it.

**2+a| Power is available to the storage system and you must shred the data immediately**

**a| .. If you want to make the data on the disks inaccessible and still be able to reuse the disks, sanitize the disks:**

.. If the storage system is configured as an HA pair, disable takeover.

.. Set the privilege level to advanced:

+

```
set -privilege advanced
```

.. If the drive is in FIPS-compliance mode, set the FIPS authentication key ID for the node back to the default MSID:

+

```
storage encryption disk modify -disk * -fips-key-id 0x0
```

.. Sanitize the disk:

+

```
storage encryption disk sanitize -disk * -force-all-states true
```

**a| .. If you want to make the data on the disks inaccessible and you do not need to save the disks, destroy the disks:**

.. If the storage system is configured as an HA pair, disable takeover.

.. Set the privilege level to advanced:

+

```
set -privilege advanced
```

.. Destroy the disks:

```
storage encryption disk destroy -disk * -force-all-states true
```

2+a| The storage system panics, leaving the system in a permanently disabled state with all data erased.

To use the system again, you must reconfigure it.

a|Power is available to the KMIP server but not to the storage system

2+a|

.. Log in to the KMIP server.

.. Destroy all keys associated with the FIPS drives or SEDs that contain the data you want to prevent access to.

This prevents access to disk encryption keys by the storage system.

a|Power is not available to the KMIP server or the storage system

2+a|

Destroy the authentication item for the KMIP server (for example, the smart card). This prevents access to disk encryption keys by the storage system.

+

For complete command syntax, see the man pages.

:leveloffset: -1

= Return a FIPS drive or SED to service when authentication keys are lost

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

:hardbreaks-option:

[.lead]

The system treats a FIPS drive or SED as broken if you lose the authentication keys for it permanently and cannot retrieve them from the KMIP server. Although you cannot access or recover the data on the disk, you can take steps to make the SED's unused space available again for data.

.Before you begin

You must be a cluster administrator to perform this task.

.About this task

You should use this process only if you are certain that the authentication keys for the FIPS drive or SED are permanently lost and that you cannot recover them.

If the disks are partitioned, they must first be unpartitioned before you can start this process.

include::.../\_include/unpartition-disk.adoc[]

.Steps

. Return a FIPS drive or SED to service:

+

[cols="25,75"]

h| If the SEDS are... h| Use these steps...

a|

Not in FIPS-compliance mode, or in FIPS-compliance mode and the FIPS key is available

a|

.. Set the privilege level to advanced:

```
set -privilege advanced
```

.. Reset the FIPS key to the default manufacture secure ID 0x0:

```
storage encryption disk modify -fips-key-id 0x0 -disk disk_id
```

.. Verify the operation succeeded:

```
storage encryption disk show-status
```

If the operation failed, use the PSID process in this topic.

.. Sanitize the broken disk:

```
storage encryption disk sanitize -disk disk_id
```

Verify the operation succeeded with the command `storage encryption disk show-status` before proceeding to the next step.

.. Unfail the sanitized disk:

```
storage disk unfail -spare true -disk disk_id
```

.. Check whether the disk has an owner:

```
storage disk show -disk disk_id
```

.. If the disk does not have an owner, assign one, then unfail the disk again:

```
storage disk assign -owner node -disk disk_id
```

```
storage disk unfail -spare true -disk disk_id
```

.. Verify that the disk is now a spare and ready to be reused in an aggregate:

```
storage disk show -disk disk_id
```

a|

In FIPS-compliance mode, the FIPS key is not available, and the SEDs have a PSID printed on the label

a|

a. Obtain the PSID of the disk from the disk label.

b. Set the privilege level to advanced:

```
set -privilege advanced
```

c. Reset the disk to its factory-configured settings:

```
storage encryption disk revert-to-original-state -disk disk_id -psid  
disk_physical_secure_id
```

Verify the operation succeeded with the command `storage encryption disk show-status` before proceeding to the next step.

d. Unfail the sanitized disk:

```
storage disk unfail -spare true -disk disk_id
```

e. Check whether the disk has an owner:

```
storage disk show -disk disk_id
```

f. If the disk does not have an owner, assign one, then unfail the disk again:

```
storage disk assign -owner node -disk disk_id
```

```
storage disk unfail -spare true -disk disk_id
```

g. Verify that the disk is now a spare and ready to be reused in an aggregate:

```
storage disk show -disk disk_id
```

For complete command syntax, see the man pages.

= Return a FIPS drive or SED to unprotected mode

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

[.lead]

A FIPS drive or SED is protected from unauthorized access only if the authentication key ID for the node is set to a value other than the default. You can return a FIPS drive or SED to unprotected mode by using the `storage encryption disk modify` command to set the key ID to the default.

If an HA pair is using encrypting SAS or NVMe drives (SED, NSE, FIPS), you must follow this process for all drives within the HA pair prior to initializing the system (boot options 4 or 9). Failure to do this may result in future data loss if the drives are repurposed.

.What you'll need

You must be a cluster administrator to perform this task.

.Steps

. Set the privilege level to advanced:

+

```
set -privilege advanced
```

. If a FIPS drive is running in FIPS-compliance mode, set the FIPS authentication key ID for the node back to the default MSID 0x0:

+

```
storage encryption disk modify -disk disk_id -fips-key-id 0x0
```

+

You can use the `security key-manager query` command to view key IDs.

+

----

```
cluster1::> storage encryption disk modify -disk 2.10.11 -fips-key-id 0x0
```

Info: Starting modify on 14 disks.

View the status of the operation by using the `storage encryption disk show-status` command.

----

+

Confirm the operation succeeded with the command:

+

```
storage encryption disk show-status
```

+

Repeat the `show-status` command until the numbers in "Disks Begun" and "Disks Done" are the same.

+

----

```
cluster1:: storage encryption disk show-status
```

```
FIPS Latest Start Execution Disks Disks Disks
```

If you plan to continue using external key management after disconnecting a KMIP server, make sure another KMIP server is available to serve authentication keys.

### Step

1. Disconnect a KMIP server from the current node:

For this ONTAP version...	Use this command...
ONTAP 9.6 and later	<pre>security key-manager external remove-servers -vserver SVM -key-servers host_name IP_address:port,...</pre>
ONTAP 9.5 and earlier	<pre>security key-manager delete -address key_management_server_ipaddress</pre>

For complete command syntax, see the man pages.

The following ONTAP 9.6 command disables the connections to two external key management servers for `cluster1`, the first named `ks1`, listening on the default port 5696, the second with the IP address 10.0.0.20, listening on port 24482:

```
cluster1::> security key-manager external remove-servers -vserver
cluster-1 -key-servers ks1,10.0.0.20:24482
```

= Modify external key management server properties

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.6, you can use the `security key-manager external modify-server` command to change the I/O timeout and user name of an external key management server.

### Before you begin

- You must be a cluster or SVM administrator to perform this task.
- Advanced privileges are required for this task.

### Steps

1. On the storage system, change to advanced privilege level:

```
set -privilege advanced
```

2. Modify external key manager server properties for the cluster:

```
security key-manager external modify-server -vserver admin_SVM -key-server
host_name|IP_address:port,... -timeout 1...60 -username user_name
```

The timeout value is expressed in seconds. If you modify the user name, you are prompted to enter a new password. If you run the command at the cluster login prompt, *admin\_SVM* defaults to the admin SVM of the current cluster. You must be the cluster administrator to modify external key manager server properties.

+

The following command changes the timeout value to 45 seconds for the `cluster1` external key management server listening on the default port 5696:

+

```
cluster1::> security key-manager external modify-server -vserver
cluster1 -key-server ks1.local -timeout 45
```

1. Modify external key manager server properties for an SVM (NVE only):

```
security key-manager external modify-server -vserver SVM -key-server
host_name|IP_address:port,... -timeout 1..60 -username user_name
```

The timeout value is expressed in seconds. If you modify the user name, you are prompted to enter a new password. If you run the command at the SVM login prompt, *SVM* defaults to the current SVM. You must be the cluster or SVM administrator to modify external key manager server properties.

+

The following command changes the username and password of the `svm1` external key management server listening on the default port 5696:

+

```
svm1::> security key-manager external modify-server -vserver svm11 -key
-server ks1.local -username svm1user
Enter the password:
Reenter the password:
```

1. Repeat the last step for any additional SVMs.

= Transition to external key management from onboard key management

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

If you want to switch to external key management from onboard key management, you must delete the onboard key management configuration before you can enable external key management.

#### What you'll need

- For hardware-based encryption, you must reset the data keys of all FIPS drives or SEDs to the default value.

[Returning a FIPS drive or SED to unprotected mode](#)

- For software-based encryption, you must unencrypt all volumes.

[Unencrypting volume data](#)

- You must be a cluster administrator to perform this task.

#### Step

1. Delete the onboard key management configuration for a cluster:

For this ONTAP version...	Use this command...
ONTAP 9.6 and later	<code>security key-manager onboard disable -vserver SVM</code>
ONTAP 9.5 and earlier	<code>security key-manager delete-key-database</code>

For complete command syntax, see the [ONTAP manual pages](#).

= Transition to onboard key management from external key management

:icons: font



```
:relative_path: ./encryption-at-rest/
```

```
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/
```

If you want to switch to onboard key management from external key management, you must delete the external key management configuration before you can enable onboard key management.

#### Before you begin

- For hardware-based encryption, you must reset the data keys of all FIPS drives or SEDs to the default value.

[Returning a FIPS drive or SED to unprotected mode](#)

- You must have deleted all external key manager connections.

[Deleting an external key manager connection](#)

- You must be a cluster administrator to perform this task.

== Procedure

#### ONTAP 9.6 and later

1. Change to the advanced privilege level:

```
set -privilege advanced
```

2. Use the command:

```
security key-manager external disable -vserver admin_SVM
```

#### ONTAP 9.5 and earlier

Use the command:

```
security key-manager delete-knip-config
```

= What happens when key management servers are not reachable during the boot process

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

ONTAP takes certain precautions to avoid undesired behavior in the event that a storage system configured for NSE cannot reach any of the specified key management servers during the boot process.

If the storage system is configured for NSE, the SEDs are rekeyed and locked, and the SEDs are powered on, the storage system must retrieve the required authentication keys from the key management servers to authenticate itself to the SEDs before it can access the data.

The storage system attempts to contact the specified key management servers for up to three hours. If the storage system cannot reach any of them after that time, the boot process stops and the storage system halts.

If the storage system successfully contacts any specified key management server, it then attempts to establish an SSL connection for up to 15 minutes. If the storage system cannot establish an SSL connection with any specified key management server, the boot process stops and the storage system halts.

While the storage system attempts to contact and connect to key management servers, it displays detailed information about the failed contact attempts at the CLI. You can interrupt the contact attempts at any time by pressing Ctrl-C.

As a security measure, SEDs allow only a limited number of unauthorized access attempts, after which they disable access to the existing data. If the storage system cannot contact any specified key management servers to obtain the proper authentication keys, it can only attempt to authenticate with the default key which leads to a failed attempt and a panic. If the storage system is configured to automatically reboot in case of a panic, it enters a boot loop which results in continuous failed authentication attempts on the SEDs.

Halting the storage system in these scenarios is by design to prevent the storage system from entering a boot loop and possible unintended data loss as a result of the SEDs locked permanently due to exceeding the safety limit of a certain number of consecutive failed authentication attempts. The limit and the type of lockout protection depends on the manufacturing specifications and type of SED:

<b>SED type</b>	<b>Number of consecutive failed authentication attempts resulting in lockout</b>	<b>Lockout protection type when safety limit is reached</b>
HDD	1024	Permanent. Data cannot be recovered, even when the proper authentication key becomes available again.

X440_PHM2800MCTO 800GB NSE SSDs with firmware revisions NA00 or NA01	5	Temporary. Lockout is only in effect until disk is power-cycled.
X577_PHM2800MCTO 800GB NSE SSDs with firmware revisions NA00 or NA01	5	Temporary. Lockout is only in effect until disk is power-cycled.
X440_PHM2800MCTO 800GB NSE SSDs with higher firmware revisions	1024	Permanent. Data cannot be recovered, even when the proper authentication key becomes available again.
X577_PHM2800MCTO 800GB NSE SSDs with higher firmware revisions	1024	Permanent. Data cannot be recovered, even when the proper authentication key becomes available again.
All other SSD models	1024	Permanent. Data cannot be recovered, even when the proper authentication key becomes available again.

For all SED types, a successful authentication resets the try count to zero.

If you encounter this scenario where the storage system is halted due to failure to reach any specified key management servers, you must first identify and correct the cause for the communication failure before you attempt to continue booting the storage system.

= Disable encryption by default with ONTAP 9.7 and later

:icons: font

:relative\_path: ./encryption-at-rest/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.7, aggregate and volume encryption is enabled by default if you have a volume encryption (VE) license and use an onboard or external key manager. You can disable encryption by default for the entire cluster, if required.

### What you'll need

You must be a cluster administrator to perform this task, or an SVM administrator to whom the cluster administrator has delegated authority.

### Step

1. To disable encryption by default for the entire cluster in ONTAP 9.7 or later, run the following command:

```
options -option-name encryption.data_at_rest_encryption.disable_by_default
-option-value on
```

= Data protection and disaster recovery

:hardbreaks:

:linkattrs:

```
:relative_path: ./data-protection-disaster-recovery/  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/
```

= Data protection with System Manager

= Data protection overview with System Manager

```
:toc: macro  
:toclevels: 1  
:hardbreaks:  
:icons: font  
:linkattrs:  
:relative_path: ./  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/
```

The topics in this section show you how to configure and manage data protection with System Manager in ONTAP 9.7 and later releases.

If you are using System Manager in ONTAP 9.7 or earlier, see [ONTAP System Manager Classic documentation](#)

Protect your data by creating and managing Snapshot copies, mirrors, vaults, and mirror-and-vault relationships.

*SnapMirror* is disaster recovery technology, designed for failover from primary storage to secondary storage at a geographically remote site. As its name implies, SnapMirror creates a replica, or mirror, of your working data in secondary storage from which you can continue to serve data in the event of a catastrophe at the primary site.

A *vault* is designed for disk-to-disk Snapshot copy replication for standards compliance and other governance-related purposes. In contrast to a SnapMirror relationship, in which the destination usually contains only the Snapshot copies currently in the source volume, a vault destination typically retains point-in-time Snapshot copies created over a much longer period.

Beginning with ONTAP 9.10.1, you can create data protection relationships between S3 buckets using S3 SnapMirror. Destination buckets can be on local or remote ONTAP systems, or on non-ONTAP systems such as StorageGRID and AWS. For more information, see [S3 SnapMirror overview](#).



= Create custom data protection policies

```
:toc: macro  
:toclevels: 1  
:hardbreaks:  
:icons: font  
:linkattrs:  
:relative_path: ./  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/
```

You can create custom data protection policies with System Manager when the existing default protection policies are not appropriate for your needs. Beginning with ONTAP 9.11.1, you can use System Manager to create custom mirror and vault policies, to display and select legacy policies. This capability is also available in ONTAP 9.8P12 and later patches of ONTAP 9.8.

Create custom protection policies on both the source and destination cluster.

### Steps

1. Click **Protection > Local Policy Settings**.
2. Under **Protection Policies**, click .
3. In the **Protection Policies** pane, click  **Add**.
4. Enter the new policy name, and select the policy scope.
5. Choose a policy type. To add a vault-only or mirror-only policy, choose **Asynchronous**, and click **Use a legacy policy type**.
6. Complete the required fields.
7. Click **Save**.
8. Repeat these steps on the other cluster.

= Configure Snapshot copies

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:




:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can create Snapshot copy policies to specify the maximum number of Snapshot copies that are automatically created and how frequently they are created. The policy specifies when to create Snapshot copies, how many copies to retain, and how to name them.

This procedure creates a Snapshot copy policy on the local cluster only.

### Steps

1. Click **Protection > Overview > Local Policy Settings**.
2. Under **Snapshot Policies**, click , and then click  **Add**.
3. Type the policy name, select the policy scope, and under **Schedules**, click  **Add** to enter the schedule details.

= Calculate reclaimable space before deleting Snapshot copies

:icons: font

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.10.1, you can use System Manager to select Snapshot copies you want to delete and calculate the reclaimable space before you delete them.

### Steps

1. Click **Storage > Volumes**.
2. Select the volume from which you want to delete Snapshot copies.
3. Click **Snapshot Copies**.

4. Select one or more Snapshot copies.
5. Click **Calculate Reclaimable Space**.

= Enable or disable client access to Snapshot copy directory

:icons: font

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/


Beginning with ONTAP 9.10.1, you can use System Manager to enable or disable client systems to access to a Snapshot copy directory on a volume. Enabling access makes the Snapshot copy directory visible to clients and allows Windows clients to map a drive to the Snapshot copies directory to view and access its contents.

You can enable or disable access to a volume's Snapshot copy directory by editing the volume settings or by editing the volume's share settings.

== Enable or disable client access to Snapshot copy directory by editing a volume

The Snapshot copy directory on a volume is accessible to clients by default.


### Steps

1. Click **Storage > Volumes**.
2. Select the volume containing the Snapshot copies directory you want to either show or hide.
3. Click  and select **Edit**.
4. In the **Snapshot Copies (Local) Settings** section, select or deselect **Show the Snapshot copies directory to clients**.
5. Click **Save**.

== Enable or disable client access to Snapshot copy directory by editing a share

The Snapshot copy directory on a volume is accessible to clients by default.

### Steps

1. Click **Storage > Shares**.
2. Select the volume containing the Snapshot copies directory you want to either show or hide.
3. Click  and select **Edit**.
4. In the **Share Properties** section, select or deselect **Allow clients to access Snapshot copies directory**.
5. Click **Save**.

= Recover from Snapshot copies

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can recover a volume to an earlier point in time by restoring from a Snapshot copy.

This procedure restores a volume from a Snapshot copy.

### Steps

1. Click **Storage** and select a volume.
2. Under **Snapshot Copies**, click  next to the Snapshot copy you want to restore, and select **Restore**.

= Prepare for mirroring and vaulting

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can protect your data by replicating it to a remote cluster for data backup and disaster recovery purposes.




Several default protection policies are available. You must have created your protection policies if you want to use custom policies.



### Steps

1. In the local cluster, click **Protection > Overview**.
2. Expand **Intercluster Settings**. Click **Add Network Interfaces** and add intercluster network interfaces for the cluster.

Repeat this step on the remote cluster.

3. In the remote cluster, click **Protection > Overview**. Click  in the Cluster Peers section and click **Generate Passphrase**.
4. Copy the generated passphrase and paste it in the local cluster.
5. In the local cluster, under Cluster Peers, click **Peer Clusters** and peer the local and remote clusters.
6. Optionally, under Storage VM Peers, click  and then **Peer Storage VMs** to peer the storage VMs.
7. Click **Protect Volumes** to protect your volumes. To protect your LUNs, click **Storage > LUNs**, select a LUN to protect, and then click  **Protect**.

Select the protection policy based on the type of data protection you need.

8. To verify the volumes and LUNs are successfully protected from the local cluster, click **Storage > Volumes** or **Storage > LUNs** and, expand the volume/LUN view.

== Other ways to do this in ONTAP

To perform these tasks with...	See this content...
System Manager Classic (available with ONTAP 9.7 and earlier)	<a href="#">Volume disaster recovery preparation overview</a>
The ONTAP command line interface	<a href="#">Create a cluster peer relationship</a>

= Configure mirrors and vaults

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Create a mirror and vault of a volume to protect data in case of a disaster and to have multiple archived versions of data to which you can roll back. Beginning with ONTAP 9.11.1, you can use System Manager to select pre-created and custom mirror and vault policies, to display and select legacy policies, and to override the transfer schedules defined in a protection policy when protecting volumes and storage VMs. This capability is also available in ONTAP 9.8P12 and later patches of ONTAP 9.8.



If you are using ONTAP 9.8P12 or later ONTAP 9.8 patch release and you configured SnapMirror using System Manager, you should contact NetApp Support before upgrading to ONTAP 9.9.1 or ONTAP 9.10.1 patch releases.

This procedure creates a data protection policy on a remote cluster. The source cluster and destination cluster use intercluster network interfaces for exchanging data. The procedure assumes the [intercluster network interfaces are created and the clusters containing the volumes are peered](#) (paired). You can also peer storage VMs for data protection; however, if storage VMs are not peered, but permissions are enabled, storage VMs are automatically peered when the protection relationship is created.



### Steps

1. Select the volume or LUN to protect: click **Storage > Volumes** or **Storage > LUNs**, and then click the desired volume or LUN name.
2. Click **Protect**.
3. Select the destination cluster and storage VM.
4. The asynchronous policy is selected by default. To select a synchronous policy, click **More Options**.
5. Click **Protect**.
6. Click the **SnapMirror (Local or Remote)** tab for the selected volume or LUN to verify that protection is set up correctly.



== Other ways to do this in ONTAP

To perform these tasks with...	See this content...
System Manager Classic (available with ONTAP 9.7 and earlier)	<a href="#">Volume backup using SnapVault overview</a>
The ONTAP command line interface	<a href="#">Create a replication relationship</a>

= Configure storage VM disaster recovery

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Using System Manager, you can create an storage VM disaster recovery (storage VM DR) relationship to replicate one storage VM configuration to another. In the event of a disaster at the primary site, you can quickly activate the destination storage VM.

Complete this procedure from the destination. If you need to create a new protection policy, for instance, when your source storage VM has SMB configured, you should use System Manager to create the policy and select the **Copy source storage VM configuration** option in the **Add Protection Policy** window. For details see [Create custom data protection policies](#).

### Steps

1. On the destination cluster, click **Protection > Relationships**.
2. Under **Relationships**, click Protect and choose **Storage VMs (DR)**.
3. Select a protection policy. If you created a custom protection policy, select it, then choose the source cluster and storage VM you want to replicate. You can also create a new destination storage VM by entering a new storage VM name.
4. Click **Save**.

= Serve data from a SnapMirror destination

:toc: macro

:toclevels: 1

:hardbreaks:

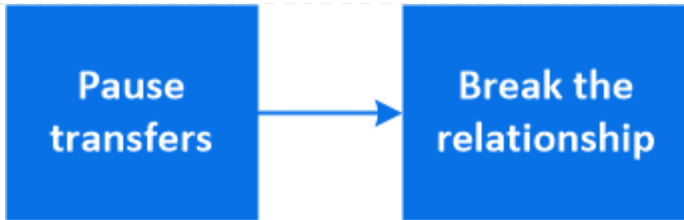
:icons: font

:linkattrs:


:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

To serve data from a mirror destination when a source becomes unavailable, stop scheduled transfers to the destination, and then break the SnapMirror relationship to make the destination writable.



### Steps

1. Select the desired protection relationship: click **Protection > Relationships**, and then click the desired volume name.
2. Click .
3. Stop scheduled transfers : click **Pause**.
4. Make the destination writable: click **Break**.
5. Go to the main **Relationships** page to verify that the relationship state displays as "broken off".

### Next steps:

When the disabled source volume is available again, you should resynchronize the relationship to copy the current data to the original source volume. This process replaces the data on the original source volume.

== Other ways to do this in ONTAP

To perform these tasks with...	See this content...
System Manager Classic (available with ONTAP 9.7 and earlier)	<a href="#">Volume disaster recovery overview</a>
The ONTAP command line interface	<a href="#">Activate the destination volume</a>

= Resynchronize a protection relationship

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:


:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

When your original source volume is available again after a disaster, you can resynchronize data from the destination volume and reestablish the protection relationship.

This procedure replaces the data in the original source volume in an asynchronous relationship so that you can start serving data from the original source volume again and resume the original protection relationship.

### Steps

1. Click **Protection > Relationships** and then click the broken off relationship you want to resynchronize.
2. Click  and then select **Resync**.

3. Under **Relationships**, monitor the resynchronization progress by checking the relationship state. The state changes to "Mirrored" when resynchronization is complete.

= Restore a volume from an earlier Snapshot copy

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:


:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

When data in a volume is lost or corrupted, you can roll back your data by restoring from an earlier Snapshot copy.

This procedure replaces the current data on the source volume with data from an earlier Snapshot copy version. You should perform this task on the destination cluster.

### Steps

1. Click **Protection > Relationships**, and then click the source volume name.
2. Click  and then select **Restore**.
3. Under **Source**, the source volume is selected by default. Click **Other Volume** if you want to choose a volume other than the source.
4. Under **Destination**, choose the Snapshot copy you want to restore.
5. If your source and destination are located on different clusters, on the remote cluster, click **Protection > Relationships** to monitor the restore progress.

== Other ways to do this in ONTAP

To perform these tasks with...	See this content...
System Manager Classic (available with ONTAP 9.7 and earlier)	<a href="#">Volume restore using SnapVault overview</a>
The ONTAP command line interface	<a href="#">Restore the contents of a volume from a SnapMirror destination</a>

= Recover from Snapshot copies

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can recover a volume to an earlier point in time by restoring from a Snapshot copy.

This procedure restores a volume from a Snapshot copy.

### Steps

1. Click **Storage** and select a volume.
2. Under **Snapshot Copies**, click  next to the Snapshot copy you want to restore, and select **Restore**.

= Restore to a new volume

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:


:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.8, you can use System Manager to restore backed up data on the destination volume to a volume other than the original source.

When you restore to a different volume, you can select an existing volume, or you can create a new volume.

### Steps

1. Select the desired protection relationship: click **Protection > Relationships**.
2. Click  and click **Restore**.
3. In the **Source** section, select **Other Volume** and select the cluster and Storage VM.
4. Select either **Existing volume** or **Create a new volume**.
5. If you are creating a new volume, enter the volume name.
6. In the **Destination** section, select the Snapshot copy to restore.
7. Click **Save**.
8. Under **Relationships**, monitor the restore progress by viewing **Transfer Status** for the relationship.

= Reverse Resynchronizing a Protection Relationship

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./


:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.8, you can use System Manager to perform a reverse resynchronization operation to delete an existing protection relationship and reverse the functions of the source and destination volumes. Then you use the destination volume to serve data while you repair or replace the source, update the source, and reestablish the original configuration of the systems.

When you perform a reverse resynch operation, any data on the source volume that is newer than the data in the common Snapshot copy is deleted.

### Steps

1. Select the desired protection relationship: click **Protection > Relationships**.

2. Click  and click **Reverse Resync**.
3. Under **Relationships**, monitor the reverse resynchronization progress by viewing **Transfer Status** for the relationship.

= Reactivate a source storage VM

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font


:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.8, you can use System Manager to reactivate a source storage VM after a disaster. Reactivating the source storage VM stops the destination storage VM, and it reenables replication from the source to the destination.

### Steps

1. Select the desired protection relationship: click **Protection > Relationships**.
2. Click  and click **Reactivate Source Storage VM**.
3. Under **Relationships**, monitor the source reactivation progress by viewing **Transfer Status** for the protection relationship.

= Resynchronize a destination storage VM

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./


:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.8, you can use System Manager to resynchronize the data and configuration details from the source storage VM to the destination storage VM in a broken protection relationship and reestablish the relationship.

ONTAP 9.11.1 introduces an option to bypass a full data warehouse rebuild when you perform a disaster recovery rehearsal, enabling you to return to production faster.

You perform the resync operation only from the destination of the original relationship. The resync deletes any data in the destination storage VM that is newer than the data in the source storage VM.

### Steps

1. Select the desired protection relationship: click **Protection > Relationships**.
2. Optionally, select **Perform a quick resync** to bypass a full data warehouse rebuild during a disaster recovery rehearsal.
3. Click  and click **Resync**.
4. Under **Relationships**, monitor the resynchronization progress by viewing **Transfer Status** for the relationship.

```
= Back up data to the cloud using SnapMirror
:toc: macro
:toclevels: 1
:hardbreaks:
:icons: font
:linkattrs:
:relative_path: ./
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/
```

Beginning with ONTAP 9.9.1, you can back up your data to the cloud and to restore your data from cloud storage to a different volume by using System Manager. You can use either StorageGRID or ONTAP S3 as your cloud object store.

Before using the SnapMirror Cloud feature, you should request a SnapMirror Cloud API license key from the NetApp Support Site: [Request SnapMirror Cloud API license key](#).

Following the instructions, you should provide a simple description of your business opportunity and request the API key by sending an email to the provided email address. You should receive an email response within 24 hours with further instructions on how to acquire the API key.

== Add a cloud object store

Before you configure SnapMirror Cloud backups, you need to add a StorageGRID or ONTAP S3 cloud object store.

### Steps

1. Click **Protection > Overview > Cloud Object Stores**.
2. Click **+ Add**.

== Back up using the default policy

You can quickly configure a SnapMirror Cloud backup for an existing volume using the default cloud protection policy, DailyBackup.

### Steps

1. Click **Protection > Overview** and select **Back Up Volumes to Cloud**.
2. If this is your first time backing up to the cloud, enter your SnapMirror Cloud API license key in the license field as indicated.
3. Click **Authenticate and Continue**.
4. Select a source volume.
5. Select a cloud object store.
6. Click **Save**.

== Create a custom cloud backup policy

If you do not want to use the default DailyBackup cloud policy for your SnapMirror Cloud backups, you can create your own policy.

### Steps

1. Click **Protection > Overview > Local Policy Settings** and select **Protection Policies**.
2. Click **Add** and enter the new policy details.

3. In the **Policy Type** section, select **Back up to Cloud** to indicate that you are creating a cloud policy.
4. Click **Save**.

== Create a backup from the **Volumes** page

You can use the System Manager **Volumes** page to when you want to select and create cloud backups for multiple volumes at one time or when you want to use a custom protection policy.

### Steps

1. Click **Storage > Volumes**.
2. Select the volumes you want to back up to the cloud, and click **Protect**.
3. In the **Protect Volume** window, click **More Options**.
4. Select a policy.


You can select the default policy, DailyBackup, or a custom cloud policy you created.

5. Select a cloud object store.
6. Click **Save**.

== Restore from the cloud

You can use System Manager to restore backed up data from cloud storage to a different volume on the source cluster.


### Steps

1. Click **Storage > Volumes**.
2. Select the **Back Up to Cloud** tab.
3. Click  next to the source volume you want to restore, and select **Restore**.
4. Under **Source**, select a storage VM and then enter the name of the volume to which you want the data restored.
5. Under **Destination**, select the Snapshot copy you want to restore.
6. Click **Save**.

== Delete a SnapMirror Cloud relationship

You can use System Manager to delete a cloud relationship.


### Steps

1. Click **Storage > Volumes** and select the volume you want to delete.
2. Click  next to the source volume and select **Delete**.
3. Select **Delete the cloud object store endpoint (optional)** if you want to delete the cloud object store endpoint.
4. Click **Delete**.

== Remove a cloud object store

You can use System Manager to remove a cloud object store if it is not part of a cloud backup relationship. When a cloud object store is part of a cloud backup relationship, it cannot be deleted.

## Steps

1. Click **Protection > Overview > Cloud Object Stores**.
2. Select the object store you want to delete, click  and select **Delete**.

= Back up data using Cloud Backup

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.9.1, you can use System Manager to back up data in the cloud using Cloud Backup.



Cloud Backup supports FlexVol read-write volumes and data-protection (DP) volumes. FlexGroup volumes and SnapLock volumes are not supported.

## Before you begin

You should perform the following procedures to establish an account in Cloud Manager. For the service account, you need to create the role as "Account Admin". (Other service account roles do not have the required privileges needed to establish a connection from System Manager.)

1. [Create an account in Cloud Manager](#).
2. [Create a connector in Cloud Manager](#) with one of the following cloud providers:
  - Microsoft Azure
  - Amazon Web Services (AWS)
  - Google Cloud Platform (GCP)
  - StorageGrid (ONTAP 9.10.1)



Beginning with ONTAP 9.10.1, you can select StorageGrid as a cloud backup provider, but only if Cloud Manager is deployed on premises. The Cloud Manager connector must be installed on premises and available through the Cloud Manager software-as-a-service (SaaS) application.

3. [Subscribe to Cloud Backup Service in Cloud Manager](#) (requires the appropriate license).
4. [Generate an access key and a secret key using Cloud Manager](#).

== Register the cluster with Cloud Manager

You can register the cluster with Cloud Manager by using either Cloud Manager or System Manager.

## Steps

1. In System Manager, go to **Protection Overview**.
2. Under **Cloud Backup Service**, provide the following details:
  - Client ID
  - Client secret key



### 3. Select **Register and Continue**.

== Enable Cloud Backup

After the cluster is registered with Cloud Manager, you need to enable the Cloud Backup and initiate the first backup to the cloud.

#### Steps

1. In System Manager, click **Protection > Overview**, then scroll to the **Cloud Backup Service** section.
2. Enter the **Client ID** and **Client Secret**.



Beginning with ONTAP 9.10.1, you can learn about the cost of using the cloud by clicking **Learn more about the cost of using the cloud**.

3. Click **Connect and Enable Cloud Backup Service**.
4. On the **Enable Cloud Backup Service** page, provide the following details, depending on the provider you selected.

For this cloud provider...	Enter the following data...
Azure	<ul style="list-style-type: none"><li>• Azure Subscription ID</li><li>• Region</li><li>• Resource group name (existing or new)</li></ul>
AWS	<ul style="list-style-type: none"><li>• AWS Account ID</li><li>• Access key</li><li>• Secret key</li><li>• Region</li></ul>
Google Cloud Project (GCP)	<ul style="list-style-type: none"><li>• Google Cloud Project name</li><li>• Google Cloud Access key</li><li>• Google Cloud Secret key</li><li>• Region</li></ul>
StorageGrid (ONTAP 9.10.1 and later, and only for on-premises deployment of Cloud Manager)	<ul style="list-style-type: none"><li>• Server</li><li>• SG Access Key</li><li>• SG Secret Key</li></ul>

### 5. Select a **Protection policy**:

- **Existing policy**: Choose an existing policy.
- **New Policy**: Specify a name and set up a transfer schedule.



Beginning with ONTAP 9.10.1, you can specify whether you want to enable archiving with Azure or AWS.



If you enable archiving for a volume with Azure or AWS, you cannot disable the archiving.

If you enable archiving for Azure or AWS, specify the following:

- The number of days after which the volume is archived.
- The number of backups to retain in the archive. Specify “0” (zero) to archive up to the latest backup.
- For AWS, select the archive storage class.


6. Select the volumes you want to back up.

7. Select **Save**.

== Edit the protection policy used for Cloud Backup

You can change which protection policy is used with Cloud Backup.

### Steps

1. In System Manager, click **Protection > Overview**, then scroll to the **Cloud Backup Service** section.
2. Click , then **Edit**.
3. Select a **Protection policy**:
  - **Existing policy**: Choose an existing policy.
  - **New Policy**: Specify a name and set up a transfer schedule.



Beginning with ONTAP 9.10.1, you can specify whether you want to enable archiving with Azure or AWS.



If you enable archiving for a volume with Azure or AWS, you cannot disable the archiving.

If you enable archiving for Azure or AWS, specify the following:

- The number of days after which the volume is archived.
- The number of backups to retain in the archive. Specify “0” (zero) to archive up to the latest backup.
- For AWS, select the archive storage class.

4. Select **Save**.

== Protect new volumes or LUNs on the cloud

When you create a new volume or LUN, you can establish a SnapMirror protection relationship that enables backing up to the cloud for the volume or LUN.

### Before you begin

- You should have a SnapMirror license.
- Intercluster LIFs should be configured.
- NTP should be configured.

- Cluster must be running ONTAP 9.9.1.

### About this task

You cannot protect new volumes or LUNs on the cloud for the following cluster configurations:

- The cluster cannot be in a MetroCluster environment.
- SVM-DR is not supported.
- FlexGroups cannot be backed up using Cloud Backup.

### Steps

1. When provisioning a volume or LUN, on the **Protection** page in System Manager, select the checkbox labeled **Enable SnapMirror (Local or Remote)**.
2. Select the Cloud Backup policy type.
3. If the Cloud Backup is not enabled, select **Enable Cloud Backup Service**.

== Protect existing volumes or LUNs on the cloud

You can establish a SnapMirror protection relationship for existing volumes and LUNs.

### Steps

1. Select an existing volume or LUN, and click **Protect**.
2. On the **Protect Volumes** page, specify **Backup using Cloud Backup Service** for the protection policy.
3. Click **Protect**.
4. On the **Protection** page, select the checkbox labeled **Enable SnapMirror (Local or Remote)**.
5. Select **Enable Cloud Backup Service**.

== Restore data from backup files

You can perform backup management operations, such as restoring data, updating relationships, and deleting relationships, only when using the Cloud Manager interface. Refer to [Restoring data from backup files](#) for more information.

= Cluster and SVM peering with the CLI

= Cluster and SVM peering overview with the CLI

:icons: font

:relative\_path: ./peering/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can create peer relationships between source and destination clusters and between source and destination storage virtual machines (SVMs). You must create peer relationships between these entities before you can replicate Snapshot copies using SnapMirror.

ONTAP 9.3 offers enhancements that simplify the way you configure peer relationships between clusters and SVMs. The cluster and SVMs peering procedures are available for all ONTAP 9 versions. You should use the appropriate procedure for your version of ONTAP.

You perform the procedures using the command-line interface (CLI), not System Manager or an automated scripting tool.

= Prepare for cluster and SVM peering

= Peering basics

:icons: font

:relative\_path: ./peering/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You must create *peer relationships* between source and destination clusters and between source and destination SVMs before you can replicate Snapshot copies using SnapMirror. A peer relationship defines network connections that enable clusters and SVMs to exchange data securely.

Clusters and SVMs in peer relationships communicate over the intercluster network using *intercluster logical interfaces (LIFs)*. An intercluster LIF is a LIF that supports the "intercluster-core" network interface service and is typically created using the "default-intercluster" network interface service policy. You must create intercluster LIFs on every node in the clusters being peered.

Intercluster LIFs use routes that belong to the system SVM to which they are assigned. ONTAP automatically creates a system SVM for cluster-level communications within an IPspace.

Fan-out and cascade topologies are both supported. In a cascade topology, you need only create intercluster networks between the primary and secondary clusters and between the secondary and tertiary clusters. You need not create an intercluster network between the primary and the tertiary cluster.

It is possible (but not advisable) for an administrator to remove the intercluster-core service from the default-intercluster service policy. If this occurs, LIFs created using "default-intercluster" will not actually be intercluster LIFs. To confirm that the default-intercluster service policy contains the intercluster-core service, use the following command:

```
network interface service-policy show -policy default-intercluster
```

= Prerequisites for cluster peering

:icons: font

:relative\_path: ./peering/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Before you set up cluster peering, you should confirm that the connectivity, port, IP address, subnet, firewall, and cluster-naming requirements are met.

== Connectivity requirements

Every intercluster LIF on the local cluster must be able to communicate with every intercluster LIF on the remote cluster.

Although it is not required, it is typically simpler to configure the IP addresses used for intercluster LIFs in the same subnet. The IP addresses can reside in the same subnet as data LIFs, or in a different subnet. The subnet used in each cluster must meet the following requirements:

- The subnet must belong to the broadcast domain that contains the ports that are used for intercluster communication.
- The subnet must have enough IP addresses available to allocate to one intercluster LIF per node.

For example, in a four-node cluster, the subnet used for intercluster communication must have four available IP addresses.

Each node must have an intercluster LIF with an IP address on the intercluster network.

Intercluster LIFs can have an IPv4 address or an IPv6 address.

ONTAP 9 enables you to migrate your peering networks from IPv4 to IPv6 by optionally allowing both protocols to be present simultaneously on the intercluster LIFs. In earlier releases, all intercluster relationships for an entire cluster were either IPv4 or IPv6. This meant that changing protocols was a potentially disruptive event.

## == Port requirements

You can use dedicated ports for intercluster communication, or share ports used by the data network. Ports must meet the following requirements:

- All ports that are used to communicate with a given remote cluster must be in the same IPspace.

You can use multiple IPspaces to peer with multiple clusters. Pair-wise full-mesh connectivity is required only within an IPspace.

- The broadcast domain that is used for intercluster communication must include at least two ports per node so that intercluster communication can fail over from one port to another port.

Ports added to a broadcast domain can be physical network ports, VLANs, or interface groups (ifgrps).

- All ports must be cabled.
- All ports must be in a healthy state.
- The MTU settings of the ports must be consistent.

## == Firewall requirements

Firewalls and the intercluster firewall policy must allow the following protocols:

- ICMP service
- TCP to the IP addresses of all the intercluster LIFs over the ports 10000, 11104, and 11105
- Bidirectional HTTPS between the intercluster LIFs

Although HTTPS is not required when you set up cluster peering using the CLI, HTTPS is required later if you use System Manager to configure data protection.

The default `intercluster` firewall policy allows access through the HTTPS protocol and from all IP addresses (0.0.0.0/0). You can modify or replace the policy if necessary.

## == Cluster requirement

Clusters must meet the following requirement:

- A cluster cannot be in a peer relationship with more than 255 clusters.

## = Use shared or dedicated ports

:icons: font

:relative\_path: ./peering/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use dedicated ports for intercluster communication, or share ports used by the data network. In deciding whether to share ports, you need to consider network bandwidth, the replication interval, and port availability.

You can share ports on one peered cluster while using dedicated ports on the other.

## == Network bandwidth

If you have a high-speed network, such as 10 GbE, you might have enough local LAN bandwidth to perform replication using the same 10 GbE ports used for data access.

Even then, you should compare your available WAN bandwidth to your LAN bandwidth. If the available WAN bandwidth is significantly less than 10 GbE, you might need to use dedicated ports.

The one exception to this rule might be when all or many nodes in the cluster replicate data, in which case bandwidth utilization is typically spread across nodes.

If you are not using dedicated ports, the maximum transmission unit (MTU) size of the replication network should typically be the same as the MTU size of the data network.

== Replication interval

If replication takes place in off-peak hours, you should be able to use data ports for replication even without a 10-GbE LAN connection.

If replication takes place during normal business hours, you need to consider the amount of data that will be replicated and whether it requires so much bandwidth that it could cause contention with data protocols. If network utilization by data protocols (SMB, NFS, iSCSI) is above 50%, you should use dedicated ports for intercluster communication, to allow for non-degraded performance if node failover occurs.

== Port availability

If you determine that replication traffic is interfering with data traffic, you can migrate intercluster LIFs to any other intercluster-capable shared port on the same node.

You can also dedicate VLAN ports for replication. The bandwidth of the port is shared between all VLANs and the base port.

= Use custom IPspaces to isolate replication traffic

:icons: font

:relative\_path: ./peering/

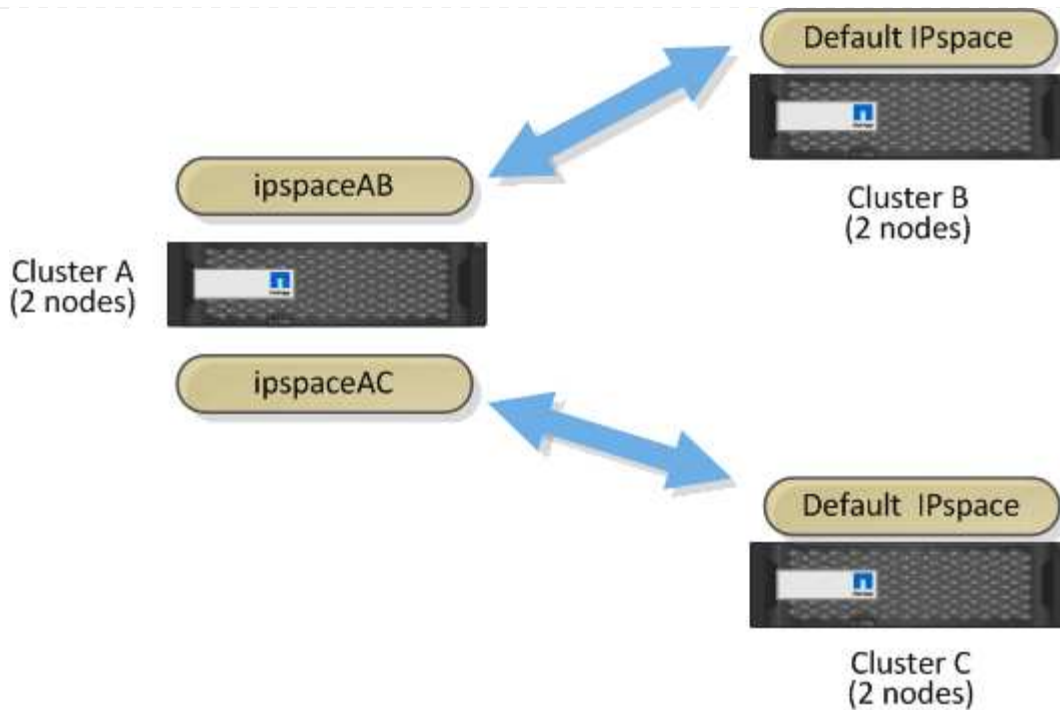
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use custom IPspaces to separate the interactions that a cluster has with its peers. Called *designated intercluster connectivity*, this configuration allows service providers to isolate replication traffic in multitenant environments.

Suppose, for example, that you want replication traffic between Cluster A and Cluster B to be separated from replication traffic between Cluster A and Cluster C. To accomplish this, you can create two IPspaces on Cluster A.

One IPspace contains the intercluster LIFs that you use to communicate with Cluster B. The other contains the intercluster LIFs that you use to communicate with Cluster C, as shown in the following illustration.





For custom IPspace configuration, see the *Network Management Guide*.

= Configure intercluster LIFs

= Configure intercluster LIFs on shared data ports

:icons: font

:relative\_path: ./peering/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can configure intercluster LIFs on ports shared with the data network. Doing so reduces the number of ports you need for intercluster networking.

### Steps

1. List the ports in the cluster:

```
network port show
```

For complete command syntax, see the man page.

The following example shows the network ports in `cluster01`:

```

cluster01::> network port show

```

						Speed
(Mbps)						
Node	Port	IPspace	Broadcast Domain	Link	MTU	
Admin/Oper						
-----						-----
cluster01-01						
	e0a	Cluster	Cluster	up	1500	
auto/1000						
	e0b	Cluster	Cluster	up	1500	
auto/1000						
	e0c	Default	Default	up	1500	
auto/1000						
	e0d	Default	Default	up	1500	
auto/1000						
cluster01-02						
	e0a	Cluster	Cluster	up	1500	
auto/1000						
	e0b	Cluster	Cluster	up	1500	
auto/1000						
	e0c	Default	Default	up	1500	
auto/1000						
	e0d	Default	Default	up	1500	
auto/1000						

## 2. Create intercluster LIFs on the system SVM:

Option	Description
<b>In ONTAP 9.6 and later:</b>	<code>network interface create -vserver <i>system_SVM</i> -lif <i>LIF_name</i> -service -policy default-intercluster -home -node <i>node</i> -home-port <i>port</i> -address <i>port_IP</i> -netmask <i>netmask</i></code>
<b>In ONTAP 9.5 and earlier:</b>	<code>network interface create -vserver <i>system_SVM</i> -lif <i>LIF_name</i> -role intercluster -home-node <i>node</i> -home -port <i>port</i> -address <i>port_IP</i> -netmask <i>netmask</i></code>

For complete command syntax, see the man page.

The following example creates intercluster LIFs `cluster01_ic101` and `cluster01_ic102`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0
```

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Verify that the intercluster LIFs were created:

Option	Description
<b>In ONTAP 9.6 and later:</b>	<code>network interface show -service-policy default-intercluster</code>
<b>In ONTAP 9.5 and earlier:</b>	<code>network interface show -role intercluster</code>

For complete command syntax, see the man page.

```
cluster01::> network interface show -service-policy default-
intercluster
          Logical      Status      Network      Current
Current Is
Vserver   Interface  Admin/Oper  Address/Mask  Node
Port      Home
-----
cluster01
          cluster01_icl01
          up/up      192.168.1.201/24  cluster01-01
e0c      true
          cluster01_icl02
          up/up      192.168.1.202/24  cluster01-02
e0c      true
```

4. Verify that the intercluster LIFs are redundant:

Option	Description
In ONTAP 9.6 and later:	network interface show -service-policy default-intercluster -failover
In ONTAP 9.5 and earlier:	network interface show -role intercluster -failover

For complete command syntax, see the man page.

The following example shows that the intercluster LIFs `cluster01_icl01` and `cluster01_icl02` on the `e0c` port will fail over to the `e0d` port.

```
cluster01::> network interface show -service-policy default-
intercluster -failover
          Logical          Home          Failover
Failover
Vserver  Interface          Node:Port          Policy          Group
-----  -----
cluster01
          cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                                     Failover Targets: cluster01-01:e0c,
                                                         cluster01-01:e0d
          cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                                     Failover Targets: cluster01-02:e0c,
                                                         cluster01-02:e0d
```

= Configure intercluster LIFs on dedicated ports

:icons: font

:relative\_path: ./peering/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can configure intercluster LIFs on dedicated ports. Doing so typically increases the available bandwidth for replication traffic.

### Steps

1. List the ports in the cluster:

```
network port show
```

For complete command syntax, see the man page.

The following example shows the network ports in `cluster01`:

```

cluster01::> network port show

```

						Speed
(Mbps)						
Node	Port	IPspace	Broadcast Domain	Link	MTU	
Admin/Oper						
-----						-----
cluster01-01						
	e0a	Cluster	Cluster	up	1500	
auto/1000						
	e0b	Cluster	Cluster	up	1500	
auto/1000						
	e0c	Default	Default	up	1500	
auto/1000						
	e0d	Default	Default	up	1500	
auto/1000						
	e0e	Default	Default	up	1500	
auto/1000						
	e0f	Default	Default	up	1500	
auto/1000						
cluster01-02						
	e0a	Cluster	Cluster	up	1500	
auto/1000						
	e0b	Cluster	Cluster	up	1500	
auto/1000						
	e0c	Default	Default	up	1500	
auto/1000						
	e0d	Default	Default	up	1500	
auto/1000						
	e0e	Default	Default	up	1500	
auto/1000						
	e0f	Default	Default	up	1500	
auto/1000						

2. Determine which ports are available to dedicate to intercluster communication:

```
network interface show -fields home-port,curr-port
```

For complete command syntax, see the man page.

The following example shows that ports e0e and e0f have not been assigned LIFs:

```

cluster01::> network interface show -fields home-port,curr-port
vserver lif                home-port curr-port
-----
Cluster cluster01-01_clus1  e0a       e0a
Cluster cluster01-01_clus2  e0b       e0b
Cluster cluster01-02_clus1  e0a       e0a
Cluster cluster01-02_clus2  e0b       e0b
cluster01
      cluster_mgmt           e0c       e0c
cluster01
      cluster01-01_mgmt1     e0c       e0c
cluster01
      cluster01-02_mgmt1     e0c       e0c

```

### 3. Create a failover group for the dedicated ports:

```

network interface failover-groups create -vserver system_SVM -failover
-group failover_group -targets physical_or_logical_ports

```

The following example assigns ports e0e and e0f to the failover group intercluster01 on the system SVM cluster01:

```

cluster01::> network interface failover-groups create -vserver
cluster01 -failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f

```

### 4. Verify that the failover group was created:

```

network interface failover-groups show

```

For complete command syntax, see the man page.

```

cluster01::> network interface failover-groups show
                                Failover
Vserver          Group          Targets
-----
Cluster
                                Cluster
01:e0b,          cluster01-01:e0a, cluster01-
cluster01        cluster01-02:e0a, cluster01-02:e0b
                                Default
01:e0d,          cluster01-01:e0c, cluster01-
02:e0d,          cluster01-02:e0c, cluster01-
                                intercluster01
                                cluster01-01:e0e, cluster01-01:e0f
                                cluster01-02:e0e, cluster01-02:e0f
                                cluster01-01:e0e, cluster01-01:e0f
                                cluster01-02:e0e, cluster01-02:e0f

```

5. Create intercluster LIFs on the system SVM and assign them to the failover group.

Option	Description
<b>In ONTAP 9.6 and later:</b>	<code>network interface create -vserver <i>system_SVM</i> -lif <i>LIF_name</i> -service -policy default-intercluster -home -node <i>node</i> -home- port <i>port</i> -address <i>port_IP</i> -netmask <i>netmask</i> -failover -group <i>failover_group</i></code>
<b>In ONTAP 9.5 and earlier:</b>	<code>network interface create -vserver <i>system_SVM</i> -lif <i>LIF_name</i> -role intercluster -home-node <i>node</i> -home -port <i>port</i> -address <i>port_IP</i> -netmask <i>netmask</i> -failover-group <i>failover_group</i></code>

For complete command syntax, see the man page.

The following example creates intercluster LIFs `cluster01_icl01` and `cluster01_icl02` in the failover group `intercluster01`:

```

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01

```

6. Verify that the intercluster LIFs were created:

Option	Description
<b>In ONTAP 9.6 and later:</b>	<code>network interface show -service-policy default-intercluster</code>
<b>In ONTAP 9.5 and earlier:</b>	<code>network interface show -role intercluster</code>

For complete command syntax, see the man page.

```

cluster01::> network interface show -service-policy default-
intercluster

```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----				
-----				
cluster01	cluster01_icl01	up/up	192.168.1.201/24	cluster01-01
e0e	true			
	cluster01_icl02	up/up	192.168.1.202/24	cluster01-02
e0f	true			

7. Verify that the intercluster LIFs are redundant:



Option	Description
In ONTAP 9.6 and later:	network interface show -service -policy default-intercluster -failover
In ONTAP 9.5 and earlier:	network interface show -role intercluster -failover

For complete command syntax, see the man page.

The following example shows that the intercluster LIFs `cluster01_icl01` and `cluster01_icl02` on the SVM `e0e` port will fail over to the `e0f` port.

```
cluster01::> network interface show -service-policy default-
intercluster -failover
          Logical          Home          Failover
Failover
Vserver  Interface          Node:Port          Policy          Group
-----  -
cluster01
          cluster01_icl01 cluster01-01:e0e  local-only
intercluster01
          Failover Targets: cluster01-01:e0e,
                           cluster01-01:e0f
          cluster01_icl02 cluster01-02:e0e  local-only
intercluster01
          Failover Targets: cluster01-02:e0e,
                           cluster01-02:e0f
```

= Configure intercluster LIFs in custom IPspaces

:icons: font

:relative\_path: ./peering/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can configure intercluster LIFs in custom IPspaces. Doing so allows you to isolate replication traffic in multitenant environments.

When you create a custom IPspace, the system creates a system storage virtual machine (SVM) to serve as a container for the system objects in that IPspace. You can use the new SVM as the container for any intercluster LIFs in the new IPspace. The new SVM has the same name as the custom IPspace.

### Steps

1. List the ports in the cluster:

```
network port show
```

For complete command syntax, see the man page.

The following example shows the network ports in `cluster01`:

```
cluster01::> network port show
```

(Mbps)					Speed
Node	Port	IPspace	Broadcast Domain	Link	MTU
Admin/Oper					
-----					
cluster01-01					
	e0a	Cluster	Cluster	up	1500
auto/1000					
	e0b	Cluster	Cluster	up	1500
auto/1000					
	e0c	Default	Default	up	1500
auto/1000					
	e0d	Default	Default	up	1500
auto/1000					
	e0e	Default	Default	up	1500
auto/1000					
	e0f	Default	Default	up	1500
auto/1000					
cluster01-02					
	e0a	Cluster	Cluster	up	1500
auto/1000					
	e0b	Cluster	Cluster	up	1500
auto/1000					
	e0c	Default	Default	up	1500
auto/1000					
	e0d	Default	Default	up	1500
auto/1000					
	e0e	Default	Default	up	1500
auto/1000					
	e0f	Default	Default	up	1500
auto/1000					

2. Create custom IPspaces on the cluster:

```
network ipspace create -ipspace ipspace
```

The following example creates the custom IPspace `ipspace-IC1`:

```
cluster01::> network ipspace create -ipspace ipspace-IC1
```

3. Determine which ports are available to dedicate to intercluster communication:

```
network interface show -fields home-port,curr-port
```

For complete command syntax, see the man page.

The following example shows that ports e0e and e0f have not been assigned LIFs:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                home-port curr-port
-----
Cluster cluster01_clus1    e0a      e0a
Cluster cluster01_clus2    e0b      e0b
Cluster cluster02_clus1    e0a      e0a
Cluster cluster02_clus2    e0b      e0b
cluster01
  cluster_mgmt              e0c      e0c
cluster01
  cluster01-01_mgmt1        e0c      e0c
cluster01
  cluster01-02_mgmt1        e0c      e0c
```

4. Remove the available ports from the default broadcast domain:

```
network port broadcast-domain remove-ports -broadcast-domain Default -ports
ports
```

A port cannot be in more than one broadcast domain at a time. For complete command syntax, see the man page.

The following example removes ports e0e and e0f from the default broadcast domain:

```
cluster01::> network port broadcast-domain remove-ports -broadcast
-domain Default -ports
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

5. Verify that the ports have been removed from the default broadcast domain:

```
network port show
```

For complete command syntax, see the man page.

The following example shows that ports e0e and e0f have been removed from the default broadcast domain:

```
cluster01::> network port show
```

Node	Port	IPspace	Broadcast Domain	Link	MTU	Speed (Mbps) Admin/Oper
cluster01-01						
	e0a	Cluster	Cluster	up	9000	auto/1000
	e0b	Cluster	Cluster	up	9000	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	-	up	1500	auto/1000
	e0f	Default	-	up	1500	auto/1000
	e0g	Default	Default	up	1500	auto/1000
cluster01-02						
	e0a	Cluster	Cluster	up	9000	auto/1000
	e0b	Cluster	Cluster	up	9000	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	-	up	1500	auto/1000
	e0f	Default	-	up	1500	auto/1000
	e0g	Default	Default	up	1500	auto/1000

#### 6. Create a broadcast domain in the custom IPspace:

```
network port broadcast-domain create -ipspace ipspace -broadcast-domain  
broadcast_domain -mtu MTU -ports ports
```

The following example creates the broadcast domain `ipspace-IC1-bd` in the IPspace `ipspace-IC1`:

```
cluster01::> network port broadcast-domain create -ipspace ipspace-  
IC1 -broadcast-domain  
ipspace-IC1-bd -mtu 1500 -ports cluster01-01:e0e,cluster01-01:e0f,  
cluster01-02:e0e,cluster01-02:e0f
```

#### 7. Verify that the broadcast domain was created:

```
network port broadcast-domain show
```

For complete command syntax, see the man page.

```

cluster01::> network port broadcast-domain show
IPspace Broadcast                               Update
Name      Domain Name      MTU  Port List      Status
Details
-----
Cluster Cluster          9000
          cluster01-01:e0a      complete
          cluster01-01:e0b      complete
          cluster01-02:e0a      complete
          cluster01-02:e0b      complete
Default Default          1500
          cluster01-01:e0c      complete
          cluster01-01:e0d      complete
          cluster01-01:e0f      complete
          cluster01-01:e0g      complete
          cluster01-02:e0c      complete
          cluster01-02:e0d      complete
          cluster01-02:e0f      complete
          cluster01-02:e0g      complete
ipspace-IC1
  ipspace-IC1-bd
                1500
          cluster01-01:e0e      complete
          cluster01-01:e0f      complete
          cluster01-02:e0e      complete
          cluster01-02:e0f      complete

```

8. Create intercluster LIFs on the system SVM and assign them to the broadcast domain:

Option	Description
<b>In ONTAP 9.6 and later:</b>	<code>network interface create -vserver <i>system_SVM</i> -lif <i>LIF_name</i> -service -policy default-intercluster -home -node <i>node</i> -home-port <i>port</i> -address <i>port_IP</i> -netmask <i>netmask</i></code>
<b>In ONTAP 9.5 and earlier:</b>	<code>network interface create -vserver <i>system_SVM</i> -lif <i>LIF_name</i> -role intercluster -home-node <i>node</i> -home -port <i>port</i> -address <i>port_IP</i> -netmask <i>netmask</i></code>

The LIF is created in the broadcast domain that the home port is assigned to. The broadcast domain has a default failover group with the same name as the broadcast domain. For complete command

syntax, see the man page.

The following example creates intercluster LIFs `cluster01_icl01` and `cluster01_icl02` in the broadcast domain `ipspace-IC1-bd`:

```
cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0
```

9. Verify that the intercluster LIFs were created:

Option	Description
<b>In ONTAP 9.6 and later:</b>	<code>network interface show -service-policy default-intercluster</code>
<b>In ONTAP 9.5 and earlier:</b>	<code>network interface show -role intercluster</code>

For complete command syntax, see the man page.

```
cluster01::> network interface show -service-policy default-
intercluster

          Logical      Status      Network      Current
Current Is
Vserver   Interface  Admin/Oper  Address/Mask  Node
Port      Home
-----
-----
ipspace-IC1
          cluster01_icl01
          up/up      192.168.1.201/24  cluster01-01
e0e      true
          cluster01_icl02
          up/up      192.168.1.202/24  cluster01-02
e0f      true
```

10. Verify that the intercluster LIFs are redundant:

Option	Description
<b>In ONTAP 9.6 and later:</b>	<code>network interface show -service -policy default-intercluster -failover</code>
<b>In ONTAP 9.5 and earlier:</b>	<code>network interface show -role intercluster -failover</code>

For complete command syntax, see the man page.

The following example shows that the intercluster LIFs `cluster01_icl01` and `cluster01_icl02` on the SVM `e0e` port fail over to the `e0f` port:

```
cluster01::> network interface show -service-policy default-
intercluster -failover
          Logical          Home          Failover
Failover
Vserver  Interface          Node:Port          Policy          Group
-----  -----
ipspace-IC1
          cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                                Failover Targets: cluster01-01:e0e,
                                                cluster01-01:e0f
          cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                                Failover Targets: cluster01-02:e0e,
                                                cluster01-02:e0f
```

= Configure peer relationships

= Create a cluster peer relationship

:icons: font

:relative\_path: ./peering/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the `cluster peer create` command to create a peer relationship between a local and remote cluster. After the peer relationship has been created, you can run `cluster peer create` on the remote cluster to authenticate it to the local cluster.

**Before you begin**

- You must have created intercluster LIFs on every node in the clusters that are being peered.
- The clusters must be running ONTAP 9.3 or later. (If the clusters are running ONTAP 9.2 or earlier, refer to the procedures in [this archived document](#).)

## Steps

1. On the destination cluster, create a peer relationship with the source cluster:

```
cluster peer create -generate-passphrase -offer-expiration MM/DD/YYYY
HH:MM:SS|1...7days|1...168hours -peer-addr peer_LIF_IPs -initial-allowed
-vserver-peers svm_name,..|* -ip-space ip-space
```

If you specify both `-generate-passphrase` and `-peer-addr`s, only the cluster whose intercluster LIFs are specified in `-peer-addr`s can use the generated password.

You can ignore the `-ip-space` option if you are not using a custom IPspace. For complete command syntax, see the man page.

If you are creating the peering relationship in ONTAP 9.6 or later and you do not want cross-cluster peering communications to be encrypted, you must use the `-encryption-protocol-proposed none` option to disable encryption.

The following example creates a cluster peer relationship with an unspecified remote cluster, and pre-authorizes peer relationships with SVMs `vs1` and `vs2` on the local cluster:

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

                Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
                Expiration Time: 6/7/2017 08:16:10 EST
Initial Allowed Vserver Peers: vs1,vs2
                Intercluster LIF IP: 192.140.112.101
                Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

The following example creates a cluster peer relationship with the remote cluster at intercluster LIF IP addresses 192.140.112.103 and 192.140.112.104, and pre-authorizes a peer relationship with any SVM on the local cluster:



```
cluster02::> cluster peer create -generate-passphrase -peer-addr  
192.140.112.103,192.140.112.104 -offer-expiration 2days -initial  
-allowed-vserver-peers *
```

```
                Passphrase: UCa+6lRVICXeL/gq1WrK7ShR  
                Expiration Time: 6/7/2017 08:16:10 EST  
Initial Allowed Vserver Peers: vs1,vs2  
                Intercluster LIF IP: 192.140.112.101,192.140.112.102  
                Peer Cluster Name: Clus_7ShR (temporary generated)
```

Warning: make a note of the passphrase - it cannot be displayed again.

The following example creates a cluster peer relationship with an unspecified remote cluster, and pre-authorizes peer relationships with SVMs `vs1` and `vs2` on the local cluster:

```
cluster02::> cluster peer create -generate-passphrase -offer  
-expiration 2days -initial-allowed-vserver-peers vs1,vs2
```

```
                Passphrase: UCa+6lRVICXeL/gq1WrK7ShR  
                Expiration Time: 6/7/2017 08:16:10 EST  
Initial Allowed Vserver Peers: vs1,vs2  
                Intercluster LIF IP: 192.140.112.101  
                Peer Cluster Name: Clus_7ShR (temporary generated)
```

Warning: make a note of the passphrase - it cannot be displayed again.

2. On source cluster, authenticate the source cluster to the destination cluster:

```
cluster peer create -peer-addr peer_LIF_IPs -ip-space ip-space
```

For complete command syntax, see the man page.

The following example authenticates the local cluster to the remote cluster at intercluster LIF IP addresses 192.140.112.101 and 192.140.112.102:

```
cluster01::> cluster peer create -peer-addr  
192.140.112.101,192.140.112.102
```

Notice: Use a generated passphrase or choose a passphrase of 8 or more characters.

To ensure the authenticity of the peering relationship, use a phrase or sequence of characters that would be hard to guess.

```
Enter the passphrase:  
Confirm the passphrase:
```

```
Clusters cluster02 and cluster01 are peered.
```

Enter the passphrase for the peer relationship when prompted.

### 3. Verify that the cluster peer relationship was created:

```
cluster peer show -instance
```

```
cluster01::> cluster peer show -instance  
  
Peer Cluster Name: cluster02  
Remote Intercluster Addresses: 192.140.112.101,  
192.140.112.102  
Availability of the Remote Cluster: Available  
Remote Cluster Name: cluster2  
Active IP Addresses: 192.140.112.101,  
192.140.112.102  
  
Cluster Serial Number: 1-80-123456  
Address Family of Relationship: ipv4  
Authentication Status Administrative: no-authentication  
Authentication Status Operational: absent  
Last Update Time: 02/05 21:05:41  
IPspace for the Relationship: Default
```

### 4. Check the connectivity and status of the nodes in the peer relationship:

```
cluster peer health show
```

```

cluster01::> cluster peer health show
Node          cluster-Name          Node-Name
              Ping-Status          RDB-Health Cluster-Health
Avail...
-----
cluster01-01
              cluster02          cluster02-01
              Data: interface_reachable
              ICMP: interface_reachable true          true
true
              cluster02-02
              Data: interface_reachable
              ICMP: interface_reachable true          true
true
cluster01-02
              cluster02          cluster02-01
              Data: interface_reachable
              ICMP: interface_reachable true          true
true
              cluster02-02
              Data: interface_reachable
              ICMP: interface_reachable true          true
true

```

== Other ways to do this in ONTAP

To perform these tasks with...	See this content...
The redesigned System Manager (available with ONTAP 9.7 and later)	<a href="#">Prepare for mirroring and vaulting</a>
System Manager Classic (available with ONTAP 9.7 and earlier)	<a href="#">Volume disaster recovery preparation overview</a>

= Create an intercluster SVM peer relationship

:icons: font

:relative\_path: ./peering/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the `vserver peer create` command to create a peer relationship between SVMs on local and remote clusters.

#### Before you begin

- The source and destination clusters must be peered.
- The clusters must be running ONTAP 9.3. (If the clusters are running ONTAP 9.2 or earlier, refer to the procedures in [this archived document](#).)

- You must have "pre-authorized" peer relationships for the SVMs on the remote cluster.

For more information, see [Creating a cluster peer relationship](#).

### About this task

Previous releases of ONTAP let you authorize a peer relationship for only one SVM at a time. You needed to run the `vserver peer accept` command each time you authorized a pending SVM peer relationship.

Beginning with ONTAP 9.3, you can "pre-authorize" peer relationships for multiple SVMs by listing the SVMs in the `-initial-allowed-vserver` option when you create a cluster peer relationship. For more information, see [Creating a cluster peer relationship](#).

### Steps

1. On the data protection destination cluster, display the SVMs that are pre-authorized for peering:

```
vserver peer permission show
```

```
cluster02::> vserver peer permission show
Peer Cluster          Vserver              Applications
-----
cluster02            vs1,vs2              snapmirror
```

2. On the data protection source cluster, create a peer relationship to a pre-authorized SVM on the data protection destination cluster:

```
vserver peer create -vserver local_SVM -peer-vserver remote_SVM
```

For complete command syntax, see the man page.

The following example creates a peer relationship between the local SVM `pvs1` and the pre-authorized remote SVM `vs1`:

```
cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
```

3. Verify the SVM peer relationship:

```
vserver peer show
```

```

cluster01::> vserver peer show
          Peer          Peer          Peering
Remote
Vserver  Vserver  State      Peer Cluster  Applications
Vserver
-----
pvs1     vs1       peered     cluster02    snapmirror
vs1

```

= Add an intercluster SVM peer relationship

:icons: font

:relative\_path: ./peering/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

If you create an SVM after configuring a cluster peer relationship, you will need to add a peer relationship for the SVM manually. You can use the `vserver peer create` command to create a peer relationship between SVMs. After the peer relationship has been created, you can run `vserver peer accept` on the remote cluster to authorize the peer relationship.

### Before you begin

The source and destination clusters must be peered.

### About this task

You can create a peer relationships between SVMs in the same cluster for local data backup. For more information, see the `vserver peer create` man page.

Administrators occasionally use the `vserver peer reject` command to reject a proposed SVM peer relationship. If the relationship between SVMs is in the `rejected` state, you must delete the relationship before you can create a new one. For more information, see the `vserver peer delete` man page.

### Steps

1. On the data protection source cluster, create a peer relationship with an SVM on the data protection destination cluster:

```

vserver peer create -vserver local_SVM -peer-vserver remote_SVM
-applications snapmirror|file-copy|lun-copy -peer-cluster remote_cluster

```

The following example creates a peer relationship between the local SVM`pvs1` and the remote SVM`vs1`

```

cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
-applications snapmirror -peer-cluster cluster02

```

If the local and remote SVMs have the same names, you must use a *local name* to create the SVM

peer relationship:

```
cluster01::> vserver peer create -vserver vs1 -peer-vserver  
vs1 -applications snapmirror -peer-cluster cluster01  
-local-name cluster1vs1LocallyUniqueName
```

2. On the data protection source cluster, verify that the peer relationship has been initiated:

```
vserver peer show-all
```

For complete command syntax, see the man page.

The following example shows that the peer relationship between SVM<sub>pvs1</sub> and SVM<sub>vs1</sub> has been initiated:

```
cluster01::> vserver peer show-all
```

Vserver	Peer Vserver	Peer State	Peer Cluster	Peering Applications
pvs1	vs1	initiated	Cluster02	snapmirror

3. On the data protection destination cluster, display the pending SVM peer relationship:

```
vserver peer show
```

For complete command syntax, see the man page.

The following example lists the pending peer relationships for cluster02:

```
cluster02::> vserver peer show
```

Vserver	Peer Vserver	Peer State
vs1	pvs1	pending

4. On the data protection destination cluster, authorize the pending peer relationship:

```
vserver peer accept -vserver local_SVM -peer-vserver remote_SVM
```

For complete command syntax, see the man page.

The following example authorizes the peer relationship between the local SVM <sub>vs1</sub> and the remote SVM <sub>pvs1</sub>:

```
cluster02::> vserver peer accept -vserver vs1 -peer-vserver pvs1
```

#### 5. Verify the SVM peer relationship:

```
vserver peer show
```

```
cluster01::> vserver peer show
```

Remote Vserver	Peer Vserver	Peer State	Peer Cluster	Peering Applications
pvs1	vs1	peered	cluster02	snapmirror

= Enable cluster peering encryption on an existing peer relationship

:icons: font

:relative\_path: ./peering/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.6, cluster peering encryption is enabled by default on all newly created cluster peering relationships. Cluster peering encryption uses a pre-shared key (PSK) and the Transport Security Layer (TLS) to secure cross-cluster peering communications. This adds an additional layer of security between the peered clusters.

#### About this task

If you are upgrading peered clusters to ONTAP 9.6 or later, and the peering relationship was created in ONTAP 9.5 or earlier, cluster peering encryption must be enabled manually after upgrading. Both clusters in the peering relationship must be running ONTAP 9.6 or later in order to enable cluster peering encryption.

#### Steps

1. On the destination cluster, enable encryption for communications with the source cluster:

```
cluster peer modify source_cluster -auth-status-admin use-authentication  
-encryption-protocol-proposed tls-psk
```

2. When prompted enter a passphrase.

3. On the data protection source cluster, enable encryption for communication with the data protection destination cluster:

```
cluster peer modify data_protection_destination_cluster -auth-status-admin  
use-authentication -encryption-protocol-proposed tls-psk
```

4. When prompted, enter the same passphrase entered on the destination cluster.

= Remove cluster peering encryption from an existing peer relationship

:icons: font

:relative\_path: ./peering/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

By default, cluster peering encryption is enabled on all peer relationships created in ONTAP 9.6 or later. If you do not want to use encryption for cross-cluster peering communications, you can disable it.

### Steps

1. On the destination cluster, modify communications with the source cluster to discontinue use of cluster peering encryption :

- To remove encryption, but maintain authentication enter:

```
cluster peer modify source_cluster -auth-status-admin use-authentication  
-encryption none
```

- To remove encryption and authentication, enter:

```
cluster peer modify source_cluster -auth-status no-authentication
```

2. When prompted enter a passphrase.

3. On the source cluster, disable encryption for communication with the destination cluster:

- To remove encryption, but maintain authentication enter:

```
cluster peer modify destination_cluster -auth-status-admin use-  
authentication -encrypt none
```

- To remove encryption and authentication, enter:

```
cluster peer modify destination_cluster -auth-status no-authentication
```

4. When prompted, enter the same passphrase entered on the destination cluster.

= Where to find additional information

:icons: font

:relative\_path: ./peering/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can learn more about tasks related to cluster and SVM peering in NetApp's extensive documentation library.

- [ONTAP concepts](#)

Describes the concepts that inform ONTAP data management software, including data protection and transfer.

- [Data protection](#)

Describes how to use the ONTAP CLI to perform SnapMirror replication.



- [Volume disaster recovery preparation](#)

Describes how to use System Manager to quickly configure a destination volume for disaster recovery.

- [Volume disaster recovery preparation](#)

Describes how to use System Manager to quickly recover a destination volume after a disaster.

- [Volume backup using SnapVault](#)

Describes how to use System Manager to quickly configure a SnapVault relationship between volumes.

- [Volume restore management using SnapVault](#)

Describes how to use System Manager to quickly restore files from a destination volume in a SnapVault relationship.

- [Archive and compliance using SnapLock technology](#)

Describes how to replicate WORM files in a SnapLock volume.

= Data protection with the CLI

= Data protection overview with the CLI

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use CLI commands to manage Snapshot copies on a local ONTAP system and to replicate Snapshot copies to a remote system using SnapMirror. You can replicate Snapshot copies for disaster recovery or long-term retention.

Use these procedures under the following circumstances:

- You want to understand the range of ONTAP backup and recovery capabilities.
- You want to use the command-line interface (CLI), not System Manager, an automated scripting tool, or [SnapCenter Software](#).
- You have already created peer relationships between the source and destination clusters and the source and destination SVMs.

#### [Cluster and SVM peering](#)

- You are backing up volumes or SVMs from AFF or FAS storage systems to AFF or FAS storage systems.
  - If you are replicating Element volumes to ONTAP, or ONTAP LUNs to an Element system, see the NetApp Element software documentation.

#### [Replication between NetApp element software and ONTAP](#)

- Beginning with ONTAP 9.10.1, you can create data protection relationships between S3 buckets using S3 SnapMirror. For more information, see [S3 SnapMirror overview](#).

- You want to provide data protection using online methods, not tape.

== Other ways to do this in ONTAP

To perform these tasks with...	Refer to...
The redesigned System Manager (available with ONTAP 9.7 and later)	<a href="#">Prepare for mirroring and vaulting</a>
System Manager Classic (available with ONTAP 9.7 and earlier)	<a href="#">Volume disaster recovery preparation overview</a>

= Manage local Snapshot copies

= Manage local Snapshot copies overview

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

A *Snapshot copy* is a read-only, point-in-time image of a volume. The image consumes minimal storage space and incurs negligible performance overhead because it records only changes to files since the last Snapshot copy.

You can use a Snapshot copy to restore the entire contents of a volume, or to recover individual files or LUNs. Snapshot copies are stored in the directory `.snapshot` on the volume.

In ONTAP 9.3 and earlier, a volume can contain up to 255 Snapshot copies. In ONTAP 9.4 and later, a FlexVol volume can contain up to 1023 Snapshot copies.

Beginning with ONTAP 9.8, FlexGroup volumes can contain 1023 Snapshot copies. For more information, see [Protect FlexGroup volumes using Snapshot copies](#).

= Configure custom Snapshot policies

= Configure custom Snapshot policies overview

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

A *Snapshot policy* defines how the system creates Snapshot copies. The policy specifies when to create Snapshot copies, how many copies to retain, and how to name them. For example, a system might create one Snapshot copy every day at 12:10 a.m., retain the two most recent copies, and name the copies

“*daily.timestamp*.”

The default policy for a volume automatically creates Snapshot copies on the following schedule, with the oldest Snapshot copies deleted to make room for newer copies:

- A maximum of six hourly Snapshot copies taken five minutes past the hour.
- A maximum of two daily Snapshot copies taken Monday through Saturday at 10 minutes after midnight.
- A maximum of two weekly Snapshot copies taken every Sunday at 15 minutes after midnight.

Unless you specify a Snapshot policy when you create a volume, the volume inherits the Snapshot policy associated with its containing storage virtual machine (SVM).

= When to configure a custom Snapshot policy

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

If the default Snapshot policy is not appropriate for a volume, you can configure a custom policy that modifies the frequency, retention, and name of Snapshot copies. The schedule will be dictated mainly by the rate of change of the active file system.

You might back up a heavily used file system like a database every hour, while you back up rarely used files once a day. Even for a database, you will typically run a full backup once or twice a day, while backing up transaction logs every hour.

Other factors are the importance of the files to your organization, your Service Level Agreement (SLA), your Recovery Point Objective (RPO), and your Recovery Time Objective (RTO). Generally speaking, you should retain only as many Snapshot copies as necessary.

= Create a Snapshot job schedule

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

A Snapshot policy requires at least one Snapshot copy job schedule. You can use the `job schedule cron create` command to create a job schedule.

**About this task**

By default, ONTAP forms the names of Snapshot copies by appending a timestamp to the job schedule name.

If you specify values for both day of the month and day of the week, the values are considered independently. For example, a cron schedule with the day specification `Friday` and the day of the month specification `13` runs every Friday and on the 13th day of each month, not just on every Friday the 13th.

### Step

1. Create a job schedule:

```
job schedule cron create -name job_name -month month -dayofweek day_of_week  
-day day_of_month -hour hour -minute minute
```

For `-month`, `-dayofweek`, and `-hour`, you can specify `all` to run the job every month, day of the week, and hour, respectively.

Beginning with ONTAP 9.10.1, you can include the Vserver for your job schedule:

```
job schedule cron create -name job_name -vserver Vserver_name -month month  
-dayofweek day_of_week -day day_of_month -hour hour -minute minute
```

The following example creates a job schedule named `myweekly` that runs on Saturdays at 3:00 a.m.:

```
cluster1::> job schedule cron create -name myweekly -dayofweek  
"Saturday" -hour 3 -minute 0
```

The following example creates a schedule named `myweeklymulti` that specifies multiple days, hours and minutes:

```
job schedule cron create -name myweeklymulti -dayofweek  
"Monday,Wednesday,Sunday" -hour 3,9,12 -minute 0,20,50
```

= Create a Snapshot policy

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

A Snapshot policy specifies when to create Snapshot copies, how many copies to retain, and how to name them. For example, a system might create one Snapshot copy every day at 12:10 a.m., retain the two most recent copies, and name them “daily.*timestamp*.” A Snapshot policy can contain up to five job schedules.

### About this task

By default, ONTAP forms the names of Snapshot copies by appending a timestamp to the job schedule name:

```
daily.2017-05-14_0013/          hourly.2017-05-15_1106/
daily.2017-05-15_0012/          hourly.2017-05-15_1206/
hourly.2017-05-15_1006/         hourly.2017-05-15_1306/
```

You can substitute a prefix for the job schedule name if you prefer.

The `snapmirror-label` option is for SnapMirror replication. For more information, see [Defining a rule for a policy](#).

### Step

1. Create a Snapshot policy:

```
volume snapshot policy create -vserver SVM -policy policy_name -enabled
true|false -schedule1 schedule1_name -count1 copies_to_retain -prefix1
snapshot_prefix -snapmirror-label1 snapshot_label ... -schedule1
schedule5_name -count5 copies_to_retain-prefix5 snapshot_prefix -snapmirror
-label5 snapshot_label
```

The following example creates a Snapshot policy named `snap_policy_daily` that runs on a `daily` schedule. The policy has a maximum of five Snapshot copies, each with the name `daily.timestamp` and the SnapMirror label `daily`:

```
cluster1::> volume snapshot policy create -vserver vs0 -policy
snap_policy_daily -schedule1 daily -count1 5 -snapmirror-label1
daily
```

= Manage the Snapshot copy reserve

= Manage the Snapshot copy reserve overview

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

The *Snapshot copy reserve* sets aside a percentage of disk space for Snapshot copies, five percent by default. Because Snapshot copies use space in the active file system when the Snapshot copy reserve is exhausted, you might want to increase the Snapshot copy reserve as needed. Alternatively, you can autodelete Snapshot copies when the reserve is full.

= When to increase the Snapshot copy reserve

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

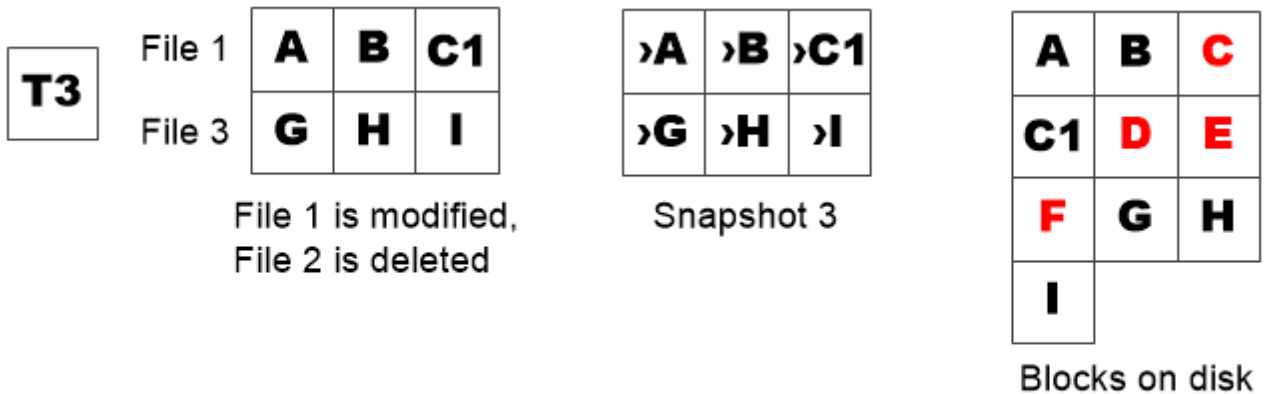
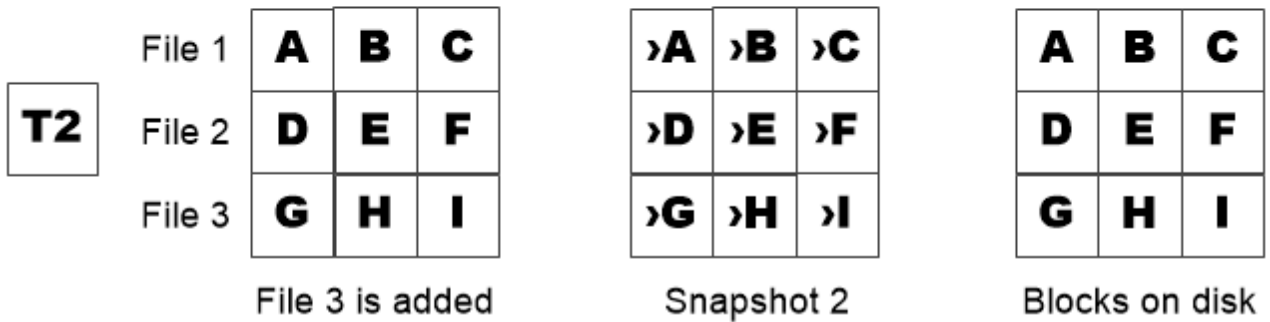
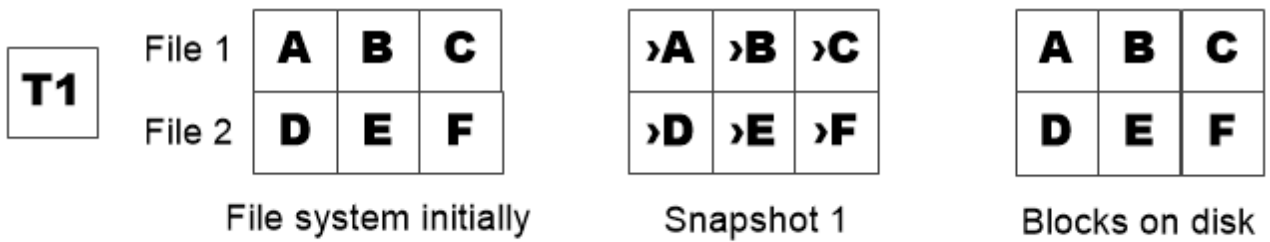
In deciding whether to increase the Snapshot reserve, it's important to remember that a Snapshot copy records only changes to files since the last Snapshot copy was made. It consumes disk space only when blocks in the active file system are modified

or deleted.

This means that the rate of change of the file system is the key factor in determining the amount of disk space used by Snapshot copies. No matter how many Snapshot copies you create, they will not consume disk space if the active file system has not changed.

A FlexVol volume containing database transaction logs, for example, might have a Snapshot copy reserve as large as 20% to account for its greater rate of change. Not only will you want to create more Snapshot copies to capture the more frequent updates to the database, you will also want to have a larger Snapshot copy reserve to handle the additional disk space the Snapshot copies consume.

A Snapshot copy consists of pointers to blocks rather than copies of blocks. You can think of a pointer as a “claim” on a block: ONTAP “holds” the block until the Snapshot copy is deleted.



*A Snapshot copy consumes disk space only when blocks in the active file system are modified or deleted.*

= How deleting protected files can lead to less file space than expected

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

A Snapshot copy points to a block even after you delete the file that used the block. This explains why an exhausted Snapshot copy reserve might lead to the counter-intuitive result in which deleting an entire file system results in less space being available than the file system occupied.

Consider the following example. Before deleting any files, the `df` command output is as follows:

```

Filesystem      kbytes  used  avail  capacity
/vol/vol0/      3000000 3000000 0      100%
/vol/vol0/.snapshot 1000000 500000 500000 50%

```

After deleting the entire file system and making a Snapshot copy of the volume, the `df` command generates the following output:

```

Filesystem      kbytes  used  avail  capacity
/vol/vol0/      3000000 2500000 500000 83%
/vol/vol0/.snapshot 1000000 3500000 0      350%

```

As the output shows, the entire 3 GB formerly used by the active file system is now being used by Snapshot copies, in addition to the 0.5 GB used before the deletion.

Because the disk space used by the Snapshot copies now exceeds the Snapshot copy reserve, the overflow of 2.5 GB “spills” into the space reserved for active files, leaving you with 0.5 GB free space for files where you might reasonably have expected 3 GB.

= Monitor Snapshot copy disk consumption

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can monitor Snapshot copy disk consumption using the `df` command. The command displays the amount of free space in the active file system and the Snapshot copy reserve.

### Step

1. Display Snapshot copy disk consumption: `df`

The following example shows Snapshot copy disk consumption:

```

cluster1::> df
Filesystem      kbytes  used  avail  capacity
/vol/vol0/      3000000 3000000 0      100%
/vol/vol0/.snapshot 1000000 500000 500000 50%

```

= Check available Snapshot copy reserve on a volume

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You might want to check how much Snapshot copy reserve is available on a volume by using the `snapshot-reserve-available` parameter with the `volume show` command.



## Step

1. Check the Snapshot copy reserve available on a volume:

```
vol show -vserver SVM -volume volume -fields snapshot-reserve-available
```

For complete command syntax, see the man page.

The following example displays the available Snapshot copy reserve for `vol1`:

```
cluster1::> vol show -vserver vs0 -volume vol1 -fields snapshot-
reserve-available

vserver volume snapshot-reserve-available
-----
vs0      vol1      4.84GB
```

= Modify the Snapshot copy reserve

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You might want to configure a larger Snapshot copy reserve to prevent Snapshot copies from using space reserved for the active file system. You can decrease the Snapshot copy reserve when you no longer need as much space for Snapshot copies.

## Step

1. Modify the Snapshot copy reserve:

```
volume modify -vserver SVM -volume volume -percent-snapshot-space
snap_reserve
```

For complete command syntax, see the man page.

The following example sets the Snapshot copy reserve for `vol1` to 10 percent:

```
cluster1::> volume modify -vserver vs0 -volume vol1 -percent
-snapshot-space 10
```

= Autodelete Snapshot copies

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the `volume snapshot autodelete modify` command to trigger automatic deletion of Snapshot copies when the Snapshot reserve is exceeded. By

default, the oldest Snapshot copies are deleted first.

### About this task

LUN and file clones are deleted when there are no more Snapshot copies to be deleted.

### Step

1. Autodelete Snapshot copies:

```
volume snapshot autodelete modify -vserver SVM -volume volume -enabled true|false -trigger volume|snap_reserve
```

For complete command syntax, see the man page.

The following example autodeletes Snapshot copies for `vol1` when the Snapshot copy reserve is exhausted:

```
cluster1::> volume snapshot autodelete modify -vserver vs0 -volume vol1 -enabled true -trigger snap_reserve
```

= Restore files from Snapshot copies

= Restore a file from a Snapshot copy on an NFS or SMB client

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

A user on an NFS or SMB client can restore a file directly from a Snapshot copy without the intervention of a storage system administrator.

Every directory in the file system contains a subdirectory named `.snapshot` accessible to NFS and SMB users. The `.snapshot` subdirectory contains subdirectories corresponding to the Snapshot copies of the volume:

```
$ ls .snapshot
daily.2017-05-14_0013/          hourly.2017-05-15_1106/
daily.2017-05-15_0012/        hourly.2017-05-15_1206/
hourly.2017-05-15_1006/       hourly.2017-05-15_1306/
```

Each subdirectory contains the files referenced by the Snapshot copy. If users accidentally delete or overwrite a file, they can restore the file to the parent read-write directory by copying the file from the Snapshot subdirectory to the read-write directory:

```

$ ls my.txt
ls: my.txt: No such file or directory
$ ls .snapshot
daily.2017-05-14_0013/          hourly.2017-05-15_1106/
daily.2017-05-15_0012/          hourly.2017-05-15_1206/
hourly.2017-05-15_1006/        hourly.2017-05-15_1306/
$ ls .snapshot/hourly.2017-05-15_1306/my.txt
my.txt
$ cp .snapshot/hourly.2017-05-15_1306/my.txt .
$ ls my.txt
my.txt

```

= Enable and disable NFS and SMB client access to Snapshot copy directory

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

To determine whether the Snapshot copy directory is visible to NFS and SMB clients to restore a file or LUN from a Snapshot copy, you can enable and disable access to the Snapshot copy directory using the `-snapdir-access` option of the `volume modify` command.

### Steps

1. Check the Snapshot directory access status:

```

`volume show -vserver _SVM_name_ -volume _vol_name_ -fields snapdir-
access`

```

Example:

```

clus1::> volume show -vserver vs0 -volume vol1 -fields snapdir-
access
vserver volume snapdir-access
-----
vs0      vol1    false

```

2. Enable or disable the Snapshot copy directory access:

```

volume modify -volume vol_name -snapdir-access true|false

```

The following example enables Snapshot copy directory access on vol1:

```
clus1::> volume modify -volume voll -snapdir-access true
Volume modify successful on volume voll of Vserver vs0.
```

= Restore a single file from a Snapshot copy

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the `volume snapshot restore-file` command to restore a single file or LUN from a Snapshot copy. You can restore the file to a different location in the parent read-write volume if you do not want to replace an existing file.

### About this task

If you are restoring an existing LUN, a LUN clone is created and backed up in the form of a Snapshot copy. During the restore operation, you can read to and write from the LUN.

Files with streams are restored by default.

### Steps

1. List the Snapshot copies in a volume:

```
volume snapshot show -vserver SVM -volume volume
```

For complete command syntax, see the man page.

The following example shows the Snapshot copies in `voll`:

```
clus1::> volume snapshot show -vserver vs1 -volume voll
```

Vserver	Volume	Snapshot	State	Size	Total%	Used%
vs1	voll	hourly.2013-01-25_0005	valid	224KB	0%	0%
		daily.2013-01-25_0010	valid	92KB	0%	0%
		hourly.2013-01-25_0105	valid	228KB	0%	0%
		hourly.2013-01-25_0205	valid	236KB	0%	0%
		hourly.2013-01-25_0305	valid	244KB	0%	0%
		hourly.2013-01-25_0405	valid	244KB	0%	0%
		hourly.2013-01-25_0505	valid	244KB	0%	0%

7 entries were displayed.

2. Restore a file from a Snapshot copy:

```
volume snapshot restore-file -vserver SVM -volume volume -snapshot snapshot
-path file_path -restore-path destination_path
```

For complete command syntax, see the man page.

The following example restores the file `myfile.txt`:

```
cluster1::> volume snapshot restore-file -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010 -path /myfile.txt
```

= Restore part of a file from a Snapshot copy

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the `volume snapshot partial-restore-file` command to restore a range of data from a Snapshot copy to a LUN or to an NFS or SMB container file, assuming you know the starting byte offset of the data and the byte count. You might use this command to restore one of the databases on a host that stores multiple databases in the same LUN.

### Steps

1. List the Snapshot copies in a volume:

```
volume snapshot show -vserver SVM -volume volume
```

For complete command syntax, see the man page.

The following example shows the Snapshot copies in `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1
```

Vserver	Volume	Snapshot	State	Size	Total%	Used%
vs1	vol1	hourly.2013-01-25_0005	valid	224KB	0%	0%
		daily.2013-01-25_0010	valid	92KB	0%	0%
		hourly.2013-01-25_0105	valid	228KB	0%	0%
		hourly.2013-01-25_0205	valid	236KB	0%	0%
		hourly.2013-01-25_0305	valid	244KB	0%	0%
		hourly.2013-01-25_0405	valid	244KB	0%	0%
		hourly.2013-01-25_0505	valid	244KB	0%	0%

7 entries were displayed.

2. Restore part of a file from a Snapshot copy:

```
volume snapshot partial-restore-file -vserver SVM -volume volume -snapshot
snapshot -path file_path -start-byte starting_byte -byte-count byte_count
```

The starting byte offset and byte count must be multiples of 4,096.

The following example restores the first 4,096 bytes of the file `myfile.txt`:

```
cluster1::> volume snapshot partial-restore-file -vserver vs0
-volume vol1 -snapshot daily.2013-01-25_0010 -path /myfile.txt
-start-byte 0 -byte-count 4096
```

= Restore the contents of a volume from a Snapshot copy

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the `volume snapshot restore` command to restore the contents of a volume from a Snapshot copy.

### About this task

If the volume has SnapMirror relationships, manually replicate all mirror copies of the volume immediately after you restore from a Snapshot copy. Not doing so can result in unusable mirror copies that must be deleted and recreated.

### Steps

1. List the Snapshot copies in a volume:

```
volume snapshot show -vserver SVM -volume volume
```

For complete command syntax, see the man page.

The following example shows the Snapshot copies in `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1
```

Vserver	Volume	Snapshot	State	Size	Total%	Used%
vs1	vol1	hourly.2013-01-25_0005	valid	224KB	0%	0%
		daily.2013-01-25_0010	valid	92KB	0%	0%
		hourly.2013-01-25_0105	valid	228KB	0%	0%
		hourly.2013-01-25_0205	valid	236KB	0%	0%
		hourly.2013-01-25_0305	valid	244KB	0%	0%
		hourly.2013-01-25_0405	valid	244KB	0%	0%
		hourly.2013-01-25_0505	valid	244KB	0%	0%

7 entries were displayed.

2. Restore the contents of a volume from a Snapshot copy:

```
volume snapshot restore -vserver SVM -volume volume -snapshot snapshot
```

For complete command syntax, see the man page.

The following example restores the contents of `vol1`:

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

= SnapMirror volume replication

= About SnapMirror volume replication

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Traditionally, ONTAP replication technologies served the need for disaster recovery (DR) and data archiving. In ONTAP 9.3, these technologies were combined in a way that allows you to configure disaster recovery and archiving on the same destination volume.

= Asynchronous SnapMirror disaster recovery basics

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

*SnapMirror* is disaster recovery technology, designed for failover from primary storage to secondary storage at a geographically remote site. As its name implies, SnapMirror creates a replica, or *mirror*, of your working data in secondary storage from which you can continue to serve data in the event of a catastrophe at the primary site.

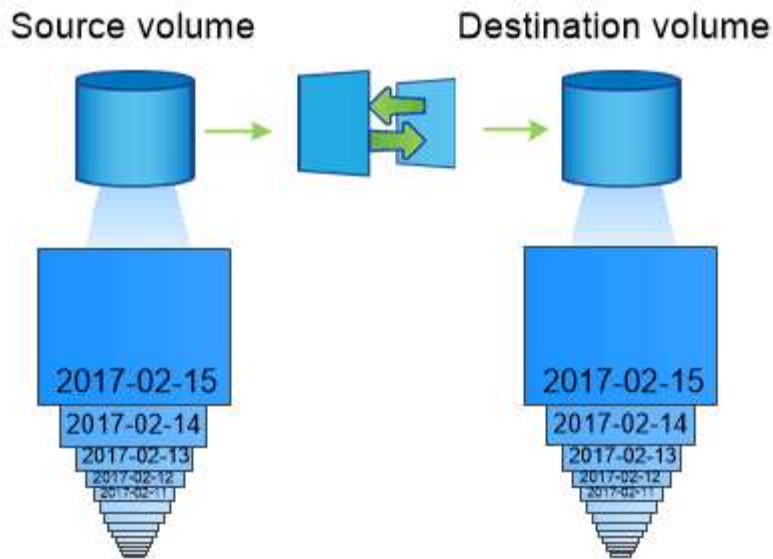
If the primary site is still available to serve data, you can simply transfer any needed data back to it, and not serve clients from the mirror at all. As the failover use case implies, the controllers on the secondary system should be equivalent or nearly equivalent to the controllers on the primary system to serve data efficiently from mirrored storage.

== Data protection relationships

Data is mirrored at the volume level. The relationship between the source volume in primary storage and the destination volume in secondary storage is called a *data protection relationship*. The clusters in which the volumes reside and the SVMs that serve data from the volumes must be *peered*. A peer relationship enables clusters and SVMs to exchange data securely.

### [Cluster and SVM peering](#)

The figure below illustrates SnapMirror data protection relationships.



*A SnapMirror data protection relationship typically mirrors the Snapshot copies available on the source volume.*

== Scope of data protection relationships

You can create a data protection relationship directly between volumes or between the SVMs that own the volumes. In an *SVM data protection relationship*, all or part of the SVM configuration, from NFS exports and SMB shares to RBAC, is replicated, as well as the data in the volumes that the SVM owns.

You can also use SnapMirror for two special data protection applications:

- A *load-sharing mirror* copy of the SVM root volume ensures that data remains accessible in the event of a node outage or failover.
- A data protection relationship between *SnapLock volumes* lets you replicate WORM files to secondary storage.

[Archive and compliance using SnapLock technology](#)

== How SnapMirror data protection relationships are initialized

The first time you invoke SnapMirror, it performs a *baseline transfer* from the source volume to the destination volume. The *SnapMirror policy* for the relationship defines the contents of the baseline and any updates.

A baseline transfer under the default SnapMirror policy `MirrorAllSnapshots` involves the following steps:

- Make a Snapshot copy of the source volume.
- Transfer the Snapshot copy and all the data blocks it references to the destination volume.
- Transfer the remaining, less recent Snapshot copies on the source volume to the destination volume for use in case the “active” mirror is corrupted.

== How SnapMirror data protection relationships are updated

Updates are asynchronous, following the schedule you configure. Retention mirrors the Snapshot policy



on the source.

At each update under the `MirrorAllSnapshots` policy, `SnapMirror` creates a Snapshot copy of the source volume and transfers that Snapshot copy and any Snapshot copies that have been made since the last update. In the following output from the `snapmirror policy show` command for the `MirrorAllSnapshots` policy, note the following:

- `Create Snapshot` is “true”, indicating that `MirrorAllSnapshots` creates a Snapshot copy when `SnapMirror` updates the relationship.
- `MirrorAllSnapshots` has rules “`sm_created`” and “`all_source_snapshots`”, indicating that both the Snapshot copy created by `SnapMirror` and any Snapshot copies that have been made since the last update are transferred when `SnapMirror` updates the relationship.

```
cluster_dst::> snapmirror policy show -policy MirrorAllSnapshots
-instance

                Vserver: vs0
SnapMirror Policy Name: MirrorAllSnapshots
SnapMirror Policy Type: async-mirror
                Policy Owner: cluster-admin
                Tries Limit: 8
                Transfer Priority: normal
Ignore accesstime Enabled: false
                Transfer Restartability: always
Network Compression Enabled: false
                Create Snapshot: true
                Comment: Asynchronous SnapMirror policy for
mirroring all snapshots
                                and the latest active file system.
                Total Number of Rules: 2
                Total Keep: 2
                Rules: SnapMirror Label      Keep  Preserve Warn
Schedule Prefix
-----
-----
                                sm_created          1  false    0
- - - - -
                                all_source_snapshots  1  false    0
- - - - -
```

**== MirrorLatest policy**

The preconfigured `MirrorLatest` policy works exactly the same way as `MirrorAllSnapshots`, except that only the Snapshot copy created by `SnapMirror` is transferred at initialization and update.

```

Rules: SnapMirror Label      Keep  Preserve Warn
Schedule Prefix
-----
sm_created                  1    false    0
-

```

= SnapMirror Synchronous disaster recovery basics

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

:hardbreaks-option:

Beginning with ONTAP 9.5, SnapMirror Synchronous (SM-S) technology is supported on all FAS and AFF platforms that have at least 16 GB of memory and on all ONTAP Select platforms. SnapMirror Synchronous technology is a per-node, licensed feature that provides synchronous data replication at the volume level.

This functionality addresses the regulatory and national mandates for synchronous replication in financial, healthcare, and other regulated industries where zero data loss is required.

The limit on the number of SnapMirror Synchronous replication operations per HA pair depends on the controller model.

The following table lists the number of SnapMirror Synchronous operations that are allowed per HA pair according to platform type and ONTAP release.

Platform	Releases earlier than ONTAP 9.9.1	ONTAP 9.9.1	ONTAP 9.10.1	ONTAP 9.11.1
AFF	80	160	200	400
FAS	40	80	80	80
ONTAP Select	20	40	40	40

== Supported features

The following features are supported for SnapMirror Synchronous technology in ONTAP 9.10.1; provided all nodes in the source and destination cluster are running ONTAP 9.10.1:

- NFSv4.2
- NVMe/TCP

In ONTAP 9.5 and later, SnapMirror Synchronous technology supports the NFSv3, FC, and iSCSI protocols over all networks for which the latency does not exceed 10ms.

The following features are supported for SnapMirror Synchronous technology in ONTAP 9.7:

- Replication of application-created Snapshot copies  
If a Snapshot copy is tagged with the appropriate label at the time of the `snapshot create` operation, using the CLI or the ONTAP API, SnapMirror Synchronous replicates the Snapshot copies, both user created or those created with external scripts, after quiescing the applications. Scheduled Snapshot copies created using a Snapshot policy are not replicated. For more information about replicating application-created Snapshot copies, see the Knowledge Base article: [How to replicate application created snapshots with SnapMirror Synchronous](#).
- FC-NVMe
- LUN clones and NVMe namespace clones  
LUN clones backed by application-created Snapshot copies are also supported.

The following features are supported for SnapMirror Synchronous technology in ONTAP 9.6; provided all nodes in the source and destination cluster are running ONTAP 9.6:

- SVM DR
  - A SnapMirror Synchronous source can also be a SVM DR source, for example, a fan-out configuration with SM-S as one leg and SVM DR as the other.
  - A SnapMirror Synchronous source cannot be an SVM DR destination because SM-S does not support cascading a DP source.  
You must release the synchronous relationship before performing an SVM DR flip resync in the destination cluster.
  - A SnapMirror Synchronous destination cannot be an SVM DR source because SVM DR does not support replication of DP volumes.  
A flip resync of the synchronous source would result in the SVM DR excluding the DP volume in the destination cluster.
- NFSv4.0 and NFSv4.1
- SMB 2.0 or later
- Mixed protocol access (NFSv3 and SMB)
- Antivirus on the primary volume of the SnapMirror Synchronous relationship
- Hard or soft quotas on the primary volume of the SnapMirror Synchronous relationship  
The quota rules are not replicated to the destination; therefore, the quota database is not replicated to the destination.
- FPolicy on the primary volume of the SnapMirror Synchronous relationship
- SnapMirror Synchronous mirror-mirror cascade  
The relationship from the destination volume of the SnapMirror Synchronous relationship must be an asynchronous SnapMirror relationship.
- Timestamp parity between source and destination volumes for NAS  
If you have upgraded from ONTAP 9.5 to ONTAP 9.6, the timestamp is replicated only for any new and modified files in the source volume. The timestamp of existing files in the source volume is not synchronized.
- Removal of high metadata operation frequency limitation
- Security for sensitive data in-transit using TLS 1.2 encryption
- Clone autodelete

== Unsupported features

The following features are not supported with Synchronous SnapMirror relationships:

- MetroCluster configurations
- SFMoD
- SFCoD
- VVol
- Mixed SAN and NAS access  
The primary volume of a SnapMirror Synchronous relationship can either serve NAS data or SAN data. Both SAN and NAS access from the primary volume of a SnapMirror Synchronous relationship is not supported.
- Mixed SAN and NVMe access  
LUNs and NVMe namespaces are not supported on the same volume or SVM.
- SnapLock volumes
- FlexGroup volumes
- FlexCache volumes
- SnapRestore
- DP\_Optimized (DPO) systems
- Tape backup or restore using dump and SMTape on the destination volume
- Tape based restore to the source volume
- Throughput floor (QoS Min) for source volumes
- In a fan-out configuration, only one relationship can be a SnapMirror Synchronous relationship; all the other relationships from the source volume must be asynchronous SnapMirror relationships.
- Global throttling

== Modes of operation

SnapMirror Synchronous has two modes of operation based on the type of the SnapMirror policy used:

- **Sync mode**

In Sync mode, application I/O operations are sent in parallel to the primary and secondary storage systems. If the write to the secondary storage is not completed for any reason, the application is allowed to continue writing to the primary storage. When the error condition is corrected, SnapMirror Synchronous technology automatically resynchronizes with the secondary storage and resumes replicating from primary storage to secondary storage in Synchronous mode.

In Sync mode, RPO=0 and RTO is very low until a secondary replication failure occurs at which time RPO and RTO become indeterminate, but equal the time to repair the issue that caused secondary replication to fail and for the resync to complete.

- **StrictSync mode**

SnapMirror Synchronous can optionally operate in StrictSync mode. If the write to the secondary storage is not completed for any reason, the application I/O fails, thereby ensuring that the primary and secondary storage are identical. Application I/O to the primary resumes only after the SnapMirror relationship returns to the `InSync` status. If the primary storage fails, application I/O can be resumed on the secondary storage, after failover, with no loss of data.

In StrictSync mode RPO is always zero, and RTO is very low.

== Relationship status

The status of a SnapMirror Synchronous relationship is always in the `InSync` status during normal operation. If the SnapMirror transfer fails for any reason, the destination is not in sync with the source and

can go to the `OutOfSync` status.

For SnapMirror Synchronous relationships, the system automatically checks the relationship status (`InSync` or `OutOfSync`) at a fixed interval. If the relationship status is `OutOfSync`, ONTAP automatically triggers the auto resync process to bring back the relationship to the `InSync` status. Auto resync is triggered only if the transfer fails due to any operation, such as unplanned storage failover at source or destination or a network outage. User-initiated operations such as `snapmirror quiesce` and `snapmirror break` do not trigger auto resync.

If the relationship status becomes `OutOfSync` for a SnapMirror Synchronous relationship in the `StrictSync` mode, all I/O operations to the primary volume are stopped. The `OutOfSync` state for SnapMirror Synchronous relationship in the `Sync` mode is not disruptive to the primary and I/O operations are allowed on the primary volume.

#### Related information

[NetApp Technical Report 4733: SnapMirror Synchronous for ONTAP 9.11.1](#)

= About workloads supported by `StrictSync` and `Sync` policies

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

`StrictSync` and `Sync` policies support all LUN-based applications with FC, iSCSI, and FC-NVMe protocols, as well as NFSv3 and NFSv4 protocols for enterprise applications such as databases, VMWare, quota, SMB, and so on. Beginning with ONTAP 9.6, SnapMirror Synchronous can be used for enterprise file services such as electronic design automation (EDA), home directories, and software build workloads.

In ONTAP 9.5, for a `Sync` policy, you need to consider a few important aspects while selecting the NFSv3 or NFSv4 workloads. The amount of data read or write operations by workloads is not a consideration, as `Sync` policy can handle high read or write IO workloads. In ONTAP 9.5, workloads that have excessive file creation, directory creation, file permission changes, or directory permission changes may not be suitable (these are referred to as high-metadata workloads). A typical example of a high-metadata workload is a DevOps workload in which you create multiple test files, run automation, and delete the files. Another example is parallel build workload that generate multiple temporary files during compilation. The impact of a high rate of write metadata activity is that it can cause synchronization between mirrors to temporarily break which stalls the read and write IOs from the client.

Beginning with ONTAP 9.6, these limitations are removed and SnapMirror Synchronous can be used for enterprise file services workloads that include multiuser environments, such as home directories and software build workloads.

#### Related information

[SnapMirror Synchronous Configuration and Best Practices](#)

= Vault archiving using SnapMirror technology

:icons: font

:relative\_path: ./data-protection/

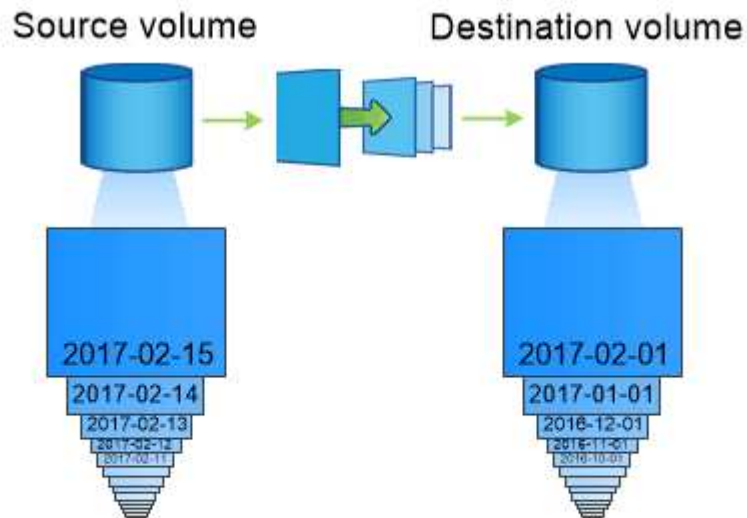
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

SnapMirror vault policies replace SnapVault technology in ONTAP 9.3 and later. You use a SnapMirror vault policy for disk-to-disk Snapshot copy replication for standards

compliance and other governance-related purposes. In contrast to a SnapMirror relationship, in which the destination usually contains only the Snapshot copies currently in the source volume, a vault destination typically retains point-in-time Snapshot copies created over a much longer period.

You might want to keep monthly Snapshot copies of your data over a 20-year span, for example, to comply with government accounting regulations for your business. Since there is no requirement to serve data from vault storage, you can use slower, less expensive disks on the destination system.

The figure below illustrates SnapMirror vault data protection relationships.



*A SnapVault data protection relationship typically retains point-in-time Snapshot copies created over a longer period than the Snapshot copies on the source volume.*

== How vault data protection relationships are initialized

The SnapMirror policy for the relationship defines the contents of the baseline and any updates.

A baseline transfer under the default vault policy `XDPDefault` makes a Snapshot copy of the source volume, then transfers that copy and the data blocks it references to the destination volume. Unlike SnapMirror relationships, a vault backup does not include older Snapshot copies in the baseline.

== How vault data protection relationships are updated

Updates are asynchronous, following the schedule you configure. The rules you define in the policy for the relationship identify which new Snapshot copies to include in updates and how many copies to retain. The labels defined in the policy (“monthly,” for example) must match one or more labels defined in the Snapshot policy on the source. Otherwise, replication fails.

At each update under the `XDPDefault` policy, SnapMirror transfers Snapshot copies that have been made since the last update, provided they have labels matching the labels defined in the policy rules. In the following output from the `snapmirror policy show` command for the `XDPDefault` policy, note the following:

- `Create Snapshot` is “false”, indicating that `XDPDefault` does not create a Snapshot copy when SnapMirror updates the relationship.

- XDPDefault has rules “daily” and “weekly”, indicating that all Snapshot copies with matching labels on the source are transferred when SnapMirror updates the relationship.

```
cluster_dst::> snapmirror policy show -policy XDPDefault -instance
                    Vserver: vs0
SnapMirror Policy Name: XDPDefault
SnapMirror Policy Type: vault
                    Policy Owner: cluster-admin
                    Tries Limit: 8
                    Transfer Priority: normal
Ignore accesstime Enabled: false
                    Transfer Restartability: always
Network Compression Enabled: false
                    Create Snapshot: false
                    Comment: Default policy for XDP relationships with
daily and weekly
                    rules.
                    Total Number of Rules: 2
                    Total Keep: 59
                    Rules: SnapMirror Label      Keep  Preserve Warn
Schedule Prefix
-----
-----
                    daily          7  false    0
-      -
                    weekly        52  false    0
-      -
```

= SnapMirror unified replication basics

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

SnapMirror *unified replication* allows you to configure disaster recovery and archiving on the same destination volume. When unified replication is appropriate, it offers benefits in reducing the amount of secondary storage you need, limiting the number of baseline transfers, and decreasing network traffic.

== How unified data protection relationships are initialized

As with SnapMirror, unified data protection performs a baseline transfer the first time you invoke it. The SnapMirror policy for the relationship defines the contents of the baseline and any updates.

A baseline transfer under the default unified data protection policy `MirrorAndVault` makes a Snapshot copy of the source volume, then transfers that copy and the data blocks it references to the destination volume. Like vault archiving, unified data protection does not include older Snapshot copies in the

baseline.

== How unified data protection relationships are updated

At each update under the `MirrorAndVault` policy, `SnapMirror` creates a Snapshot copy of the source volume and transfers that Snapshot copy and any Snapshot copies that have been made since the last update, provided they have labels matching the labels defined in the Snapshot policy rules. In the following output from the `snapmirror policy show` command for the `MirrorAndVault` policy, note the following:

- `Create Snapshot` is “true”, indicating that `MirrorAndVault` creates a Snapshot copy when `SnapMirror` updates the relationship.
- `MirrorAndVault` has rules “sm\_created”, “daily”, and “weekly”, indicating that both the Snapshot copy created by `SnapMirror` and the Snapshot copies with matching labels on the source are transferred when `SnapMirror` updates the relationship.

```
cluster_dst::> snapmirror policy show -policy MirrorAndVault -instance
                                Vserver: vs0
SnapMirror Policy Name: MirrorAndVault
SnapMirror Policy Type: mirror-vault
Policy Owner: cluster-admin
Tries Limit: 8
Transfer Priority: normal
Ignore accesstime Enabled: false
Transfer Restartability: always
Network Compression Enabled: false
Create Snapshot: true
Comment: A unified Synchronous SnapMirror and
SnapVault policy for
                                mirroring the latest file system and
daily and weekly snapshots.
Total Number of Rules: 3
Total Keep: 59
Rules: SnapMirror Label      Keep  Preserve Warn
Schedule Prefix
-----
sm_created                   1  false    0
daily                         7  false    0
weekly                       52  false    0
```

== Unified7year policy



The preconfigured `Unified7year` policy works exactly the same way as `MirrorAndVault`, except that a fourth rule transfers monthly Snapshot copies and retains them for seven years.

Schedule	Prefix	Rules: SnapMirror Label	Keep	Preserve	Warn
-----	-----	-----	----	-----	----
-	-	sm_created	1	false	0
-	-	daily	7	false	0
-	-	weekly	52	false	0
-	-	monthly	84	false	0
-	-				

== Protect against possible data corruption

Unified replication limits the contents of the baseline transfer to the Snapshot copy created by SnapMirror at initialization. At each update, SnapMirror creates another Snapshot copy of the source and transfers that Snapshot copy and any new Snapshot copies that have labels matching the labels defined in the Snapshot policy rules.

You can protect against the possibility that an updated Snapshot copy is corrupted by creating a copy of the last transferred Snapshot copy on the destination. This “local copy” is retained regardless of the retention rules on the source, so that even if the Snapshot originally transferred by SnapMirror is no longer available on the source, a copy of it will be available on the destination.

== When to use unified data replication

You need to weigh the benefit of maintaining a full mirror against the advantages that unified replication offers in reducing the amount of secondary storage, limiting the number of baseline transfers, and decreasing network traffic.

The key factor in determining the appropriateness of unified replication is the rate of change of the active file system. A traditional mirror might be better suited to a volume holding hourly Snapshot copies of database transaction logs, for example.

= XDP replaces DP as the SnapMirror default

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.3, SnapMirror extended data protection (XDP) mode replaces SnapMirror data protection (DP) mode as the SnapMirror default.

Until ONTAP 9.3, SnapMirror invoked in DP mode and SnapMirror invoked in XDP mode used different replication engines, with different approaches to version-dependence:

- SnapMirror invoked in DP mode used a *version-dependent* replication engine in which the ONTAP version was required to be the same on primary and secondary storage:

```
cluster_dst::> snapmirror create -type DP -source-path ...
-destination-path ...
```

- SnapMirror invoked in XDP mode used a *version-flexible* replication engine that supported different ONTAP versions on primary and secondary storage:

```
cluster_dst::> snapmirror create -type XDP -source-path ...
-destination-path ...
```

With improvements in performance, the significant benefits of version-flexible SnapMirror outweigh the slight advantage in replication throughput obtained with version-dependent mode. For this reason, beginning with ONTAP 9.3, XDP mode has been made the new default, and any invocations of DP mode on the command line or in new or existing scripts are automatically converted to XDP mode.

Existing relationships are not affected. If a relationship is already of type DP, it will continue to be of type DP. Beginning with ONTAP 9.5, MirrorAndVault is the new default policy when no data protection mode is specified or when XDP mode is specified as the relationship type. The table below shows the behavior you can expect.

If you specify...	The type is...	The default policy (if you do not specify a policy) is...
DP	XDP	MirrorAllSnapshots (SnapMirror DR)
Nothing	XDP	MirrorAndVault (unified replication)
XDP	XDP	MirrorAndVault (unified replication)

As the table shows, the default policies assigned to XDP in different circumstances ensure that the conversion maintains the functional equivalence of the old types. Of course, you can use different policies as needed, including policies for unified replication:

If you specify...	And the policy is...	The result is...
DP	MirrorAllSnapshots	SnapMirror DR
	XDPDefault	SnapVault
	MirrorAndVault	Unified replication

XDP	MirrorAllSnapshots	SnapMirror DR
	XDPDefault	SnapVault
	MirrorAndVault	Unified replication

The only exceptions to conversion are as follows:

- SVM data protection relationships continue to default to DP mode in ONTAP 9.3 and earlier.

Beginning with ONTAP 9.4, SVM data protection relationships default to XDP mode.

- Root volume load-sharing data protection relationships continue to default to DP mode.
- SnapLock data protection relationships continue to default to DP mode in ONTAP 9.4 and earlier.

Beginning with ONTAP 9.5, SnapLock data protection relationships default to XDP mode.

- Explicit invocations of DP continue to default to DP mode if you set the following cluster-wide option:

```
options replication.create_data_protection_rels.enable on
```

This option is ignored if you do not explicitly invoke DP.

= When a destination volume grows automatically

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

During a data protection mirror transfer, the destination volume grows automatically in size if the source volume has grown, provided there is available space in the aggregate that contains the volume.

This behavior occurs irrespective of any automatic growth setting on the destination. You cannot limit the volume's growth or prevent ONTAP from growing it.

By default, data protection volumes are set to the `grow_shrink` autosize mode, which enables the volume to grow or shrink in response to the amount of used space. The max-autosize for data protection volumes is equal to the maximum FlexVol size and is platform dependent. For example:

- FAS2220, default DP volume max-autosize = 60TB
- FAS6220, default DP volume max-autosize = 70TB
- FAS8200, default DP volume max-autosize = 100TB

For more information, see [NetApp Hardware Universe](#).

= Fan-out and cascade data protection deployments

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use a *fan-out* deployment to extend data protection to multiple secondary systems. You can use a *cascade* deployment to extend data protection to tertiary systems.

Both fan-out and cascade deployments support any combination of SnapMirror DR, SnapVault, or unified replication; however, SnapMirror Synchronous relationships (supported beginning with ONTAP 9.5) support only fan-out deployments with one or more asynchronous SnapMirror relationships and do not support cascade deployments. Only one relationship in the fan-out configuration can be a SnapMirror Synchronous relationship, all the other relationships from the source volume must be asynchronous SnapMirror relationships. [SnapMirror Business Continuity](#) (supported beginning with ONTAP 9.8) also supports fan-out configurations.

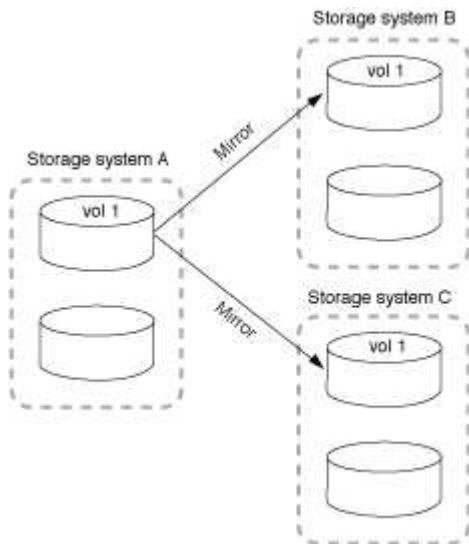
You can use a *fan-in* deployment to create data protection relationships between multiple primary systems and a single secondary system. Each relationship must use a different volume on the secondary system.

You should be aware that volumes that are part of a fan-out or cascade configuration can take longer to resynchronize. It is not uncommon to see the SnapMirror relationship reporting the status "preparing" for an extended time period.

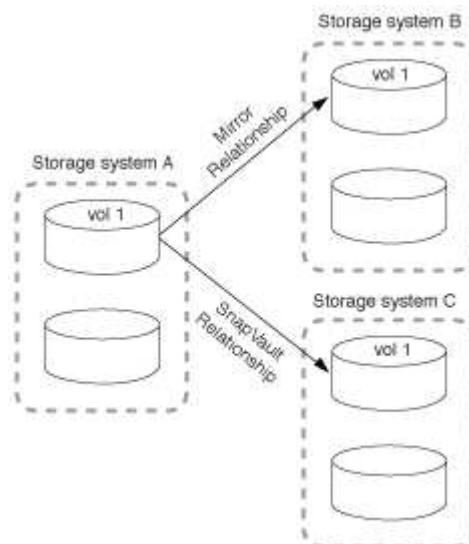
== How fan-out deployments work

SnapMirror supports *multiple-mirrors* and *mirror-vault* fan-out deployments.

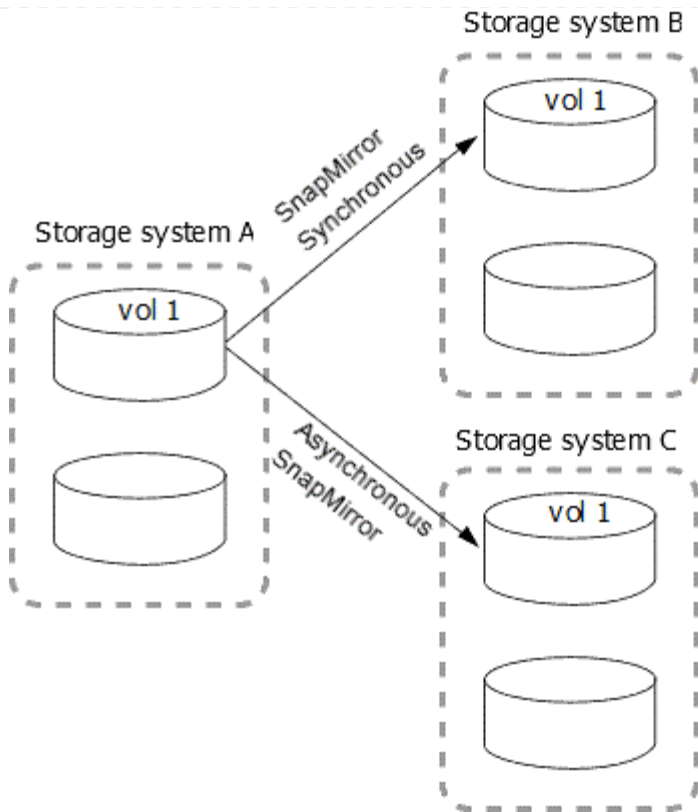
A multiple-mirrors fan-out deployment consists of a source volume that has a mirror relationship to multiple secondary volumes.



A mirror-vault fan-out deployment consists of a source volume that has a mirror relationship to a secondary volume and a SnapVault relationship to a different secondary volume.



Beginning with ONTAP 9.5, you can have fan-out deployments with SnapMirror Synchronous relationships; however, only one relationship in the fan-out configuration can be a SnapMirror Synchronous relationship, all the other relationships from the source volume must be asynchronous SnapMirror relationships.

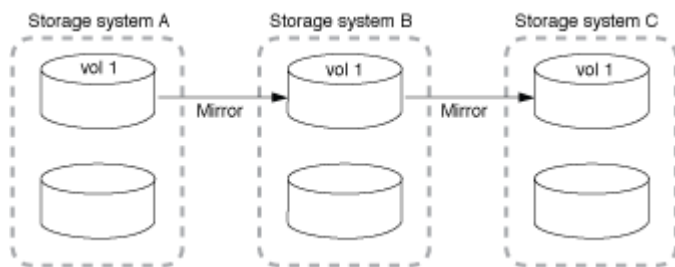


== How cascade deployments work

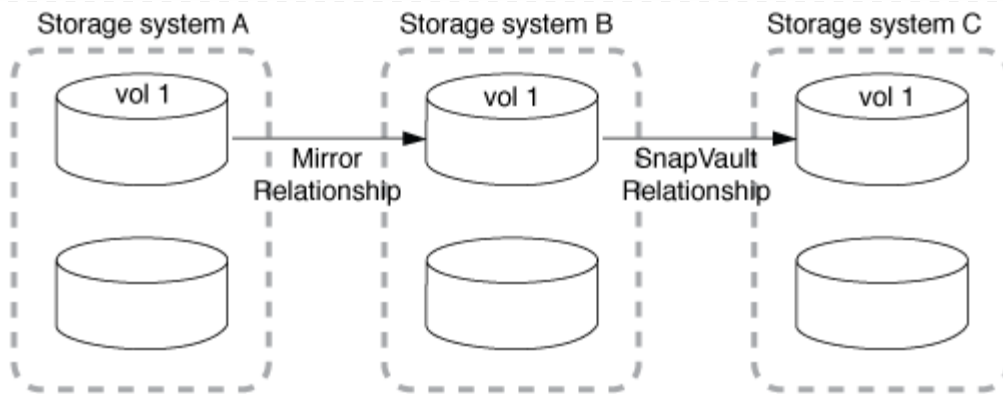
SnapMirror supports *mirror-mirror*, *mirror-vault*, *vault-mirror*, and *vault-vault* cascade deployments.

A mirror-mirror cascade deployment consists of a chain of relationships in which a source volume is mirrored to a secondary volume, and the secondary volume is mirrored to a tertiary volume. If the secondary volume becomes unavailable, you can synchronize the relationship between the primary and tertiary volumes without performing a new baseline transfer.

Beginning with ONTAP 9.6, SnapMirror Synchronous relationships are supported in a mirror-mirror cascade deployment. Only the primary and secondary volumes can be in a SnapMirror Synchronous relationship. The relationship between the secondary volumes and tertiary volumes must be asynchronous.



A mirror-vault cascade deployment consists of a chain of relationships in which a source volume is mirrored to a secondary volume, and the secondary volume is vaulted to a tertiary volume.



Vault-mirror and, beginning with ONTAP 9.2, vault-vault cascade deployments are also supported:

- A vault-mirror cascade deployment consists of a chain of relationships in which a source volume is vaulted to a secondary volume, and the secondary volume is mirrored to a tertiary volume.
- (Beginning with ONTAP 9.2) A vault-vault cascade deployment consists of a chain of relationships in which a source volume is vaulted to a secondary volume, and the secondary volume is vaulted to a tertiary volume.

#### Further Reading

- [Resume protection in a fan-out configuration with SM-BC](#)

= SnapMirror licensing

= SnapMirror licensing overview

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.3, licensing has been simplified for replicating between ONTAP instances. In ONTAP 9 releases, the SnapMirror license supports both vault and mirror relationships. Users can now purchase a SnapMirror license to support ONTAP replication for both backup and disaster recovery use cases.

Prior to the ONTAP 9.3 release, two licenses were available to support different replication use cases. A SnapVault license was needed to configure *vault* relationships between ONTAP instances, where the DP instance could retain a higher number of Snapshot copies to support backup use cases where retention times are longer. A SnapMirror license was needed to configure *mirror* relationships between ONTAP instances, where each ONTAP instance would maintain the same number of snapshot copies (that is, a *mirror* image) to support disaster recovery use cases where cluster failovers would be possible. Both SnapMirror and SnapVault licenses can continue to be used and supported for ONTAP 8.x and 9.x releases.

SnapVault licenses continue to function and are supported for both ONTAP 8.x and 9.x releases, but they are no longer being sold. The SnapMirror license continues to be available and can be used in place of SnapVault and can be used for both mirror and vault configurations.

For ONTAP asynchronous replication, beginning with ONTAP 9.3 a single unified replication engine is used to configure extended data protection mode (XDP) policies, where the SnapMirror license can be configured for a mirror policy, a vault policy, or a mirror-vault policy. A SnapMirror license is required on both the source and destination clusters. A SnapVault license is not required if a SnapMirror license is

already installed. The SnapMirror asynchronous perpetual license is included in the Data Protection bundle which you can purchase for your ONTAP clusters. The Data Protection bundle price is based on the raw capacity of the cluster.

Data protection configuration limits are determined using several factors, including your ONTAP version, hardware platform, and the licenses installed. For more information, see [Hardware Universe](#).

#### == SnapMirror Synchronous license

Beginning with ONTAP 9.5, SnapMirror Synchronous relationships are supported. You require the following licenses for creating a SnapMirror Synchronous relationship:

- The SnapMirror Synchronous license is required on both the source cluster and the destination cluster.

The SnapMirror Synchronous license is enabled with either the Premium bundle or the Data Protection bundle.

If your system was purchased before June 2019 with a Premium or Flash Bundle, you can download a NetApp master key to get the required SnapMirror Synchronous license from the NetApp Support Site: [Master License Keys](#)

- The SnapMirror license is required on both the source cluster and the destination cluster.

#### == SnapMirror Cloud license

Beginning with ONTAP 9.8, the SnapMirror Cloud license provides asynchronous replication of Snapshot copies from ONTAP instances to object storage endpoints. Replication targets can be configured using both on-premises object stores as well as S3 and S3-compatible public cloud object storage services. SnapMirror Cloud relationships are supported from ONTAP systems to pre-qualified object storage targets. ONTAP 9.8 approved object storage targets include ONTAP S3, StorageGRID, AWS S3 Standard, S3 Standard-IA, and S3 One Zone-IA, Microsoft Azure Blob Premium, Hot and Cool, and GCP Standard and Nearline storage.

SnapMirror Cloud is not available as a standalone license and is available only with purchase of the Hybrid Cloud Bundle. Hybrid Cloud Bundle is a term-based subscription license that is priced based on capacity. Only one license is needed per ONTAP cluster. Capacity is defined as the “used” capacity (not raw capacity) within any volume which is protected by SnapMirror Cloud. Users will purchase this license based on the total used capacity of volumes on the cluster being backed up by SnapMirror Cloud. As of October 2021, the Hybrid Cloud Bundle includes only a SnapMirror Cloud license (previously Hybrid Cloud Bundle included a FabricPool license, which was removed from the bundle effective October 2021). In addition to SnapMirror Cloud, the async SnapMirror license is also required and is available only with the purchase of the Data Protection Bundle.

You require the following licenses for creating a SnapMirror Cloud relationship:

- Both a SnapMirror license (purchased through Data Protection Bundle, or through Premium Bundle) and a SnapMirror Cloud license (purchased through Hybrid Cloud Bundle) are needed for replicating directly to the object store endpoint.
- When configuring a multi-policy replication workflow (for example, Disk-to-Disk-to-Cloud), a SnapMirror license is required on all ONTAP instances, while the SnapMirror Cloud license is only required for the source cluster which is replicating directly to the object storage endpoint.

SnapMirror Cloud is an end user license which can be purchased from NetApp or from an approved NetApp reseller partner. The SnapMirror Cloud license provides end user entitlement but does not enable



asynchronous ONTAP to object storage replication. To invoke ONTAP APIs for SnapMirror Cloud, a unique API key from an authorized application is required. Authorized and licensed applications used to orchestrate SnapMirror Cloud replication include System Manager, and are also available from multiple third-party application providers. These authorized applications will embed the unique API key to invoke ONTAP APIs. A combination of the SnapMirror Cloud end user license and an authorized third-party backup application is required to orchestrate and enable SnapMirror Cloud replication.

Beginning with ONTAP 9.9.1, you can use System Manager for SnapMirror Cloud replication. For more information, see [Back up to the cloud](#).

A list of authorized SnapMirror Cloud third-party applications is published on the NetApp web site.

#### == Data Protection Optimized (DPO)

Beginning with ONTAP 9.1, new ONTAP data protection features were packaged with the FAS8200 as part of a solution called the Data Protection Bundle. This new hardware and software bundle included a new DP\_Optimized (DPO) license that provided unique ONTAP features for secondary workloads. With the introduction of ONTAP 9.3 the DPO license increased the number of volumes per node from 1,000 to 1,500. Also introduced with ONTAP 9.3 were new configurations of the Data Protection Bundle based on configurations of FAS2620.

The DPO license was specifically designed for ONTAP clusters that were to be dedicated as secondary targets for SnapMirror replication. In addition to increasing the maximum volumes per node on the DPO controller, the DPO license also modified controller QoS settings to support greater replication traffic at the expense of application I/O. For this reason, the DPO license should never be installed on a cluster that supports application I/O, as application performance would be impacted. Later, Data Protection Bundles based on the FAS8200 and FAS2620 were offered as a solution and included programmatic free licenses based on the customer environment. When purchasing the solution bundles, free SnapMirror licenses would be provided for select older clusters which replicated to the DPO secondary. While the DPO license is needed on the Data Protection solution cluster, primary clusters from the following platform list would be provided free SnapMirror licenses. Primary clusters not included in this list would require purchase of SnapMirror licenses. The DPO hardware and software bundle was based on both FAS2620 and FAS8200 systems which are both EOA status and no are longer available.

- FAS2200 Series
- FAS3000 Series
- FAS6000 Series
- FAS8000 Series

#### == Data Protection Optimized (DPO) License

Data Protection hardware and software solution bundles introduced with ONTAP 9.1 and 9.3 were based on FAS8200 and FAS2620 only. As these platforms matured and new platforms were introduced new requests to support ONTAP features for secondary replication use cases increased. As a result, a new standalone DPO license was introduced in November 2018 with the ONTAP 9.5 release.

The standalone DPO license was supported on both FAS and AFF platforms and could be purchased pre-configured with new clusters or added to deployed clusters as a software upgrade in the field. Because these new DPO licenses were not part of a hardware and software solution bundle, they carried a lower price, and free SnapMirror licenses for primary clusters were not provided. Secondary clusters configured with the a la carte DPO license must also purchase a SnapMirror license, and all primary clusters replicating to the DPO secondary cluster must purchase a SnapMirror license.

Additional ONTAP features were delivered with the DPO across multiple ONTAP releases.

Feature	9.3	9.4	9.5	9.6	9.7+
Max vols/node	1500	1500	1500	1500/2500	1500/2500
Max concurrent repl sessions	100	200	200	200	200
Workload bias*	client apps	Apps/SM	SnapMirror	SnapMirror	SnapMirror
Cross volume aggregate deduplication for HDD	No	Yes	Yes	Yes	Yes

- Details about priority for the SnapMirror backoff (workload bias) feature:
- Client: cluster I/O priority is set to client workloads (production apps), not SnapMirror traffic.
- Equality: SnapMirror replication requests have equal priority to I/O for production apps.
- SnapMirror: all SnapMirror I/O requests have higher priority than I/O for production apps.

**Table 1: Max FlexVolumes per node across ONTAP releases**

	9.3—9.5 Without DPO	9.3—9.5 With DPO	9.6 Without DPO	9.6 With DPO	9.7—9.9.1 Without DPO	9.7—9.9.1 With DPO
FAS2620	1000	1500	1000	1500	1000	1500
FAS2650	1000	1500	1000	1500	1000	1500
FAS2720	1000	1500	1000	1500	1000	1500
FAS2750	1000	1500	1000	1500	1000	1500
A200	1000	1500	1000	1500	1000	1500
A220	1000	1500	1000	1500	1000	1500
FAS8200/8300	1000	1500	1000	2500	1000	2500
A300	1000	1500	1000	2500	2500	2500
A400	1000	1500	1000	2500	2500	2500
FAS8700/9000	1000	1500	1000	2500	1000	2500

A700	1000	1500	1000	2500	2500	2500
A700s	1000	1500	1000	2500	2500	2500
A800	1000	1500	1000	2500	2500	2500

For the latest maximum FlexVol volume support for your configuration, see [Hardware Universe](#).

== Considerations for all new DPO installations

- After it is enabled, the DPO license feature cannot be disabled or undone.
- Installation of the DPO license requires a re-boot of ONTAP or failover to enable.
- The DPO solution is intended for secondary storage workloads; application workload performance on DPO clusters may be impacted
- The DPO license is supported on a select list of NetApp storage platform models.
- DPO features vary by ONTAP release. Refer to the compatibility table for reference.
- New FAS and AFF systems are not qualified with DPO. DPO licenses cannot be purchased for clusters not listed above.

= Install a SnapMirror Cloud license

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.8, SnapMirror Cloud provides asynchronous snapshot replication from ONTAP to object storage endpoints. SnapMirror Cloud relationships can only be configured using pre-qualified third-party backup applications. To configure ONTAP to object storage replication, both SnapMirror and SnapMirror Cloud licenses are required on the ONTAP source cluster configured for replication to the object store endpoint.

#### About this task

The SnapMirror Cloud license is a single-instance cluster-wide license, which means it does not need to be installed on every node in the cluster. It is a term-based license where both term and backup capacity are enforced. In addition to this end user license, SnapMirror Cloud requires an authorized and approved backup application to configure and invoke ONTAP APIs for replication. Both SnapMirror Cloud end user license and authorized app are necessary to utilize SnapMirror Cloud replication.

SnapMirror Cloud licenses are acquired through purchase of the Hybrid Cloud Bundle, which can be purchased with 1 or 3 year terms in 1 TB increments. The Hybrid Cloud Bundle includes a license for SnapMirror Cloud. Each license has a unique serial number. Purchases of the Hybrid Cloud Bundle are based on capacity, where the purchased capacity of the Hybrid Cloud Bundle is applied to the SnapMirror Cloud license.

The SnapMirror Cloud license can be installed on the cluster using the ONTAP command line or System Manager.

#### Steps

1. Download two NetApp License File (NLF) for SnapMirror Cloud from the NetApp Support Site.

[NetApp Support](#)

2. Use System Manager to upload the SnapMirror Cloud NLF file to the cluster:
  - a. Click **Configuration > Licenses**.
  - b. In the **Cluster Settings** pane, click **Licenses**.
  - c. In the **Packages** window, click **Add**.
  - d. In the **Add License Packages** dialog box, click **Choose Files** to select the NLF you downloaded, and then click **Add** to upload the file to the cluster.

#### Related information

[NetApp Software License Search](#)

= DPO systems feature enhancements

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.6, the maximum number of FlexVol volumes supported increases when the DP\_Optimized (DPO) license is installed. Beginning with ONTAP 9.4, systems with the DPO license support SnapMirror backoff, cross-volume background deduplication, cross-volume inline deduplication, use of Snapshot blocks as donors, and compaction.

Beginning with ONTAP 9.6, the maximum supported number of FlexVol volumes on secondary or data protection systems has increased, enabling you to scale up to 2,500 FlexVol volumes per node, or up to 5,000 in failover mode. The increase in FlexVol volumes is enabled with the DP\_Optimized (DPO) license. A SnapMirror license is still required on both the source and destination nodes.

Beginning with ONTAP 9.4, the following feature enhancements are made to DPO systems:

- SnapMirror backoff: In DPO systems, replication traffic is given the same priority that client workloads are given.

SnapMirror backoff is disabled by default on DPO systems.

- Volume background deduplication and cross-volume background deduplication: Volume background deduplication and cross-volume background deduplication are enabled in DPO systems.

You can run the `storage aggregate efficiency cross-volume-dedupe start -aggregate aggregate_name -scan-old-data true` command to deduplicate the existing data. The best practice is to run the command during off-peak hours to reduce the impact on performance.

- Increased savings by using Snapshot blocks as donors: The data blocks that are not available in the active file system but are trapped in Snapshot copies are used as donors for volume deduplication.

The new data can be deduplicated with the data that was trapped in Snapshot copies, effectively sharing the Snapshot blocks as well. The increased donor space provides more savings, especially when the volume has a large number of Snapshot copies.

- **Compaction:** Data compaction is enabled by default on DPO volumes.

= Manage SnapMirror volume replication

= SnapMirror replication workflow

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injpo/source/./encryption-at-rest/./media/

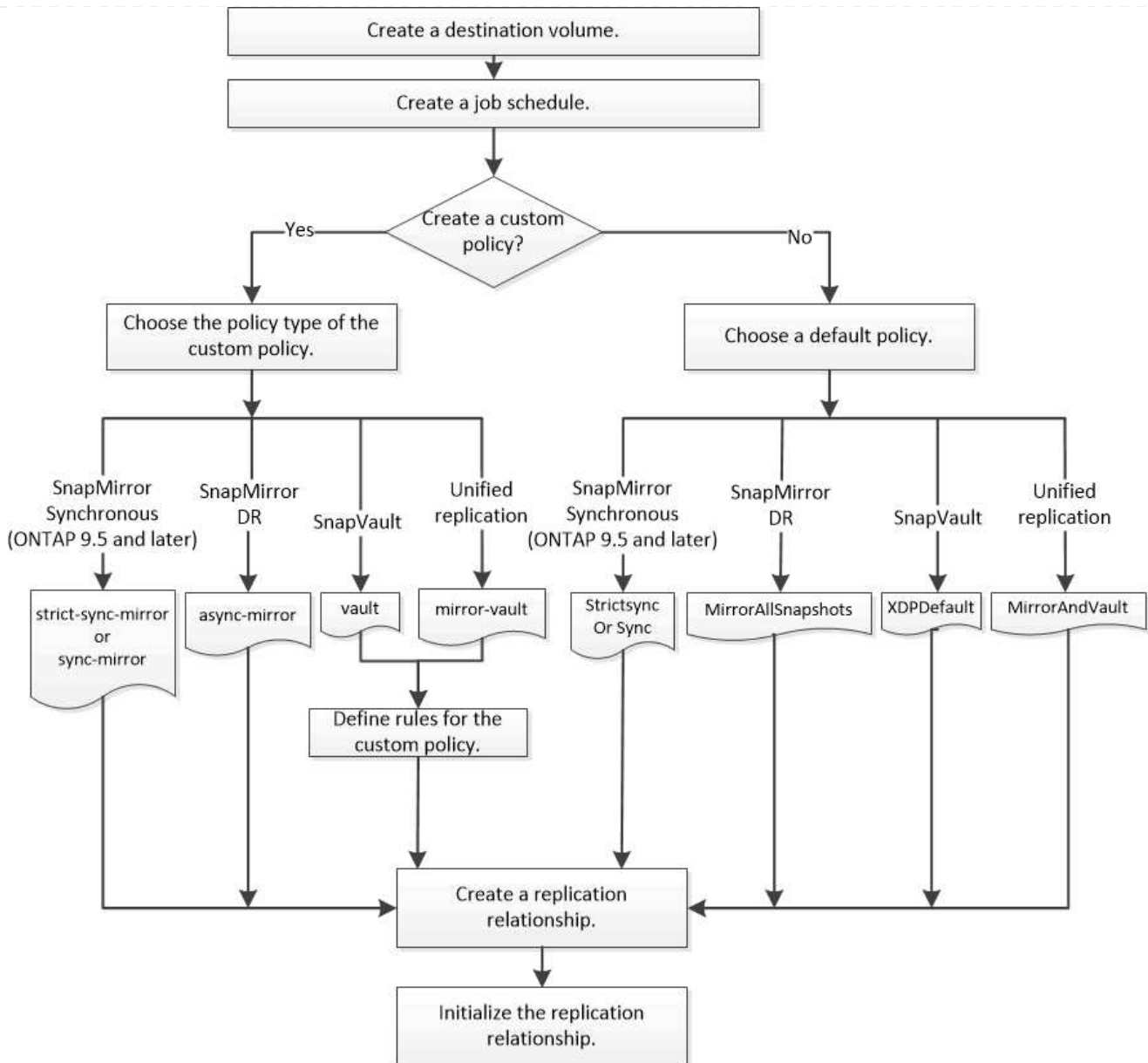
SnapMirror offers three types of data protection relationship: SnapMirror DR, archive (previously known as SnapVault), and unified replication. You can follow the same basic workflow to configure each type of relationship.

Beginning with general availability in ONTAP 9.9.1, SnapMirror Business Continuity (SM-BC) provides Zero Recovery Time Objective (Zero RTO) or Transparent Application Failover (TAF) to enable automatic failover of business-critical applications in SAN environments. SM-BC is supported in a configuration of either two AFF clusters or two All SAN Array (ASA) clusters.

[NetApp Documentation: SnapMirror Business Continuity](#)

For each type of SnapMirror data protection relationship, the workflow is the same: create a destination volume, create a job schedule, specify a policy, create and initialize the relationship.

Beginning with ONTAP 9.3, you can use the `snapmirror protect` command to configure a data protection relationship in a single step. Even if you use `snapmirror protect`, you need to understand each step in the workflow.



= Configure a replication relationship in one step

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.3, you can use the `snapmirror protect` command to configure a data protection relationship in a single step. You specify a list of volumes to be replicated, an SVM on the destination cluster, a job schedule, and a SnapMirror policy. `snapmirror protect` does the rest.

#### What you'll need

- The source and destination clusters and SVMs must be peered.

[Cluster and SVM peering](#)

- The language on the destination volume must be the same as the language on the source volume.

### About this task

The `snapmirror protect` command chooses an aggregate associated with the specified SVM. If no aggregate is associated with the SVM, it chooses from all the aggregates in the cluster. The choice of aggregate is based on the amount of free space and the number of volumes on the aggregate.

The `snapmirror protect` command then performs the following steps:

- Creates a destination volume with an appropriate type and amount of reserved space for each volume in the list of volumes to be replicated.
- Configures a replication relationship appropriate for the policy you specify.
- Initializes the relationship.

The name of the destination volume is of the form `source_volume_name_dst`. In case of a conflict with an existing name, the command appends a number to the volume name. You can specify a prefix and/or suffix in the command options. The suffix replaces the system-supplied `dst` suffix.

In ONTAP 9.3 and earlier, a destination volume can contain up to 251 Snapshot copies. In ONTAP 9.4 and later, a destination volume can contain up to 1019 Snapshot copies.

Initialization can be time-consuming. `snapmirror protect` does not wait for initialization to complete before the job finishes. For this reason, you should use the `snapmirror show` command rather than the `job show` command to determine when initialization is complete.

Beginning with ONTAP 9.5, SnapMirror Synchronous relationships can be created by using the `snapmirror protect` command.

### Step

1. Create and initialize a replication relationship in one step:

```
snapmirror protect -path-list SVM:volume|cluster://SVM/volume, ...  
-destination-vserver destination_SVM -policy policy -schedule schedule  
-auto-initialize true|false -destination-volume-prefix prefix -destination  
-volume-suffix suffix
```

You must run this command from the destination SVM or the destination cluster. The `-auto-initialize` option defaults to “true”.

+

The following example creates and initializes a SnapMirror DR relationship using the default MirrorAllSnapshots policy:

+

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy MirrorAllSnapshots -schedule
replication_daily
```

+

You can use a custom policy if you prefer. For more information, see [Creating a custom replication policy](#).



+

The following example creates and initializes a SnapVault relationship using the default XDPDefault policy:

+

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy XDPDefault -schedule
replication_daily
```

+

The following example creates and initializes a unified replication relationship using the default MirrorAndVault policy:

+

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy MirrorAndVault
```

+

The following example creates and initializes a SnapMirror Synchronous relationship using the default Sync policy:

+

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_sync -policy Sync
```

+

For SnapVault and unified replication policies, you might find it useful to define a schedule for creating a copy of the last transferred Snapshot copy on the destination. For more information, see [Defining a schedule for creating a local copy on the destination](#).

## After you finish

Use the `snapmirror show` command to verify that the SnapMirror relationship was created. For complete command syntax, see the man page.

= Configure a replication relationship one step at a time

= Create a destination volume

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the `volume create` command on the destination to create a destination volume. The destination volume should be the same or greater in size than the source volume.

### Step

1. Create a destination volume:

```
volume create -vserver SVM -volume volume -aggregate aggregate -type DP  
-size size
```

For complete command syntax, see the man page.

The following example creates a 2-GB destination volume named `volA_dst`:

```
cluster_dst::> volume create -vserver SVM_backup -volume volA_dst  
-aggregate node01_aggr -type DP -size 2GB
```

= Create a replication job schedule

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the `job schedule cron create` command to create a replication job schedule. The job schedule determines when SnapMirror automatically updates the data protection relationship to which the schedule is assigned.

### About this task

You assign a job schedule when you create a data protection relationship. If you do not assign a job schedule, you must update the relationship manually.

### Step

1. Create a job schedule:

```
job schedule cron create -name job_name -month month -dayofweek day_of_week  
-day day_of_month -hour hour -minute minute
```

For `-month`, `-dayofweek`, and `-hour`, you can specify `all` to run the job every month, day of the

week, and hour, respectively.

Beginning with ONTAP 9.10.1, you can include the Vserver for your job schedule:

```
job schedule cron create -name job_name -vserver Vserver_name -month month
-dayofweek day_of_week -day day_of_month -hour hour -minute minute
```

The following example creates a job schedule named `my_weekly` that runs on Saturdays at 3:00 a.m.:

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

= Customize a replication policy

= Create a custom replication policy

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can create a custom replication policy if the default policy for a relationship is not suitable. You might want to compress data in a network transfer, for example, or modify the number of attempts SnapMirror makes to transfer Snapshot copies.

You can use a default or custom policy when you create a replication relationship. For a custom archive (formerly SnapVault) or unified replication policy, you must define one or more *rules* that determine which Snapshot copies are transferred during initialization and update. You might also want to define a schedule for creating local Snapshot copies on the destination.

The *policy type* of the replication policy determines the type of relationship it supports. The table below shows the available policy types.

Policy type	Relationship type
async-mirror	SnapMirror DR
vault	SnapVault
mirror-vault	Unified replication
strict-sync-mirror	SnapMirror Synchronous in the StrictSync mode (supported beginning with ONTAP 9.5)
sync-mirror	SnapMirror Synchronous in the Sync mode (supported beginning with ONTAP 9.5)

When you create a custom replication policy, it is a good idea to model the policy after a default policy.

## Step

1. Create a custom replication policy:

```
snapmirror policy create -vserver SVM -policy policy -type async-  
mirror|vault|mirror-vault|strict-sync-mirror|sync-mirror -comment comment  
-tries transfer_tries -transfer-priority low|normal -is-network-compression  
-enabled true|false
```

For complete command syntax, see the man page.

Beginning with ONTAP 9.5, you can specify the schedule for creating a common Snapshot copy schedule for SnapMirror Synchronous relationships by using the `-common-snapshot-schedule` parameter. By default, the common Snapshot copy schedule for SnapMirror Synchronous relationships is one hour. You can specify a value from 30 minutes to two hours for the Snapshot copy schedule for SnapMirror Synchronous relationships.

The following example creates a custom replication policy for SnapMirror DR that enables network compression for data transfers:

```
cluster_dst::> snapmirror policy create -vserver svml -policy  
DR_compressed -type async-mirror -comment "DR with network  
compression enabled" -is-network-compression-enabled true
```

The following example creates a custom replication policy for SnapVault:

```
cluster_dst::> snapmirror policy create -vserver svml -policy  
my_snapvault -type vault
```

The following example creates a custom replication policy for unified replication:

```
cluster_dst::> snapmirror policy create -vserver svml -policy  
my_unified -type mirror-vault
```

The following example creates a custom replication policy for SnapMirror Synchronous relationship in the StrictSync mode:

```
cluster_dst::> snapmirror policy create -vserver svml -policy  
my_strictsync -type strict-sync-mirror -common-snapshot-schedule  
my_sync_schedule
```

## After you finish

For “vault” and “mirror-vault” policy types, you must define rules that determine which Snapshot copies are transferred during initialization and update.

Use the `snapmirror policy show` command to verify that the SnapMirror policy was created. For complete command syntax, see the man page.

= Define a rule for a policy

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

For custom policies with the “vault” or “mirror-vault” policy type, you must define at least one rule that determines which Snapshot copies are transferred during initialization and update. You can also define rules for default policies with the “vault” or “mirror-vault” policy type.

### About this task

Every policy with the “vault” or “mirror-vault” policy type must have a rule that specifies which Snapshot copies to replicate. The rule “bi-monthly”, for example, indicates that only Snapshot copies assigned the SnapMirror label “bi-monthly” should be replicated. You specify the SnapMirror label when you configure the Snapshot policy on the source.

Each policy type is associated with one or more system-defined rules. These rules are automatically assigned to a policy when you specify its policy type. The table below shows the system-defined rules.

System-defined rule	Used in policy types	Result
sm_created	async-mirror, mirror-vault, Sync, StrictSync	A Snapshot copy created by SnapMirror is transferred on initialization and update.
all_source_snapshots	async-mirror	New Snapshot copies on the source are transferred on initialization and update.
daily	vault,mirror-vault	New Snapshot copies on the source with the SnapMirror label “daily” are transferred on initialization and update.
weekly	vault,mirror-vault	New Snapshot copies on the source with the SnapMirror label “weekly” are transferred on initialization and update.
monthly	mirror-vault	New Snapshot copies on the source with the SnapMirror label “monthly” are transferred on initialization and update.

app_consistent	Sync, StrictSync	Snapshot copies with the SnapMirror label “app_consistent” on source are synchronously replicated to the destination. Supported Beginning with ONTAP 9.7.
----------------	------------------	---

Except for the “async-mirror” policy type, you can specify additional rules as needed, for default or custom policies. For example:

- For the default `MirrorAndVault` policy, you might create a rule called “bi-monthly” to match Snapshot copies on the source with the “bi-monthly” SnapMirror label.
- For a custom policy with the “mirror-vault” policy type, you might create a rule called “bi-weekly” to match Snapshot copies on the source with the “bi-weekly” SnapMirror label.

### Step

1. Define a rule for a policy:

```
snapmirror policy add-rule -vserver SVM -policy policy_for_rule -snapmirror
-label snapmirror-label -keep retention_count
```

For complete command syntax, see the man page.

The following example adds a rule with the SnapMirror label `bi-monthly` to the default `MirrorAndVault` policy:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
MirrorAndVault -snapmirror-label bi-monthly -keep 6
```

The following example adds a rule with the SnapMirror label `bi-weekly` to the custom `my_snapvault` policy:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
my_snapvault -snapmirror-label bi-weekly -keep 26
```

The following example adds a rule with the SnapMirror label `app_consistent` to the custom `Sync` policy:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy Sync
-snapmirror-label app_consistent -keep 1
```

You can then replicate Snapshot copies from the source cluster that match this SnapMirror label:

```
cluster_src::> snapshot create -vserver vs1 -volume voll -snapshot
snapshot1 -snapmirror-label app_consistent
```

= Define a schedule for creating a local copy on the destination

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

For SnapVault and unified replication relationships, you can protect against the possibility that an updated Snapshot copy is corrupted by creating a copy of the last transferred Snapshot copy on the destination. This “local copy” is retained regardless of the retention rules on the source, so that even if the Snapshot originally transferred by SnapMirror is no longer available on the source, a copy of it will be available on the destination.

### About this task

You specify the schedule for creating a local copy in the `-schedule` option of the `snapmirror policy add-rule` command.

### Step

1. Define a schedule for creating a local copy on the destination:

```
snapmirror policy add-rule -vserver SVM -policy policy_for_rule -snapmirror
-label snapmirror-label -schedule schedule
```

For complete command syntax, see the man page. For an example of how to create a job schedule, see [Creating a replication job schedule](#).

The following example adds a schedule for creating a local copy to the default `MirrorAndVault` policy:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
MirrorAndVault -snapmirror-label my_monthly -schedule my_monthly
```

The following example adds a schedule for creating a local copy to the custom `my_unified` policy:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
my_unified -snapmirror-label my_monthly -schedule my_monthly
```

= Create a replication relationship

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

The relationship between the source volume in primary storage and the destination

volume in secondary storage is called a *data protection relationship*. You can use the `snapmirror create` command to create SnapMirror DR, SnapVault, or unified replication data protection relationships.

#### What you'll need

- The source and destination clusters and SVMs must be peered.

#### [Cluster and SVM peering](#)

- The language on the destination volume must be the same as the language on the source volume.

#### About this task

Until ONTAP 9.3, SnapMirror invoked in DP mode and SnapMirror invoked in XDP mode used different replication engines, with different approaches to version-dependence:

- SnapMirror invoked in DP mode used a *version-dependent* replication engine in which the ONTAP version was required to be the same on primary and secondary storage:

```
cluster_dst::> snapmirror create -type DP -source-path ...  
-destination-path ...
```

- SnapMirror invoked in XDP mode used a *version-flexible* replication engine that supported different ONTAP versions on primary and secondary storage:

```
cluster_dst::> snapmirror create -type XDP -source-path ...  
-destination-path ...
```

With improvements in performance, the significant benefits of version-flexible SnapMirror outweigh the slight advantage in replication throughput obtained with version-dependent mode. For this reason, beginning with ONTAP 9.3, XDP mode has been made the new default, and any invocations of DP mode on the command line or in new or existing scripts are automatically converted to XDP mode.

Existing relationships are not affected. If a relationship is already of type DP, it will continue to be of type DP. The table below shows the behavior you can expect.

If you specify...	The type is...	The default policy (if you do not specify a policy) is...
DP	XDP	MirrorAllSnapshots (SnapMirror DR)
Nothing	XDP	MirrorAllSnapshots (SnapMirror DR)
XDP	XDP	XDPDefault (SnapVault)

See also the examples in the procedure below.

The only exceptions to conversion are as follows:



- SVM data protection relationships continue to default to DP mode.

Specify XDP explicitly to obtain XDP mode with the default `MirrorAllSnapshots` policy.

- Load-sharing data protection relationships continue to default to DP mode.
- SnapLock data protection relationships continue to default to DP mode.
- Explicit invocations of DP continue to default to DP mode if you set the following cluster-wide option:

```
options replication.create_data_protection_rels.enable on
```

This option is ignored if you do not explicitly invoke DP.

In ONTAP 9.3 and earlier, a destination volume can contain up to 251 Snapshot copies. In ONTAP 9.4 and later, a destination volume can contain up to 1019 Snapshot copies.

Beginning with ONTAP 9.5, SnapMirror Synchronous relationships are supported.

### Step

1. From the destination cluster, create a replication relationship:

```
snapmirror create -source-path SVM:volume|cluster://SVM/volume, ...  
-destination-path SVM:volume|cluster://SVM/volume, ... -type DP|XDP -schedule  
schedule -policy policy
```

For complete command syntax, see the man page.

The `schedule` parameter is not applicable when creating SnapMirror Synchronous relationships.

+

The following example creates a SnapMirror DR relationship using the default `MirrorLatest` policy:

+

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
MirrorLatest
```

+

The following example creates a SnapVault relationship using the default `XDPDefault` policy:

+

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
XDPDefault
```

+

The following example creates a unified replication relationship using the default `MirrorAndVault` policy:

+

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
MirrorAndVault
```

+

The following example creates a unified replication relationship using the custom `my_unified` policy:

+

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
my_unified
```

+

The following example creates a SnapMirror Synchronous relationship using the default `Sync` policy:

+

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy Sync
```

+

The following example creates a SnapMirror Synchronous relationship using the default `StrictSync` policy:

+

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy StrictSync
```

+

The following example creates a SnapMirror DR relationship. With the DP type automatically converted to XDP and with no policy specified, the policy defaults to the `MirrorAllSnapshots` policy:

+

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type DP -schedule my_daily
```

+

The following example creates a SnapMirror DR relationship. With no type or policy specified, the policy defaults to the `MirrorAllSnapshots` policy:

+

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -schedule my_daily
```

+

The following example creates a SnapMirror DR relationship. With no policy specified, the policy defaults to the `XDPDefault` policy:

+

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily
```

+

The following example creates a SnapMirror Synchronous relationship with the predefined policy `SnapCenterSync`:

+

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination  
-path svm_backup:volA_dst -type XDP -policy SnapCenterSync
```

+

The predefined policy `SnapCenterSync` is of type `Sync`. This policy replicates any Snapshot copy that is created with the `snapmirror-label` of `"app_consistent"`.

## After you finish

Use the `snapmirror show` command to verify that the SnapMirror relationship was created. For complete command syntax, see the man page.

== Other ways to do this in ONTAP

To perform these tasks with...	See this content...
The redesigned System Manager (available with ONTAP 9.7 and later)	<a href="#">Configure mirrors and vaults</a>
System Manager Classic (available with ONTAP 9.7 and earlier)	<a href="#">Volume backup using SnapVault overview</a>

= Initialize a replication relationship

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

For all relationship types, initialization performs a *baseline transfer*: it makes a Snapshot copy of the source volume, then transfers that copy and all the data blocks it references to the destination volume. Otherwise, the contents of the transfer depend on the policy.

## What you'll need

The source and destination clusters and SVMs must be peered.

### [Cluster and SVM peering](#)

## About this task

Initialization can be time-consuming. You might want to run the baseline transfer in off-peak hours.

Beginning with ONTAP 9.5, SnapMirror Synchronous relationships are supported.

## Step

1. Initialize a replication relationship:

```
snapmirror initialize -source-path SVM:volume|cluster://SVM/volume, ...  
-destination-path SVM:volume|cluster://SVM/volume, ...
```

For complete command syntax, see the man page.

You must run this command from the destination SVM or the destination cluster.

+

The following example initializes the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

+

```
cluster_dst::> snapmirror initialize -source-path svm1:volA
                -destination-path svm_backup:volA_dst
```

= Example: Configure a vault-vault cascade

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

An example will show in concrete terms how you can configure replication relationships one step at a time. You can use the vault-vault cascade deployment configured in the example to retain more than 251 Snapshot copies labeled “my-weekly”.

### What you’ll need

- The source and destination clusters and SVMs must be peered.
- You must be running ONTAP 9.2 or later. Vault-vault cascades are not supported in earlier ONTAP releases.

### About this task

The example assumes the following:

- You have configured Snapshot copies on the source cluster with the SnapMirror labels “my-daily”, “my-weekly”, and “my-monthly”.
- You have configured destination volumes named “volA” on the secondary and tertiary destination clusters.
- You have configured replication job schedules named “my\_snapvault” on the secondary and tertiary destination clusters.

The example shows how to create replication relationships based on two custom policies:

- The “snapvault\_secondary” policy retains 7 daily, 52 weekly, and 180 monthly Snapshot copies on the secondary destination cluster.
- The “snapvault\_tertiary policy” retains 250 weekly Snapshot copies on the tertiary destination cluster.

### Steps

1. On the secondary destination cluster, create the “snapvault\_secondary” policy:

```
cluster_secondary::> snapmirror policy create -policy snapvault_secondary
                -type vault -comment "Policy on secondary for vault to vault cascade"
                -vserver svm_secondary
```

2. On the secondary destination cluster, define the “my-daily” rule for the policy:

```
cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
-snapmirror-label my-daily -keep 7 -vserver svm_secondary
```

3. On the secondary destination cluster, define the “my-weekly” rule for the policy:

```
cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
-snapmirror-label my-weekly -keep 52 -vserver svm_secondary
```

4. On the secondary destination cluster, define the “my-monthly” rule for the policy:

```
cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
-snapmirror-label my-monthly -keep 180 -vserver svm_secondary
```

5. On the secondary destination cluster, verify the policy:

```
cluster_secondary::> snapmirror policy show snapvault_secondary -instance
```

```

                Vserver: svm_secondary
SnapMirror Policy Name: snapvault_secondary
SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                Tries Limit: 8
                Transfer Priority: normal
Ignore accesstime Enabled: false
                Transfer Restartability: always
Network Compression Enabled: false
                Create Snapshot: false
                Comment: Policy on secondary for vault to vault
cascade
                Total Number of Rules: 3
                Total Keep: 239
                Rules: SnapMirror Label      Keep  Preserve
Warn Schedule Prefix
-----
0 - - - - - my-daily          7  false
0 - - - - - my-weekly       52  false
0 - - - - - my-monthly      180  false
0 - - - - -
```

6. On the secondary destination cluster, create the relationship with the source cluster:

```
cluster_secondary::> snapmirror create -source-path svm_primary:volA
-destination-path svm_secondary:volA -type XDP -schedule my_snapvault
-policy snapvault_secondary
```

7. On the secondary destination cluster, initialize the relationship with the source cluster:

```
cluster_secondary::> snapmirror initialize -source-path svm_primary:volA  
-destination-path svm_secondary:volA
```

8. On the tertiary destination cluster, create the “snapvault\_tertiary” policy:

```
cluster_tertiary::> snapmirror policy create -policy snapvault_tertiary  
-type vault -comment "Policy on tertiary for vault to vault cascade"  
-vserver svm_tertiary
```

9. On the tertiary destination cluster, define the “my-weekly” rule for the policy:

```
cluster_tertiary::> snapmirror policy add-rule -policy snapvault_tertiary  
-snapmirror-label my-weekly -keep 250 -vserver svm_tertiary
```

10. On the tertiary destination cluster, verify the policy:

```
cluster_tertiary::> snapmirror policy show snapvault_tertiary -instance
```

```
                Vserver: svm_tertiary  
SnapMirror Policy Name: snapvault_tertiary  
SnapMirror Policy Type: vault  
                Policy Owner: cluster-admin  
                Tries Limit: 8  
                Transfer Priority: normal  
Ignore accesstime Enabled: false  
                Transfer Restartability: always  
Network Compression Enabled: false  
                Create Snapshot: false  
                Comment: Policy on tertiary for vault to vault  
cascade  
                Total Number of Rules: 1  
                Total Keep: 250  
                Rules: SnapMirror Label      Keep  Preserve  
Warn Schedule Prefix  
-----  
-----  
                my-weekly                250  false  
0 -      -
```

11. On the tertiary destination cluster, create the relationship with the secondary cluster:

```
cluster_tertiary::> snapmirror create -source-path svm_secondary:volA  
-destination-path svm_tertiary:volA -type XDP -schedule my_snapvault  
-policy snapvault_tertiary
```

12. On the tertiary destination cluster, initialize the relationship with the secondary cluster:



```
cluster_tertiary::> snapmirror initialize -source-path svm_secondary:volA  
-destination-path svm_tertiary:volA
```

= Convert an existing DP-type relationship to XDP

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can easily convert an existing DP-type relationship to XDP to take advantage of version-flexible SnapMirror.

#### About this task

- SnapMirror does not automatically convert existing DP-type relationships to XDP. To convert the relationship, you need to break and delete the existing relationship, create a new XDP relationship, and resync the relationship. For background information, see [XDP replaces DP as the SnapMirror default](#).
- When planning your conversion, you should be aware that background preparation and the data warehousing phase of an XDP SnapMirror relationship can take a long time. It is not uncommon to see the SnapMirror relationship reporting the status "preparing" for an extended time period.

After you convert a SnapMirror relationship type from DP to XDP, space-related settings, such as autosize and space guarantee are no longer replicated to the destination.

## Steps

1. From the destination cluster, ensure that the SnapMirror relationship is type DP, that the mirror state is SnapMirrored, the relationship status is Idle, and the relationship is healthy:

```
snapmirror show -destination-path SVM:volume|cluster://SVM/volume
```

The following example shows the output from the `snapmirror show` command:

```
cluster_dst::>snapmirror show -destination-path svm_backup:volA_dst

Source Path: svm1:volA
Destination Path: svm_backup:volA_dst
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Exported Snapshot Timestamp: 06/27 10:00:55
Healthy: true
```

You might find it helpful to retain a copy of the `snapmirror show` command output to keep track existing of the relationship settings.

1. From the source and the destination volumes, ensure that both volumes have a common Snapshot copy:

```
volume snapshot show -vserver SVM -volume volume
```

The following example shows the `volume snapshot show` output for the source and the destination volumes:

```

cluster_src:> volume snapshot show -vserver vsml -volume volA
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-----
-----
svm1 volA
weekly.2014-06-09_0736 valid 76KB 0% 28%
weekly.2014-06-16_1305 valid 80KB 0% 29%
daily.2014-06-26_0842 valid 76KB 0% 28%
hourly.2014-06-26_1205 valid 72KB 0% 27%
hourly.2014-06-26_1305 valid 72KB 0% 27%
hourly.2014-06-26_1405 valid 76KB 0% 28%
hourly.2014-06-26_1505 valid 72KB 0% 27%
hourly.2014-06-26_1605 valid 72KB 0% 27%
daily.2014-06-27_0921 valid 60KB 0% 24%
hourly.2014-06-27_0921 valid 76KB 0% 28%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
valid 44KB 0% 19%
11 entries were displayed.

```

```

cluster_dest:> volume snapshot show -vserver svm_backup -volume
volA_dst
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-----
-----
svm_backup volA_dst
weekly.2014-06-09_0736 valid 76KB 0% 30%
weekly.2014-06-16_1305 valid 80KB 0% 31%
daily.2014-06-26_0842 valid 76KB 0% 30%
hourly.2014-06-26_1205 valid 72KB 0% 29%
hourly.2014-06-26_1305 valid 72KB 0% 29%
hourly.2014-06-26_1405 valid 76KB 0% 30%
hourly.2014-06-26_1505 valid 72KB 0% 29%
hourly.2014-06-26_1605 valid 72KB 0% 29%
daily.2014-06-27_0921 valid 60KB 0% 25%
hourly.2014-06-27_0921 valid 76KB 0% 30%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026

```

2. To ensure scheduled updates will not run during the conversion, quiesce the existing DP-type relationship:

```
snapmirror quiesce -source-path SVM:volume|cluster://SVM/volume, ...  
-destination-path SVM:volume|cluster://SVM/volume, ...
```

For complete command syntax, see the man page.

You must run this command from the destination SVM or the destination cluster.

+

The following example quiesces the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

+

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

1. Break the existing DP-type relationship:

```
snapmirror break -destination-path SVM:volume|cluster://SVM/volume, ...
```

For complete command syntax, see the man page.

You must run this command from the destination SVM or the destination cluster.

+

The following example breaks the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

+

```
cluster_dst::> snapmirror break -destination-path svm_backup:volA_dst
```

1. If automatic deletion of Snapshot copies is enabled on the destination volume, disable it:

```
volume snapshot autodelete modify -vserver SVM -volume volume -enabled false
```

The following example disables Snapshot copy autodelete on the destination volume `volA_dst`:

```
cluster_dst::> volume snapshot autodelete modify -vserver svm_backup -volume volA_dst -enabled false
```

2. Delete the existing DP-type relationship:

```
snapmirror delete -destination-path SVM:volume|cluster://SVM/volume, ...
```

For complete command syntax, see the man page.

You must run this command from the destination SVM or the destination cluster.

+

The following example deletes the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

+

```
cluster_dst::> snapmirror delete -destination-path svm_backup:volA_dst
```

1. You can use the output you retained from the `snapmirror show` command to create the new XDP-type relationship:

```
snapmirror create -source-path SVM:volume|cluster://SVM/volume, ...  
-destination-path SVM:volume|cluster://SVM/volume, ... -type XDP -schedule  
schedule -policy policy
```

The new relationship must use the same source and destination volume. For complete command syntax, see the man page.

You must run this command from the destination SVM or the destination cluster.

+

The following example creates a SnapMirror DR relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup` using the default `MirrorAllSnapshots` policy:

+

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst
-type XDP -schedule my_daily -policy MirrorAllSnapshots
```

1. Resync the source and destination volumes:

```
snapmirror resync -source-path SVM:volume|cluster://SVM/volume, ...
-destination-path SVM:volume|cluster://SVM/volume, ...
```

For complete command syntax, see the man page.

You must run this command from the destination SVM or the destination cluster. Although resync does not require a baseline transfer, it can be time-consuming. You might want to run the resync in off-peak hours.

+

The following example resyncs the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

+

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

1. If you disabled automatic deletion of Snapshot copies, reenable it:

```
volume snapshot autodelete modify -vserver SVM -volume volume -enabled true
```

### After you finish

1. Use the `snapmirror show` command to verify that the SnapMirror relationship was created. For complete command syntax, see the man page.
2. Once the SnapMirror XDP destination volume begins updating Snapshot copies as defined by the SnapMirror policy, you can use the output of `snapmirror list-destinations` command from the source cluster to display the new SnapMirror XDP relationship.

= Convert the type of a SnapMirror relationship

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.5, SnapMirror Synchronous is supported. You can convert an asynchronous SnapMirror relationship to a SnapMirror Synchronous relationship or vice versa without performing a baseline transfer.

### About this task

You cannot convert an asynchronous SnapMirror relationship to a SnapMirror Synchronous relationship or vice versa by changing the SnapMirror policy

### Steps

- **Converting an asynchronous SnapMirror relationship to a SnapMirror Synchronous relationship**

- a. From the destination cluster, delete the asynchronous SnapMirror relationship:

```
snapmirror delete -destination-path SVM:volume
```

```
cluster2::>snapmirror delete -destination-path vs1_dr:vol1
```

- b. From the source cluster, release the SnapMirror relationship without deleting the common Snapshot copies:

```
snapmirror release -relationship-info-only true -destination-path
dest_SVM:dest_volume
```



```
cluster1::>snapmirror release -relationship-info-only true
-destination-path vs1_dr:vol1
```

- c. From the destination cluster, create a SnapMirror Synchronous relationship:

```
snapmirror create -source-path src_SVM:src_volume -destination-path
dest_SVM:dest_volume -policy sync-mirror
```

```
cluster2::>snapmirror create -source-path vs1:vol1 -destination
-path vs1_dr:vol1 -policy sync
```

- d. Resynchronize the SnapMirror Synchronous relationship:

```
snapmirror resync -destination-path dest_SVM:dest_volume
```

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

• **Converting a SnapMirror Synchronous relationship to an asynchronous SnapMirror relationship**

- a. From the destination cluster, quiesce the existing SnapMirror Synchronous relationship:

```
snapmirror quiesce -destination-path dest_SVM:dest_volume
```

```
cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
```

- b. From the destination cluster, delete the asynchronous SnapMirror relationship:

```
snapmirror delete -destination-path SVM:volume
```

```
cluster2::>snapmirror delete -destination-path vs1_dr:vol1
```

- c. From the source cluster, release the SnapMirror relationship without deleting the common Snapshot copies:

```
snapmirror release -relationship-info-only true -destination-path
dest_SVM:dest_volume
```

```
cluster1::>snapmirror release -relationship-info-only true
-destination-path vs1_dr:vol1
```

- d. From the destination cluster, create an asynchronous SnapMirror relationship:

```
snapmirror create -source-path src_SVM:src_volume -destination-path
dest_SVM:dest_volume -policy MirrorAllSnapshots
```

```
cluster2::>snapmirror create -source-path vs1:vol1 -destination
-path vs1_dr:vol1 -policy sync
```

e. Resynchronize the SnapMirror Synchronous relationship:

```
snapmirror resync -destination-path dest_SVM:dest_volume
```

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

= Convert the mode of a SnapMirror Synchronous relationship

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.5, SnapMirror Synchronous relationships are supported. You can convert the mode of a SnapMirror Synchronous relationship from StrictSync to Sync or vice versa.

#### About this task

You cannot modify the policy of a Snapmirror Synchronous relationship to convert its mode.

#### Steps

1. From the destination cluster, quiesce the existing SnapMirror Synchronous relationship:

```
snapmirror quiesce -destination-path dest_SVM:dest_volume
```

```
cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
```

2. From the destination cluster, delete the existing SnapMirror Synchronous relationship:

```
snapmirror delete -destination-path dest_SVM:dest_volume
```

```
cluster2::> snapmirror delete -destination-path vs1_dr:vol1
```

3. From the source cluster, release the SnapMirror relationship without deleting the common Snapshot copies:

```
snapmirror release -relationship-info-only true -destination-path
dest_SVM:dest_volume
```

```
cluster1::> snapmirror release -relationship-info-only true
-destination-path vs1_dr:vol1
```

4. From the destination cluster, create a SnapMirror Synchronous relationship by specifying the mode to which you want to convert the SnapMirror Synchronous relationship:

```
snapmirror create -source-path vs1:vol1 -destination-path
dest_SVM:dest_volume -policy Sync|StrictSync
```

```
cluster2::> snapmirror create -source-path vs1:vol1 -destination
-path vs1_dr:vol1 -policy Sync
```

5. From the destination cluster, resynchronize the SnapMirror relationship:

```
snapmirror resync -destination-path dest_SVM:dest_volume
```

```
cluster2::> snapmirror resync -destination-path vs1_dr:vol1
```

= Serve data from a SnapMirror DR destination volume

= Make the destination volume writeable

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You need to make the destination volume writeable before you can serve data from the volume to clients. You can use the `snapmirror quiesce` command to stop scheduled transfers to the destination, the `snapmirror abort` command to stop ongoing transfers, and the `snapmirror break` command to make the destination writeable.

### About this task

You must perform this task from the destination SVM or the destination cluster.

### Steps

1. Stop scheduled transfers to the destination:

```
snapmirror quiesce -source-path SVM:volume|cluster://SVM/volume, ...
-destination-path SVM:volume|cluster://SVM/volume, ...
```

For complete command syntax, see the man page.

The following example stops scheduled transfers between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror quiesce -source-path svm1:volA  
-destination-path svm_backup:volA_dst
```

2. Stop ongoing transfers to the destination:

```
snapmirror abort -source-path SVM:volume|cluster://SVM/volume, ...  
-destination-path SVM:volume|cluster://SVM/volume, ...
```

For complete command syntax, see the man page.

This step is not required for SnapMirror Synchronous relationships (supported beginning with ONTAP 9.5).

+

The following example stops ongoing transfers between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

+

```
cluster_dst::> snapmirror abort -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

#### 1. Break the SnapMirror DR relationship:

```
snapmirror break -source-path SVM:volume|cluster://SVM/volume, ...
-destination-path SVM:volume|cluster://SVM/volume, ...
```

For complete command syntax, see the man page.

The following example breaks the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup` and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror break -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

== Other ways to do this in ONTAP

To perform these tasks with...	See this content...
The redesigned System Manager (available with ONTAP 9.7 and later)	<a href="#">Serve data from a SnapMirror destination</a>
System Manager Classic (available with ONTAP 9.7 and earlier)	<a href="#">Volume disaster recovery overview</a>

= Configure the destination volume for data access

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

After making the destination volume writeable, you must configure the volume for data access. NAS clients, NVMe subsystem, and SAN hosts can access the data from the destination volume until the source volume is reactivated.

NAS environment:

1. Mount the NAS volume to the namespace using the same junction path that the source volume was mounted to in the source SVM.
2. Apply the appropriate ACLs to the SMB shares at the destination volume.

3. Assign the NFS export policies to the destination volume.
4. Apply the quota rules to the destination volume.
5. Redirect clients to the destination volume.
6. Remount the NFS and SMB shares on the clients.

SAN environment:

1. Map the LUNs in the volume to the appropriate initiator group.
2. For iSCSI, create iSCSI sessions from the SAN host initiators to the SAN LIFs.
3. On the SAN client, perform a storage re-scan to detect the connected LUNs.

For information about NVMe environment, see [SAN administration](#).

= Reactivate the original source volume

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can reestablish the original data protection relationship between the source and destination volumes when you no longer need to serve data from the destination.

#### About this task

- The procedure below assumes that the baseline in the original source volume is intact. If the baseline is not intact, you must create and initialize the relationship between the volume you are serving data from and the original source volume before performing the procedure.
- Background preparation and the data warehousing phase of an XDP SnapMirror relationship can take a long time. It is not uncommon to see the SnapMirror relationship reporting the status "preparing" for an extended time period.

#### Steps

1. Delete the original data protection relationship:

```
snapmirror delete -source-path SVM:volume|cluster://SVM/volume, ...  
-destination-path SVM:volume|cluster://SVM/volume, ...
```

For complete command syntax, see the man page.

You must run this command from the destination SVM or the destination cluster.

The following example deletes the relationship between the original source volume, volA on svm1, and the volume you are serving data from, volA\_dst on svm\_backup:

```
cluster_dst::> snapmirror delete -source-path svm1:volA -destination  
-path svm_backup:volA_dst
```

2. Reverse the original data protection relationship:

```
snapmirror resync -source-path SVM:volume|cluster://SVM/volume, ...  
-destination-path SVM:volume|cluster://SVM/volume, ...
```

For complete command syntax, see the man page.

You must run this command from the destination SVM or the destination cluster. Although `resync` does not require a baseline transfer, it can be time-consuming. You might want to run the `resync` in off-peak hours.

The following example reverses the relationship between the original source volume, `volA` on `svm1`, and the volume you are serving data from, `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

### 3. Stop the source SVM for the reversed relationship:

```
vserver stop -vserver SVM
```

For complete command syntax, see the man page.

The following example stops the source SVM for the reversed relationship:

```
cluster_src::> vserver stop svm_backup
```

### 4. Update the reversed relationship:

```
snapmirror update -source-path SVM:volume|cluster://SVM/volume, ...
-destination-path SVM:volume|cluster://SVM/volume, ...
```

For complete command syntax, see the man page.

You must run this command from the destination SVM or the destination cluster. The command fails if a common Snapshot copy does not exist on the source and destination. Use `snapmirror initialize` to re-initialize the relationship.

+

The following example updates the relationship between the volume you are serving data from, volA\_dst on svm\_backup, and the original source volume, volA on svm1:

+

```
cluster_dst::> snapmirror update -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

1. Stop scheduled transfers for the reversed relationship:

```
snapmirror quiesce -source-path SVM:volume|cluster://SVM/volume, ...
-destination-path SVM:volume|cluster://SVM/volume, ...
```

For complete command syntax, see the man page.

You must run this command from the destination SVM or the destination cluster.

+

The following example stops scheduled transfers between the volume you are serving data from, volA\_dst on svm\_backup, and the original source volume, volA on svm1:

+

```
cluster_dst::> snapmirror quiesce -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

1. Stop ongoing transfers for the reversed relationship:

```
snapmirror abort -source-path SVM:volume|cluster://SVM/volume, ...
-destination-path SVM:volume|cluster://SVM/volume, ...
```

For complete command syntax, see the man page.

You must run this command from the destination SVM or the destination cluster.



+

The following example stops ongoing transfers between the volume you are serving data from, `volA_dst` on `svm_backup`, and the original source volume, `volA` on `svm1`:

+

```
cluster_dst::> snapmirror abort -source-path svm_backup:volA_dst  
-destination-path svm1:volA
```

1. Break the reversed relationship:

```
snapmirror break -source-path SVM:volume|cluster://SVM/volume, ...  
-destination-path SVM:volume|cluster://SVM/volume, ...
```

For complete command syntax, see the man page.

You must run this command from the destination SVM or the destination cluster.

+

The following example breaks the relationship between the volume you are serving data from, `volA_dst` on `svm_backup`, and the original source volume, `volA` on `svm1`:

+

```
cluster_dst::> snapmirror break -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

### 1. Start the original source SVM:

```
vserver start -vserver SVM
```

For complete command syntax, see the man page.

The following example starts the original source SVM:

```
cluster_dst::> vserver start svm1
```

### 2. Delete the reversed data protection relationship:

```
snapmirror delete -source-path SVM:volume|cluster://SVM/volume, ...
-destination-path SVM:volume|cluster://SVM/volume, ...
```

For complete command syntax, see the man page.

You must run this command from the source SVM or the source cluster for the reversed relationship.

The following example deletes the reversed relationship between the original source volume, `volA` on `svm1`, and the volume you are serving data from, `volA_dst` on `svm_backup`:

```
cluster_src::> snapmirror delete -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

### 3. Reestablish the original data protection relationship:

```
snapmirror resync -source-path SVM:volume|cluster://SVM/volume, ...
-destination-path SVM:volume|cluster://SVM/volume, ...
```

For complete command syntax, see the man page.

The following example reestablishes the relationship between the original source volume, `volA` on `svm1`, and the original destination volume, `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

### After you finish

Use the `snapmirror show` command to verify that the SnapMirror relationship was created. For complete command syntax, see the man page.

= Restore files from a SnapMirror destination volume

= Restore a single file, LUN, or NVMe namespace from a SnapMirror destination

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can restore a single file, LUN, a set of files or LUNs from a Snapshot copy, or an NVMe namespace from a SnapMirror destination volume. Beginning with ONTAP 9.7, you can also restore NVMe namespaces from a SnapMirror Synchronous destination. You can restore files to the original source volume or to a different volume.

### What you'll need

To restore a file or LUN from a SnapMirror Synchronous destination (supported beginning with ONTAP 9.5), you must first delete and release the relationship.

### About this task

The volume to which you are restoring files or LUNs (the destination volume) must be a read-write volume:

- SnapMirror performs an *incremental restore* if the source and destination volumes have a common Snapshot copy (as is typically the case when you are restoring to the original source volume).
- Otherwise, SnapMirror performs a *baseline restore*, in which the specified Snapshot copy and all the data blocks it references are transferred to the destination volume.

### Steps

1. List the Snapshot copies in the destination volume:

```
volume snapshot show -vserver SVM -volume volume
```

For complete command syntax, see the man page.

The following example shows the Snapshot copies on the `vserverB:secondary1` destination:

```
cluster_dst::> volume snapshot show -vserver vserverB -volume
secondary1
```

Vserver	Volume	Snapshot	State	Size	Total%	Used%
vserverB	secondary1	hourly.2013-01-25_0005	valid	224KB	0%	0%
		daily.2013-01-25_0010	valid	92KB	0%	0%
		hourly.2013-01-25_0105	valid	228KB	0%	0%
		hourly.2013-01-25_0205	valid	236KB	0%	0%
		hourly.2013-01-25_0305	valid	244KB	0%	0%
		hourly.2013-01-25_0405	valid	244KB	0%	0%
		hourly.2013-01-25_0505	valid	244KB	0%	0%

7 entries were displayed.

2. Restore a single file or LUN or a set of files or LUNs from a Snapshot copy in a SnapMirror destination volume:

```
snapmirror restore -source-path SVM:volume|cluster://SVM/volume, ...
-destination-path SVM:volume|cluster://SVM/volume, ... -source-snapshot
snapshot -file-list source_file_path,@destination_file_path
```

For complete command syntax, see the man page.

You must run this command from the destination SVM or the destination cluster.

+

The following command restores the files `file1` and `file2` from the Snapshot copy `daily.2013-01-25_0010` in the original destination volume `secondary1`, to the same location in the active file system of the original source volume `primary1`:

+

```
cluster_dst:> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list /dir1/file1,/dir2/file2
```

```
[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

+

The following command restores the files `file1` and `file2` from the Snapshot copy `daily.2013-01-25_0010` in the original destination volume `secondary1`, to a different location in the active file system of the original source volume `primary1`.

+

The destination file path begins with the `@` symbol followed by the path of the file from the root of the original source volume. In this example, `file1` is restored to `/dir1/file1.new` and `file2` is restored to `/dir2.new/file2` on `primary1`:

+

```
cluster_dst:> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,@/dir2.new/file2
```

```
[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

+

The following command restores the files `file1` and `file3` from the Snapshot copy `daily.2013-01-25_0010` in the original destination volume `secondary1`, to different locations in the active file system of the original source volume `primary1`, and restores `file2` from `snap1` to the same location in the active file system of `primary1`.

+

In this example, the file `file1` is restored to `/dir1/file1.new` and `file3` is restored to `/dir3.new/file3`:

+

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,/dir3/file3,@/dir3.new/file3
```

```
[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

= Restore the contents of a volume from a SnapMirror destination

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can restore the contents of an entire volume from a Snapshot copy in a SnapMirror destination volume. You can restore the volume's contents to the original source volume or to a different volume.

#### **About this task**

The destination volume for the restore operation must be one of the following:

- A read-write volume, in which case SnapMirror performs an *incremental restore*, provided that the source and destination volumes have a common Snapshot copy (as is typically the case when you are restoring to the original source volume).

The command fails if there is not a common Snapshot copy. You cannot restore the contents of a volume to an empty read-write volume.

- An empty data protection volume, in which case SnapMirror performs a *baseline restore*, in which the specified Snapshot copy and all the data blocks it references are transferred to the source volume.

Restoring the contents of a volume is a disruptive operation. SMB traffic must not be running on the SnapVault primary volume when a restore operation is running.

If the destination volume for the restore operation has compression enabled, and the source volume does not have compression enabled, disable compression on the destination volume. You need to re-enable compression after the restore operation is complete.

Any quota rules defined for the destination volume are deactivated before the restore is performed. You can use the `volume quota modify` command to reactivate quota rules after the restore operation is complete.

### Steps

1. List the Snapshot copies in the destination volume:

```
volume snapshot show -vserver SVM -volume volume
```

For complete command syntax, see the man page.

The following example shows the Snapshot copies on the `vserverB:secondary1` destination:

```
cluster_dst::> volume snapshot show -vserver vserverB -volume
secondary1
```

Vserver	Volume	Snapshot	State	Size	Total% Used%
vserverB	secondary1	hourly.2013-01-25_0005	valid	224KB	0%
		daily.2013-01-25_0010	valid	92KB	0%
		hourly.2013-01-25_0105	valid	228KB	0%
		hourly.2013-01-25_0205	valid	236KB	0%
		hourly.2013-01-25_0305	valid	244KB	0%
		hourly.2013-01-25_0405	valid	244KB	0%
		hourly.2013-01-25_0505	valid	244KB	0%

7 entries were displayed.

2. Restore the contents of a volume from a Snapshot copy in a SnapMirror destination volume:

```
snapmirror restore -source-path SVM:volume|cluster://SVM/volume, ...  
-destination-path SVM:volume|cluster://SVM/volume, ... -source-snapshot  
snapshot
```

For complete command syntax, see the man page.

You must run this command from the destination SVM or the destination cluster.



+

The following command restores the contents of the original source volume `primary1` from the Snapshot copy `daily.2013-01-25_0010` in the original destination volume `secondary1`:

+

```
cluster_dst:> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010
```

```
Warning: All data newer than Snapshot copy daily.2013-01-25_0010 on
volume vserverA:primary1 will be deleted.
```

```
Do you want to continue? {y|n}: y
```

```
[Job 34] Job is queued: snapmirror restore from source
vserverB:secondary1 for the snapshot daily.2013-01-25_0010.
```

1. Remount the restored volume and restart all applications that use the volume.

== Other ways to do this in ONTAP

To perform these tasks with...	See this content...
The redesigned System Manager (available with ONTAP 9.7 and later)	<a href="#">Restore a volume from an earlier Snapshot copy</a>
System Manager Classic (available with ONTAP 9.7 and earlier)	<a href="#">Volume restore using SnapVault overview</a>

= Update a replication relationship manually

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You might need to update a replication relationship manually if an update fails because the source volume has been moved.

### About this task

SnapMirror aborts any transfers from a moved source volume until you update the replication relationship manually.

Beginning with ONTAP 9.5, SnapMirror Synchronous relationships are supported. Although the source and destination volumes are in sync at all times in these relationships, the view from the secondary cluster is synchronized with the primary only on an hourly basis. If you want to view the point-in-time data at the destination, you should perform a manual update by running the `snapmirror update` command.

### Step

1. Update a replication relationship manually:

```
snapmirror update -source-path SVM:volume|cluster://SVM/volume, ...  
-destination-path SVM:volume|cluster://SVM/volume, ...
```

For complete command syntax, see the man page.

You must run this command from the destination SVM or the destination cluster. The command fails if a common Snapshot copy does not exist on the source and destination. Use `snapmirror initialize` to re-initialize the relationship.

+

The following example updates the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

+

```
cluster_src::> snapmirror update -source-path svm1:volA -destination  
-path svm_backup:volA_dst
```

= Resynchronize a replication relationship

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You need to resynchronize a replication relationship after you make a destination volume writeable, after an update fails because a common Snapshot copy does not exist on the source and destination volumes, or if you want to change the replication policy for the relationship.

#### About this task

- Although `resync` does not require a baseline transfer, it can be time-consuming. You might want to run the `resync` in off-peak hours.
- Volumes that are part of a fan-out or cascade configuration can take longer to resynchronize. It is not uncommon to see the SnapMirror relationship reporting the status "preparing" for an extended time period.

#### Step

1. Resync the source and destination volumes:

```
snapmirror resync -source-path SVM:volume|cluster://SVM/volume, ...  
-destination-path SVM:volume|cluster://SVM/volume, ... -type DP|XDP -schedule  
schedule -policy policy
```

For complete command syntax, see the man page.

You must run this command from the destination SVM or the destination cluster.

+

The following example resyncs the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

+

```
cluster_dst:> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

= Delete a volume replication relationship

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the `snapmirror delete` and `snapmirror release` commands to delete a volume replication relationship. You can then delete unneeded destination volumes manually.

#### About this task

The `snapmirror release` command deletes any SnapMirror-created Snapshot copies from the source. You can use the `-relationship-info-only` option to preserve the Snapshot copies.

#### Steps

1. Quiesce the replication relationship:

```
snapmirror quiesce -destination-path SVM:volume|cluster://SVM/volume
```

```
cluster_dst:> snapmirror quiesce -destination-path
svm_backup:volA_dst
```

2. Break the replication relationship:

```
snapmirror break -source-path SVM:volume|cluster://SVM/volume, ...
-destination-path SVM:volume|cluster://SVM/volume, ...
```

```
cluster_dst:> snapmirror break -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

3. Delete the replication relationship:

```
snapmirror delete -source-path SVM:volume|cluster://SVM/volume, ...
-destination-path SVM:volume|cluster://SVM/volume, ...
```

For complete command syntax, see the man page.

You must run this command from the destination cluster or destination SVM.

+

The following example deletes the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

+

```
cluster_dst::> snapmirror delete -source-path svm1:volA -destination  
-path svm_backup:volA_dst
```

1. Release replication relationship information from the source SVM:

```
snapmirror release -source-path SVM:volume|cluster://SVM/volume, ...  
-destination-path SVM:volume|cluster://SVM/volume, ...
```

For complete command syntax, see the man page.

You must run this command from the source cluster or source SVM.

+

The following example releases information for the specified replication relationship from the source SVM svm1:

+

```
cluster_src::> snapmirror release -source-path svm1:volA -destination  
-path svm_backup:volA_dst
```

= Manage storage efficiency

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

SnapMirror preserves storage efficiency on the source and destination volumes, with one exception, when postprocess data compression is enabled on the destination. In that case, all storage efficiency is lost on the destination. To correct this issue, you need to disable postprocess compression on the destination, update the relationship manually, and re-enable storage efficiency.

#### What you'll need

- The source and destination clusters and SVMs must be peered.

[Cluster and SVM peering](#)

- You must disable postprocess compression on the destination.

#### About this task

You can use the `volume efficiency show` command to determine whether efficiency is enabled on a volume. For more information, see the man pages.

You can check if SnapMirror is maintaining storage efficiency by viewing the SnapMirror audit logs and locating the transfer description. If the transfer description displays `transfer_desc=Logical Transfer`, SnapMirror is not maintaining storage efficiency. If the transfer description displays `transfer_desc=Logical Transfer with Storage Efficiency`, SnapMirror is maintaining storage efficiency. For example:

```
Fri May 22 02:13:02 CDT 2020 ScheduledUpdate[May 22 02:12:00]:cc0fbc29-  
b665-11e5-a626-00a09860c273 Operation-Uid=39fbcf48-550a-4282-a906-  
df35632c73a1 Group=none Operation-Cookie=0 action=End  
source=<sourcepath> destination=<destpath> status=Success  
bytes_transferred=117080571 network_compression_ratio=1.0:1  
transfer_desc=Logical Transfer - Optimized Directory Mode
```

#### Logical Transfer with storage

Beginning with ONTAP 9.3, manual update is no longer required to re-enable storage efficiency. If

SnapMirror detects that postprocess compression has been disabled, it automatically re-enables storage efficiency at the next scheduled update. Both the source and the destination must be running ONTAP 9.3.

Beginning with ONTAP 9.3, AFF systems manage storage efficiency settings differently from FAS systems after a destination volume is made writeable:

- After you make a destination volume writeable using the `snapmirror break` command, the caching policy on the volume is automatically set to “auto” (the default).

This behavior is applicable to FlexVol volumes, only, and it does not apply to FlexGroup volumes.

- On resync, the caching policy is automatically set to “none”, and deduplication and inline compression are automatically disabled, regardless of your original settings. You must modify the settings manually as needed.

Manual updates with storage efficiency enabled can be time-consuming. You might want to run the operation in off-peak hours.

### Step

1. Update a replication relationship and re-enable storage efficiency:

```
snapmirror update -source-path SVM:volume|cluster://SVM/volume, ...  
-destination-path SVM:volume|cluster://SVM/volume, ... -enable-storage  
-efficiency true
```

For complete command syntax, see the man page.

You must run this command from the destination SVM or the destination cluster. The command fails if a common Snapshot copy does not exist on the source and destination. Use `snapmirror initialize` to re-initialize the relationship.

+

The following example updates the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`, and re-enables storage efficiency:

+

```
cluster_dst::> snapmirror update -source-path svm1:volA -destination  
-path svm_backup:volA_dst -enable-storage-efficiency true
```

= Use SnapMirror global throttling

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Global network throttling is available for all SnapMirror and SnapVault transfers at a per-node level.

#### About this task

SnapMirror global throttling restricts the bandwidth used by incoming and/or outgoing SnapMirror and SnapVault transfers. The restriction is enforced cluster wide on all nodes in the cluster.

For example, if the outgoing throttle is set to 100 Mbps, each node in the cluster will have the outgoing bandwidth set to 100 Mbps. If global throttling is disabled, it is disabled on all nodes.

The throttle has no effect on `volume move` transfers or load-sharing mirror transfers. Although data transfer rates are often expressed in bits per second (bps), the throttle values must be entered in kilobytes per second (KBps).

Global throttling works with the per-relationship throttle feature for SnapMirror and SnapVault transfers. The per-relationship throttle is enforced until the combined bandwidth of per-relationship transfers exceeds the value of the global throttle, after which the global throttle is enforced. A throttle value 0 implies that global throttling is disabled.

SnapMirror global throttling has no effect on SnapMirror Synchronous relationships when they are In-Sync. However, the throttle does effect SnapMirror Synchronous relationships when they perform an asynchronous transfer phase such as an initialization operation or after an Out Of Sync event. For this reason, enabling global throttling with SnapMirror Synchronous relationships is not recommended.

## Steps

1. Enable global throttling:

```
options -option-name replication.throttle.enable on|off
```

The following example shows how to enable SnapMirror global throttling on `cluster_dst`:

```
cluster_dst::> options -option-name replication.throttle.enable on
```

2. Specify the maximum total bandwidth used by incoming transfers on the destination cluster:

```
options -option-name replication.throttle.incoming.max_kbs KBps
```

The recommended minimum throttle bandwidth is 4 KBps and the maximum is up to 2 TBps. The default value for this option is `unlimited`, which means there is no limit on total bandwidth used.

The following example shows how to set the maximum total bandwidth used by incoming transfers to 100 Mbps:

```
cluster_dst::> options -option-name  
replication.throttle.incoming.max_kbs 12500
```

100 Mbps = 12500 KBps



1. Specify the maximum total bandwidth used by outgoing transfers on the source cluster:

```
options -option-name replication.throttle.outgoing.max_kbs KBps
```

KBps is the maximum transfer rate in kilobytes per second. Valid transfer rate values are 1 to 125000. The default value for this option is `unlimited`, which means there is no limit on total bandwidth used.

The following example shows how to set the maximum total bandwidth used by outgoing transfers to 100 Mbps:

```
cluster_src::> options -option-name  
replication.throttle.outgoing.max_kbs 12500
```

= About SnapMirror SVM replication

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use SnapMirror to create a data protection relationship between SVMs. In this type of data protection relationship, all or part of the SVM's configuration, from NFS exports and SMB shares to RBAC, is replicated, as well as the data in the volumes that the SVM owns.

== Supported relationship types

Only data-serving SVMs can be replicated. The following data protection relationship types are supported:

- *SnapMirror DR*, in which the destination typically contains only the Snapshot copies currently on the source.

Beginning with ONTAP 9.9.1, this behavior changes when you are using the mirror-vault policy. Beginning with ONTAP 9.9.1, you can create different Snapshot policies on the source and destination, and the Snapshot copies on the destination are not overwritten by Snapshot copies on the source:

- They are not overwritten from the source to the destination during normal scheduled operations, updates and resync
- They are not deleted during break operations.
- They are not deleted during flip-resync operations.  
When you configure an SVM DR relationship using the mirror-vault policy using ONTAP 9.9.1 and later, the policy behaves as follows:
- User-defined Snapshot copy policies at the source are not copied to the destination.
- System-defined Snapshot copy policies are not copied to the destination.
- Volume association with user and system defined Snapshot policies are not copied to the destination.

SVM.

- Beginning with ONTAP 9.2, *SnapMirror unified replication*, in which the destination is configured for both DR and long-term retention.

Details about these relationship types can be found here: [Understanding SnapMirror volume replication](#).

The *policy type* of the replication policy determines the type of relationship it supports. The following table shows the available policy types.

Policy type	Relationship type
async-mirror	SnapMirror DR
mirror-vault	Unified replication

== XDP replaces DP as the SVM replication default in ONTAP 9.4

Beginning with ONTAP 9.4, SVM data protection relationships default to XDP mode. SVM data protection relationships continue to default to DP mode in ONTAP 9.3 and earlier.

Existing relationships are not affected by the new default. If a relationship is already of type DP, it will continue to be of type DP. The following table shows the behavior you can expect.

If you specify...	The type is...	The default policy (if you do not specify a policy) is...
DP	XDP	MirrorAllSnapshots (SnapMirror DR)
Nothing	XDP	MirrorAllSnapshots (SnapMirror DR)
XDP	XDP	MirrorAndVault (Unified replication)

Details about the changes in the default can be found here: [XDP replaces DP as the SnapMirror default](#).

Version-independence is not supported for SVM replication. In an SVM DR configuration, the destination SVM must be on a cluster running the same ONTAP version as the source SVM cluster to support failover and fail back operations.

## Compatible ONTAP versions for SnapMirror relationships

== How SVM configurations are replicated

The content of an SVM replication relationship is determined by the interaction of the following fields:

- The `-identity-preserve true` option of the `snapmirror create` command replicates the entire SVM configuration.

The `-identity-preserve false` option replicates only the volumes and authentication and authorization configurations of the SVM, and the protocol and name service settings listed in [Configurations replicated in SVM DR relationships](#).

- The `-discard-configs network` option of the `snapmirror policy create` command excludes LIFs and related network settings from SVM replication, for use in cases where the source and destination SVMs are in different subnets.
- The `-vserver-dr-protection unprotected` option of the `volume modify` command excludes the specified volume from SVM replication.

Otherwise, SVM replication is almost identical to volume replication. You can use virtually the same workflow for SVM replication as you use for volume replication.

== Support details

The following table shows support details for SnapMirror SVM replication.

Resource or feature	Support details
Relationship types	<ul style="list-style-type: none"><li>• SnapMirror DR</li><li>• Beginning with ONTAP 9.2, SnapMirror unified replication</li></ul>
Replication scope	Intercluster only. You cannot replicate SVMs in the same cluster.
Version-independence	Not supported.
Deployment types	<ul style="list-style-type: none"><li>• Single source to single destination</li><li>• Beginning with ONTAP 9.4, fan-out. You can fan-out to two destinations only.</li></ul> <p>By default, only one <code>-identity-preserve true</code> relationship is allowed per source SVM.</p>

Volume encryption	<ul style="list-style-type: none"> <li>• Encrypted volumes on the source are encrypted on the destination.</li> <li>• Onboard Key Manager or KMIP servers must be configured on the destination.</li> <li>• New encryption keys are generated at the destination.</li> <li>• If the destination does not contain a node that supports volume .encryption, replication succeeds, but the destination volumes are not encrypted.</li> </ul>
FabricPool	Beginning with ONTAP 9.6, SnapMirror SVM replication is supported with FabricPools.
MetroCluster	<p>Beginning with ONTAP 9.11.1, both sides of a SVM DR relationship within a MetroCluster configuration can act as a source for additional SVM DR configurations.</p> <p>Beginning with ONTAP 9.5, SnapMirror SVM replication is supported on MetroCluster configurations.</p> <ul style="list-style-type: none"> <li>• A MetroCluster configuration cannot be the destination of an SVM DR relationship.</li> <li>• Only an active SVM within a MetroCluster configuration can be the source of an SVM DR relationship.</li> </ul> <p>A source can be a sync-source SVM before switchover or a sync-destination SVM after switchover.</p> <ul style="list-style-type: none"> <li>• When a MetroCluster configuration is in a steady state, the MetroCluster sync-destination SVM cannot be the source of an SVM DR relationship, since the volumes are not online.</li> <li>• When the sync-source SVM is the source of an SVM DR relationship, the source SVM DR relationship information is replicated to the MetroCluster partner.</li> <li>• During the switchover and switchback processes, replication to the SVM DR destination might fail.</li> </ul> <p>However, after the switchover or switchback process completes, the next SVM DR scheduled updates will succeed.</p>

SnapMirror Synchronous

Not supported with SVM DR.

== Configurations replicated in SVM DR relationships

The following table shows the interaction of the `snapmirror create -identity-preserve` option and the `snapmirror policy create -discard-configs network` option:

Configuration replicated		<code>-identity-preserve true</code>		<code>-identity-preserve false</code>
		Policy without <code>-discard -configs network set</code>	Policy with <code>-discard -configs network set</code>	
Network	NAS LIFs	Yes	No	No
	LIF Kerberos configuration	Yes	No	No
	SAN LIFs	No	No	No
	Firewall policies	Yes	Yes	No
	Routes	Yes	No	No
	Broadcast domain	No	No	No
	Subnet	No	No	No
	IPspace	No	No	No

SMB	SMB server	Yes	Yes	No
	Local groups and local user	Yes	Yes	Yes
	Privilege	Yes	Yes	Yes
	Shadow copy	Yes	Yes	Yes
	BranchCache	Yes	Yes	Yes
	Server options	Yes	Yes	Yes
	Server security	Yes	Yes	No
	Home directory, share	Yes	Yes	Yes
	Symlink	Yes	Yes	Yes
	Fpolicy policy, Fsecurity policy, and Fsecurity NTFS	Yes	Yes	Yes
	Name mapping and group mapping	Yes	Yes	Yes
	Audit information	Yes	Yes	Yes
NFS	Export policies	Yes	Yes	No
	Export policy rules	Yes	Yes	No
	NFS server	Yes	Yes	No
RBAC	Security certificates	Yes	Yes	No
	Login user, public key, role, and role configuration	Yes	Yes	Yes
	SSL	Yes	Yes	No

Name services	DNS and DNS hosts	Yes	Yes	No
	UNIX user and UNIX group	Yes	Yes	Yes
	Kerberos realm and Kerberos keyblocks	Yes	Yes	No
	LDAP and LDAP client	Yes	Yes	No
	Netgroup	Yes	Yes	No
	NIS	Yes	Yes	No
	Web and web access	Yes	Yes	No
Volume	Object	Yes	Yes	Yes
	Snapshot copies, Snapshot policy, and autodelete policy	Yes	Yes	Yes
	Efficiency policy	Yes	Yes	Yes
	Quota policy and quota policy rule	Yes	Yes	Yes
	Recovery queue	Yes	Yes	Yes

Root volume	Namespace	Yes	Yes	Yes
	User data	No	No	No
	Qtrees	No	No	No
	Quotas	No	No	No
	File-level QoS	No	No	No
	Attributes: state of the root volume, space guarantee, size, autosize, and total number of files	No	No	No
Storage QoS	QoS policy group	Yes	Yes	Yes
Fibre Channel (FC)		No	No	No
iSCSI		No	No	No
LUNs	Object	Yes	Yes	Yes
	igroups	No	No	No
	portsets	No	No	No
	Serial numbers	No	No	No
SNMP	v3 users	Yes	Yes	No

== SVM DR storage limits

The following table shows the recommended maximum number of volumes and SVM DR relationships supported per storage object. You should be aware that limits are often platform dependent. Refer to the [Hardware Universe](#) to learn the limits for your specific configuration.

Storage object	Limit
SVM	300 Flexible volumes
HA pair	1,000 Flexible Volumes
Cluster	128 SVM DR relationships



= Manage SnapMirror SVM replication

= Replicate SVM configurations

= SnapMirror SVM replication workflow

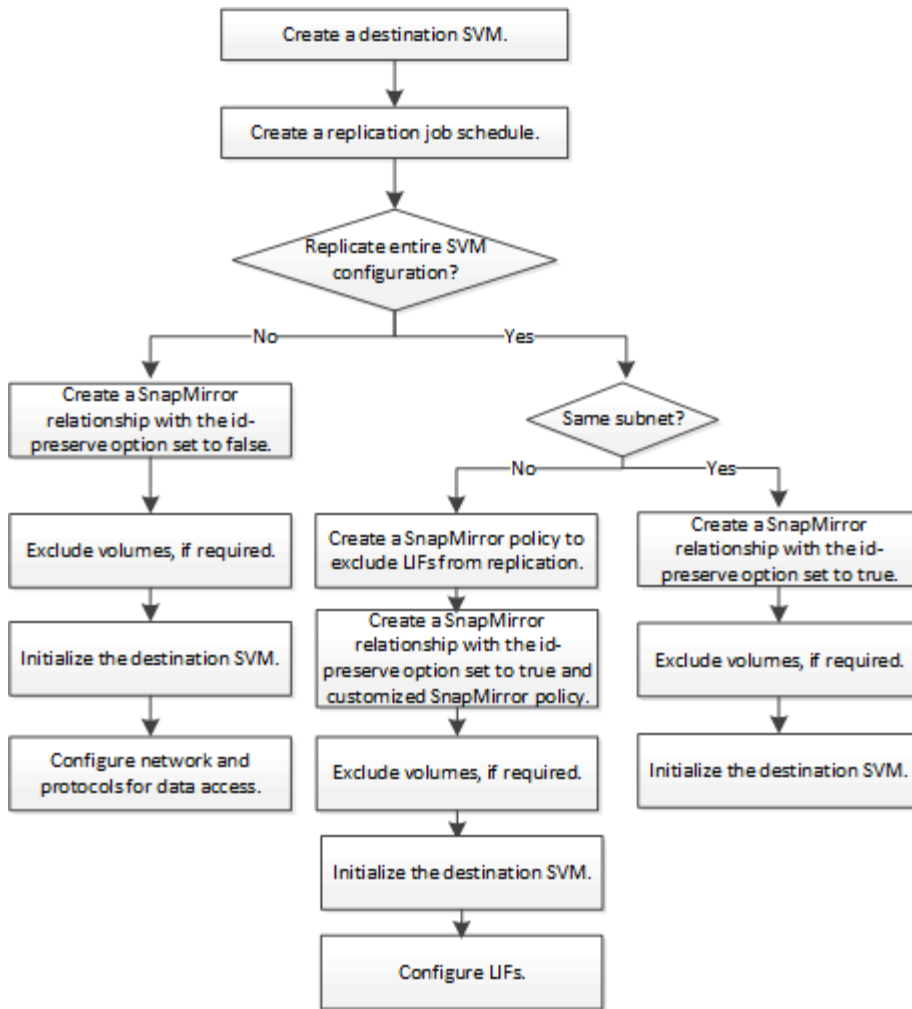
:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

SnapMirror SVM replication involves creating the destination SVM, creating a replication job schedule, and creating and initializing a SnapMirror relationship.

This workflow assumes that you are already using a default policy or a custom replication policy.



= Criteria for placing volumes on destination SVMs

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

When replicating volumes from the source SVM to the destination SVM, it's important to know the criteria for selecting aggregates.

Aggregates are selected based on the following criteria:

- Volumes are always placed on non-root aggregates.
- Non-root aggregates are selected based on the available free space and the number of volumes already hosted on the aggregate.

Aggregates with more free space and fewer volumes are given priority. The aggregate with the highest priority is selected.

- Source volumes on FabricPool aggregates are placed on FabricPool aggregates on the destination with the same tiering-policy.
- If a volume on the source SVM is located on a Flash Pool aggregate, then the volume is placed on a Flash Pool aggregate on the destination SVM, if such an aggregate exists and has enough free space.

- If the `-space-guarantee` option of the volume that is replicated is set to `volume`, only aggregates with free space greater than the volume size are considered.
- The volume size grows automatically on the destination SVM during replication, based on the source volume size.

If you want to pre-reserve the size on the destination SVM, you must resize the volume. The volume size does not shrink automatically on the destination SVM based on the source SVM.

If you want to move a volume from one aggregate to another, you can use the `volume move` command on the destination SVM.

= Replicate an entire SVM configuration

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the `-identity-preserve true` option of the `snapmirror create` command to replicate an entire SVM configuration.

### Before you begin

The source and destination clusters and SVMs must be peered.

For more information, see [Create a cluster peer relationship](#) and [Create an SVM intercluster peer relationship](#).

For complete command syntax, see the man page.

### About this task

This workflow assumes that you are already using a default policy or a custom replication policy.

Beginning with ONTAP 9.9.1, when you use the `mirror-vault` policy, you can create different Snapshot policies on the source and destination SVM, and the Snapshot copies on the destination are not overwritten by Snapshot copies on the source. For more information, see [Understanding SnapMirror SVM replication](#).

### Steps

1. Create a destination SVM:

```
vserver create -vserver SVM_name -subtype dp-destination
```

The SVM name must be unique across the source and destination clusters.

The following example creates a destination SVM named `svm_backup`:

```
cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
```

2. From the destination cluster, create an SVM peer relationship using the `vserver peer create` command.

For more information, see [Create an SVM intercluster peer relationship](#).

### 3. Create a replication job schedule:

```
job schedule cron create -name job_name -month month -dayofweek day_of_week  
-day day_of_month -hour hour -minute minute
```

For `-month`, `-dayofweek`, and `-hour`, you can specify `all` to run the job every month, day of the week, and hour, respectively.

The following example creates a job schedule named `my_weekly` that runs on Saturdays at 3:00 a.m.:

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek  
saturday -hour 3 -minute 0
```

### 4. From the destination SVM or the destination cluster, create a replication relationship:

```
snapmirror create -source-path SVM_name: -destination-path SVM_name: -type  
DP|XDP -schedule schedule -policy policy -identity-preserve true
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options.

+

The following example creates a SnapMirror DR relationship using the default `MirrorAllSnapshots` policy:

+

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAllSnapshots
-identity-preserve true
```

+

The following example creates a unified replication relationship using the default `MirrorAndVault` policy:

+

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAndVault
-identity-preserve true
```

+

Assuming you have created a custom policy with the policy type `async-mirror`, the following example creates a SnapMirror DR relationship:

+

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_mirrored -identity
-preserve true
```

+

Assuming you have created a custom policy with the policy type `mirror-vault`, the following example creates a unified replication relationship:

+

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_unified -identity
-preserve true
```

#### 1. Stop the destination SVM:

```
vserver stop
```

```
SVM name
```

The following example stops a destination SVM named `dvs1`:

```
cluster_dst:> vserver stop -vserver dvs1
```

2. From the destination SVM or the destination cluster, initialize the SVM replication relationship: +

```
snapmirror initialize -source-path SVM_name: -destination-path SVM_name:
```

The following example initializes the relationship between the source SVM, `svm1`, and the destination SVM, `svm_backup`:

```
cluster_dst:> snapmirror initialize -source-path svm1: -destination  
-path svm_backup:
```

= Exclude LIFs and related network settings from SVM replication

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

If the source and destination SVMs are in different subnets, you can use the `-discard-configs network` option of the `snapmirror policy create` command to exclude LIFs and related network settings from SVM replication.

### What you'll need

The source and destination clusters and SVMs must be peered.

For more information, see [Create a cluster peer relationship](#) and [Create an SVM intercluster peer relationship](#).

### About this task

The `-identity-preserve` option of the `snapmirror create` command must be set to `true` when you create the SVM replication relationship.

For complete command syntax, see the man page.

### Steps

1. Create a destination SVM:

```
vserver create -vserver SVM -subtype dp-destination
```

The SVM name must be unique across the source and destination clusters.

The following example creates a destination SVM named `svm_backup`:

```
cluster_dst:> vserver create -vserver svm_backup -subtype dp-  
destination
```

2. From the destination cluster, create an SVM peer relationship using the `vserver peer create` command.

For more information, see [Create an SVM intercluster peer relationship](#).

3. Create a job schedule:

```
job schedule cron create -name job_name -month month -dayofweek day_of_week
-day day_of_month -hour hour -minute minute
```

For `-month`, `-dayofweek`, and `-hour`, you can specify `all` to run the job every month, day of the week, and hour, respectively.

The following example creates a job schedule named `my_weekly` that runs on Saturdays at 3:00 a.m.:

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

4. Create a custom replication policy:

```
snapmirror policy create -vserver SVM -policy policy -type async-
mirror|vault|mirror-vault -comment comment -tries transfer_tries -transfer
-priority low|normal -is-network-compression-enabled true|false -discard
-configs network
```

For complete command syntax, see the man page.

The following example creates a custom replication policy for SnapMirror DR that excludes LIFs:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
DR_exclude_LIFs -type async-mirror -discard-configs network
```

The following example creates a custom replication policy for unified replication that excludes LIFs:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
unified_exclude_LIFs -type mirror-vault -discard-configs network
```

5. From the destination SVM or the destination cluster, run the following command to create a replication relationship:

```
snapmirror create -source-path SVM: -destination-path SVM: -type DP|XDP
-schedule schedule -policy policy -identity-preserve true|false
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the examples below.

+

The following example creates a SnapMirror DR relationship that excludes LIFs:

+

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy DR_exclude_LIFs
-identity-preserve true
```

+

The following example creates a SnapMirror unified replication relationship that excludes LIFs:

+

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy unified_exclude_LIFs
-identity-preserve true
```

#### 1. Stop the destination SVM:

```
vserver stop
```

*SVM name*

The following example stops a destination SVM named dvs1:

```
cluster_dst::> vserver stop -vserver dvs1
```

#### 2. From the destination SVM or the destination cluster, initialize a replication relationship:

```
snapmirror initialize -source-path SVM: -destination-path SVM:
```

For complete command syntax, see the man page.

The following example initializes the relationship between the source, svm1 and the destination, svm\_backup:

```
cluster_dst::> snapmirror initialize -source-path svm1: -destination
-path svm_backup:
```

#### After you finish

You must configure the network and protocols on the destination SVM for data access in the event a disaster occurs.

= Exclude network, name service, and other settings from SVM replication



```
:icons: font
:relative_path: ./data-protection/
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/
```

You can use the `-identity-preserve false` option of the `snapmirror create` command to replicate only the volumes and security configurations of an SVM. Some protocol and name service settings are also preserved.

### What you'll need

The source and destination clusters and SVMs must be peered.

For more information, see [Create a cluster peer relationship](#) and [Create an SVM intercluster peer relationship](#).

### About this task

For a list of preserved protocol and name service settings, see [Configurations replicated in SVM DR relationships](#).

For complete command syntax, see the man page.

### Steps

1. Create a destination SVM:

```
vserver create -vserver SVM -subtype dp-destination
```

The SVM name must be unique across the source and destination clusters.

The following example creates a destination SVM named `svm_backup`:

```
cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
```

2. From the destination cluster, create an SVM peer relationship using the `vserver peer create` command.

For more information, see [Create an SVM intercluster peer relationship](#).

3. Create a replication job schedule:

```
job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute
```

For `-month`, `-dayofweek`, and `-hour`, you can specify `all` to run the job every month, day of the week, and hour, respectively.

The following example creates a job schedule named `my_weekly` that runs on Saturdays at 3:00 a.m.:

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

4. Create a replication relationship that excludes network, name service, and other configuration settings:

```
snapmirror create -source-path SVM: -destination-path SVM: -type DP|XDP
-schedule schedule -policy policy -identity-preserve false
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the examples below. You must run this command from the destination SVM or the destination cluster.

+

The following example creates a SnapMirror DR relationship using the default `MirrorAllSnapshots` policy. The relationship excludes network, name service, and other configuration settings from SVM replication:

+

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAllSnapshots
-identity-preserve false
```

+

The following example creates a unified replication relationship using the default `MirrorAndVault` policy. The relationship excludes network, name service, and other configuration settings:

+

```
cluster_dst:> snapmirror create svm1: -destination-path svm_backup:
-type XDP -schedule my_daily -policy MirrorAndVault -identity-preserve
false
```

+

Assuming you have created a custom policy with the policy type `async-mirror`, the following example creates a SnapMirror DR relationship. The relationship excludes network, name service, and other configuration settings from SVM replication:

+

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_mirrored -identity
-preserve false
```

+

Assuming you have created a custom policy with the policy type `mirror-vault`, the following example creates a unified replication relationship. The relationship excludes network, name service, and other configuration settings from SVM replication:

+

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_unified -identity
-preserve false
```

1. Stop the destination SVM:

```
vserver stop
```

*SVM name*

The following example stops a destination SVM named dvs1:

```
destination_cluster::> vserver stop -vserver dvs1
```

2. If you are using SMB, you must also configure an SMB server.

See [SMB only: Creating an SMB server](#).

3. From the destination SVM or the destination cluster, initialize the SVM replication relationship:

```
snapmirror initialize -source-path SVM_name: -destination-path SVM_name:
```

### After you finish

You must configure the network and protocols on the destination SVM for data access in the event a disaster occurs.

= Specify aggregates to use for SVM DR relationships

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

After a disaster recovery SVM is created, you can use the `aggr-list` option with `vserver modify` command to limit which aggregates are used to host SVM DR destination volumes.

### Step

1. Create a destination SVM:

```
vserver create -vserver SVM -subtype dp-destination
```

2. Modify the disaster recovery SVM's `aggr-list` to limit the aggregates that are used to host the disaster recovery SVM's volume:

```
cluster_dest::> vserver modify -vserver SVM -aggr-list <comma-separated-list>
```

= SMB only: Create a SMB server

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

If the source SVM has an SMB configuration, and you chose to set `identity-preserve` to `false`, you must create a SMB server for the destination SVM. SMB server is required for some SMB configurations, such as shares during initialization of the SnapMirror relationship.

## Steps

1. Start the destination SVM by using the `vserver start` command.

```
destination_cluster::> vserver start -vserver dvs1
[Job 30] Job succeeded: DONE
```

2. Verify that the destination SVM is in the running state and subtype is `dp-destination` by using the `vserver show` command.

```
destination_cluster::> vserver show
```

Vserver	Type	Subtype	Admin State	Operational State	Root Volume
Aggregate					
-----	-----	-----	-----	-----	-----
dvs1	data	dp-destination	running	running	-
-					

3. Create a LIF by using the `network interface create` command.

```
destination_cluster::>network interface create -vserver dvs1 -lif
NAS1 -role data -data-protocol cifs -home-node destination_cluster-
01 -home-port a0a-101 -address 192.0.2.128 -netmask 255.255.255.128
```

4. Create a route by using the `network route create` command.

```
destination_cluster::>network route create -vserver dvs1
-destination 0.0.0.0/0
-gateway 192.0.2.1
```

## Network management

5. Configure DNS by using the `vserver services dns create` command.

```
destination_cluster::>vserver services dns create -domains
mydomain.example.com -vserver
dvs1 -name-servers 192.0.2.128 -state enabled
```

6. Add the preferred domain controller by using the `vserver cifs domain preferred-dc add` command.

```
destination_cluster::>vserver cifs domain preferred-dc add -vserver
dvs1 -preferred-dc
192.0.2.128 -domain mydomain.example.com
```

7. Create the SMB server by using the `vserver cifs create` command.

```
destination_cluster::>vserver cifs create -vserver dvs1 -domain
mydomain.example.com
-cifs-server CIFS1
```

8. Stop the destination SVM by using the `vserver stop` command.

```
destination_cluster::> vserver stop -vserver dvs1
[Job 46] Job succeeded: DONE
```

= Exclude volumes from SVM replication

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

By default, all RW data volumes of the source SVM are replicated. If you do not want to protect all the volumes on the source SVM, you can use the `-vserver-dr -protection unprotected` option of the `volume modify` command to exclude volumes from SVM replication.

### Steps

1. Exclude a volume from SVM replication:

```
volume modify -vserver SVM -volume volume -vserver-dr-protection
unprotected
```

For complete command syntax, see the man page.

The following example excludes the volume `volA_src` from SVM replication:

```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver
-dr-protection unprotected
```

If you later want to include a volume in the SVM replication that you originally excluded, run the following command:

```
volume modify -vserver SVM -volume volume -vserver-dr-protection protected
```

The following example includes the volume `volA_src` in the SVM replication:

```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver  
-dr-protection protected
```

2. Create and initialize the SVM replication relationship as described in [Replicating an entire SVM configuration](#).

= Serve data from an SVM DR destination

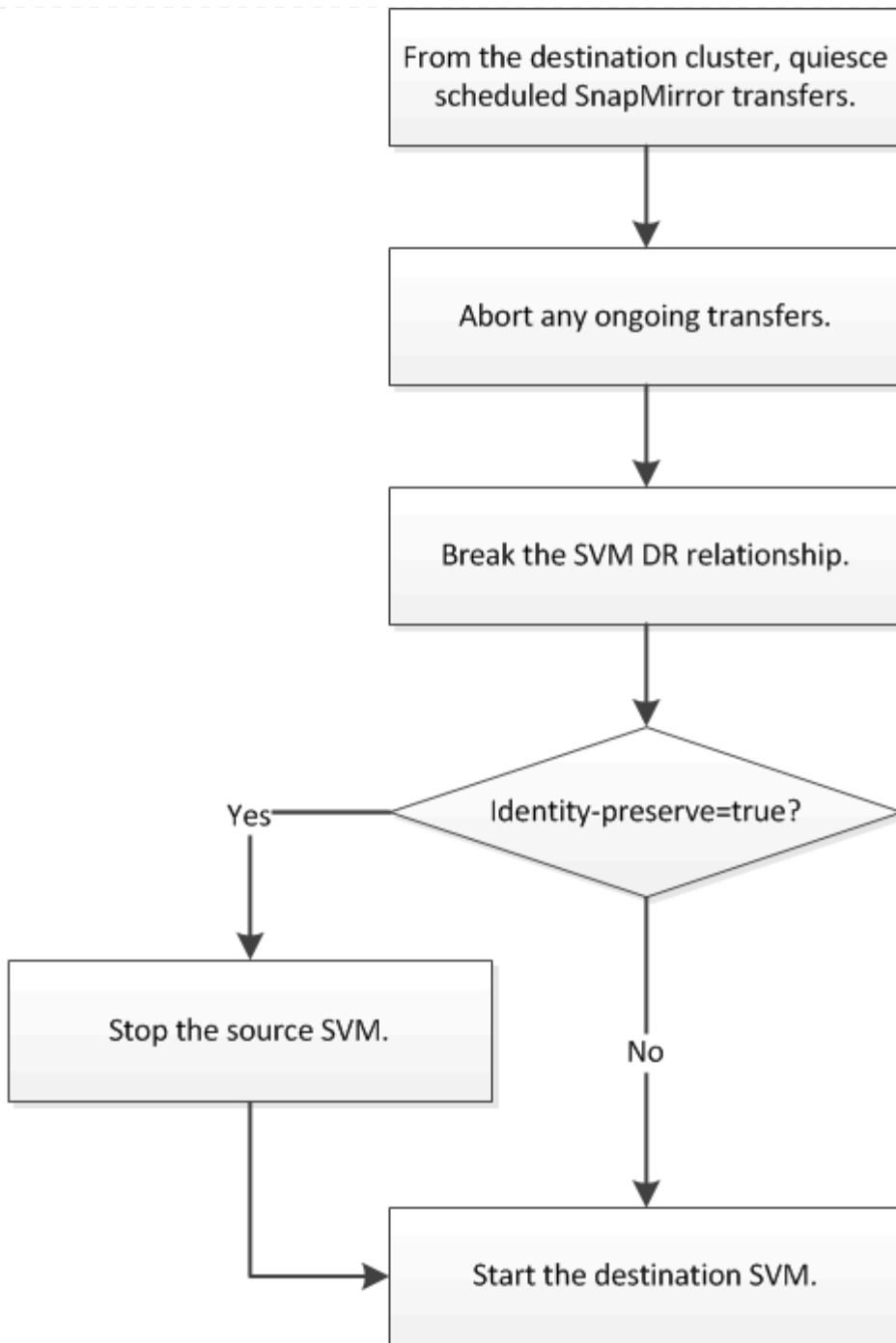
= SVM disaster recovery workflow

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

To recover from a disaster and serve data from the destination SVM, you must activate the destination SVM. Activating the destination SVM involves stopping scheduled SnapMirror transfers, aborting ongoing SnapMirror transfers, breaking the replication relationship, stopping the source SVM, and starting the destination SVM.



= Make SVM destination volumes writeable

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You need to make SVM destination volumes writeable before you can serve data to clients. The procedure is largely identical to the procedure for volume replication, with one exception. If you set `-identity-preserve true` when you created the SVM replication relationship, you must stop the source SVM before activating the destination SVM.

**About this task**



For complete command syntax, see the man page.

In a disaster recovery scenario, you cannot perform a SnapMirror update from the source SVM to the disaster recovery destination SVM because your source SVM and its data will be inaccessible, and because updates since the last resync might be bad or corrupt.

### Steps

1. From the destination SVM or the destination cluster, stop scheduled transfers to the destination:

```
snapmirror quiesce -source-path SVM: -destination-path SVM:
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

+

The following example stops scheduled transfers between the source SVM `svm1` and the destination SVM `svm_backup`:

+

```
cluster_dst::> snapmirror quiesce -source-path svm1: -destination-path  
svm_backup:
```

1. From the destination SVM or the destination cluster, stop ongoing transfers to the destination:

```
snapmirror abort -source-path SVM: -destination-path SVM:
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

+

The following example stops ongoing transfers between the source SVM `svm1` and the destination SVM `svm_backup`:

+

```
cluster_dst::> snapmirror abort -source-path svm1: -destination-path  
svm_backup:
```

1. From the destination SVM or the destination cluster, break the replication relationship:

```
snapmirror break -source-path SVM: -destination-path SVM:
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

+

The following example breaks the relationship between the source SVM `svm1` and the destination SVM `svm_backup`:

+

```
cluster_dst:> snapmirror break -source-path svm1: -destination-path
svm_backup:
```

1. If you set `-identity-preserve true` when you created the SVM replication relationship, stop the source SVM:

```
vserver stop -vserver SVM
```

The following example stops the source SVM `svm1`:

```
cluster_src:> vserver stop svm1
```

2. Start the destination SVM:

```
vserver start -vserver SVM
```

The following example starts the destination SVM `svm_backup`:

```
cluster_dst:> vserver start svm_backup
```

### After you finish

Configure SVM destination volumes for data access, as described in [Configuring the destination volume for data access](#).

= Reactivate the source SVM

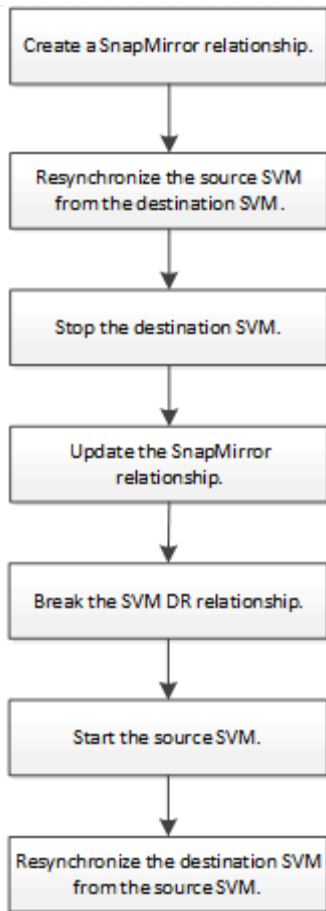
= Source SVM reactivation workflow

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

If the source SVM exists after a disaster, you can reactivate it and protect it by recreating the SVM disaster recovery relationship.



= Reactivate the original source SVM

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can reestablish the original data protection relationship between the source and destination SVM when you no longer need to serve data from the destination. The procedure is largely identical to the procedure for volume replication, with one exception. You must stop the destination SVM before reactivating the source SVM.

### What you'll need

If you have increased the size of destination volume while serving data from it, before you reactivate the source volume, you should manually increase `max-autosize` on the original source volume to ensure it can grow sufficiently.

### When a destination volume grows automatically

### About this task

Beginning with ONTAP 9.11.1, you can reduce resynchronization time during a disaster recovery rehearsal by using the `-quick-resync true` option of the `snapmirror resync` command while performing a reverse resync of an SVM DR relationship. A quick resync can reduce the time it takes to return to production by bypassing the data warehouse rebuild and restore operations.



Quick resync does not preserve the storage efficiency of the destination volumes. Enabling quick resync might increase the volume space used by the destination volumes.

This procedure assumes that the baseline in the original source volume is intact. If the baseline is not intact, you must create and initialize the relationship between the volume you are serving data from and the original source volume before performing the procedure.

For complete command syntax on commands, see the man page.

### Steps

1. From the original source SVM or the original source cluster, create a reverse SVM DR relationship using the same configuration, policy, and identity-preserve setting as the original SVM DR relationship:

```
snapmirror create -source-path SVM: -destination-path SVM:
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

+

The following example creates a relationship between the SVM from which you are serving data, `svm_backup`, and the original source SVM, `svm1`:

+

```
cluster_src::> snapmirror create -source-path svm_backup: -destination  
-path svm1:
```

1. From the original source SVM or the original source cluster, run the following command to reverse the data protection relationship:

```
snapmirror resync -source-path SVM: -destination-path SVM:
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

+

Although `resync` does not require a baseline transfer, it can be time-consuming. You might want to run the `resync` in off-peak hours.

+

The command fails if a common Snapshot copy does not exist on the source and destination. Use `snapmirror initialize` to reinitialize the relationship.

+

The following example reverses the relationship between the original source SVM, `svm1`, and the SVM from which you are serving data, `svm_backup`:

+

```
cluster_src::> snapmirror resync -source-path svm_backup: -destination
-path svm1:
```

+

Example using `-quick-resync` option:

+

```
cluster_src::> snapmirror resync -source-path svm_backup: -destination
-path svm1: -quick-resync true
```

1. When you are ready to reestablish data access to the original source SVM, stop the original destination SVM to disconnect any clients currently connected to the original destination SVM.

```
vserver stop -vserver SVM
```

The following example stops the original destination SVM which is currently serving data:

```
cluster_dst::> vserver stop svm_backup
```

2. Verify that the original destination SVM is in the stopped state by using the `vserver show` command.

```
cluster_dst::> vserver show
```

Vserver	Type	Subtype	Admin State	Operational State	Root Volume
Aggregate					
svm_backup	data	default	stopped	stopped	rv
aggr1					

3. From the original source SVM or the original source cluster, run the following command to perform the final update of the reversed relationship to transfer all changes from the original destination SVM to the original source SVM:

```
snapmirror update -source-path SVM: -destination-path SVM:
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

+

The following example updates the relationship between the original destination SVM from which you are serving data, `svm_backup`, and the original source SVM, `svm1`:

+

```
cluster_src::> snapmirror update -source-path svm_backup: -destination
-path svm1:
```

1. From the original source SVM or the original source cluster, run the following command to stop scheduled transfers for the reversed relationship:

```
snapmirror quiesce -source-path SVM: -destination-path SVM:
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

+

The following example stops scheduled transfers between the SVM you are serving data from, `svm_backup`, and the original SVM, `svm1`:

+

```
cluster_src::> snapmirror quiesce -source-path svm_backup: -destination
-path svm1:
```

1. When the final update is complete and the relationship indicates "Quiesced" for the relationship status, run the following command from the original source SVM or the original source cluster to break the reversed relationship:

```
snapmirror break -source-path SVM: -destination-path SVM:
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

+

The following example breaks the relationship between the original destination SVM from which you were serving data, `svm_backup`, and the original source SVM, `svm1`:

+

```
cluster_src::> snapmirror break -source-path svm_backup: -destination
-path svm1:
```

1. If the original source SVM was previously stopped, from the original source cluster, start the original source SVM:

```
vserver start -vserver SVM
```

The following example starts the original source SVM:

```
cluster_src::> vserver start svm1
```

2. From the original destination SVM or the original destination cluster, reestablish the original data protection relationship:

```
snapmirror resync -source-path SVM: -destination-path SVM:
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

+

The following example reestablishes the relationship between the original source SVM, `svm1`, and the original destination SVM, `svm_backup`:

+

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

1. From the original source SVM or the original source cluster, run the following command to delete the reversed data protection relationship:

```
snapmirror delete -source-path SVM: -destination-path SVM:
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.



+

The following example deletes the reversed relationship between the original destination SVM, `svm_backup`, and the original source SVM, `svm1`:

+

```
cluster_src::> snapmirror delete -source-path svm_backup: -destination  
-path svm1:
```

1. From the original destination SVM or the original destination cluster, release the reversed data protection relationship:

```
snapmirror release -source-path SVM: -destination-path SVM:
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

+

The following example releases the reversed relationship between the original destination SVM, `svm_backup`, and the original source SVM, `svm1`

+

```
cluster_dst::> snapmirror release -source-path svm_backup: -destination
-path svm1:
```

### After you finish

Use the `snapmirror show` command to verify that the SnapMirror relationship was created. For complete command syntax, see the man page.

= Reactivate the original source SVM (FlexGroup volumes only)

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can reestablish the original data protection relationship between the source and destination SVM when you no longer need to serve data from the destination. To reactivate the original source SVM when you are using FlexGroup volumes, you need to perform some additional steps, including deleting the original SVM DR relationship and releasing the original relationship before you reverse the relationship. You also need to release the reversed relationship and recreate the original relationship before stopping scheduled transfers.

### Steps

1. From the original destination SVM or the original destination cluster, delete the original SVM DR relationship:

```
snapmirror delete -source-path SVM: -destination-path SVM:
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

+

The following example deletes the original relationship between the original source SVM, `svm1`, and the original destination SVM, `svm_backup`:

+

```
cluster_dst::> snapmirror delete -source-path svm1: -destination-path
svm_backup:
```

1. From the original source SVM or the original source cluster, release the original relationship while keeping the Snapshot copies intact:

```
snapmirror release -source-path SVM: -destination-path SVM: -relationship
-info-only true
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

+

The following example releases the original relationship between the original source SVM, `svm1`, and the original destination SVM, `svm_backup`.

+

```
cluster_src::> snapmirror release -source-path svm1: -destination-path
svm_backup: -relationship-info-only true
```

1. From the original source SVM or the original source cluster, create a reverse SVM DR relationship using the same configuration, policy, and identity-preserve setting as the original SVM DR relationship:

```
snapmirror create -source-path SVM: -destination-path SVM:
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

+

The following example creates a relationship between the SVM from which you are serving data, `svm_backup`, and the original source SVM, `svm1`:

+

```
cluster_src::> snapmirror create -source-path svm_backup: -destination  
-path svm1:
```

1. From the original source SVM or the original source cluster, run the following command to reverse the data protection relationship:

```
snapmirror resync -source-path SVM: -destination-path SVM:
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

+

Although `resync` does not require a baseline transfer, it can be time-consuming. You might want to run the `resync` in off-peak hours.

+

The command fails if a common Snapshot copy does not exist on the source and destination. Use `snapmirror initialize` to reinitialize the relationship.

+

The following example reverses the relationship between the original source SVM, `svm1`, and the SVM from which you are serving data, `svm_backup`:

+

```
cluster_src::> snapmirror resync -source-path svm_backup: -destination
-path svm1:
```

1. When you are ready to reestablish data access to the original source SVM, stop the original destination SVM to disconnect any clients currently connected to the original destination SVM.

```
vserver stop -vserver SVM
```

The following example stops the original destination SVM which is currently serving data:

```
cluster_dst::> vserver stop svm_backup
```

2. Verify that the original destination SVM is in the stopped state by using the `vserver show` command.

```
cluster_dst::> vserver show
```

Vserver	Type	Subtype	Admin State	Operational State	Root Volume
svm_backup	data	default	stopped	stopped	rv
aggr1					

3. From the original source SVM or the original source cluster, run the following command to perform the final update of the reversed relationship to transfer all changes from the original destination SVM to the original source SVM:

```
snapmirror update -source-path SVM: -destination-path SVM:
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

+

The following example updates the relationship between the original destination SVM from which you are serving data, `svm_backup`, and the original source SVM, `svm1`:

+

```
cluster_src::> snapmirror update -source-path svm_backup: -destination  
-path svm1:
```

1. From the original source SVM or the original source cluster, run the following command to stop scheduled transfers for the reversed relationship:

```
snapmirror quiesce -source-path SVM: -destination-path SVM:
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

+

The following example stops scheduled transfers between the SVM you are serving data from, `svm_backup`, and the original SVM, `svm1`:

+

```
cluster_src::> snapmirror quiesce -source-path svm_backup: -destination  
-path svm1:
```

1. When the final update is complete and the relationship indicates "Quiesced" for the relationship status, run the following command from the original source SVM or the original source cluster to break the reversed relationship:

```
snapmirror break -source-path SVM: -destination-path SVM:
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

+

The following example breaks the relationship between the original destination SVM from which you were serving data, `svm_backup`, and the original source SVM, `svm1`:

+

```
cluster_src::> snapmirror break -source-path svm_backup: -destination
-path svm1:
```

1. If the original source SVM was previously stopped, from the original source cluster, start the original source SVM:

```
vserver start -vserver SVM
```

The following example starts the original source SVM:

```
cluster_src::> vserver start svm1
```

2. From the original source SVM or the original source cluster, delete the reversed SVM DR relationship:

```
snapmirror delete -source-path SVM: -destination-path SVM:
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

+

The following example deletes the reversed relationship between the original destination SVM, `svm_backup`, and the original source SVM, `svm1`:

+

```
cluster_src::> snapmirror delete -source-path svm_backup: -destination
-path svm1:
```

1. From the original destination SVM or the original destination cluster, release the reversed relationship while keeping the Snapshot copies intact:

```
snapmirror release -source-path SVM: -destination-path SVM: -relationship
-info-only true
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

+

The following example releases the reversed relationship between the original destination SVM, `svm_backup`, and the original source SVM, `svm1`:

+

```
cluster_dst::> snapmirror release -source-path svm_backup: -destination
-path svm1: -relationship-info-only true
```

1. From the original destination SVM or the original destination cluster, recreate the original relationship. Use the same configuration, policy, and identity-preserve setting as the original SVM DR relationship:

```
snapmirror create -source-path SVM: -destination-path SVM:
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

+

The following example creates a relationship between the original source SVM, `svm1`, and the original destination SVM, `svm_backup`:

+

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup:
```

1. From the original destination SVM or the original destination cluster, reestablish the original data protection relationship:

```
snapmirror resync -source-path SVM: -destination-path SVM:
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.



+

The following example reestablishes the relationship between the original source SVM, `svm1`, and the original destination SVM, `svm_backup`:

+

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

= Convert volume replication relationships to an SVM replication relationship

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can convert replication relationships between volumes to a replication relationship between the storage virtual machines (SVMs) that own the volumes, provided that each volume on the source (except the root volume) is being replicated, and each volume on the source (including the root volume) has the same name as the volume on the destination.

#### About this task

Use the `volume rename` command when the SnapMirror relationship is idle to rename destination volumes if necessary.

#### Steps

1. From the destination SVM or the destination cluster, run the following command to resync the source and destination volumes:

```
snapmirror resync -source-path SVM:volume -destination-path SVM:volume
-type DP|XDP -schedule schedule -policy policy
```

For complete command syntax, see the man page.

Although `resync` does not require a baseline transfer, it can be time-consuming. You might want to run the `resync` in off-peak hours.

+

The following example resyncs the relationship between the source volume `volA` on `svm1` and the destination volume `volA` on `svm_backup`:

+

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA
```

1. Create an SVM replication relationship between the source and destination SVMs, as described in [Replicating SVM configurations](#).

You must use the `-identity-preserve true` option of the `snapmirror create` command when you create your replication relationship.

2. Stop the destination SVM:

```
vserver stop -vserver SVM
```

For complete command syntax, see the man page.

The following example stops the destination SVM `svm_backup`:

```
cluster_dst::> vserver stop svm_backup
```

3. From the destination SVM or the destination cluster, run the following command to resync the source and destination SVMs:

```
snapmirror resync -source-path SVM: -destination-path SVM: -type DP|XDP
-schedule schedule -policy policy
```

For complete command syntax, see the man page.

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

Although `resync` does not require a baseline transfer, it can be time-consuming. You might want to run the `resync` in off-peak hours.

+

The following example resyncs the relationship between the source SVM `svm1` and the destination SVM `svm_backup`:

+

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

= Delete an SVM replication relationship

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the `snapmirror delete` and `snapmirror release` commands to delete an SVM replication relationship. You can then delete unneeded destination volumes manually.

#### About this task

The `snapmirror release` command deletes any SnapMirror-created Snapshot copies from the source. You can use the `-relationship-info-only` option to preserve the Snapshot copies.

For complete command syntax on commands, see the man page.

#### Steps

1. Run the following command from the destination SVM or the destination cluster to break the replication relationship:

```
snapmirror break -source-path SVM: -destination-path SVM:
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

+

The following example breaks the relationship between the source SVM `svm1` and the destination SVM `svm_backup`:

+

```
cluster_dst::> snapmirror break -source-path svm1: -destination-path
svm_backup:
```

1. Run the following command from the destination SVM or the destination cluster to delete the replication relationship:

```
snapmirror delete -source-path SVM: -destination-path SVM:
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

+

The following example deletes the relationship between the source SVM `svm1` and the destination SVM `svm_backup`:

+

```
cluster_dst::> snapmirror delete -source-path svm1: -destination-path
svm_backup:
```

1. Run the following command from the source cluster or source SVM to release the replication relationship information from the source SVM:

```
snapmirror release -source-path SVM: -destination-path SVM:
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

+

The following example releases information for the specified replication relationship from the source SVM svm1:

+

```
cluster_src::> snapmirror release -source-path svm1: -destination-path  
svm_backup:
```

= Manage SnapMirror root volume replication

= Manage SnapMirror root volume replication overview

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Every SVM in a NAS environment has a unique namespace. The SVM *root volume*, containing operating system and related information, is the entry point to the namespace hierarchy. To ensure that data remains accessible to clients in the event of a node outage or failover, you should create a load-sharing mirror copy of the SVM root volume.

The main purpose of load-sharing mirrors for SVM root volumes is no longer for load sharing; instead, their purpose is for disaster recovery.

- If the root volume is temporarily unavailable, the load-sharing mirror automatically provides read-only access to root volume data.
- If the root volume is permanently unavailable, you can promote one of the load-sharing volumes to provide write access to root volume data.

= Create and initializing load-sharing mirror relationships

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You should create a load-sharing mirror (LSM) for each SVM root volume that serves NAS data in the cluster. You can create the LSM on any node other than the one containing the root volume, such as the partner node in an HA pair, or preferably in a different HA pair. For a two-node cluster, you should create the LSM on the partner of the node with the SVM root volume.

#### About this task

If you create an LSM on the same node, and the node is unavailable, you have a single point of failure, and you do not have a second copy to ensure the data remains accessible to clients. But when you create the LSM on a node other than the one containing the root volume, or on a different HA pair, your data is still accessible in the event of an outage.

For example, in a four-node cluster with a root volume on three nodes:

- For the root volume on HA 1 node 1, create the LSM on HA 2 node 1 or HA 2 node 2.
- For the root volume on HA 1 node 2, create the LSM on HA 2 node 1 or HA 2 node 2.
- For the root volume on HA 2 node 1, create the LSM on HA 1 node 1 or HA 1 node 2.

## Steps

1. Create a destination volume for the LSM:

```
volume create -vserver SVM -volume volume -aggregate aggregate -type DP
-size size
```

The destination volume should be the same or greater in size than the root volume.

It is a best practice to name the root and destination volume with suffixes, such as `_root` and `_m1`.

For complete command syntax, see the man page.

The following example creates a load-sharing mirror volume for the root volume `svm1_root` in `cluster_src`:

```
cluster_src:> volume create -vserver svm1 -volume svm1_m1 -aggregate
aggr_1 -size 1gb -state online -type DP
```

2. Create a replication job schedule, as described in [Creating a replication job schedule](#).
3. Create a load-sharing mirror relationship between the SVM root volume and the destination volume for the LSM:

```
snapmirror create -source-path SVM:volume|cluster://SVM/volume -destination
-path SVM:volume|cluster://SVM/volume -type LS -schedule schedule
```

For complete command syntax, see the man page.

The following example creates a load-sharing mirror relationship between the root volume `svm1_root` and the load-sharing mirror volume `svm1_m1`:

```
cluster_src::> snapmirror create -source-path svm1:svm1_root
-destination-path svm1:svm1_m1 -type LS -schedule hourly
```

The type attribute of the load-sharing mirror changes from `DP` to `LS`.

4. Initialize the load-sharing mirror:

```
snapmirror initialize-ls-set -source-path SVM:volume|cluster://SVM/volume
```

Initialization can be time-consuming. You might want to run the baseline transfer in off-peak hours.

For complete command syntax, see the man page.

The following example initializes the load-sharing mirror for the root volume `svm1_root`:

```
cluster_src::> snapmirror initialize-ls-set -source-path
svml:svml_root
```

= Update a load-sharing mirror relationship

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Load-sharing mirror (LSM) relationships are updated automatically for SVM root volumes after a volume in the SVM is mounted or unmounted, and during `volume create` operations that include the ``junction-path`` option. You can manually update a LSM relationship if you want it updated before the next scheduled update.

Load-sharing mirror relationships update automatically in the following circumstances:

- It's time for a scheduled update
- A mount or unmount operation is performed on a volume in the SVM root volume
- A `volume create` command is issued that includes the `junction-path` option

### Step

1. Update a load-sharing mirror relationship manually:

```
snapmirror update-ls-set -source-path SVM:volume|cluster://SVM/volume
```

The following example updates the load-sharing mirror relationship for the root volume `svml_root`:

```
cluster_src::> snapmirror update-ls-set -source-path svml:svml_root
```

= Promote a load-sharing mirror

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

If a root volume is permanently unavailable, you can promote the load-sharing mirror (LSM) volume to provide write access to root volume data.

### What you'll need

You must use advanced privilege level commands for this task.

### Steps

1. Change to advanced privilege level:

```
set -privilege advanced
```

2. Promote an LSM volume:

```
snapmirror promote -destination-path SVM:volume|cluster://SVM/volume
```

For complete command syntax, see the man page.

The following example promotes the volume `svm1_m2` as the new SVM root volume:

```
cluster_src::*> snapmirror promote -destination-path svm1:svm1_m2
```

```
Warning: Promote will delete the offline read-write volume  
cluster_src://svm1/svm1_root and replace it with  
cluster_src://svm1/svm1_m2. Because the volume is offline,  
it is not possible to determine whether this promote will  
affect other relationships associated with this source.
```

```
Do you want to continue? {y|n}: y
```

Enter `y`. ONTAP makes the LSM volume a read/write volume, and deletes the original root volume if it is accessible.

The promoted root volume might not have all of the data that was in the original root volume if the last update did not occur recently.



1. Return to admin privilege level:

```
set -privilege admin
```

2. Rename the promoted volume following the naming convention you used for the root volume:

```
volume rename -vserver SVM -volume volume -newname new_name
```

The following example renames the promoted volume `svm1_m2` with the name `svm1_root`:

```
cluster_src::> volume rename -vserver svm11 -volume svm1_m2 -newname
svm1_root
```

3. Protect the renamed root volume, as described in step 3 through step 4 in [Creating and initializing load-sharing mirror relationships](#).

= SnapMirror technical details

= Use path name pattern matching

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injpo/source/./encryption-at-rest/./media/

You can use pattern matching to specify the source and destination paths in `snapmirror` commands.

`snapmirror` commands use fully qualified path names in the following format: `vserver:volume`. You can abbreviate the path name by not entering the SVM name. If you do this, the `snapmirror` command assumes the local SVM context of the user.

Assuming that the SVM is called “vserver1” and the volume is called “vol1”, the fully qualified path name is `vserver1:vol1`.

You can use the asterisk (\*) in paths as a wildcard to select matching, fully qualified path names. The following table provides examples of using the wildcard to select a range of volumes.

<code>*</code>	Matches all paths.
<code>vs*</code>	Matches all SVMs and volumes with SVM names beginning with <code>vs</code> .
<code>:*src</code>	Matches all SVMs with volume names containing the <code>src</code> text.
<code>:vol</code>	Matches all SVMs with volume names beginning with <code>vol</code> .

```
vs1::> snapmirror show -destination-path *:*dest*
```

```
Progress
Source          Destination  Mirror      Relationship  Total
Last
Path            Type  Path        State        Status        Progress
Healthy Updated
-----
vs1:sm_src2
                DP    vs2:sm_dest1
                Snapmirrored  Idle          -
true    -
```

= Use extended queries to act on many SnapMirror relationships

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use *extended queries* to perform SnapMirror operations on many SnapMirror relationships at one time. For example, you might have multiple uninitialized SnapMirror relationships that you want to initialize using one command.

### About this task

You can apply extended queries to the following SnapMirror operations:

- Initializing uninitialized relationships
- Resuming quiesced relationships
- Resynchronizing broken relationships
- Updating idle relationships
- Aborting relationship data transfers

### Step

1. Perform a SnapMirror operation on many relationships:

```
snapmirror command {-state state } *
```

The following command initializes SnapMirror relationships that are in an Uninitialized state:

```
vs1::> snapmirror initialize {-state Uninitialized} *
```

= Ensure a common Snapshot copy in a mirror-vault deployment

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the `snapmirror snapshot-owner create` command to preserve a labeled Snapshot copy on the secondary in a mirror-vault deployment. Doing so ensures that a common Snapshot copy exists for the update of the vault relationship.

### About this task

If you use a combination mirror-vault fan-out or cascade deployment, you should keep in mind that updates will fail if a common Snapshot copy does not exist on the source and destination volumes.

This is never an issue for the mirror relationship in a mirror-vault fan-out or cascade deployment, since SnapMirror always creates a Snapshot copy of the source volume before it performs the update.

It might be an issue for the vault relationship, however, since SnapMirror does not create a Snapshot copy of the source volume when it updates a vault relationship. You need to use the `snapmirror snapshot-owner create` to ensure that there is at least one common Snapshot copy on both the source and destination of the vault relationship.

### Steps

1. On the source volume, assign an owner to the labeled Snapshot copy you want to preserve:

```
snapmirror snapshot-owner create -vserver SVM -volume volume -snapshot snapshot -owner owner
```

The following example assigns `ApplicationA` as the owner of the `snap1` Snapshot copy:

```
clust1::> snapmirror snapshot-owner create -vserver vs1 -volume vol1 -snapshot snap1 -owner ApplicationA
```

2. Update the mirror relationship, as described in [Updating a replication relationship manually](#).

Alternatively, you can wait for the scheduled update of the mirror relationship.

3. Transfer the labeled Snapshot copy to the vault destination:

```
snapmirror update -source-path SVM:volume|cluster://SVM/volume, ... -destination-path SVM:volume|cluster://SVM/volume, ... -source-snapshot snapshot
```

For complete command syntax, see the man page.

### The following example transfers the `snap1` Snapshot copy

```
clust1::> snapmirror update -vserver vs1 -volume vol1 -source-snapshot snap1
```

The labeled Snapshot copy will be preserved when the vault relationship is updated.

4. On the source volume, remove the owner from the labeled Snapshot copy:

```
snapmirror snapshot-owner delete -vserver SVM -volume volume -snapshot snapshot -owner owner
```

The following examples removes ApplicationA as the owner of the snap1 Snapshot copy:

```
clust1::> snapmirror snapshot-owner delete -vserver vs1 -volume vol1
-snapshot snap1 -owner ApplicationA
```

= Compatible ONTAP versions for SnapMirror relationships

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You should verify that the source and destination volumes are running compatible ONTAP versions before creating a SnapMirror data protection relationship.

Version-independence is not supported for SVM replication.

== Unified replication relationships

For SnapMirror relationships of type “XDP”, using on premises or Cloud Volumes ONTAP releases:

The asterisk (\*) after the release version indicates a Cloud Volumes ONTAP-only release.

Locate the higher, more recent ONTAP version in the left column, and in the top row locate the lower ONTAP version to determine interoperability. Interoperability is bidirectional.

**Table 2: Interoperability for ONTAP version 9.0 and later**

ONTAP version ...	Interoperates with these previous ONTAP versions...															
	9.12.0*	9.11.1	9.11.0*	9.10.1	9.10.0*	9.9.1	9.9.0*	9.8	9.7	9.6	9.5	9.4	9.3	9.2	9.1	9.0
9.12.0*	Yes	Yes	No	Yes	No	Yes	No	Yes	Yes	No	No	No	No	No	No	No
9.11.1	n/a	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	No	No	No	No	No	No
9.11.0*	n/a	n/a	Yes	Yes	No	Yes	No	Yes	Yes	Yes	No	No	No	No	No	No
9.10.1	n/a	n/a	n/a	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	No	No	No
9.10.0*	n/a	n/a	n/a	n/a	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No	No	No	No
9.9.1	n/a	n/a	n/a	n/a	n/a	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No
9.9.0*	n/a	n/a	n/a	n/a	n/a	n/a	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No
9.8	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Yes	Yes	Yes	Yes	No	Yes	No	No	No
9.7	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Yes	Yes	Yes	No	Yes	No	No	No
9.6	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Yes	Yes	No	Yes	No	Yes	No
9.5	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Yes	Yes	Yes	No	Yes	No
9.4	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Yes	Yes	No	Yes	Yes
9.3	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Yes	Yes	Yes	Yes
9.2	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Yes	Yes	Yes
9.1	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Yes	Yes
9.0	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	Yes

== SnapMirror DR relationships

For SnapMirror relationships of type “DP” and policy type “async-mirror”:

DP-type mirrors cannot be initialized beginning with ONTAP 9.11.1 and will be completely deprecated in a future release. For more information, see [Deprecation of data protection SnapMirror relationships](#).

In the following table, the column on the left indicates the ONTAP version on the source volume, and the top

row indicates the ONTAP versions you can have on your destination volume.

Source	Destination												
	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5	9.4	9.3	9.2	9.1	9.0	
9.11.1	<b>Yes</b>	No	No	No	No	No	No	No	No	No	No	No	No
9.10.1	<b>Yes</b>	<b>Yes</b>	No	No	No	No	No	No	No	No	No	No	No
9.9.1	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	No	No	No	No	No	No	No	No	No	No
9.8	No	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	No	No	No	No	No	No	No	No	No
9.7	No	No	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	No	No	No	No	No	No	No	No
9.6	No	No	No	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	No	No	No	No	No	No	No
9.5	No	No	No	No	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	No	No	No	No	No	No
9.4	No	No	No	No	No	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	No	No	No	No	No
9.3	No	No	No	No	No	No	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	No	No	No	No
9.2	No	No	No	No	No	No	No	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	No	No	No
9.1	No	No	No	No	No	No	No	No	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	No
9.0	No	No	No	No	No	No	No	No	No	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>

Interoperability is not bidirectional.

= SnapMirror limitations

:icons: font

:relative\_path: ./data-protection/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You should be aware of basic SnapMirror limitations before creating a data protection relationship.

- A destination volume can have only one source volume.

A source volume can have multiple destination volumes. The destination volume can be the source volume for any type of SnapMirror replication relationship.

- You can fan out a maximum of eight destination volumes from a single source volume.
- You cannot restore files to the destination of a SnapMirror DR relationship.
- Source or destination SnapVault volumes cannot be 32-bit.
- The source volume for a SnapVault relationship should not be a FlexClone volume.

The relationship will work, but the efficiency offered by FlexClone volumes will not be preserved.

= Archive and compliance using SnapLock technology

= Archive and compliance overview

:icons: font

:relative\_path: ./snaplock/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use NetApp SnapLock technology to retain files in unmodified form for regulatory and governance purposes. It shows you how to commit files and Snapshot copies to “write once, read many” (WORM) storage, and how to set retention periods for WORM-protected data.

You should use these procedures if you want to work with SnapLock in the following ways:

- You want to use the ONTAP command-line interface (CLI), not System Manager or an automated scripting tool.

A limited but important set of SnapLock technology is available in System Manager. You can install SnapLock licenses, set the Compliance Clock, create SnapLock aggregates and volumes, and configure SnapLock volumes.

- You want to create Compliance or Enterprise aggregates to host SnapLock audit log volumes on MetroCluster configurations, with the following limitation:
  - SnapLock Enterprise is supported on mirrored and unmirrored aggregates.
  - SnapLock Compliance is supported on unmirrored aggregates only.

All MetroCluster configurations support mirrored aggregates. See the [ONTAP release notes](#) to determine if your MetroCluster configuration supports unmirrored aggregates.

- You want to use SnapLock Enterprise aggregates with FabricPool.

Beginning with ONTAP 9.8, SnapLock Enterprise aggregates are supported with [FabricPool](#).

- You are not using SAN LUNs

SAN LUNs are not supported on SnapLock volumes. Although it is possible to move SAN LUNs onto a SnapLock volume using legacy technology, this is not a supported operation, nor is any other operation involving SAN LUNs on a SnapLock volume.

- You are not using SMTape.

SMTape is not supported by SnapLock.

- You are not creating Compliance aggregates for array LUNs.

SnapLock Compliance aggregates do not support array LUNs.

- You are not creating Compliance aggregates with the SyncMirror option.

SnapLock Compliance aggregates do not support SyncMirror plexes.

SSDs and Flash Pool aggregates are supported by SnapLock beginning with ONTAP 9.1.



= What SnapLock is

:icons: font

:relative\_path: ./snaplock/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

SnapLock is a high-performance compliance solution for organizations that use WORM storage to retain files in unmodified form for regulatory and governance purposes. A single license entitles you to use SnapLock in strict *Compliance mode*, to satisfy external mandates like SEC Rule 17a-4, and a looser *Enterprise mode*, to meet internally mandated regulations for the protection of digital assets.

== Differences between Compliance and Enterprise modes

SnapLock Compliance and Enterprise modes differ mainly in the level at which each mode protects WORM files:

- Compliance-mode WORM files are protected at the disk level.  
You cannot reinitialize a disk that contains Compliance-mode aggregates.
- Enterprise-mode WORM files are protected at the file level.

A related difference involves how strictly each mode manages file deletes:

- Compliance-mode WORM files cannot be deleted during the retention period.
- Enterprise-mode WORM files can be deleted during the retention period by the compliance administrator, using an audited *privileged delete* procedure.

After the retention period has elapsed, you are responsible for deleting any files you no longer need. Once a file has been committed to WORM, whether under Compliance or Enterprise mode, it cannot be modified, even after the retention period has expired.

You cannot move a WORM file during or after the retention period. You can copy a WORM file, but the copy will not retain its WORM characteristics.

The following table shows the differences between SnapLock Compliance and Enterprise modes:

Capability	SnapLock Compliance	SnapLock Enterprise
Privileged delete	No	Yes
Reinitialize disk	No	Yes
Destroy SnapLock aggregate and volume during retention period	No	Yes, with the exception of the SnapLock audit log volume
Rename an aggregate or volume	No	Yes
Non-NetApp disks	No	Yes (with FlexArray Virtualization)

Use SnapLock volume for audit logging	Yes	Yes, beginning with ONTAP 9.5
---------------------------------------	-----	-------------------------------

== Supported and unsupported features with SnapLock

The following table shows the features that are supported with SnapLock Compliance mode, SnapLock Enterprise mode, or both:

<b>Feature</b>	<b>Supported with SnapLock Compliance</b>	<b>Supported with SnapLock Enterprise</b>
Consistency Groups	No	No
SAN	No	No
SnapMirror Synchronous	No	No
SnapMirror Business Continuity	No	No
Single-file SnapRestore	No	Yes
SnapRestore	No	Yes
FlexClone	You can clone SnapLock volumes, but you cannot clone files on a SnapLock volume.	You can clone SnapLock volumes, but you cannot clone files on a SnapLock volume.
LUNs	No	No
SMTape	No	No

MetroCluster configurations	<p>Yes, under the following conditions:</p> <ul style="list-style-type: none"> <li>• Beginning with ONTAP 9.3, SnapLock Compliance is supported on unmirrored MetroCluster aggregates.</li> <li>• Beginning with ONTAP 9.3, SnapLock Compliance is supported on mirrored aggregates, but only if the aggregate is used to host SnapLock audit log volumes.</li> <li>• SVM-specific SnapLock configurations can be replicated to primary and secondary sites using MetroCluster.</li> </ul>	<p>Yes, under the following conditions:</p> <ul style="list-style-type: none"> <li>• Beginning with ONTAP 9, SnapLock Enterprise aggregates are supported.</li> <li>• Beginning with ONTAP 9.3, SnapLock Enterprise aggregates with privileged delete are supported.</li> <li>• SVM-specific SnapLock configurations can be replicated to both sites using MetroCluster.</li> </ul>
Support FabricPools on SnapLock aggregates	No	<p>Yes, beginning with ONTAP 9.8. However, your account team needs to open a product variance request documenting that you understand that FabricPool data tiered to a public or private cloud is no longer protected by SnapLock because a cloud admin can delete that data.</p>

You should be aware that any data that FabricPool tiers to a public or private cloud is no longer protected by SnapLock because that data can be deleted by a cloud admin.

a|  
FlexGroup volumes

a|  
Yes, beginning with ONTAP 9.11.1; however, the following features are not supported:

- Legal-hold
- Event-based retention
- SnapLock for SnapVault

You should also be aware of the following behaviors:

- The volume compliance clock (VCC) of a FlexGroup volume is determined by the VCC of the root constituent. All non-root constituents will have their VCC closely synced to the root VCC.
- SnapLock configuration properties are set only on the FlexGroup as a whole. Individual constituents cannot have different configuration properties, such as default retention time and autocommit period.

a|  
Yes, beginning with ONTAP 9.11.1; however, the following features are not supported:

- Legal-hold
- Event-based retention
- SnapLock for SnapVault

You should also be aware of the following behaviors:

- The volume compliance clock (VCC) of a FlexGroup volume is determined by the VCC of the root constituent. All non-root constituents will have their VCC closely synced to the root VCC.
- SnapLock configuration properties are set only on the FlexGroup as a whole. Individual constituents cannot have different configuration properties, such as default retention time and autocommit period.

## == MetroCluster configurations and compliance clocks

MetroCluster configurations use two compliance clock mechanisms, the Volume Compliance Clock (VCC) and the System Compliance Clock (SCC). The VCC and SCC are available to all SnapLock configurations. When you create a new volume on a node, its VCC is initialized with the current value of the SCC on that node. After the volume is created, the volume and file retention time is always tracked with the VCC.

When a volume is replicated to another site, its VCC is also replicated. When a volume switchover occurs, from Site A to Site B, for example, the VCC continues to be updated on Site B while the SCC on Site A halts when Site A goes offline.

When Site A is brought back online and the volume switchback is performed, the Site A SCC clock restarts while the VCC of the volume continues to be updated. Because the VCC is continuously updated, regardless of switchover and switchback operations, the file retention times do not depend on SCC clocks and do not stretch.

## == Committing files to WORM

You can use an application to commit files to WORM over NFS or CIFS, or use the SnapLock autocommit feature to commit files to WORM automatically. You can use a *WORM appendable file* to retain data that is written incrementally, like log information.

## == Data protection

SnapLock supports data protection methods that should satisfy most compliance requirements:

- \* You can use SnapLock for SnapVault to WORM-protect Snapshot copies on secondary storage.
- \* You can use SnapMirror to replicate WORM files to another geographic location for disaster recovery.

## == Storage efficiency

Beginning with ONTAP 9.9.1, SnapLock supports storage efficiency features, such as data compaction, cross-volume-deduplication, and adaptive compression for SnapLock volumes and aggregates.

## == 7-Mode Transition

You can use the Copy-Based Transition (CBT) feature of the 7-Mode Transition Tool to migrate SnapLock volumes from 7-Mode to ONTAP. The SnapLock mode of the destination volume, Compliance or Enterprise, must match the SnapLock mode of the source volume. You cannot use Copy-Free Transition (CFT) to migrate SnapLock volumes.

## == Encryption

ONTAP offers both software- and hardware-based encryption technologies for ensuring that data at rest cannot be read if the storage medium is repurposed, returned, misplaced, or stolen.

**Disclaimer:** NetApp cannot guarantee that SnapLock-protected WORM files on self-encrypting drives or volumes will be retrievable if the authentication key is lost or if the number of failed authentication attempts exceeds the specified limit and results in the drive being permanently locked. You are responsible for ensuring against authentication failures.

[NOTE]

Beginning with ONTAP 9.2, encrypted volumes are supported on SnapLock aggregates.

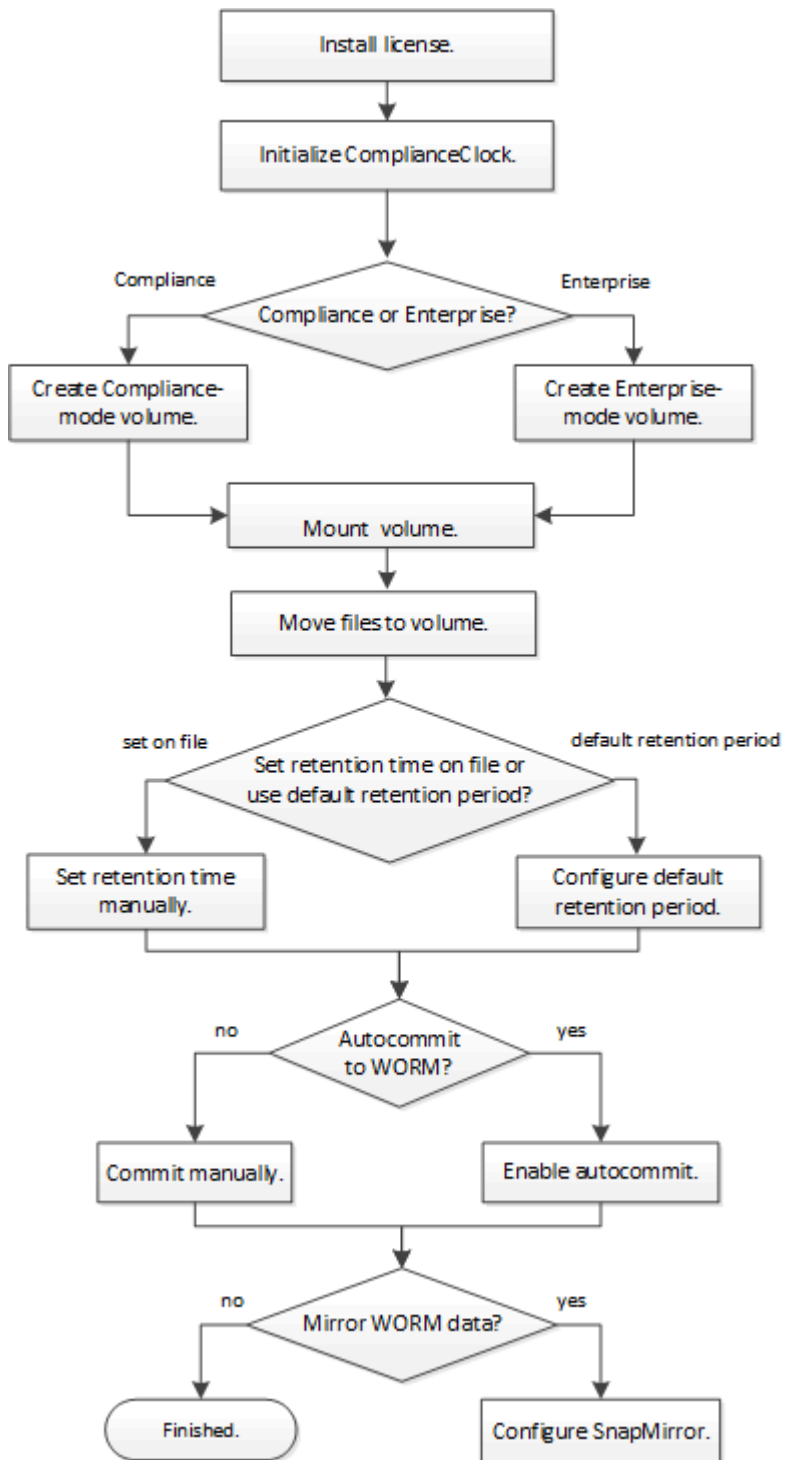
= SnapLock workflow

:icons: font

:relative\_path: ./snaplock/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You specify which SnapLock mode you want to use, Compliance or Enterprise, when you create a SnapLock volume. You typically use a file archiving application to move files from primary storage to the SnapLock volume.



= Configure SnapLock

= Install the license

:icons: font

:relative\_path: ./snaplock/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

A SnapLock license entitles you to use both SnapLock Compliance mode and SnapLock Enterprise mode. SnapLock licenses are issued on a per-node basis. You must install a license for each node that hosts a SnapLock aggregate.

### What you'll need

You must be a cluster administrator to perform this task.

### About this task

You should have received the SnapLock license keys from your sales representative.

### Steps

1. Install the SnapLock license for a node:

```
system license add -license-code license_key
```

The following command installs the license with the key `AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA`.

```
cluster1::> system license add -license-code  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

2. Repeat the previous step for each node license.

= Initialize the ComplianceClock

:icons: font

:relative\_path: ./snaplock/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

The SnapLock ComplianceClock ensures against tampering that might alter the retention period for WORM files. You must initialize the *system ComplianceClock* on each node that hosts a SnapLock aggregate. Once you initialize the ComplianceClock on a node, you cannot initialize it again.

### What you'll need

- You must be a cluster administrator to perform this task.
- The SnapLock license must be installed on the node.

### About this task

The time on the system ComplianceClock is inherited by the *volume ComplianceClock*, which controls the retention period for WORM files on the volume. The volume ComplianceClock is initialized automatically when you create a new SnapLock volume.

The initial setting of the ComplianceClock is based on the current system clock. For that reason, you should



verify that the system time and time zone are correct before initializing the ComplianceClock. Once you initialize the ComplianceClock on a node, you cannot initialize it again.

## Steps

1. Initialize the system ComplianceClock:

```
snaplock compliance-clock initialize -node node_name
```

The following command initializes the system ComplianceClock on node1:

```
cluster1::> snaplock compliance-clock initialize -node node1
```

2. When prompted, confirm that the system clock is correct and that you want to initialize the ComplianceClock:

```
Warning: You are about to initialize the secure ComplianceClock of  
the node "node1" to the current value of the node's system clock.  
This procedure can be performed only once on a given node, so you  
should ensure that the system time is set correctly before  
proceeding.
```

```
The current node's system clock is: Mon Apr 25 06:04:10 GMT 2016
```

```
Do you want to continue? (y|n): y
```

3. Repeat this procedure for each node that hosts a SnapLock aggregate.

= Create a SnapLock aggregate

```
:icons: font
```

```
:relative_path: ./snaplock/
```

```
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/
```

You use the volume `-snaplock-type` option to specify a Compliance or Enterprise SnapLock volume type. For releases earlier than ONTAP 9.10.1, you must create a separate SnapLock aggregate. Beginning with ONTAP 9.10.1, SnapLock and non-SnapLock volumes can exist on the same aggregate; therefore, you are no longer required to create a separate SnapLock aggregate if you are using ONTAP 9.10.1.

### What you'll need

- You must be a cluster administrator to perform this task.
- The SnapLock license must be installed on the node.
- The ComplianceClock on the node must be initialized.
- If you have partitioned the disks as "root", "data1", and "data2", you must ensure that spare disks are available.

### Upgrade considerations

When upgrading to ONTAP 9.10.1, existing SnapLock and non-SnapLock aggregates are upgraded to support the existence of both SnapLock and non-SnapLock volumes; however, the existing SnapLock

volume attributes are not automatically updated. For example, data-compaction, cross-volume-dedupe, and cross-volume-background-dedupe fields remain unchanged. New SnapLock volumes created on existing aggregates have the same default values as non-SnapLock volumes, and the default values for new volumes and aggregates are platform dependent.

### **Revert considerations**

If you need to revert to an ONTAP version earlier than 9.10.1, you must move all SnapLock Compliance, SnapLock Enterprise, and SnapLock volumes to their own SnapLock aggregates.

### **About this task**

- You cannot create Compliance aggregates for FlexArray LUNs, but SnapLock Compliance aggregates are supported with FlexArray LUNs.
- You cannot create Compliance aggregates with the SyncMirror option.
- You can create mirrored Compliance aggregates in a MetroCluster configuration only if the aggregate is used to host SnapLock audit log volumes.

In a MetroCluster configuration, SnapLock Enterprise is supported on mirrored and unmirrored aggregates. SnapLock Compliance is supported only on unmirrored aggregates.

## Steps

1. Create a SnapLock aggregate:

```
storage aggregate create -aggregate aggregate_name -node node_name  
-diskcount number_of_disks -snaplock-type compliance|enterprise
```

The man page for the command contains a complete list of options.

The following command creates a SnapLock Compliance aggregate named `aggr1` with three disks on `node1`:

```
cluster1::> storage aggregate create -aggregate aggr1 -node node1  
-diskcount 3 -snaplock-type compliance
```

= Create a SnapLock volume

:icons: font

:relative\_path: ./snaplock/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You must create a SnapLock volume for the files or Snapshot copies that you want to commit to the WORM state. Beginning with ONTAP 9.10.1, any volume you create, regardless of the aggregate type, is created by default as a non-SnapLock volume. You must use the `-snaplock-type` option to explicitly create a SnapLock volume by specifying either Compliance or Enterprise as the SnapLock type. By default, the SnapLock type is set to `non-snaplock`.

### What you'll need

- The SnapLock aggregate must be online.
- The SnapLock license must be installed on the node.
- The ComplianceClock on the node must be initialized.

### About this task

With the proper SnapLock permissions, you can destroy or rename an Enterprise volume at any time. You cannot destroy a Compliance volume until the retention period has elapsed. You can never rename a Compliance volume.

You can clone SnapLock volumes, but you cannot clone files on a SnapLock volume. The clone volume will be of the same SnapLock type as the parent volume.

LUNs are not supported on SnapLock volumes. Although it is possible to move LUNs onto a SnapLock volume using legacy technology, this is not a supported operation, nor is any other operation involving LUNs on a SnapLock volume.

## Steps

1. Create a SnapLock volume:

```
volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name -snaplock-type compliance|enterprise
```

For a complete list of options, see the man page for the command. The following options are not available for SnapLock volumes: `-nvfail`, `-atime-update`, `-is-autobalance-eligible`, `-space-mgmt-try-first`, and `vmalign`.

The following command creates a SnapLock Compliance volume named `vol1` on `aggr1` on `vs1`:

```
cluster1::> volume create -vserver vs1 -volume vol1 -aggregate aggr1  
-snaplock-type compliance
```

= Mount a SnapLock volume

:icons: font

:relative\_path: ./snaplock/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can mount a SnapLock volume to a junction path in the SVM namespace for NAS client access.

### What you'll need

The SnapLock volume must be online.

### About this task

- You can mount a SnapLock volume only under the root of the SVM.
- You cannot mount a regular volume under a SnapLock volume.

## Steps

1. Mount a SnapLock volume:

```
volume mount -vserver SVM_name -volume volume_name -junction-path path
```

For a complete list of options, see the man page for the command.

The following command mounts a SnapLock volume named `vol1` to the junction path `/sales` in the `vs1` namespace:

```
cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path  
/sales
```

= Set the retention time

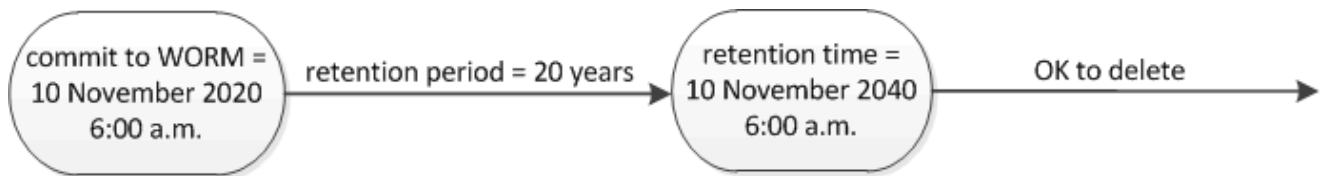
= Set the retention time overview

```
:icons: font
:relative_path: ./snaplock/
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/
```

You can set the retention time for a file explicitly, or you can use the default retention period for the volume to derive the retention time. Unless you set the retention time explicitly, SnapLock uses the default retention period to calculate the retention time.

== About retention period and retention time

The *retention period* for a WORM file specifies the length of time the file must be retained after it is committed to the WORM state. The *retention time* for a WORM file is the time after which the file no longer needs to be retained. A retention period of 20 years for a file committed to the WORM state on 10 November 2020 6:00 a.m., for example, would yield a retention time of 10 November 2040 6:00 a.m.



Beginning with ONTAP 9.10.1, you can set a retention time up to October 26, 3058 and a retention period up to 100 years. When you extend retention dates, older policies are converted automatically. In ONTAP 9.9.1 and earlier releases, unless you set the default retention period to infinite, the maximum supported retention time is January 19 2071 (GMT).

## == Important replication considerations

When establishing a SnapMirror relationship with a SnapLock source volume using a retention date later than January 19th 2071 (GMT), the destination cluster must be running ONTAP 9.10.1 or later or the SnapMirror transfer will fail.

## == Important revert considerations

ONTAP prevents you from reverting a cluster from ONTAP 9.10.1 to an earlier ONTAP version when there are any files with a retention period later than "January 19, 2071 8:44:07 AM".

## == Understanding the default retention periods

A SnapLock Compliance or Enterprise volume has four retention periods:

- Minimum retention period (`min`), with a default of 0
- Maximum retention period (`max`), with a default of 30 years
- Default retention period, with a default equal to `min` for both Compliance mode and Enterprise mode beginning with ONTAP 9.10.1. In ONTAP releases earlier than ONTAP 9.10.1, the default retention period depends on the mode:
  - For Compliance mode, the default is equal to `max`.
  - For Enterprise mode, the default is equal to `min`.
- Unspecified retention period.

Beginning with ONTAP 9.8, you can set the retention period on files in a volume to `unspecified`, to enable the file to be retained until you set an absolute retention time. You can set a file with absolute retention time to unspecified retention and back to absolute retention as long as the new absolute retention time is later than the absolute time you previously set.

So, if you do not set the retention time explicitly before committing a Compliance-mode file to the WORM state, and you do not modify the defaults, the file will be retained for 30 years. Similarly, if you do not set the retention time explicitly before committing an Enterprise-mode file to the WORM state, and you do not modify the defaults, the file will be retained for 0 years, or, effectively, not at all.

= Set the retention time for a file explicitly

```
:icons: font
```

```
:relative_path: ./snaplock/
```

```
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/
```

You can set the retention time for a file explicitly by modifying its last access time. You can use any suitable command or program over NFS or CIFS to modify the last access time.

### **About this task**

After a file has been committed to WORM, you can extend but not shorten the retention time. The retention time is stored in the `atime` field for the file.

You cannot explicitly set the retention time of a file to `infinite`. That value is only available when you use the

default retention period to calculate the retention time.

### Steps

1. Use a suitable command or program to modify the last access time for the file whose retention time you want to set.

In a UNIX shell, use the following command to set a retention time of 21 November 2020 6:00 a.m. on a file named `document.txt`:

```
touch -a -t 202011210600 document.txt
```

You can use any suitable command or program to modify the last access time in Windows.

= Set the default retention period

:icons: font

:relative\_path: ./snaplock/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the `volume snaplock modify` command to set the default retention period for files on a SnapLock volume.

### What you'll need

The SnapLock volume must be online.

### About this task

The following table shows the possible values for the default retention period option:

The default retention period must be greater than or equal to ( $\geq$ ) the minimum retention period and less than or equal to ( $\leq$ ) the maximum retention period.



Value	Unit	Notes
0 - 65535	seconds	
0 - 24	hours	
0 - 365	days	
0 - 12	months	
0 - 100	years	Beginning with ONTAP 9.10.1. For earlier ONTAP releases, the value is 0 - 70.
max	-	Use the maximum retention period.
min	-	Use the minimum retention period.
infinite	-	Retain the files forever.
unspecified	-	Retain the files until an absolute retention period is set.

The values and ranges for the maximum and minimum retention periods are identical, except for `max` and `min`, which are not applicable. For more information about this task, see [Set the retention time overview](#).

You can use the `volume snaplock show` command to view the retention period settings for the volume. For more information, see the man page for the command.

After a file has been committed to the WORM state, you can extend but not shorten the retention period.

### Steps

1. Set the default retention period for files on a SnapLock volume:

```
volume snaplock modify -vserver SVM_name -volume volume_name -default
-retention-period default_retention_period -minimum-retention-period
min_retention_period -maximum-retention-period max_retention_period
```

For a complete list of options, see the man page for the command.

The following examples assume that the minimum and maximum retention periods have not been modified previously.

+

The following command sets the default retention period for a Compliance or Enterprise volume to 20 days:

+

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period 20days
```

+

The following command sets the default retention period for a Compliance volume to 70 years:

+

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -maximum
-retention-period 70years
```

+

The following command sets the default retention period for an Enterprise volume to 10 years:

+

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period max -maximum-retention-period 10years
```

+

The following commands set the default retention period for an Enterprise volume to 10 days:

+

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -minimum
-retention-period 10days
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period min
```

+

The following command sets the default retention period for a Compliance volume to infinite:

+

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period infinite -maximum-retention-period infinite
```

= Verify SnapLock settings

:icons: font

:relative\_path: ./snaplock/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the `volume file fingerprint start` and `volume file fingerprint dump` commands to view key information about files and volumes, including the file type (regular, WORM, or WORM appendable), the volume expiration date, and so forth.

### Steps

1. Generate a file fingerprint:

```
volume file fingerprint start -vserver SVM_name -file file_path
```

```
svml::> volume file fingerprint start -vserver svml -file  
/vol/sle/vol/f1  
File fingerprint operation is queued. Run "volume file fingerprint  
show -session-id 16842791" to view the fingerprint session status.
```

The command generates a session ID that you can use as input to the `volume file fingerprint dump` command.

You can use the `volume file fingerprint show` command with the session ID to monitor the progress of the fingerprint operation. Make sure that the operation has completed before attempting to display the fingerprint.

1. Display the fingerprint for the file:

```
volume file fingerprint dump -session-id session_ID
```

```
svml:> volume file fingerprint dump -session-id 33619976
Vserver:svml
Session-ID:33619976
Volume:slc_vol
Path:/vol/slc_vol/f1
Data
Fingerprint:MOFJVevxNSJm3C/4Bn5oEEYH51CrudOzZYK4r5Cfy1g=Metadata

Fingerprint:8iMjqJXiNcggXT5XuRhLiEwIrJEihDmws0hrexnjgmc=Fingerprint
Algorithm:SHA256
    Fingerprint Scope:data-and-metadata
    Fingerprint Start Time:1460612586
    Formatted Fingerprint Start Time:Thu Apr 14 05:43:06 GMT
2016
    Fingerprint Version:3
    **SnapLock License:available**
    Vserver UUID:acf7ae64-00d6-11e6-a027-0050569c55ae
    Volume MSID:2152884007
    Volume DSID:1028
    Hostname:my_host
    Filer ID:5f18eda2-00b0-11e6-914e-6fb45e537b8d
    Volume Containing Aggregate:slc_aggr1
    Aggregate ID:c84634aa-c757-4b98-8f07-eeefe32565f67
    **SnapLock System ComplianceClock:1460610635
    Formatted SnapLock System ComplianceClock:Thu Apr 14
05:10:35 GMT 2016
    Volume SnapLock Type:compliance
    Volume ComplianceClock:1460610635
    Formatted Volume ComplianceClock:Thu Apr 14 05:10:35 GMT
2016
    Volume Expiry Date:1465880998**
    Is Volume Expiry Date Wraparound:false
    Formatted Volume Expiry Date:Tue Jun 14 05:09:58 GMT 2016
    Filesystem ID:1028
    File ID:96
    File Type:worm
    File Size:1048576
    Creation Time:1460612515
    Formatted Creation Time:Thu Apr 14 05:41:55 GMT 2016
    Modification Time:1460612515
    Formatted Modification Time:Thu Apr 14 05:41:55 GMT 2016
```

```
Changed Time:1460610598
Is Changed Time Wraparound:false
Formatted Changed Time:Thu Apr 14 05:09:58 GMT 2016
Retention Time:1465880998
Is Retention Time Wraparound:false
Formatted Retention Time:Tue Jun 14 05:09:58 GMT 2016
Access Time:-
Formatted Access Time:-
Owner ID:0
Group ID:0
Owner SID:-
Fingerprint End Time:1460612586
Formatted Fingerprint End Time:Thu Apr 14 05:43:06 GMT 2016
```

= Reset the ComplianceClock for an NTP-configured system

:icons: font

:relative\_path: ./snaplock/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

When the SnapLock secure clock daemon detects a skew beyond the threshold, the system time is used to reset both the system and volume ComplianceClocks.

#### What you'll need

- This feature is available only at the advanced privilege level.
- You must be a cluster administrator to perform this task.
- The SnapLock license must be installed on the node.
- This feature is available only for Cloud Volumes ONTAP, ONTAP Select, and VSIM platforms.

#### About this task

When the SnapLock secure clock daemon detects a skew beyond the threshold, the system time is used to reset both the system and volume ComplianceClocks. A period of 24 hours is set as the skew threshold. This means that the system ComplianceClock is synchronized to the system clock only if the skew is more than a day old.

The SnapLock secure clock daemon detects a skew and changes the ComplianceClock to the system time. Any attempt at modifying the system time to force the ComplianceClock to synchronize to the system time fails, since the ComplianceClock synchronizes to the system time only if the system time is synchronized with the NTP time.

#### Steps

1. Enable the SnapLock ComplianceClock time synchronization feature when an NTP server is configured:

```
snaplock compliance-clock ntp
```

The following command enables the system ComplianceClock time synchronization feature:

```
cluster1::*> snaplock compliance-clock ntp modify -is-sync-enabled
true
```

2. When prompted, confirm that the configured NTP servers are trusted and that the communications channel is secure to enable the feature:
3. Check that the feature is enabled:

#### **snaplock compliance-clock ntp show**

The following command checks that the system ComplianceClock time synchronization feature is enabled:

```
cluster1::*> snaplock compliance-clock ntp show

Enable clock sync to NTP system time: true
```

= Commit files to WORM

= Commit files to WORM manually

:icons: font

:relative\_path: ./snaplock/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You commit a file to WORM manually by making the file read-only. You can use any suitable command or program over NFS or CIFS to change the read-write attribute of a file to read-only.

#### **What you'll need**

- The file you want to commit must reside on a SnapLock volume.
- The file must be writable.

#### **About this task**

The volume ComplianceClock time is written to the `ctime` field of the file when the command or program is executed. The ComplianceClock time determines when the retention time for the file has been reached.

#### **Steps**

1. Use a suitable command or program to change the read-write attribute of a file to read-only.

In a UNIX shell, use the following command to make a file named `document.txt` read-only:

```
chmod -w document.txt
```

In a Windows shell, use the following command to make a file named `document.txt` read-only:

```
attrib +r document.txt
```

= Autocommit files to WORM

:icons: font

:relative\_path: ./snaplock/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

The SnapLock autocommit feature enables you to commit files to WORM automatically.

#### What you'll need

- The files you want to autocommit must reside on a SnapLock volume.
- The SnapLock volume must be online.
- The SnapLock volume must be a read-write volume.

The SnapLock autocommit feature scans through all of the files in the volume and commits a file if it meets the autocommit requirement. There might be a time interval between when the file is ready for autocommit and when it is actually committed by the SnapLock autocommit scanner. However, the file is still protected from modifications and deletion by the file system as soon as it is eligible for autocommit.

#### About this task

The *autocommit period* specifies the amount of time that files must remain unchanged before they are autocommitted. Changing a file before the autocommit period has elapsed restarts the autocommit period for the file.

The following table shows the possible values for the autocommit period:

Value	Unit	Notes
none	-	The default.
5 - 5256000	minutes	-
1 - 87600	hours	-
1 - 3650	days	-
1 - 120	months	-
1 - 10	years	-

The minimum value is 5 minutes and the maximum value is 10 years.

## Steps

1. Autocommit files on a SnapLock volume to WORM:

```
volume snaplock modify -vserver SVM_name -volume volume_name -autocommit  
-period autocommit_period
```

For a complete list of options, see the man page for the command.

The following command autocommits the files on volume `vol1` of SVM `vs1`, as long as the files remain unchanged for 5 hours:

```
cluster1:>volume snaplock modify -vserver vs1 -volume vol1  
-autocommit-period 5hours
```

= Use a command or program to create a WORM appendable file

:icons: font

:relative\_path: ./snaplock/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use any suitable command or program over NFS or CIFS to create a WORM appendable file. A WORM appendable file retains data written incrementally, like log entries. Data is appended to the file in 256 KB chunks. As each chunk is written, the previous chunk becomes WORM-protected. You cannot delete the file until the retention period has elapsed.

## What you'll need

The WORM appendable file must reside on a SnapLock volume.

## About this task

Data does not have to be written sequentially to the active 256 KB chunk. When data is written to byte  $n \times 256KB + 1$  of the file, the previous 256 KB segment becomes WORM-protected.

## Steps

1. Use a suitable command or program to create a zero-length file with the desired retention time.

In a UNIX shell, use the following command to set a retention time of 21 November 2020 6:00 a.m. on a zero-length file named `document.txt`:

```
touch -a -t 202011210600 document.txt
```

2. Use a suitable command or program to change the read-write attribute of the file to read-only.

In a UNIX shell, use the following command to make a file named `document.txt` read-only:

```
chmod 444 document.txt
```



3. Use a suitable command or program to change the read-write attribute of the file back to writable.

This step is not deemed a compliance risk because there is no data in the file.

+

In a UNIX shell, use the following command to make a file named `document.txt` writable:

+

```
chmod 777 document.txt
```

1. Use a suitable command or program to start writing data to the file.

In a UNIX shell, use the following command to write data to `document.txt`:

```
echo test data >> document.txt
```

Change the file permissions back to read-only when you no longer need to append data to the file.

= Use volume append mode to create WORM appendable files

:icons: font

:relative\_path: ./snaplock/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.3, you can use the SnapLock *volume append mode* (VAM) feature to create WORM appendable files by default. A WORM appendable file retains data written incrementally, like log entries. Data is appended to the file in 256 KB chunks. As each chunk is written, the previous chunk becomes WORM-protected. You cannot delete the file until the retention period has elapsed.

#### What you'll need

- The WORM appendable file must reside on a SnapLock volume.
- The SnapLock volume must be unmounted and empty of Snapshot copies and user-created files.

#### About this task

Data does not have to be written sequentially to the active 256 KB chunk. When data is written to byte  $n \times 256\text{KB} + 1$  of the file, the previous 256 KB segment becomes WORM-protected.

If you specify an autocommit period for the volume, WORM appendable files that are not modified for a period greater than the autocommit period are committed to WORM.

VAM is not supported on SnapLock audit log volumes.

## Steps

1. Enable VAM:

```
volume snaplock modify -vserver SVM_name -volume volume_name -is-volume-append-mode-enabled true|false
```

For a complete list of options, see the man page for the command.

The following command enables VAM on volume `vol1` of SVM`vs1`:

```
cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -is-volume-append-mode-enabled true
```

2. Use a suitable command or program to create files with write permissions.

The files are WORM-appendable by default.

= Commit Snapshot copies to WORM

:icons: font

:relative\_path: ./snaplock/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use SnapLock for SnapVault to WORM-protect Snapshot copies on secondary storage. You perform all of the basic SnapLock tasks on the SnapVault destination. The destination volume is automatically mounted read-only, so there is no need to explicitly commit the Snapshot copies to WORM; therefore, creating scheduled Snapshot copies on the destination volume using SnapMirror policies is not supported.

### Before you begin

- The source cluster must be running ONTAP 8.2.2 or later.
- The source and destination aggregates must be 64-bit.
- The source volume cannot be a SnapLock volume.
- The source and destination volumes must be created in peered clusters with peered SVMs.

For more information, see [Cluster Peering](#).

- If volume autogrow is disabled, the free space on the destination volume must be at least five percent more than the used space on the source volume.

### About this task

The source volume can use NetApp or non-NetApp storage. For non-NetApp storage, you must use FlexArray Virtualization.



You cannot rename a Snapshot copy that is committed to the WORM state.

You can clone SnapLock volumes, but you cannot clone files on a SnapLock volume.



LUNs are not supported on SnapLock volumes. Although it is possible to move LUNs onto a SnapLock volume using legacy technology, this is not a supported operation, nor is any other operation involving LUNs on a SnapLock volume.

For MetroCluster configurations, you should be aware of the following:

- You can create a SnapVault relationship only between sync-source SVMs, not between a sync-source SVM and a sync-destination SVM.
- You can create a SnapVault relationship from a volume on a sync-source SVM to a data-serving SVM.
- You can create a SnapVault relationship from a volume on a data-serving SVM to a DP volume on a sync-source SVM.

The following illustration shows the procedure for initializing a SnapVault relationship:

### Steps

1. Identify the destination cluster.
2. On the destination cluster, install the SnapLock license, initialize the ComplianceClock, and, if you are using an ONTAP release earlier than 9.10.1, create a SnapLock aggregate, as described in [SnapLock workflow](#).
3. On the destination cluster, create a SnapLock destination volume of type DP that is either the same or greater in size than the source volume:

```
volume create -vserver SVM_name -volume volume_name -aggregate  
aggregate_name -snaplock-type compliance|enterprise -type DP -size size
```

Beginning with ONTAP 9.10.1, SnapLock and non-SnapLock volumes can exist on the same aggregate; therefore, you are no longer required to create a separate SnapLock aggregate if you are using ONTAP 9.10.1. You use the volume `-snaplock-type` option to specify a Compliance or Enterprise SnapLock volume type. In ONTAP releases earlier than ONTAP 9.10.1, the SnapLock mode, Compliance or Enterprise, is inherited from the aggregate. Version-flexible destination volumes are not supported. The language setting of the destination volume must match the language setting of the source volume.

+

The following command creates a 2 GB SnapLock Compliance volume named `dstvolB` in `SVM2` on the aggregate `node01_aggr`:

+

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate  
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

1. On the destination cluster, set the default retention period, as described in [Set the default retention period](#).

A SnapLock volume that is a vault destination has a default retention period assigned to it. The value for this period is initially set to a minimum of 0 years for SnapLock Enterprise volumes and a maximum of 30 years for

SnapLock Compliance volumes. Each NetApp Snapshot copy is committed with this default retention period at first. The retention period can be extended later, if needed. For more information, see [Set retention time overview](#).

1. [Create a new replication relationship](#) between the non-SnapLock source and the new SnapLock destination you created in Step 3.

This example creates a new SnapMirror relationship with destination SnapLock volume `dstvolB` using a policy of `XDPDefault` to vault Snapshot copies labeled daily and weekly on an hourly schedule:

```
cluster2::> snapmirror create -source-path SVM1:srcvolA -destination  
-path SVM2:dstvolB -vserver SVM2 -policy XDPDefault -schedule hourly
```

[Create a custom replication policy](#) or a [custom schedule](#) if the available defaults are not suitable.

1. On the destination SVM, initialize the SnapVault relationship created in Step 5:

```
snapmirror initialize -destination-path destination_path
```

The following command initializes the relationship between the source volume `srcvolA` on SVM1 and the destination volume `dstvolB` on SVM2:

```
cluster2::> snapmirror initialize -destination-path SVM2:dstvolB
```

2. After the relationship is initialized and idle, use the `snapshot show` command on the destination to verify the SnapLock expiry time applied to the replicated Snapshot copies.

This example lists the Snapshot copies on volume `dstvolB` that have the SnapMirror label and the SnapLock expiration date:

```
cluster2::> snapshot show -vserver SVM2 -volume dstvolB -fields  
snapmirror-label, snaplock-expiry-time
```

## Related information

[Cluster and SVM peering](#)

[Volume backup using SnapVault](#)

= Mirror WORM files

:icons: font

:relative\_path: ./snaplock/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use SnapMirror to replicate WORM files to another geographic location for disaster recovery and other purposes. Both the source volume and destination volume must be configured for SnapLock, and both volumes must have the same SnapLock mode, Compliance or Enterprise. All key SnapLock properties of the volume and files are replicated.

## Prerequisites

The source and destination volumes must be created in peered clusters with peered SVMs. For more information, see [Cluster and SVM peering](#).

## About this task

- Beginning with ONTAP 9.5, you can replicate WORM files with the XDP (extended data protection) type SnapMirror relationship rather than the DP (data protection) type relationship. XDP mode is ONTAP version-independent, and is able to differentiate files stored in the same block, making it much easier to resync replicated Compliance-mode volumes. For information on how to convert an existing DP-type relationship to an XDP-type relationship, see [Data Protection](#).
- A resync operation on a DP type SnapMirror relationship fails for a Compliance-mode volume if SnapLock determines that it will result in a loss of data. If a resync operation fails, you can use the `volume clone create` command to make a clone of the destination volume. You can then resync

the source volume with the clone.

- A SnapMirror relationship of type XDP between SnapLock compliant volumes supports a resync after a break even if data on the destination has diverged from the source post the break.

On a resync, when data divergence is detected between the source the destination beyond the common snapshot, a new snapshot is cut on the destination to capture this divergence. The new snapshot and the common snapshot are both locked with a retention time as follows:

- The volume expiry time of the destination
- If the volume expiry time is in the past or has not been set, then the snapshot is locked for a period of 30 days
- If the destination has legal-holds, the actual volume expiry period is masked and shows up as 'indefinite', however the snapshot is locked for the duration of the actual volume expiry period.

If the destination volume has an expiry period that is later than the source, the destination expiry period is retained and will not be overwritten by the expiry period of the source volume post the resync.

If the destination has legal-holds placed on it that differ from the source, a resync is not allowed. The source and destination must have identical legal-holds or all legal-holds on the destination must be released before a resync is attempted.

A locked snapshot on the destination volume created to capture the divergent data can be copied to the source by running the `snapmirror update -s snapshot` command. The snapshot once copied will continue to be locked at the source as well.

- SVM data protection relationships are not supported.
- Load-sharing data protection relationships are not supported.

The following illustration shows the procedure for initializing a SnapMirror relationship:

### Steps

1. Identify the destination cluster.
2. On the destination cluster, install the SnapLock license, initialize the ComplianceClock, and, if you are using an ONTAP release earlier than 9.10.1, create a SnapLock aggregate.
3. On the destination cluster, create a SnapLock destination volume of type DP that is either the same size as or greater in size than the source volume:

```
volume create -vserver SVM_name -volume volume_name -aggregate  
aggregate_name -snaplock-type compliance|enterprise -type DP -size size
```

Beginning with ONTAP 9.10.1, SnapLock and non-SnapLock volumes can exist on the same aggregate; therefore, you are no longer required to create a separate SnapLock aggregate if you are using ONTAP 9.10.1. You use the volume `-snaplock-type` option to specify a Compliance or Enterprise SnapLock volume type. In ONTAP releases earlier than ONTAP 9.10.1, the SnapLock mode—Compliance or Enterprise—is inherited from the aggregate. Version-flexible destination volumes are not supported. The language setting of the destination volume must match the language setting of the source volume.

+

The following command creates a 2 GB SnapLock Compliance volume named `dstvolB` in SVM2 on the aggregate `node01_aggr`:

+

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

1. On the destination SVM, create a SnapMirror policy:

```
snapmirror policy create -vserver SVM_name -policy policy_name
```

The following command creates the SVM-wide policy `SVM1-mirror`:

```
SVM2::> snapmirror policy create -vserver SVM2 -policy SVM1-mirror
```

2. On the destination SVM, create a SnapMirror schedule:

```
job schedule cron create -name schedule_name -dayofweek day_of_week -hour
hour -minute minute
```

The following command creates a SnapMirror schedule named `weekendcron`:

```
SVM2::> job schedule cron create -name weekendcron -dayofweek
"Saturday, Sunday" -hour 3 -minute 0
```

3. On the destination SVM, create a SnapMirror relationship:

```
snapmirror create -source-path source_path -destination-path
destination_path -type XDP|DP -policy policy_name -schedule schedule_name
```

The following command creates a SnapMirror relationship between the source volume `srcvolA` on SVM1 and the destination volume `dstvolB` on SVM2, and assigns the policy `SVM1-mirror` and the schedule `weekendcron`:

```
SVM2::> snapmirror create -source-path SVM1:srcvolA -destination
-path SVM2:dstvolB -type XDP -policy SVM1-mirror -schedule
weekendcron
```

The XDP type is available in ONTAP 9.5 and later. You must use the DP type in ONTAP 9.4 and earlier.

1. On the destination SVM, initialize the SnapMirror relationship:

```
snapmirror initialize -destination-path destination_path
```

The initialization process performs a *baseline transfer* to the destination volume. SnapMirror makes a Snapshot copy of the source volume, then transfers the copy and all the data blocks that it references to the destination volume. It also transfers any other Snapshot copies on the source volume to the destination volume.

The following command initializes the relationship between the source volume `srcvolA` on SVM1 and the destination volume `dstvolB` on SVM2:

```
SVM2::> snapmirror initialize -destination-path SVM2:dstvolB
```

### Related information

[Cluster and SVM peering](#)

[Volume disaster recovery preparation](#)

[Data protection](#)

= Create an audit log

:icons: font

:relative\_path: ./snaplock/

:imagesdir: /tmp/d20221026-17026-1injpo/source/./encryption-at-rest/./media/

You must create a SnapLock-protected audit log before performing a privileged delete or SnapLock volume move. The audit log records the creation and deletion of SnapLock administrator accounts, modifications to the log volume, whether privileged delete is enabled, privileged delete operations, and SnapLock volume move operations.

### What you'll need

You must be a cluster administrator to create a SnapLock aggregate.

### About this task

You cannot delete an audit log until the log file retention period has elapsed. You cannot modify an audit log even after the retention period has elapsed. This is true for both SnapLock Compliance and Enterprise modes.

In ONTAP 9.4 and earlier, you cannot use a SnapLock Enterprise volume for audit logging. You must use a SnapLock Compliance volume. In ONTAP 9.5 and later, you can use either a SnapLock Enterprise volume or a SnapLock Compliance volume for audit logging. In all cases, the audit log volume must be mounted at the junction path `/snaplock_audit_log`. No other volume can use this junction path.



You can find the SnapLock audit logs in the `/snaplock_log` directory under the root of the audit log volume, in subdirectories named `privdel_log` (privileged delete operations) and `system_log` (everything else). Audit log file names contain the timestamp of the first logged operation, making it easy to search for records by the approximate time that operations were executed.

- You can use the `snaplock log file show` command to view the log files on the audit log volume.
- You can use the `snaplock log file archive` command to archive the current log file and create a new one, which is useful in cases where you need to record audit log information in a separate file.

For more information, see the man pages for the commands.

A data protection volume cannot be used as a SnapLock audit log volume.

### Steps

1. Create a SnapLock aggregate.

[Create a SnapLock aggregate](#)

2. On the SVM that you want to configure for audit logging, create a SnapLock volume.

[Create a SnapLock volume](#)

3. Configure the SVM for audit logging:

```
snaplock log create -vserver SVM_name -volume snaplock_volume_name -max  
-file-size size -retention-period default_retention_period
```

The minimum default retention period for audit log files is six months. If the retention period of an affected file is longer than the retention period of the audit log, the retention period of the log inherits the retention period of the file. So, if the retention period for a file deleted using privileged delete is 10 months, and the retention period of the audit log is 8 months, the retention period of the log is extended to 10 months.

+

The following command configures SVM1 for audit logging using the SnapLock volume logVol. The audit log has a maximum size of 20 GB and is retained for eight months.

+

```
SVM1::> snaplock log create -vserver SVM1 -volume logVol -max-file-size 20GB -retention-period 8months
```

1. On the SVM that you configured for audit logging, mount the SnapLock volume at the junction path /snaplock\_audit\_log.

### Mount a SnapLock volume

= Use the privileged delete feature

= Create a SnapLock administrator account

:icons: font

:relative\_path: ./snaplock/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You must have SnapLock administrator privileges to perform a privileged delete. These privileges are defined in the vsadmin-snaplock role. If you have not already been assigned that role, you can ask your cluster administrator to create an SVM administrator account with the SnapLock administrator role.

### What you'll need

- You must be a cluster administrator to perform this task.
- You must have logged in on a secure connection (SSH, console, or ZAPI).

### Steps

1. Create an SVM administrator account with the SnapLock administrator role:

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name -application application -authmethod authentication_method -role role -comment comment
```

The following command enables the SVM administrator account SnapLockAdmin with the predefined vsadmin-snaplock role to access SVM1 using a password:

```
cluster1::> security login create -vserver SVM1 -user-or-group-name SnapLockAdmin -application ssh -authmethod password -role vsadmin-snaplock
```

= Enable the privileged delete feature

:icons: font

:relative\_path: ./snaplock/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You must explicitly enable the privileged delete feature on the Enterprise volume that contains the WORM files you want to delete.

**About this task**

The value of the `-privileged-delete` option determines whether privileged delete is enabled.

Possible values are `enabled`, `disabled`, and `permanently-disabled`.

`permanently-disabled` is the terminal state. You cannot enable privileged delete on the volume after you set the state to `permanently-disabled`.

## Steps

1. Enable privileged delete for a SnapLock Enterprise volume:

```
volume snaplock modify -vserver SVM_name -volume volume_name -privileged  
-delete disabled|enabled|permanently-disabled
```

The following command enables the privileged delete feature for the Enterprise volume dataVol on SVM1:

```
SVM1::> volume snaplock modify -vserver SVM1 -volume dataVol  
-privileged-delete enabled
```

= Delete WORM files using privileged delete

:icons: font

:relative\_path: ./snaplock/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the privileged delete feature to delete Enterprise-mode WORM files during the retention period.

## What you'll need

- You must be a SnapLock administrator to perform this task.
- You must have created a SnapLock audit log and enabled the privileged delete feature on the Enterprise volume.

## About this task

You cannot use a privileged delete operation to delete an expired WORM file. You can use the `volume file retention show` command to view the retention time of the WORM file that you want to delete. For more information, see the man page for the command.

## Step

1. Delete a WORM file on an Enterprise volume:

```
volume file privileged-delete -vserver SVM_name -file file_path
```

The following command deletes the file `/vol/dataVol/f1` on the SVM SVM1:

```
SVM1::> volume file privileged-delete -file /vol/dataVol/f1
```

= Use the Legal Hold feature

:icons: font

:relative\_path: ./snaplock/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.3, you can use the *Legal Hold* feature to retain Compliance-mode WORM files for the duration of a litigation.

### What you'll need

- You must be a SnapLock administrator to perform this task.

[Create a SnapLock administrator account](#)

- You must have logged in on a secure connection (SSH, console, or ZAPI).

### About this task

A file under a Legal Hold behaves like a WORM file with an indefinite retention period. It is your responsibility to specify when the Legal Hold period ends.

The number of files you can place under a Legal Hold depends on the space available on the volume.

### Steps

1. Start a Legal Hold:

```
snaplock legal-hold begin -litigation-name litigation_name -volume  
volume_name -path path_name
```

The following command starts a Legal Hold for all the files in `vol1`:

```
cluster1::>snaplock legal-hold begin -litigation-name litigation1  
-volume vol1 -path /
```

2. End a Legal Hold:

```
snaplock legal-hold end -litigation-name litigation_name -volume  
volume_name -path path_name
```

The following command ends a Legal Hold for all the files in `vol1`:

```
cluster1::>snaplock legal-hold end -litigation-name litigation1  
-volume vol1 -path /
```

= Use the Event Based Retention (EBR) feature

:icons: font

:relative\_path: ./snaplock/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.3, you can use the SnapLock *Event Based Retention (EBR)* feature to define how long a file is retained after the occurrence of an event.

### What you'll need

- You must be a SnapLock administrator to perform this task.

[Create a SnapLock administrator account](#)

- You must have logged in on a secure connection (SSH, console, or ZAPI).

**About this task**

The *event retention policy* defines the retention period for the file after the event occurs. The policy can be applied to a single file or all the files in a directory.

- If a file is not a WORM file, it will be committed to the WORM state for the retention period defined in the policy.
- If a file is a WORM file or a WORM appendable file, its retention period will be extended by the retention period defined in the policy.

You can use a Compliance-mode or Enterprise-mode volume.

EBR policies cannot be applied to files under a Legal Hold.

For advanced usage, see [Compliant WORM Storage Using NetApp SnapLock](#).

### **Using EBR to extend the retention period of already existing WORM files**

EBR is convenient when you want to extend the retention period of already existing WORM files. For example, it might be your firm's policy to retain employee W-4 records in unmodified form for three years after the employee changes a withholding election. Another company policy might require that W-4 records be retained for five years after the employee is terminated.

In this situation, you could create an EBR policy with a five-year retention period. After the employee is terminated (the "event"), you would apply the EBR policy to the employee's W-4 record, causing its retention period to be extended. That will usually be easier than extending the retention period manually, particularly when a large number of files is involved.

### **Steps**

1. Create an EBR policy:

```
snaplock event-retention policy create -vserver SVM_name -name policy_name -retention-period retention_period
```

The following command creates the EBR policy `employee_exit` on `vs1` with a retention period of ten years:

```
cluster1::>snaplock event-retention policy create -vserver vs1 -name employee_exit -retention-period 10years
```

2. Apply an EBR policy:

```
snaplock event-retention apply -vserver SVM_name -name policy_name -volume volume_name -path path_name
```

The following command applies the EBR policy `employee_exit` on `vs1` to all the files in the directory `d1`:

```
cluster1::>snaplock event-retention apply -vserver vs1 -name employee_exit -volume voll -path /d1
```

= Move a SnapLock volume

= Create a SnapLock security administrator account

:icons: font

:relative\_path: ./snaplock/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You must have SnapLock security administrator privileges to perform a SnapLock volume move. This privilege is granted to you with the `snaplock` role, introduced in ONTAP 9.8. If you have not already been assigned that role, you can ask your cluster

administrator to create a SnapLock security user with this SnapLock security role.

### What you'll need

- You must be a cluster administrator to perform this task.
- You must have logged in on a secure connection (SSH, console, or ZAPI).

### About this task

The snaplock role is associated with the admin SVM, unlike the vsadmin-snaplock role, which is associated with the data SVM.

### Step

1. Create an SVM administrator account with the SnapLock administrator role:

```
security login create -vserver SVM_name -user-or-group-name  
user_or_group_name -application application -authmethod  
authentication_method -role role -comment comment
```

The following command enables the SVM administrator account SnapLockAdmin with the predefined snaplock role to access admin SVM cluster1 using a password:

```
cluster1::> security login create -vserver cluster1 -user-or-group  
-name SnapLockAdmin -application ssh -authmethod password -role  
snaplock
```

= Move a SnapLock volume

:icons: font

:relative\_path: ./snaplock/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the `volume move` command to move a SnapLock volume to a destination aggregate.

### What you'll need

- You must have created a SnapLock-protected audit log before performing SnapLock volume move.

[Create an audit log.](#)

- If you are using a version of ONTAP earlier than ONTAP 9.10.1, the destination aggregate must be the same SnapLock type as the SnapLock volume you want to move; either Compliance to Compliance or Enterprise to Enterprise. Beginning with ONTAP 9.10.1, this restriction is removed and an aggregate can include both Compliance and Enterprise SnapLock volumes, as well as non-SnapLock volumes.
- You must be a user with the SnapLock security role.

### Steps

1. Using a secure connection, log in to the ONTAP cluster management LIF:

```
ssh snaplock_user@cluster_mgmt_ip
```



2. Move a SnapLock volume:

```
volume move start -vserver SVM_name -volume SnapLock_volume_name  
-destination-aggregate destination_aggregate_name
```

3. Check the status of the volume move operation:

```
volume move show -volume SnapLock_volume_name -vserver SVM_name -fields  
volume,phase,vserver
```

= SnapLock APIs

:icons: font

:relative\_path: ./snaplock/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use Zephyr APIs to integrate with SnapLock functionality in scripts or workflow automation. The APIs use XML messaging over HTTP, HTTPS, and Windows DCE/RPC.

== file-fingerprint-abort

Abort a file fingerprint operation.

== file-fingerprint-dump

Display file fingerprint information.

== file-fingerprint-get-iter

Display the status of file fingerprint operations.

== file-fingerprint-start

Generate a file fingerprint.

== snaplock-archive-vserver-log

Archive the active audit log file.

== snaplock-create-vserver-log

Create an audit log configuration for an SVM.

== snaplock-delete-vserver-log

Delete an audit log configuration for an SVM.

== snaplock-file-privileged-delete

Execute a privileged delete operation.

== snaplock-get-file-retention

Get the retention period of a file.

== snaplock-get-node-compliance-clock

Get the node ComplianceClock date and time.

== snaplock-get-vserver-active-log-files-iter

Display the status of active log files.

== snaplock-get-vserver-log-iter

Display the audit log configuration.

== snaplock-modify-vserver-log

Modify the audit log configuration for an SVM.

== snaplock-set-file-retention

Set the retention time for a file.

== snaplock-set-node-compliance-clock

Set the node ComplianceClock date and time.

== snaplock-volume-set-privileged-delete

Set the privileged-delete option on a SnapLock Enterprise volume.

== volume-get-snaplock-attrs

Get the attributes of a SnapLock volume.

== volume-set-snaplock-attrs

Set the attributes of a SnapLock volume.

= Consistency Groups management

= Consistency groups overview

:icons: font

:relative\_path: ./consistency-groups/

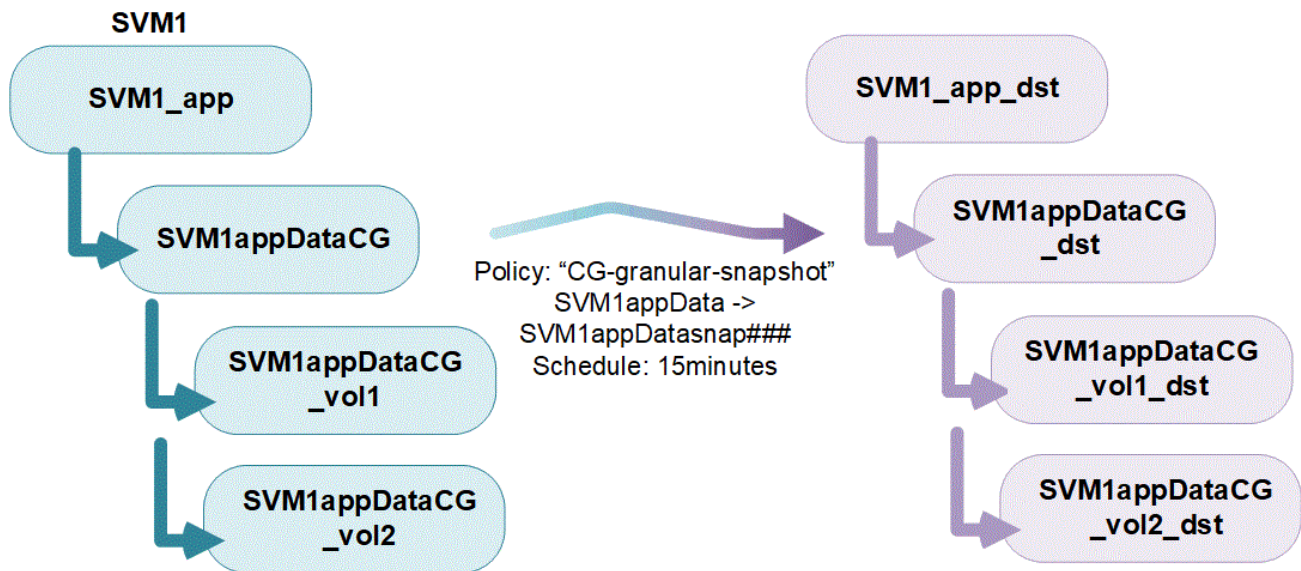
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

A consistency group is a collection of volumes that provides a write-order consistency guarantee for an application workload spanning multiple volumes.

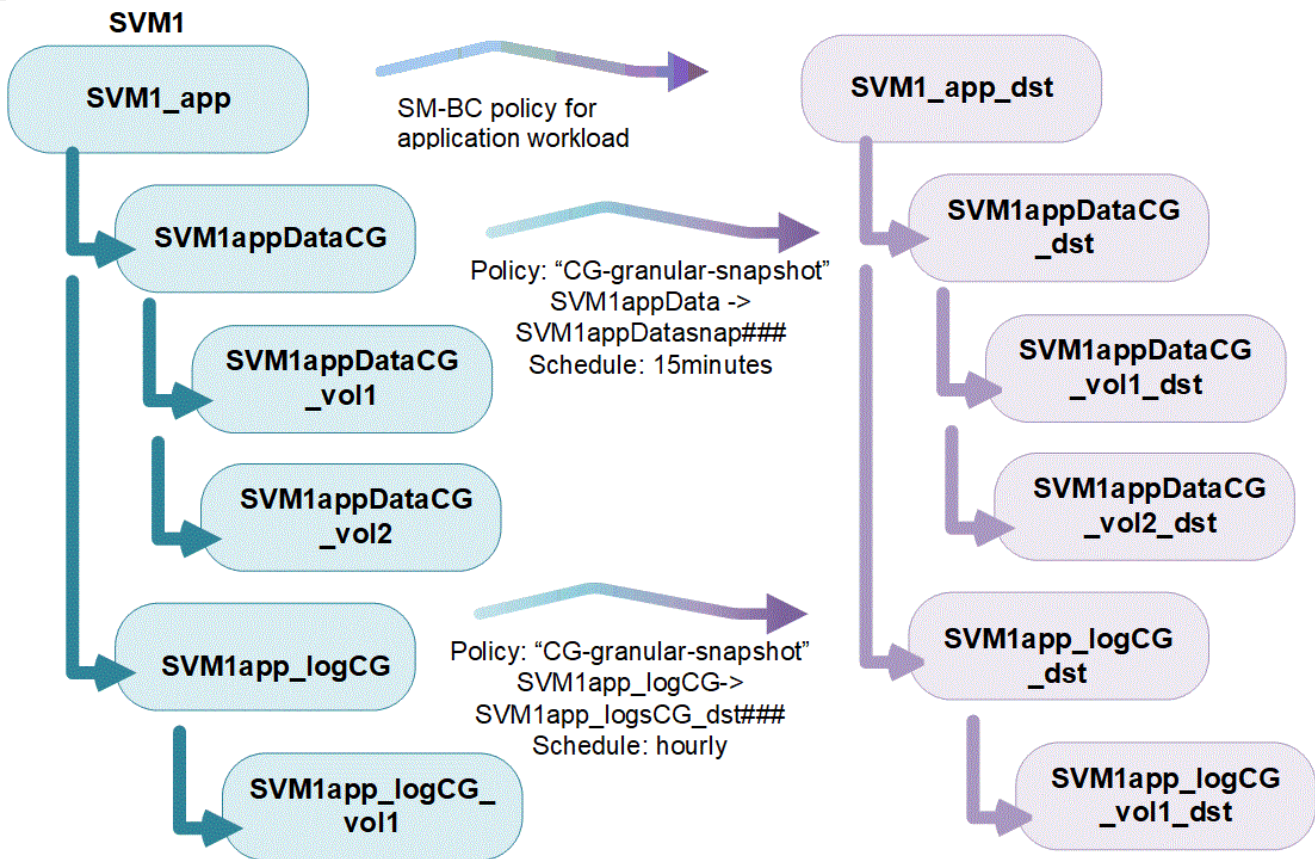
Consistency groups facilitate application workload management, providing easy management of local and remote protection policies and providing simultaneous crash-consistent or application-consistent Snapshot copies of a collection of volumes at a point in time. Snapshots in consistency groups enable an entire application workload to be restored.

Consistency groups support any FlexVol volume regardless of protocol (NAS, SAN, or NVMe) and can be managed through the ONTAP REST APIs or in System Manager under the **Storage > Consistency Groups** menu item.

Consistency groups can exist on their own or in a hierarchical relationship. An individual consistency group is a collection of volumes. Volumes can have their own volume-granular snapshot policy. In addition, the consistency group the volume is associated with can have its own snapshot policy. The consistency group can only have one SM-BC relationship and shared SM-BC policy, which can be used to recover the entire consistency group.



Larger application workloads might require multiple consistency groups. In these situations, multiple consistency groups can be placed together in a hierarchical relationship. In this configuration, single consistency groups become the child components of a parent consistency group. The parent consistency group can include up to five child consistency groups. Like in individual consistency groups, a remote SM-BC protection policy can be applied to the entire configuration of consistency groups (parent and children) to recover the application workload.



== Protection

Consistency groups offer remote protection through SnapMirror Business Continuity (SM-BC) and local protection through Snapshot policies. In order to utilize remote protection, you must meet the requirements for [SnapMirror Business Continuity deployments](#). By default, consistency groups do not have a protection policy set and will not protect your data unless a policy is selected. See ["Protect a consistency group"](#) for more information.



SM-BC relationships cannot be established on volumes mounted for NAS access.

Beginning in ONTAP 9.11.1, there is additional support for consistency groups with [two-phase consistency group snapshot creation](#).

== Consistency groups in MetroCluster configurations

Beginning with ONTAP 9.11.1, you can provision consistency groups with new volumes on a cluster within a MetroCluster configuration. These volumes are provisioned on mirrored aggregates.

After they are provisioned, you can move volumes associated with consistency groups between mirrored and unmirrored aggregates. Therefore, they can be located on mirrored aggregates, unmirrored aggregates, or both. You can modify mirrored aggregates containing volumes associated with consistency groups to become unmirrored. Similarly, you can modify unmirrored aggregates containing volumes associated with consistency groups to enable mirroring.

Volumes associated with consistency groups placed on mirrored aggregates and their Snapshots, including any consistency group Snapshots, are replicated to the remote site (site B). The contents of the volumes on site B are consistency group semantics-compliant. You can access replicated consistency group Snapshots using consistency group Snapshot REST APIs and System Manager on clusters

running ONTAP 9.11.1 or later.

If some or all of the volumes associated with a consistency group are located on unmirrored aggregates that are not currently accessible, GET or DELETE operations on the consistency group behave as if the local volumes or hosting aggregates are offline.

#### === Consistency group configuration replication

If site B is running ONTAP 9.10.1 or earlier, only the volumes associated with the consistency groups located on mirrored aggregates are replicated to site B. The consistency group configurations are only replicated to site B, if both sites are running ONTAP 9.11.1 or later. After site B is upgraded to ONTAP 9.11.1, data for consistency groups on site A that have all their associated volumes placed on mirrored aggregates are replicated to site B.

#### == Upgrade considerations

Consistency groups created with SM-BC in ONTAP 9.8 and 9.9.1 will automatically be upgraded and become manageable under **Storage > Consistency Groups** in System Manager or the ONTAP REST API when upgrading to ONTAP 9.10.1. For more information about upgrading, see [SM-BC upgrade and revert considerations](#).

Consistency group snapshots created with the ONTAP REST API can be managed through System Manager's Consistency Group interface and through consistency group API endpoints.

Snapshots created with the ONTAPI commands `cg-start` and `cg-commit` will not be recognized as consistency group snapshots and thus cannot be managed through System Manager's Consistency Group interface or the consistency group endpoints in the ONTAP API.

#### == Consistency group object limits

Consistency Groups	Scope	Minimum	Maximum
Number of consistency groups	Cluster	0	Same as maximum volume count in cluster
Number of parent consistency groups	Cluster	0	Same as maximum volume count in cluster
Number of individual and parent consistency groups	Cluster	0	Same as maximum volume count in cluster
Consistency group	Same as maximum volume count in cluster	1	80
Number of volumes in the child of a parent consistency group	Parent consistency group	1	80
Number of volumes in a child consistency group	Child consistency group	1	80
Number of child consistency groups in a parent consistency group	Parent consistency group	1	5

If you are using SM-BC, refer to [SM-BC restrictions and limitations for limits](#).

== Learn more about consistency groups



= Configure a single consistency group

.icons: font

.relative\_path: ./consistency-groups/

.imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Consistency groups can be created with existing volumes or with new volumes. Once a volume is added to a consistency group, it cannot be added to another consistency group. A volume can be removed from a consistency group by deleting the volume or deleting the consistency group.

== Create a consistency group with new volumes

### Steps

1. Select **Storage > Consistency groups**.
2. Select **+Add**, then **Using New LUNs**.
3. Name the consistency group. Designate the number of LUNs and capacity per LUN.
4. Select the host operating system and LUN format. Enter the host initiator information.
5. To configure protection policies, add a child consistency group, or show more options about host initiators, select **More options**
6. Select **Save**.
7. Confirm your consistency group has been created by returning to the main consistency group menu where it will appear once the ONTAP job completes. If you set a protection policy, look under the appropriate policy, remote or local, which should display a green shield with a checkmark.

== Create a consistency group with existing volumes

.Steps

- . Select **Storage > Consistency groups**.
- . Select **+Add**, then **Using existing volumes**.
- . Name the consistency group and select the storage VM.
- . Select the existing volumes to include. Only volumes that are not already part of a consistency group will be available for selection.

+

If creating a consistency group with new volumes, the consistency group supports FlexVol volumes. Volumes with Asynchronous or Synchronous SnapMirror relationships can be added to consistency groups, but they are not consistency group-aware. Consistency groups do not support S3 buckets, MCC, or SVMs with SVMDR relationships.

+

- . Select **Save**.
- . Confirm your consistency group has been created by returning to the main consistency group menu where it will appear once the ONTAP job completes. If you have chosen a protection policy, confirm it was properly set by selecting your consistency group from the menu. If you set a protection policy, look under the appropriate policy, remote or local, which should display a green shield with a checkmark.

= Configure a hierarchical consistency group

:icons: font

:relative\_path: ./consistency-groups/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

If your application workload consists of more than one subset of volumes, where each subset is consistent across its own associated volumes, ONTAP allows you to create a hierarchical consistency group. Hierarchical consistency groups have a parent that can include up to five individual consistency groups. Hierarchical consistency groups can support different local Snapshot policies across consistency groups or individual volumes. If you use a remote SM-BC policy, that will apply for the entire consistency group.

For object limits on consistency groups, see [Object limits for consistency groups](#).

== Create a hierarchical consistency group with new volumes

### Steps

1. Select **Storage > Consistency groups**.
2. Select **+Add**, then **Using New LUNs**.
3. Name the consistency group. Designate the number of LUNs and capacity per LUN.
4. Select the host operating system and LUN format. Enter the host initiator information.
5. To configure protection policies, add a child consistency group, or show more options about host initiators, select **More options**.
6. To add a child consistency group, select **+Add child consistency group**.
7. Select the performance level, the number of LUNs, and capacity per LUN. Designate the host operating system, LUN format, and select a new or existing host initiator group.
8. **Optional**: select a local snapshot policy.
9. Repeat for up to five child consistency groups.

10. Select **Save**.

11. Confirm your consistency group has been created by returning to the main consistency group menu where it will appear once the ONTAP job completes. If you set a protection policy, look under the appropriate policy, remote or local, which should display a green shield with a checkmark in it.

== Create a hierarchical consistency group with existing volumes

.Steps

. Select **Storage > Consistency groups**.

. Select **+Add**, then **Using existing volumes**.

. Select the storage VM.

. Select the existing volumes to include. Only volumes that are not already part of a consistency group will be available for selection.

. To add a child consistency group, select **+Add Child Consistency Group**. Create the necessary consistency groups, which will be named automatically.

. Assign existing volumes to each consistency group.

. **Optional**: select a local Snapshot policy.

. Repeat for up to five child consistency groups.

. Select **Save**.

. Confirm your consistency group has been created by returning to the main consistency group menu where it will appear once the ONTAP job completes. If you have chosen a protection policy, confirm it was properly set by selecting your consistency group from the menu. If you set a protection policy, look under the appropriate policy, remote or local, which should display a green shield with a checkmark in it.

= Protect a consistency group

:icons: font

:relative\_path: ./consistency-groups/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

:hardbreaks-option:

Consistency groups offer easily managed local and remote protection for SAN, NAS, and NVMe applications that span multiple volumes.

Creating a consistency group does not automatically enable protection. Local and/or remote protection policies can be set at the time of creation or after creating your consistency group. Protection policies can include local Snapshot copies or remote SnapMirror protection with SnapMirror Business Continuity (SM-BC). If you are utilizing nested consistency groups, you can set different protection policies for individual volumes. Beginning in ONTAP 9.11.1, consistency groups offer [two-phase consistency group Snapshot creation](#).

If you are utilizing remote SM-BC protection, to ensure Snapshot copies of consistency groups created on your consistency group are copied to the destination, the policy labels in the source and destination cluster must match. SM-BC will not replicate Snapshot copies by default unless a rule with a SnapMirror label is added to the predefined AutomatedFailOver policy and the Snapshot copies are created with that label. To learn more about this process, refer to [Configure protection for business continuity](#).

Recovery can occur for an entire consistency group, a single consistency group in a hierarchical configuration, or for individual volumes within the consistency group. Recovery can be achieved by selecting the consistency group you want to recover from, selecting the Snapshot copy type, and then identifying the particular Snapshot copy to base the restoration on. For more information about this process, see [Restore a volume from an earlier Snapshot copy](#).


Beginning with ONTAP 9.10.1, System Manager visualizes LUN maps under the **Protection > Relationships** menu. When you select a source relationship, System Manager displays a visualization of the source relationships. By selecting a volume, you can delve deeper into these relationships to see a list



of the contained LUNs and the initiator group relationships. This information can be downloaded as an Excel workbook from the individual volume view. The task will run in the background.

== Set a local Snapshot protection policy

### Steps

1. Select the consistency group you have created from the Consistency group menu.
2. At the top right of the overview page for the consistency group, select **Edit**.
3. Check the box next to **Schedule Snapshot copies (local)**.
4. Select a Snapshot policy. To configure a new, custom policy, refer to [Create a custom data protection policy](#).
5. Select **Save**.
6. Return to the consistency group overview menu. In the left column under **Snapshot Copies (Local)**, the status should say protected next to .


== Set a remote SM-BC policy

### Steps

1. Ensure you have met the prerequisites for using SM-BC. See [SM-BC prerequisites](#)



SM-BC relationships cannot be established on volumes mounted for NAS access.

1. Select the consistency group you have created from the Consistency group menu.
2. At the top right of the overview page, select **More** then **Protect**.
3. The source-side information should be autofilled on the left-hand side of the page.
4. Select the appropriate cluster and storage VM for the destination. Select a protection policy. Ensure that **Initialize relationship** is checked.
5. Click **Save**.
6. The consistency group will have to initialize and synchronize. When this is complete, under **SnapMirror (Remote)** the status should say "Protected" next to .

== Two-phase CG Snapshot creation

Beginning in ONTAP 9.11.1, consistency groups support two-phase commits for consistency group (CG) Snapshot creation. This feature is only available with the ONTAP REST API. Two-phase CG Snapshot creation is only available for Snapshot creation, not provisioning consistency groups or restoring consistency groups.

A two-phase CG Snapshot creation breaks the Snapshot creation process invoked with a POST request to the `/application/consistency-groups/{consistency_group_uuid}/snapshots` endpoint into a sequence of two phases. In the first phase initiated with a POST request, the API executes prechecks, triggers Snapshot creation, and starts a timer for designated interval. If the POST request in phase one completes with a 201 status code, you can invoke the second phase within the designated interval from the first phase, committing the Snapshot to the appropriate endpoint.

To use two-phase CG Snapshot creation, all nodes in the cluster must be running ONTAP 9.11.1. The two-phase CG Snapshot creation can be invoked with the `action=start` parameter. You can additionally use the `action_timeout` parameter that specifies the maximum number of seconds that

the Snapshot creation process can take. The `action_timeout` parameter can be set equal to an integer between 5 and 120. The default value of `action_timeout` is 7.

Only one active invocation of a consistency group Snapshot creation operation is supported on a consistency group instance at a time, whether it be a one-phase or two-phase. Attempting to invoke a Snapshot creation while another one is in progress will result in a failure.

For more information about the ONTAP REST API, refer to the [API reference](#) or visit the [ONTAP REST API page](#) at the NetApp Developer Network for a complete list of API endpoints.

### Create a two-phase commit

1. Invoke the Snapshot creation with a POST request to the consistency group endpoint using the `action=start` parameter.

```
curl -k -X POST 'https://<IP_address>/application/consistency-
groups/<cg-uuid>/snapshots?action=start&action_timeout=7' -H
"accept: application/hal+json" -H "content-type: application/json"
-d '
{
  "name": "name_of_this_snapshot",
  "consistency_type": "crash",
  "comment": "<comment>",
  "snapmirror_label": "<snap_mirror_label>"
}'
```

2. If the POST request succeeds, your output will include a snapshot uuid. Using that information, submit a PATCH request to commit the Snapshot.

```
curl -k -X PATCH 'https://<IP_address>/application/consistency-
groups/<cg_uuid>/snapshots/<snapshot_id>?action=commit' -H "accept:
application/hal+json" -H "content-type: application/json"
```

### Next Steps

[Configure Snapshot copies](#)

[Create custom data protection policies](#)

[Recover from Snapshot copies](#)

[Restore a volume from an earlier Snapshot copy](#)

= Delete a consistency group

:icons: font

:relative\_path: ./consistency-groups/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/


If you decide that you no longer need a consistency group, it can be deleted.

Deleting a consistency group deletes the instance of the consistency group and does **not** impact the constituent volumes or LUNs. Deleting a consistency group does not result in deletion of the Snapshots present on each volume, but they will no longer be accessible as consistency group Snapshots. They

can, however, continue to be managed as ordinary volume granular snapshots.

Consistency groups will also be deleted if all of the volumes in a consistency group are deleted. Volumes can only be removed from a consistency group if the volume itself is deleted, in which case the volume is automatically removed from the consistency group.

### Steps

1. In the consistency group menu under **Storage > Consistency groups**, select the consistency group you would like to delete.
2. Next to the name of the consistency group, select  and then **Delete**.

= SnapMirror Business Continuity

= Overview

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.8, you can use SnapMirror Business Continuity (SM-BC) to protect applications with LUNs, enabling applications to fail over transparently, ensuring business continuity in case of a disaster. SM-BC is supported on AFF clusters or All SAN Array (ASA) clusters, where the primary and secondary clusters can be either AFF or ASA. SM-BC protects applications with iSCSI or FCP LUNs.

== Benefits

SnapMirror Business Continuity provides the following benefits:

- Provides continuous availability for business-critical applications
- Ability to host critical applications alternately from primary and secondary site
- Simplified application management using consistency groups for dependent write-order consistency
- The ability to test failover for each application
- Instantaneous creation of mirror clones without impacting application availability
- Beginning in ONTAP 9.11.1, SM-BC supports [single-file SnapRestore](#).

== Typical use cases

=== Application deployment for zero RTO or Transparent Application Failover

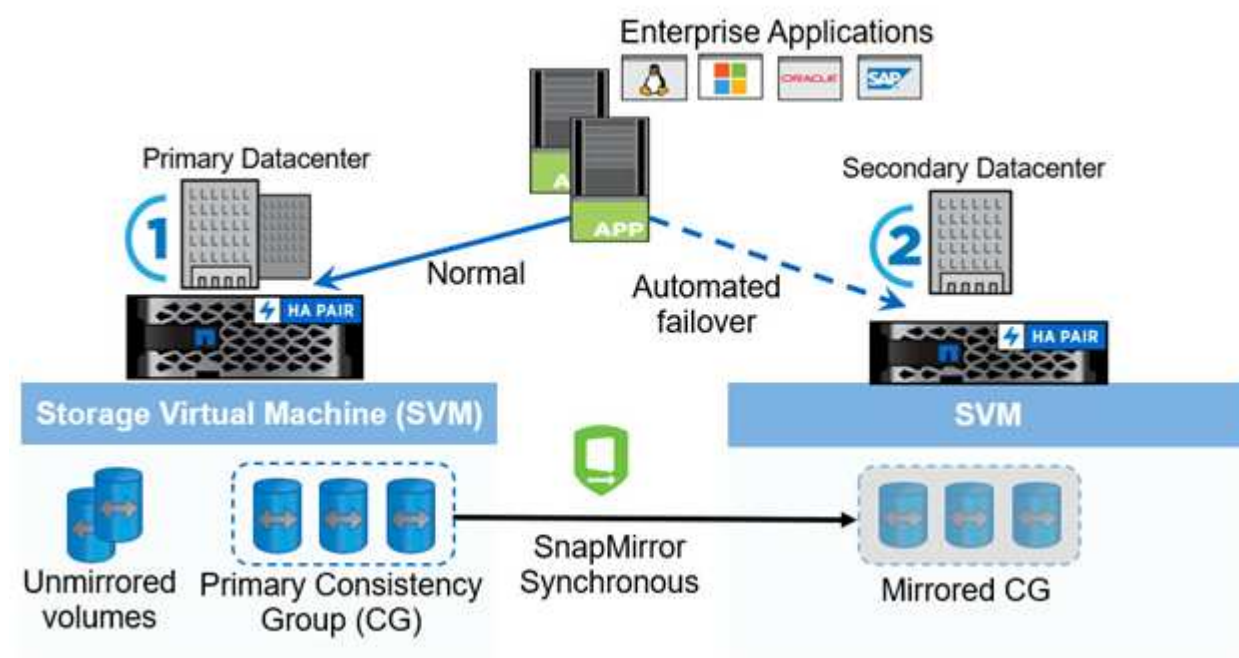
Transparent Application Failover is based on host multipath I/O (MPIO) software-based path failover to achieve non-disruptive access to the storage. Both LUN copies, for example, primary(L1P) and mirror copy(L1S), have the same identity (serial number) and are reported as read-writable to the host. However, reads and writes are serviced only by the primary volume. I/Os issued to the mirror copy are proxied to the primary copy. The host's preferred path to L1 is VS1:N1 based on Asymmetric Logical Unit Access (ALUA) access state Active Optimized (A/O). Mediator is recommended as part of the deployment, primarily to perform failover in case of a storage outage on the primary.

=== Disaster scenario

The site hosting the primary cluster experiences a disaster. Host multipathing software marks all paths through the cluster as down and uses paths from the secondary cluster. The result is a non-disruptive failover to the mirror copy for LUN L1. L1S is converted from a mirror copy to an active copy of LUN L1. The failover happens automatically when an external Mediator is configured. The host's preferred path to L1 becomes VS2:N1.

== Architecture

The following figure illustrates the operation of the SnapMirror Business Continuity feature at a high level.



== Additional information

For more information about data protection using SnapMirror Synchronous, see the [SnapMirror Synchronous disaster recovery documentation](#).

= Key concepts

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

As you begin to explore the ONTAP SnapMirror Business Continuity and plan a deployment, it is helpful to become familiar with the key terminology and concepts.

### SM-BC

Acronym for the SnapMirror Business Continuity (SM-BC) solution available with ONTAP 9.8 and later.

### Consistency group

Beginning with ONTAP 9.10.1, consistency groups have become a first-order management unit. To learn more about consistency groups, refer to [Consistency groups overview](#).

A consistency group (CG) is a collection of FlexVol volumes that provide a write order consistency

guarantee for the application workload which needs to be protected for business continuity. The purpose of a consistency group is to take simultaneous crash-consistent Snapshot copies of a collection of volumes at a point in time. In regular deployment, the group of volumes picked to be part of a CG are mapped to an application instance. SnapMirror relationships, also known as a CG relationship, is established between a source CG and a destination CG. The source and destination CGs must contain the same number and type of volumes.

### **Constituent**

The individual FlexVol volumes that are part of a consistency group.

### **Mediator**

ONTAP Mediator provides an alternate health path to the peer cluster, with the intercluster LIFs providing the other health path. With the Mediator's health information, clusters can differentiate between intercluster LIF failure and site failure. When the site goes down, Mediator passes on the health information to the peer cluster on demand, facilitating the peer cluster to fail over. With the Mediator-provided information and the intercluster LIF health check information, ONTAP determines whether to perform an auto failover, if it is failover incapable, continue or stop.

Mediator is one of three parties in the SM-BC quorum, working with the primary cluster and the secondary cluster to reach a consensus. A consensus requires at least two parties in the quorum to agree to an operation.

### **Out of Sync (OOS)**

The application I/O is not replicating to the secondary storage system. The destination volume is not in sync with the source volume because SnapMirror replication is not occurring. If the mirror state is Snapmirrored, this indicates a transfer failure or failure due to an unsupported operation.

### **Zero RPO**

Zero recovery point objective. This is the acceptable amount of data loss from downtime.

### **Zero RTO**

Zero recovery time objective or Transparent Application Failover is achieved by using host multipath I/O (MPIO) software-based path failover to provide non-disruptive access to the storage.

### **Planned failover**

A manual operation to change the roles of copies in a SM-BC relationship. The primary becomes the secondary and the secondary becomes the primary. ALUA reporting also changes.

### **Automatic unplanned failover (AUFO)**

An automatic operation to perform a failover to the mirror copy. The operation requires assistance from Mediator to detect that the primary copy is unavailable.

= Planning

= Prerequisites

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

There are several prerequisites that you should consider as part of planning a SnapMirror Business Continuity solution deployment.

## == Hardware

- Only two-node HA clusters are supported
- Both clusters must be either AFF or ASA (no mixing)

## == Software

\* ONTAP 9.8 or later

\* ONTAP Mediator 1.2 or later

\* A Linux server or virtual machine for the ONTAP Mediator running one of the following:

Mediator version	Supported Linux versions
1.4	<ul style="list-style-type: none"><li>• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5</li><li>• CentOS: 7.6, 7.7, 7.8, 7.9</li></ul>
1.3	<ul style="list-style-type: none"><li>• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3</li><li>• CentOS: 7.6, 7.7, 7.8, 7.9</li></ul>
1.2	<ul style="list-style-type: none"><li>• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 8.1</li><li>• CentOS: 7.6, 7.7, 7.8</li></ul>

## == Licensing

- SnapMirror synchronous (SM-S) license must be applied on both clusters
- SnapMirror license must be applied on both clusters



If your ONTAP storage systems were purchased before June 2019, click [NetApp ONTAP Master License Keys](#) to get the required SM-S license.

## == Networking environment

- Inter-cluster latency round trip time (RTT) must be less than 10 milliseconds
- SCSI-3 persistent reservations are **not** supported with SM-BC

## == Supported protocols

- Only SAN protocols are supported (not NFS/SMB)
- Only Fibre Channel and iSCSI protocols are supported
- The default IPspace is required by SM-BC for cluster peer relationships. Custom IPspace is not supported.

## == ONTAP Mediator

- Must be provisioned externally and attached to ONTAP for transparent application failover.
- For more information about the ONTAP Mediator, see [Prepare to install the ONTAP Mediator service](#).

## == Read-write destination volumes

- SM-BC relationships are not supported on read-write destination volumes. Before you can use a read-write volume, you must convert it to a DP volume by creating a volume-level SnapMirror relationship and then deleting the relationship. For details, see [Converting existing relationships to SM-BC relationships](#)

== Large LUNs and large volumes

- Large LUNs and large volumes greater than 100TB are supported only on All SAN Arrays



You must ensure that both the primary and secondary cluster are All SAN Arrays, and that they both have ONTAP 9.8 installed. If the secondary cluster is running a version earlier than ONTAP 9.8 or if it is not an All SAN Array, the synchronous relationship can go out of sync if the primary volume grows larger than 100 TB.

= Additional restrictions and limitations

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

There are several additional restrictions and limitations when using the SnapMirror Business Continuity solution.

== Consistency groups in a cluster

Consistency group limits for a cluster with SM-BC are calculated based on relationships and depend on the version of ONTAP used. Limits are platform-independent.

ONTAP version	Maximum number of relationships
ONTAP 9.8-9.9.1	5
ONTAP 9.10.1	20
ONTAP 9.11.1	50

== Volumes per consistency group

From ONTAP 9.8 to 9.9.1, the maximum number of volumes supported per SM-BC consistency group relationship is twelve, a limit which is platform-independent. Beginning with ONTAP 9.10.1, the maximum number of volumes supported per SM-BC relationship is sixteen.

== Volumes

Limits in SM-BC are calculated based on the number of endpoints, not the number of relationships. A consistency group with 12 volumes contributes 12 endpoints on both the source and destination. Both SM-BC and SnapMirror Synchronous relationships contribute to the total number of endpoints.

The maximum endpoints per platform are included in the following table.

S. No	Platform	Endpoints per HA for SM-BC			Overall sync and SM-BC endpoints per HA		
		ONTAP 9.8-9.9.1	ONTAP 9.10.1	ONTAP 9.11.1	ONTAP 9.8-9.9.1	ONTAP 9.10.1	ONTAP 9.11.1
1	AFF	60	200	400	80	200	400
2	ASA	60	200	400	80	200	400

== SAN object limits

The following SAN object limits are included in the following table and apply regardless of the platform.

Limits of objects in an SM-BC relationship	Count
LUNs per volume	256
LUN maps per node	2048
LUN maps per cluster	4096
LIFs per VServer (with at least one volume in an SM-BC relationship)	256
Inter-cluster LIFs per node	4
Inter-cluster LIFs per cluster	8

== NTFS Security Style

NTFS security style is not supported on SM-BC volumes.

== Fan-out configurations

SM-BC supports [fan-out configurations](#) with the `MirrorAllSnapshots` policy and, beginning in ONTAP 9.11.1, the `MirrorAndVault` policy. Fan-out configurations are not supported with `XDPDefault` policy.

If you experience a failover on the SM-BC destination in a fan-out configuration, you will have to manually [resume protection in the fan-out configuration](#).

== AIX

Beginning with ONTAP 9.11.1, AIX is supported with SM-BC. With an AIX configuration, the primary cluster is the "active" cluster.

In an AIX configuration, failovers are disruptive. With each failover, you will need to perform a re-scan on the host for I/O operations to resume.

To configure for AIX host with SM-BC, refer to the Knowledge Base article [How to configure an AIX host for SnapMirror Business Continuity \(SM-BC\)](#).

== Solaris Host setting recommendation for SM-BC configuration

Beginning with ONTAP 9.10.1, SM-BC supports Solaris 11.4. To ensure the Solaris client applications are non-disruptive when an unplanned site failover switchover occurs in an SM-BC environment, you must configure the Solaris 11.4 Host with the `f_tpgs` parameter.



Follow these steps to configure the override parameter:

1. Create configuration file `/etc/driver/drv/scsi_vhci.conf` with an entry similar to the following for the NetApp storage type connected to the host:

```
scsi-vhci-failover-override =  
"NETAPP LUN", "f_tpgs"
```

2. Use `devprop` and `mdb` commands to verify the override has been successfully applied:

```
root@host-A:~# devprop -v -n /scsi_vhci scsi-vhci-failover-override  
scsi-vhci-failover-override=NETAPP LUN + f_tpgs  
root@host-A:~# echo "*scsi_vhci_dip::print -x struct dev_info  
devi_child | ::list struct dev_info devi_sibling| ::print struct  
dev_info devi_mdi_client| ::print mdi_client_t ct_vprivate| ::print  
struct scsi_vhci_lun svl_lun_wnn svl_fops_name"| mdb -k`
```

```
svl_lun_wnn = 0xa002a1c8960 "600a098038313477543f524539787938"  
svl_fops_name = 0xa00298d69e0 "conf f_tpgs"
```



`conf` will be added to the `svl_fops_name` when a `scsi-vhci-failover-override` has been applied.

For additional information and recommended changes to default settings, refer to NetApp KB article [Solaris Host support recommended settings in SnapMirror Business Continuity \(SM-BC\) configuration](#).

== HP-UX Known issues and limitations for SM-BC configuration

Beginning in ONTAP 9.10.1, SM-BC for HP-UX is supported. If an automatic unplanned failover (AUFO) event occurs on the isolated master cluster in the SM-BC configuration, it might take more than 120 seconds for I/O to resume on the HP-UX host. Depending on the applications that are running, this might not lead to any I/O disruption or error messages. If an AUFO event on the isolated master cluster occurs, you must restart applications on the HP-UX host that have a disruption tolerance of less than 120 seconds.

An AUFO event on the isolated master cluster might cause dual event failure when the connection between the primary and the secondary cluster is lost and the connection between the primary cluster and the mediator is also lost. This is considered a rare event, unlike other AUFO events.

= ONTAP access options

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You have several access options available when configuring the ONTAP nodes participating in an SM- BC deployment. You should select the option that best matches your specific environment and deployment goals.



In all cases, you must sign in using the administrator account with a valid password.

### Command line interface

The text-based command line interface is available through the ONTAP management shell. You can access the CLI using secure shell (SSH).

### System Manager

You can connect to the System Manager using a modern web browser. The web GUI provides an intuitive and easy-to-use interface when accessing the SnapMirror Business Continuity functionality. For more information about using System Manager, see [System Manager documentation](#).

### REST API

The ONTAP REST API exposed to external clients provides another option when connecting to the ONTAP. You can access the API using any mainstream programming language or tool that supports REST web services. Popular choices include:

- Python (including the ONTAP Python client library)
- Java
- Curl

Using a programming or scripting language provides an opportunity to automate the deployment and management of a SnapMirror Business Continuity deployment. For more information, see the ONTAP online documentation page at your ONTAP storage system.

= Prepare to use the ONTAP CLI

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You should be familiar with the following commands when deploying the SnapMirror Business Continuity solution using the ONTAP command line interface.



SM-BC does not support the `snapmirror quiesce` and `snapmirror resume` commands for relationships with active sync policy.

For more information about the following ONTAP commands, see [NetApp Documentation: ONTAP 9](#).

Command	Description
<code>lun igroup create</code>	Create an igroup on a cluster
<code>lun map</code>	Map a LUN to an igroup
<code>lun show</code>	Display a list of LUNs

Command	Description
snapmirror create	Create a new SnapMirror relationship
snapmirror initialize	Initialize an SM-BC consistency group
snapmirror update	Initiates a common snapshot creation operation
snapmirror show	Display a list of SnapMirror relationships
snapmirror failover	Start a planned failover operation
snapmirror resync	Start a resynchronization operation
snapmirror delete	Delete a SnapMirror relationship
snapmirror release	Remove source information for a SnapMirror relationship
volume snapshot restore-file	Available with SM-BC beginning in ONTAP 9.11.1, <a href="#">restore a single file or LUN</a>

= Prepare to use the ONTAP Mediator

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

The ONTAP Mediator establishes a quorum for the ONTAP clusters in an SM-BC relationship. It coordinates automated failover when a failure is detected and helps to avoid split-brain scenarios when each cluster simultaneously tries to establish control as the primary cluster.

== Prerequisites for the ONTAP Mediator

The ONTAP Mediator includes its own set of prerequisites. You must meet these prerequisites before installing the mediator. For more information, see [Prepare to install the ONTAP Mediator service](#).

== Network configuration

By default, the ONTAP Mediator provides service through TCP port 31784. You should make sure that port 31784 is open and available between the ONTAP clusters and the mediator.

= Summary of deployment best practices

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

There are several best practices that you should consider as part of planning an SnapMirror Business Continuity deployment.

== SAN

The SnapMirror Business Continuity solution supports only SAN workloads. You should follow the SAN

best practices in all cases.

In addition:

- Replicated LUNs in the secondary cluster must be mapped to the host and the I/O paths to the LUNs from both the primary and secondary cluster must be discovered at the time of host configuration.
- After an out of sync (OOS) event exceeds 80 seconds, or after an automatic unplanned failover, it is important to rescan the host LUN I/O path to ensure that there is no I/O path loss. For more information, see the respective host OS vendor's documentation on rescan of LUN I/O paths.

== Mediator

To be fully functional and to enable automatic unplanned failover, the external ONTAP mediator should be provisioned and configured with ONTAP clusters.

When installing the mediator, you should replace the self-signed certificate with a valid certificate signed by a mainstream reliable CA.

== SnapMirror

You should terminate an SnapMirror relationship in the following order:

1. Perform `snapmirror delete` at the destination cluster
2. Perform `snapmirror release` at the source cluster

= Manage SnapMirror for Business Continuity using System Manager

= Configure Mediator

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Use System Manager to configure the Mediator server to be used for automated failover. You can also replace the self-signed SSL and CA with the third party validated SSL Certificate and CA if you have not already done so.

### Steps

1. Navigate to **Protection > Overview > Mediator > Configure**.
2. Click **Add**, and enter the following Mediator server information:
  - IPv4 address
  - Username
  - Password
  - Certificate

= Configure protection for business continuity

:toc: macro

:toclevels: 1

```
:hardbreaks:  
:icons: font  
:linkattrs:  
:relative_path: ./  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/
```

Configuring protection for business continuity involves selecting LUNs on the ONTAP source cluster and adding them to a consistency group. Open System Manager from a browser on the source cluster to begin configuring protection for business continuity.

This workflow is designed for ONTAP 9.8 and 9.9. Beginning with ONTAP 9.10.1, it is recommended that you begin by creating a consistency group and then use SM-BC as a remote protection.

== About this task

- LUNs must reside on the same storage VM.
- LUNs can reside on different volumes.
- The source and destination cluster cannot be the same.
- The default IPspace is required by SM-BC for cluster peer relationships. Custom IPspace is not supported.

### Steps

1. Choose the LUNs you want to protect and add them to a protection group: **Protection > Overview > Protect for Business Continuity > Protect LUNs**.
2. Select one or more LUNs to protect on the source cluster.
3. Select the destination cluster and SVM.
4. **Initialize relationship** is selected by default. Click **Save** to begin protection.
5. Go to **Dashboard > Performance** to verify IOPS activity for the LUNs.
6. On the destination cluster, use System Manager to verify that the protection for business continuity relationship is in sync: **Protection > Relationships**.

= Reestablish the original protection relationship after an unplanned failover

```
:toc: macro  
:toclevels: 1  
:hardbreaks:  
:icons: font  
:linkattrs:  
:relative_path: ./  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/
```

ONTAP uses the ONTAP Mediator to detect when a failure occurs on the primary storage system and executes automatic unplanned failover to the secondary storage system. You can use System Manager to reverse the relationship and reestablish the original protection relationship when original source cluster is back online.

### Steps

1. Navigate to **Protection > Relationships** and wait for the relationship state to show "InSync."

2. To resume operations on the original source cluster, click  and select **Failover**.

= Installation and setup using the ONTAP CLI

= High level deployment workflow

:hardbreaks:

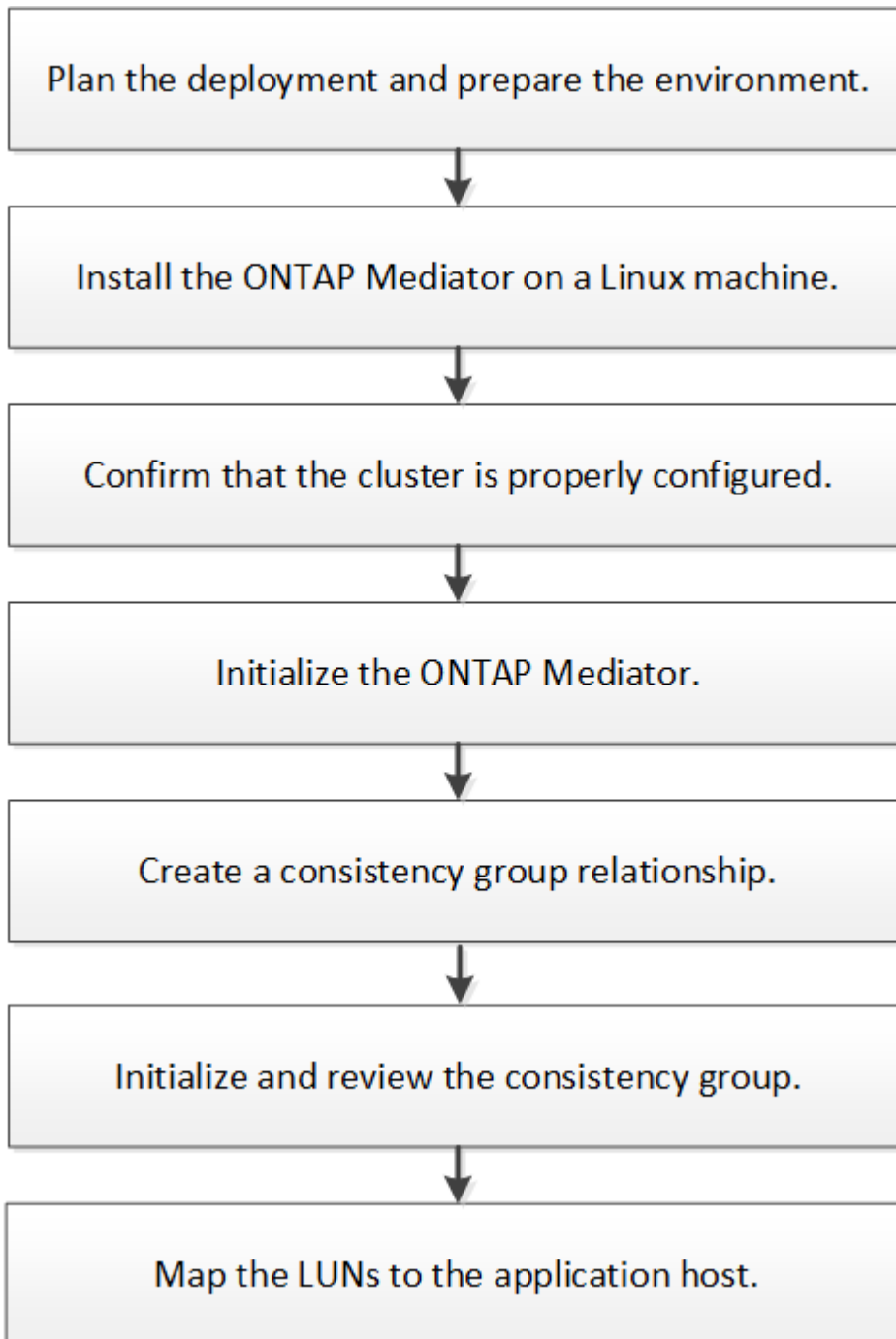
:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the following workflow to install and implement the SnapMirror Business Continuity solution.



= Install ONTAP Mediator Service and confirm the ONTAP cluster configuration

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You should make sure that your source and destination clusters are configured properly.

### About this task

Proceed through each of the following steps. For each step, you should confirm that the specific configuration has been performed. Use the link included after each step to get more information as needed.

### Steps

1. Install the ONTAP Mediator service before you ensure that your source and destination clusters are configured properly.

[ONTAP Mediator service](#)

2. Confirm that a cluster peering relationship exists between the clusters.



The default IPspace is required by SM-BC for cluster peer relationships. Custom IPspace is not supported.

[Configure peer relationships](#)

3. Confirm that the Storage VMs are created on each cluster.

[Creating an SVM](#)

4. Confirm that a peer relationship exists between the Storage VMs on each cluster.

[Creating an SVM peering relationship](#)

5. Confirm that the volumes exist for your LUNs.

[Creating a volume](#)

6. Confirm that at least one SAN LIF is created on each node in the cluster.

[Considerations for LIFs in a cluster SAN environment](#)

[Creating a LIF](#)

7. Confirm that the necessary LUNs are created and mapped to igroup, which is used to map LUNs to the initiator on the application host.

[Create LUNs and map igroups](#)

8. Rescan the application host to discover any new LUNs.

= Initialize the ONTAP Mediator

```
:hardbreaks:
:icons: font
:linkattrs:
:relative_path: ./smbc/
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/
```

You must initialize Mediator on one of your cluster peers before SM-BC can perform planned and automatic unplanned failover operations.

### About this task

You can initialize Mediator from either cluster. When you issue the `mediator add` command on one cluster, Mediator is automatically added on the other cluster.

### Steps

1. Initialize Mediator on one of the clusters:

```
snapmirror mediator add -mediator-address IP_Address -peer-cluster
cluster_name -username user_name
```

### Example

```
cluster1::> snapmirror mediator add -mediator-address 192.168.10.1
-peer-cluster cluster2 -username mediatoradmin
Notice: Enter the mediator password.

Enter the password: *****
Enter the password again: *****
```

2. Check the status of the Mediator configuration:

```
snapmirror mediator show
```

Mediator Address	Peer Cluster	Connection Status	Quorum Status
192.168.10.1	cluster-2	connected	true

`-quorum-status` indicates whether the SnapMirror consistency group relationships are synchronized with Mediator.

= Create a consistency group relationship

```
:hardbreaks:
:icons: font
:linkattrs:
:relative_path: ./smbc/
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/
```

You must create a SM-BC consistency group which also establishes the synchronous consistency group relationship.





This workflow applies to users in ONTAP 9.8 and 9.9.1. If using these ONTAP CLI commands beginning with ONTAP 9.10.1, they will still work to create a consistency group, however, it is recommended that you manage consistency groups with System Manager or the ONTAP REST API.

### Before you begin

The following prerequisites and restrictions apply:

- You must be a cluster or storage VM administrator
- You must have a SnapMirror Synchronous license
- The destination volumes must be type DP
- The primary and the secondary storage VM must be in a peered relationship
- All constituent volumes in a consistency group must be in a single Storage VM
- You cannot establish SM-BC consistency group relationships across ASA clusters and non-ASA clusters
- The name of the consistency group must be unique

### About this task

You must create the consistency group relationship from the destination cluster. You can map up to 12 constituents using the `cg-item-mappings` parameter on the `snapmirror create` command.

### Steps

1. Create a consistency group and constituent relationship. This example creates two consistency groups: `cg_src` with constituent volumes `vol1` and `vol2`, and `cg_dist` with constituent volumes `vol1_dr` and `vol2_dr`.

```
destination::> snapmirror create -source-path vs1_src:/cg/cg_src
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy AutomatedFailOver
```

= Initialize a consistency group

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

After creating a consistency group, you must initialize it.



This workflow applies to users in ONTAP 9.8 and 9.9.1. If using these ONTAP CLI commands beginning with ONTAP 9.10.1, they will still work to initialize a consistency group, however, it is recommended that you manage consistency groups with System Manager or the ONTAP REST API.

### Before you begin

You must be a cluster or storage VM administrator.

### About this task

You initialize the consistency group from the destination cluster.

## Steps

1. Sign in to the ONTAP CLI at the destination cluster and initialize the consistency group:

```
destination::>snapmirror initialize -destination-path vs1_dst:/cg/cg_dst
```

2. Confirm that the initialization operation completed successfully. The status should be InSync.

```
snapmirror show
```

= Mapping LUNs to the application hosts

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You must create an igroup on each cluster so you can map LUNs to the initiator on the application host.

## About this task

You should perform this configuration on both the source and destination clusters.

## Steps

1. Create an igroup on each cluster:

```
lun igroup create -igroup name -protocol fcp|iscsi -ostype os -initiator  
initiator_name
```

## Example

```
lun igroup create -igroup ig1 -protocol iscsi -ostype linux  
-initiator -initiator iqn.2001-04.com.example:abc123
```

2. Map LUNs to the igroup:

```
lun map -path path_name -igroup igroup_name
```

## Example:

```
lun map -path /vol/src1/11 -group ig1
```

3. Verify the LUNs are mapped:

```
lun show
```

4. On the application host, discover the new LUNs.

= Administration

= Create a common Snapshot copy

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

In addition to the regularly scheduled Snapshot copy operations, you can manually create a common Snapshot copy between the volumes in the primary SnapMirror consistency group and the volumes in the secondary SnapMirror consistency group.

In ONTAP 9.8, the scheduled snapshot creation interval is one hour. Beginning with ONTAP 9.9.1, that interval is 12 hours.

### Before you begin

The SnapMirror group relationship must be in sync.

### Steps

1. Create a common Snapshot copy:

```
destination::>snapmirror update -destination-path vs1_dst:/cg/cg_dst
```

2. Monitor the progress of the update:

```
destination::>snapmirror show -fields -newest-snapshot
```

= Perform a planned failover

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can perform a planned failover to test your disaster recovery configuration or to perform maintenance on the primary cluster.

### Before you begin

- The relationship must be in sync
- Nondisruptive operations must not be running
- The ONTAP Mediator must be configured, connected, and in quorum

### About this task

A planned failover is initiated by the administrator of the secondary cluster. The operation requires switching the primary and secondary roles so that the secondary cluster takes over from the primary. The new primary cluster can then begin processing input and output requests locally without disrupting client operations.

### Steps

1. Start the failover operation:

```
destination::>snapmirror failover start -destination-path
```

```
vs1_dst:/cg/cg_dst
```

2. Monitor the progress of the failover:

```
destination:>snapmirror failover show
```

3. When the failover operation is complete, you can monitor the Synchronous SnapMirror protection relationship status from the destination:

```
destination:>snapmirror show
```

= Automatic unplanned failover operations

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

An automatic unplanned failover (AUFO) operation occurs when the primary cluster is down or isolated. When this occurs, the secondary cluster is converted to the primary and begins serving clients. This operation is performed only with assistance from the ONTAP Mediator.



After the automatic unplanned failover, it is important to rescan the host LUN I/O paths so that there is no loss of I/O paths.

You can monitor the status of the automatic unplanned failover by using the `snapmirror failover show` command.

= Basic monitoring

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

There are several SM-BC components and operations you can monitor.

== ONTAP mediator

During normal operation, the Mediator state should be connected. If it is in any other state, this might indicate an error condition. You can review the Event Management System (EMS) messages to determine the error and appropriate corrective actions.

EMS Name	Description
sm.mediator.added	Mediator is added successfully
sm.mediator.removed	Mediator is removed successfully
sm.mediator.unusable	Mediator is unusable due to a corrupted Mediator server

EMS Name	Description
sm.mediator.misconfigured	Mediator is repurposed or the Mediator package is no longer installed on the Mediator server
sm.mediator.unreachable	Mediator is unreachable
sm.mediator.removed.force	Mediator is removed from the cluster using the "force" option
sm.mediator.cacert.expiring	Mediator certificate authority (CA) certificate is due to expire in 30 days or less
sm.mediator.serverc.expiring	Mediator server certificate is due to expire in 30 days or less
sm.mediator.clientc.expiring	Mediator client certificate is due to expire in 30 days or less
sm.mediator.cacert.expired	Mediator certificate authority (CA) certificate has expired
sm.mediator.serverc.expired	Mediator server certificate has expired
sm.mediator.clientc.expired	Mediator client certificate has expired
sm.mediator.in.quorum	All the SM-BC records are resynchronized with Mediator

#### == Planned failover operations

You can monitor status and progress of a planned failover operation using the `snapmirror failover show` command. For example:

```
ClusterB::> snapmirror failover start -destination-path vs1:/cg/dcg1
```

Once the failover operation is complete, you can monitor the Synchronous SnapMirror protection status from the new destination cluster. For example:

```
ClusterA::> snapmirror show
```

You can also review the following messages to determine if there is an error and take the appropriate corrective actions.

EMS Name	Description
smbc.pfo.failed	SMBC planned failover operation failed. Destination path:
smbc.pfo.start. Destination path:	SMBC planned failover operation started

#### == Automatic unplanned failover operations

During an unplanned automatic failover, you can monitor the status of the operation using the `snapmirror failover show` command. For example:

```

ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
    Source Path: vs1:/cg/scg3
    Destination Path: vs3:/cg/dcg3
    Failover Status: completed
    Error Reason:
        End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
    Failover Type: unplanned
Error Reason codes: -

```

You can also review the following messages to determine if there is an error and take the appropriate corrective actions.

EMS Name	Description
smbc.aufo.failed	SnapMirror automatic planned failover operation failed. Destination path:
smbc.aufo.start	SMBC planned failover operation started. Destination path:
smbc.aufo.completed:	SnapMirror automatic planned failover operation completed. Destination path:
smbc.aufo.failover.incapable	block.giveback.during.aufo

== SM-BC availability

You can check the availability of the SM-BC relationship using a series of commands, either on the primary cluster, the secondary cluster, or both.

Commands you use include the `snapmirror mediator show` command on both the primary and secondary cluster to check the connection and quorum status, the `snapmirror show` command, and the `volume show` command. For example:

```

SMBC_A::*> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status
-----
10.236.172.86    SMBC_B                connected          true

SMBC_B::*> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status
-----
10.236.172.86    SMBC_A                connected          true

SMBC_B::*> snapmirror show -expand

Progress
Source          Destination Mirror Relationship Total
Last
Path            Type Path           State Status           Progress Healthy
Updated
-----
-----
vs0:/cg/cg1 XDP vs1:/cg/cg1_dp Snapmirrored InSync -          true
-
vs0:vol1     XDP vs1:vol1_dp  Snapmirrored InSync -          true
-
2 entries were displayed.

SMBC_A::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1
vserver volume is-smbc-master is-smbc-failover-capable smbconsensus
-----
vs0      vol1    true          false          Consensus

SMBC_B::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1_dp
vserver volume is-smbc-master is-smbc-failover-capable smbconsensus
-----
vs1      vol1_dp false          true           No-consensus

```

= Add and remove volumes in a consistency group

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

If you want to change the composition of the consistency group by adding or removing a volume, you must first delete the original relationship and then create the

consistency group again with the new composition.



This workflow applies to ONTAP 9.8 and 9.9.1. Beginning with ONTAP 9.10.1, it is recommended that you manage [consistency groups](#) through System Manager or with the ONTAP REST API.

### About this task

- The composition change is not allowed when the consistency group is in the “InSync” state.
- The destination volume should be of type DP.



The new volume you add to expand the consistency group must have a pair of common Snapshot copies between the source and destination volumes.

### Steps

This procedure assumes that there are two volume mappings: `vol_src1 ↔ vol_dst1` and `vol_src2 ↔ vol_dst2`, in a consistency group relationship between the end points `vs1_src:/cg/cg_src` and `vs1_dst:/cg/cg_dst`.

1. Verify that a common Snapshot copy exists between the source and destination volumes on both the source and destination cluster:

```
source::>snapshot show -vserver vs1_src -volume vol_src3 -snapshot  
snapmirror*
```

```
destination::>snapshot show -vserver vs1_dst -volume vol_dst3 -snapshot  
snapmirror*
```

2. If no common Snapshot copy exists, create and initialize a FlexVol SnapMirror relationship:

```
destination::>snapmirror initialize -source-path vs1_src:vol_src3  
-destination-path vs1_dst:vol_dst3
```

3. Delete the zero RTO consistency group relationship:

```
destination::>snapmirror delete -destination-path vs1_dst:vol_dst3
```

4. Release the source SnapMirror relationship and retain the common Snapshot copies:

```
source::>snapmirror release -relationship-info-only true -destination-path  
vs1_dst:vol_dst3
```

5. Unmap the LUNs and delete the existing consistency group relationship:

```
destination::>lun mapping delete -vserver vs1_dst -path <lun_path> -igroup  
<igroup_name>
```



The destination LUNs are unmapped, while the LUNs on the primary copy continue to serve the host I/O.

```
destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
```



```
source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
-relationship-info-only true
```

6. **If you are using ONTAP 9.10.1 or later**, delete and recreate and the consistency group on the source with the correct composition. Follow the steps in [Delete a consistency group](#) and then [Configure a single consistency group](#). In ONTAP 9.10.1 and later, you must perform the delete and create operations in System Manager or with the ONTAP REST API; there is no CLI procedure.

**If you are using ONTAP 9.8, 9.0, or 9.9.1, skip to the next step.**

7. Create the new consistency group on the destination with the new composition:

```
destination::>snapmirror create -source-path vs1_src:/cg/cg_src
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings vol_src1:@vol_dst1,
vol_src2:@vol_dst2, vol_src3:@vol_dst3
```

8. Resynchronize the zero RTO consistency group relationship to ensure it is in sync:

```
destination::>snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

9. Remap the LUNs that you unmapped in Step 5:

```
destination::> lun map -vserver vs1_dst -path <lun_path> -igroup
<igroup_name>
```

10. Rescan host LUN I/O paths to restore all paths to the LUNs.

= Resume protection in a fan-out configuration with SM-BC

:icons: font

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

:hardbreaks-option:

SM-BC supports [fan-out configurations](#). Your source volume can be mirrored to an SM-BC destination endpoint and to one or more asynchronous SnapMirror relationships.

Fan-out configurations are supported with the `MirrorAllSnapshots` policy, and, beginning with ONTAP 9.11.1, the `MirrorAndVault` policy. Beginning in ONTAP 9.11.1, fan-out configurations in SM-BC are not supported with the `XDPDefault` policy.

If you experience a failover on the SM-BC destination, the asynchronous SnapMirror destination will become unhealthy, and you must manually restore protection by deleting and recreating the relationship with the asynchronous SnapMirror endpoint.

### Resume protection in a fan-out configuration

1. Verify the failover has completed successfully:

```
snapmirror failover show
```

2. On the asynchronous Snapmirror endpoint, delete the fan-out endpoint:

```
snapmirror delete -destination-path destination_path
```

3. On the third site, create an asynchronous SnapMirror relationships between the new SM-BC primary volume and the async fan-out destination volume:

```
snapmirror create -source-path source_path -destination-path  
destination_path -policy MirrorAllSnapshots -schedule schedule
```

4. Resynchronize the relationship:

```
SnapMirror resync -destination-path destination_path
```

5. Verify the relationship status and health:

```
snapmirror show
```

= Convert existing relationships to SM-BC relationships

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can convert an existing zero recovery point protection (zero RPO) Synchronous SnapMirror relationship to an SM-BC zero RTO Synchronous SnapMirror consistency group relationship.

### Before you begin

- A zero RPO Synchronous SnapMirror relationship exists between the primary and secondary.
- All LUNs on the destination volume are unmapped before the zero RTO SnapMirror relationship is created.
- SM-BC only supports SAN protocols (not NFS/CIFS). Ensure no constituent of the consistency group is mounted for NAS access.

### About this task

- You must be a cluster and SVM administrator on the source and destination.
- You cannot convert zero RPO to zero RTO sync by changing the SnapMirror policy.
- If existing LUNs on the secondary volume are mapped, `snapmirror create` with `AutomatedFailover` policy triggers an error.  
You must ensure the LUNs are unmapped before issuing the `snapmirror create` command.

### Steps

1. Perform a SnapMirror update operation on the existing relationship:

```
destination::>snapmirror update -destination-path vs1_dst:vol1
```

2. Verify that the SnapMirror update completed successfully:

```
destination::>snapmirror show
```

3. Quiesce each of the zero RPO synchronous relationships:

```
destination::>snapmirror quiesce -destination-path vs1_dst:vol1
```

```
destination::>snapmirror quiesce -destination-path vs1_dst:vol2
```

4. Delete each of the zero RPO synchronous relationships:

```
destination::>snapmirror delete -destination-path vs1_dst:vol1
```

```
destination::>snapmirror delete -destination-path vs1_dst:vol2
```

5. Release the source SnapMirror relationship but retain the common Snapshot copies:

```
source::>snapmirror release -relationship-info-only true -destination-path vs1_dst:vol1
```

```
source::>snapmirror release -relationship-info-only true -destination-path vs1_dst:vol2
```

6. Create a group zero RTO Synchronous Snapmirror relationship:

```
destination::> snapmirror create -source-path vs1_src:/cg/cg_src  
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings  
vol1:@vol1,vol2:@vol2 -policy AutomatedFailover
```

7. Resynchronize the zero RTO consistency group:

```
destination::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

8. Rescan host LUN I/O paths to restore all paths to the LUNs.

= SM-BC upgrade and revert considerations

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You should be aware of the requirements for upgrading and reverting an SM-BC configuration.

== Upgrade

Before you can configure and use SM-BC, you must upgrade all nodes on the source and destination clusters to ONTAP 9.8 or later.

xref:./encryption-at-rest/[Upgrading software on ONTAP clusters](#)



SM-BC is not supported with mixed ONTAP 9.7 and ONTAP 9.8 clusters.

Upgrading clusters from 9.8 or 9.9.1 to 9.10.1 creates new consistency groups on both source and destination for SM-BC relationships.

== Reverting to ONTAP 9.9.1 from ONTAP 9.10.1

To revert relationships from 9.10.1 to 9.9.1, SM-BC relationships must be deleted, followed by the 9.10.1 consistency group instance. Consistency groups cannot be deleted with an active SMBC relationship. Any FlexVol volumes that were upgraded to 9.10.1 previously associated with another Smart Container or Enterprise App in 9.9.1 or earlier will no longer be associated on revert. Deleting consistency groups does not delete the constituent volumes or volume granular snapshots. Refer to [Delete a consistency group](#) for more information on this task.

## == Reverting to ONTAP 9.7 from ONTAP 9.8

When you revert from ONTAP 9.8 to ONTAP 9.7, you must be aware of the following:

- If the cluster is hosting an SM-BC destination, reverting to ONTAP 9.7 is not allowed until the relationship is broken and deleted.
- If the cluster is hosting an SM-BC source, reverting to ONTAP 9.7 is not allowed until the relationship is released.
- All user-created custom SM-BC SnapMirror policies must be deleted before reverting to ONTAP 9.7.

### Steps

1. Perform a revert check from one of the clusters in the SM-BC relationship:

```
cluster::*> system node revert-to -version 9.7 -check-only
```

Example:

```
cluster::*> system node revert-to -version 9.7 -check-only
Error: command failed: The revert check phase failed. The following
issues must be resolved before revert can be completed. Bring the
data LIFs down on running vservers. Command to list the running
vservers: vserver show -admin-state running Command to list the data
LIFs that are up: network interface show -role data -status-admin up
Command to bring all data LIFs down: network interface modify {-role
data} -status-admin down
Disable snapshot policies.
    Command to list snapshot policies: "snapshot policy show".
    Command to disable snapshot policies: "snapshot policy modify
-vserver
* -enabled false"

Break off the initialized online data-protection (DP) volumes and
delete
Uninitialized online data-protection (DP) volumes present on the
local
node.
    Command to list all online data-protection volumes on the local
node:
    volume show -type DP -state online -node <local-node-name>
    Before breaking off the initialized online data-protection
volumes,
    quiesce and abort transfers on associated SnapMirror
relationships and
    wait for the Relationship Status to be Quiesced.
    Command to quiesce a SnapMirror relationship: snapmirror quiesce
    Command to abort transfers on a SnapMirror relationship:
snapmirror
```

```

abort
  Command to see if the Relationship Status of a SnapMirror
relationship
  is Quiesced: snapmirror show
  Command to break off a data-protection volume: snapmirror break
  Command to break off a data-protection volume which is the
destination
  of a SnapMirror relationship with a policy of type "vault":
snapmirror
  break -delete-snapshots
  Uninitialized data-protection volumes are reported by the
"snapmirror
break" command when applied on a DP volume.
  Command to delete volume: volume delete

Delete current version snapshots in advanced privilege level.
  Command to list snapshots: "snapshot show -fs-version 9.8"
  Command to delete snapshots: "snapshot prepare-for-revert -node
<nodename>"

Delete all user-created policies of the type active-strict-sync-
mirror
and active-sync-mirror.
  The command to see all active-strict-sync-mirror and active-sync-
mirror
  type policies is:
  snapmirror policy show -type
  active-strict-sync-mirror,active-sync-mirror
  The command to delete a policy is :
  snapmirror policy delete -vserver <SVM-name> -policy <policy-
name>

```

For information on reverting clusters, see [Revert ONTAP](#).

= Remove an SM-BC configuration

```

:hardbreaks:
:icons: font
:linkattrs:
:relative_path: ./smbc/
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

```

You can remove zero RTO Synchronous SnapMirror protection and delete the SM-BC relationship configuration.

#### About this task

Before you delete the SM-BC relationship, all LUNs in the destination cluster must be unmapped. After the LUNs are unmapped and the host is rescanned, the SCSI target notifies the hosts that the LUN

inventory has changed. The existing LUNs on the zero RTO secondary volumes change to reflect a new identity after the zero RTO relationship is deleted. Hosts discover the secondary volume LUNs as new LUNs that have no relationship to the source volume LUNs.

The secondary volumes remain DP volumes after the relationship is deleted. You can issue the `snapmirror break` command to convert them to read/write.

Deleting the relationship is not allowed in the failed-over state when the relationship is not reversed.

### Steps

1. Delete the SM-BC consistency group relationship between the source endpoint and destination endpoint:

```
Destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
```

2. From the source cluster, release the consistency group relationship and the Snapshot copies created for the relationship:

```
Source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
```

3. Perform a host rescan to update the LUN inventory.
4. Beginning with ONTAP 9.10.1, deleting the SnapMirror relationship does not delete the consistency group. If you want to delete the consistency group, you must use System Manager or the ONTAP REST API. See [Delete a consistency group](#) for more information.

= Remove ONTAP Mediator

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

If you want to remove an existing ONTAP Mediator configuration from your ONTAP clusters, you can do so by using the `snapmirror mediator remove` command.

### Steps

1. Remove ONTAP Mediator:

```
snapmirror mediator remove -mediator-address 12.345.678.90 -peer-cluster  
cluster_xyz
```

= Troubleshooting

= SnapMirror delete operation fails in takeover state

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

### Issue:

When ONTAP 9.9.1 is installed on a cluster, executing the `snapmirror delete` command fails when an SM-BC consistency group relationship is in takeover state.

**Example:**

```
C2_cluster::> snapmirror delete vs1:/cg/dd

Error: command failed: RPC: Couldn't make connection
```

**Solution**

When the nodes in an SM-BC relationship are in takeover state, perform the SnapMirror delete and release operation with the "-force" option set to true.

**Example:**

```
C2_cluster::> snapmirror delete vs1:/cg/dd -force true

Warning: The relationship between source "vs0:/cg/ss" and destination
        "vs1:/cg/dd" will be deleted, however the items of the
destination
        Consistency Group might not be made writable, deletable, or
modifiable
        after the operation. Manual recovery might be required.
Do you want to continue? {y|n}: y
Operation succeeded: snapmirror delete for the relationship with
destination "vs1:/cg/dd".
```

= Failure creating a SnapMirror relationship and initializing consistency group

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

**Issue:**

Creation of SnapMirror relationship and consistency group initialization fails.

**Solution:**

Ensure that you have not exceeded the limit of consistency groups per cluster. Consistency group limits in SM-BC are platform independent and differ based on the version of ONTAP. See [Additional restrictions and limitations](#) for limitations based on ONTAP version.

**Error:**

If the consistency group is stuck initializing, check the status of your consistency group initializations with the ONTAP REST API, System Manager or the command `sn show -expand`.


**Solution:**

If consistency groups fail to initialize, remove the SM-BC relationship, delete the consistency group, then recreate the relationship and initialize it. This workflow differs depending on the version of ONTAP you are using.

**If you are using ONTAP 9.8-9.9.1**

1. [Remove the SM-BC configuration](#)
2. [Create a consistency group relationship](#)
3. [Initialize the consistency group relationship](#)

**If you are using ONTAP 9.10.1 or later**

1. Under **Protection > Relationships**, find the SM-BC relationship on the consistency group. Select , then **Delete** to remove the SM-BC relationship.
2. [Delete the consistency group](#)
3. [Configure the consistency group](#)

= Planned failover unsuccessful

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

**Issue:**

After executing the `snapmirror failover start` command, the output for the `snapmirror failover show` command displays a message indicates that a nondisruptive operation is in progress.

**Example:**

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-----
vs1:/cg/cg vs0:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
Failover cannot start because a volume move is running. Retry the
command once volume move has finished.
08:35:04
```

**Cause:**

Planned failover cannot begin when a nondisruptive operation is in progress, including volume move, aggregate relocation, and storage failover.

**Solution:**

Wait for the nondisruptive operation to complete and try the failover operation again.

= Mediator not reachable or Mediator quorum status is false

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/



**Issue:**

After executing the `snapmirror failover start` command, the output for the `snapmirror failover show` command displays a message indicating that Mediator is not configured.

See [Initialize the ONTAP Mediator](#).

**Example:**

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-----
vs0:/cg/cg vs1:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
failover cannot start because the source-side precheck failed. reason:
Mediator not configured.
05:50:42 05:50:43
```

**Cause:**

Mediator is not configured or there are network connectivity issues.

**Solution:**

If Mediator is not configured, you must configure Mediator before you can establish an SM-BC relationship. Fix any network connectivity issues. Make sure Mediator is connected and quorum status is true on both the source and destination site using the `snapmirror mediator show` command.

**Example:**

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster Connection Status Quorum Status
-----
10.234.10.143 cluster2 connected true
```

= Automatic unplanned failover not triggered on Site B

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

**Issue:**

A failure on Site A does not trigger an unplanned failover on Site B.

**Possible cause #1:**

Mediator is not configured. To determine if this is the cause, issue the `snapmirror mediator show` command on the Site B cluster.

**Example:**

```
Cluster2::*> snapmirror mediator show
This table is currently empty.
```

This example indicates that Mediator is not configured on Site B.

**Solution:**

Ensure that Mediator is configured on both clusters, that the status is connected, and quorum is set to True.

**Possible cause #2:**

SnapMirror consistency group is out of sync. To determine if this is the cause, view the event log to view if the consistency group was in sync during the time at which the Site A failure occurred.

**Example:**

```
cluster::*> event log show -event *out.of.sync*

Time                Node                Severity            Event
-----
-----
10/1/2020 23:26:12  sti42-vsimsim-ucs511w ERROR
sms.status.out.of.sync: Source volume "vs0:zrto_cg_556844_511u_RW1" and
destination volume "vs1:zrto_cg_556881_511w_DP1" with relationship UUID
"55ab7942-03e5-11eb-ba5a-005056a7dc14" is in "out-of-sync" status due
to the following reason: "Transfer failed."
```

**Solution:**

Complete the following steps to perform a forced failover on Site B.

1. Unmap all LUNs belonging to the consistency group from Site B.
2. Delete the SnapMirror consistency group relationship using the `force` option.
3. Enter the `snapmirror break` command on the consistency group constituent volumes to convert volumes from DP to R/W, to enable I/O from Site B.
4. Boot up the Site A nodes to create a zero RTO relationship from Site B to Site A.
5. Release the consistency group with `relationship-info-only` on Site A to retain common Snapshot copy and unmap the LUNs belonging to the consistency group.
6. Convert volumes on Site A from R/W to DP by setting up a volume level relationship using either the Sync policy or Async policy.
7. Issue the `snapmirror resync` to synchronize the relationships.
8. Delete the SnapMirror relationships with the Sync policy on Site A.
9. Release the SnapMirror relationships with Sync policy using `relationship-info-only true` on Site B.
10. Create a consistency group relationship from Site B to Site A.

11. Perform a consistency group resync from Site A, and then verify that the consistency group is in sync.
12. Rescan host LUN I/O paths to restore all paths to the LUNs.

= Link between Site B and Mediator down and Site A down

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

To check on the connection of the Mediator, use the `snapmirror mediator show` command. If the connection status is unreachable and Site B is unable to reach Site B, you will have an output similar to the one below. Follow the steps in the solution to restore connection

### Example:

```
cluster::*> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status
-----
10.237.86.17      C1_cluster      unreachable      true
SnapMirror consistency group relationship status is out of sync.

C2_cluster::*> snapmirror show -expand
Source          Destination Mirror Relationship Total
Last
Path           Type Path           State Status           Progress Healthy
Updated
-----
vs0:/cg/src_cg_1 XDP vs1:/cg/dst_cg_1 Snapmirrored OutOfSync - false
-
vs0:zrto_cg_655724_188a_RW1 XDP vs1:zrto_cg_655755_188c_DP1
Snapmirrored OutOfSync - false -
vs0:zrto_cg_655733_188a_RW2 XDP vs1:zrto_cg_655762_188c_DP2
Snapmirrored OutOfSync - false -
vs0:zrto_cg_655739_188b_RW1 XDP vs1:zrto_cg_655768_188d_DP1
Snapmirrored OutOfSync - false -
vs0:zrto_cg_655748_188b_RW2 XDP vs1:zrto_cg_655776_188d_DP2
Snapmirrored OutOfSync - false -
5 entries were displayed.

Site B cluster is unable to reach Site A.
C2_cluster::*> cluster peer show
Peer Cluster Name      Cluster Serial Number Availability
Authentication
-----
C1_cluster              1-80-000011          Unavailable      ok
```

### Solution

Force a failover to enable I/O from Site B and then establish a zero RTO relationship from Site B to Site A.

Complete the following steps to perform a forced failover on Site B.

1. Unmap all LUNs belonging to the consistency group from Site B.
2. Delete the SnapMirror consistency group relationship using the force option.
3. Enter the snapmirror break command on the consistency group constituent volumes to convert volumes from DP to RW, to enable I/O from Site B.
4. Boot up the Site A nodes to create a zero RTO relationship from Site B to Site A.

5. Release the consistency group with relationship-info-only on Site A to retain common Snapshot copy and unmap the LUNs belonging to the consistency group.
6. Convert volumes on Site A from RW to DP by setting up a volume level relationship using either Sync policy or Async policy.
7. Issue the snapmirror resync to synchronize the relationships.
8. Delete the SnapMirror relationships with Sync policy on Site A.
9. Release the SnapMirror relationships with Sync policy using relationship-info-only true on Site B.
10. Create a consistency group relationship from Site B to Site A.
11. Perform a consistency group resync from Site A, and then verify that the consistency group is in sync.
12. Rescan host LUN I/O paths to restore all paths to the LUNs.

= Link between Site A and Mediator down and Site B down

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

When using SM-BC, you may lose connectivity between the mediator or your peered clusters. You can diagnose the issue by checking the connection, availability, and consensus status of the different parts of the SM-BC relationship and then forcefully resuming connection.

**Table 3. Determining the cause**

What to check	CLI command	Indicator
Mediator from Site A	<code>snapmirror mediator show</code>	The connection status will be unreachable
Site B connectivity	<code>cluster peer show</code>	Availability will be unavailable
Consensus status of the SM-BC volume	<code>volume show volume_name -fields smbc-consensus</code>	The sm-bc consensus field will read Awaiting-consensus

For additional information about diagnosing and resolving this issue, refer to the Knowledge Base article [Link between Site A and Mediator down and Site B down when using SM-BC](#).

= SM-BC SnapMirror delete operation fails when fence is set on destination volume

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

**Issue:**

SnapMirror delete operation fails when any of the destination volumes have redirection fence set.

**Solution**

Performing the following operations to retry the redirection and remove the fence from the destination

volume.

- SnapMirror resync
- SnapMirror update

= Volume move operation stuck when primary is down

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

**Issue:**

A volume move operation is stuck indefinitely in cutover deferred state when the primary site is down in an SM-BC relationship.

When the primary site is down, the secondary site performs an automatic unplanned failover (AUFO). When a volume move operation is in progress when the AUFO is triggered the volume move becomes stuck.

**Solution:**

Abort the volume move instance that is stuck and restart the volume move operation.

= SnapMirror release fails when unable to delete Snapshot copy

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

**Issue:**

The SnapMirror release operation fails when the Snapshot copy cannot be deleted.

**Solution:**

The Snapshot copy contains a transient tag. Use the `snapshot delete` command with the `-ignore-owners` option to remove the transient Snapshot copy.

```
snapshot delete -volume <volume_name> -snapshot <snapshot_name> -ignore-owners true -force true
```

Retry the `snapmirror release` command.

= Volume move reference Snapshot copy shows as the newest

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./smbc/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

**Issue:**

After performing a volume move operation on a consistency group volume, the volume move reference Snapshot copy might display as the newest for the SnapMirror relationship.

You can view the newest Snapshot copy with the following command:

```
snapmirror show -fields newest-snapshot status -expand
```

**Solution:**

Manually perform a `snapmirror resync` or wait for the next automatic resync operation after the volume move operation completes.

= Mediator service for MetroCluster and SnapMirror Business Continuity

= Install or upgrade the ONTAP Mediator service

:icons: font

:relative\_path: ./mediator/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

To install the ONTAP Mediator service, you must ensure all prerequisites are met, get the installation package and run the installer on the host. This procedure is used for an installation or an upgrade of an existing installation.

**About this task**

- Beginning with ONTAP 9.7, you can use any version of ONTAP Mediator to monitor a MetroCluster IP configuration.
- Beginning with ONTAP 9.8, you can use any version of ONTAP Mediator to monitor an SM-BC relationship.

**Before you begin**

You must meet the following prerequisites.

Mediator version	Supported Linux versions
1.4	<ul style="list-style-type: none"><li>• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5</li><li>• CentOS: 7.6, 7.7, 7.8, 7.9</li></ul>
1.3	<ul style="list-style-type: none"><li>• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3</li><li>• CentOS: 7.6, 7.7, 7.8, 7.9</li></ul>
1.2	<ul style="list-style-type: none"><li>• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 8.1</li><li>• CentOS: 7.6, 7.7, 7.8</li></ul>



The kernel version must match the operating system version.

- 64-bit physical installation or virtual machine
- 8 GB RAM
- User: Root access

== Upgrade the host operating system and then the Mediator

The following table provides the upgrade guidelines if you are upgrading from RHEL/CentOS 7.6 to a later

RHEL/CentOS release in addition upgrading the Mediator version.

Target Linux version	Target Mediator version	Upgrade notes
<ul style="list-style-type: none"> <li>Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 8.1</li> <li>CentOS: 7.6, 7.7, 7.8</li> </ul>	1.2	<ul style="list-style-type: none"> <li>The upgrade must be performed in the following order:               <ol style="list-style-type: none"> <li>Upgrade the operating system from RHEL/CentOS version.</li> <li>Reboot the host to apply the kernel module changes.</li> <li>Upgrade the Mediator from the immediately prior version to the current version.</li> </ol> </li> <li>For MetroCluster:               <ol style="list-style-type: none"> <li>The storage iscsi-initiator show command will report that the connection to the Mediator service is down during the upgrade.</li> <li>The ONTAP operating system will generate the following EMS events:                   <ol style="list-style-type: none"> <li>cf.mccip.med.auso.stDisabled during the upgrade</li> <li>cf.mccip.med.auso.stEnabled when automatic unplanned switchover is re-enabled</li> </ol> </li> </ol> </li> </ul>
<ul style="list-style-type: none"> <li>Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3</li> <li>CentOS: 7.6, 7.7, 7.8, 7.9</li> </ul>	1.3	<ol style="list-style-type: none"> <li>Upgrade the operating system from RHEL/CentOS version.</li> <li>Reboot the host to apply the kernel module changes.</li> <li>Upgrade the Mediator from the immediately prior version to the current version.</li> </ol>
<ul style="list-style-type: none"> <li>Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5</li> <li>CentOS: 7.6, 7.7, 7.8, 7.9</li> </ul>	1.4	<ol style="list-style-type: none"> <li>Upgrade the operating system from RHEL/CentOS version.</li> <li>Reboot the host to apply the kernel module changes.</li> <li>Upgrade the Mediator from the immediately prior version to the current version.</li> </ol>

The best practices for installing Red Hat Enterprise Linux or CentOS and the associated repositories on your system are listed below. Systems installed or configured differently might require additional steps.

- You must install Red Hat Enterprise Linux or CentOS according to Red Hat best practices. Due to end-of-life support for CentOS 8.x versions, compatible versions of CentOS 8.x are not recommended.
- While installing the ONTAP Mediator service on Red Hat Enterprise Linux or CentOS, the system must have access to the appropriate repository so that the installation program can access and install all the required software dependencies.



- For the yum installer to find dependent software in the Red Hat Enterprise Linux repositories, you must have registered the system during the Red Hat Enterprise Linux installation or afterwards by using a valid Red Hat subscription.

See the Red Hat documentation for information about the Red Hat Subscription Manager.

- The following ports must be unused and available for the Mediator:
  - 31784
  - 3260
- If using a third-party firewall: refer to [Firewall requirements for ONTAP Mediator](#)
- If the Linux host is in a location without access to the internet, you must ensure that the required packages are available in a local repository.

If you are using Link Aggregation Control Protocol (LACP) in a Linux environment, you must correctly configure the kernel and make sure the `sysctl net.ipv4.conf.all.arp_ignore` is set to "2".

The following packages are required by the ONTAP Mediator service:

All RHEL/CentOS versions	Additional packages for RHEL/CentOS 7.x	Additional packages for RHEL 8.x
<ul style="list-style-type: none"> <li>• openssl</li> <li>• openssl-devel</li> <li>• kernel-devel</li> <li>• gcc</li> <li>• libselinux-utils</li> <li>• make</li> <li>• redhat-lsb-core</li> <li>• patch</li> <li>• bzip2</li> <li>• python36</li> <li>• python36-devel</li> <li>• perl-Data-Dumper</li> <li>• perl-ExtUtils-MakeMaker</li> <li>• python3-pip</li> </ul>	<ul style="list-style-type: none"> <li>• policycoreutils-python</li> <li>• python36-pip</li> </ul>	<ul style="list-style-type: none"> <li>• elfutils-libelf-devel</li> <li>• policycoreutils-python-utils</li> </ul>

The Mediator installation package is a self-extracting compressed tar file that includes:

- An RPM file containing all dependencies that cannot be obtained from the supported release's repository.
- An install script.

A valid SSL certification is recommended, as documented in this procedure.

== Enable access to the repositories

If your operating system is...	You must provide access to these repositories...
RHEL 7.x	rhel-7-server-optional-rpms
CentOS 7.x	C7.6.1810 - Base repository
RHEL 8.x	<ul style="list-style-type: none"><li>• rhel-8-for-x86_64-baseos-rpms</li><li>• rhel-8-for-x86_64-appstream-rpms</li></ul>

Enable access to the repositories listed above so Mediator can access the required packages during the installation process. Use the procedure below for your operating system.

- Procedure for [RHEL 7.x](#) operating system.
- Procedure for [RHEL 8.x](#) operating system.
- Procedure for [CentOS 7.x](#) operating system.

=== Procedure for RHEL 7.x operating system

If your operating system is **RHEL 7.x**:

### Steps

1. Subscribe to the required repository:

```
subscription-manager repos --enable rhel-7-server-optional-rpms
```

The following example shows the execution of this command:

```
[root@localhost ~]# subscription-manager repos --enable rhel-7-  
server-optional-rpms  
Repository 'rhel-7-server-optional-rpms' is enabled for this system.
```

2. Run the `yum repolist` command.

The following example shows the execution of this command. The "rhel-7-server-optional-rpms" repository should appear in the list.

```

[root@localhost ~]# yum repolist
Loaded plugins: product-id, search-disabled-repos, subscription-
manager
rhel-7-server-optional-rpms | 3.2 kB  00:00:00
rhel-7-server-rpms | 3.5 kB  00:00:00
(1/3): rhel-7-server-optional-rpms/7Server/x86_64/group
| 26 kB  00:00:00
(2/3): rhel-7-server-optional-rpms/7Server/x86_64/updateinfo
| 2.5 MB  00:00:00
(3/3): rhel-7-server-optional-rpms/7Server/x86_64/primary_db
| 8.3 MB  00:00:01
repo id                                repo name
status
rhel-7-server-optional-rpms/7Server/x86_64  Red Hat Enterprise
Linux 7 Server - Optional (RPMs)  19,447
rhel-7-server-rpms/7Server/x86_64          Red Hat Enterprise
Linux 7 Server (RPMs)              26,758
repolist: 46,205
[root@localhost ~]#

```

=== Procedure for RHEL 8.x operating system

If your operating system is **RHEL 8.x**:

### Steps

1. Subscribe to the required repository:

```
subscription-manager repos --enable rhel-8-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-8-for-x86_64-appstream-rpms
```

The following example shows the execution of this command:

```

[root@localhost ~]# subscription-manager repos --enable rhel-8-for-
x86_64-baseos-rpms
[root@localhost ~]# subscription-manager repos --enable rhel-8-for-
x86_64-appstream-rpms
Repository 'rhel-8-for-x86_64-baseos-rpms' is enabled for this
system.
Repository 'rhel-8-for-x86_64-appstream-rpms' is enabled for this
system.

```

2. Run the `yum repolist` command.

The newly subscribed repositories should appear in the list.

=== Procedure for CentOS 7.x operating system

If your operating system is **CentOS 7.x**:



The following examples are showing a repository for CentOS 7.6 and may not work for other CentOS versions. Use the base repository for your version of CentOS.

### Steps

1. Add the C7.6.1810 - Base repository. The C7.6.1810 - Base vault repository contains the kernel-level package needed for ONTAP Mediator.
2. Add the following lines to `/etc/yum.repos.d/CentOS-Vault.repo`.

```
[C7.6.1810-base]
name=CentOS-7.6.1810 - Base
baseurl=http://vault.centos.org/7.6.1810/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
enabled=1
```

3. Run the `yum repolist` command.

The following example shows the execution of this command. The CentOS-7.6.1810 - Base repository should appear in the list.

```

Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: distro.ibiblio.org
 * extras: distro.ibiblio.org
 * updates: ewr.edge.kernel.org
C7.6.1810-base |
3.6 kB 00:00:00
(1/2): C7.6.1810-base/x86_64/group_gz |
166 kB 00:00:00
(2/2): C7.6.1810-base/x86_64/primary_db |
6.0 MB 00:00:04
repo id                repo name
status
C7.6.1810-base/x86_64  CentOS-7.6.1810 -
Base
10,019
base/7/x86_64          CentOS-7 - Base
10,097
extras/7/x86_64       CentOS-7 - Extras
307
updates/7/x86_64      CentOS-7 - Updates
1,010
repolist: 21,433
[root@localhost ~]#

```

== Download the Mediator installation package

### Steps

1. Download the Mediator installation package from the ONTAP Mediator page.

[ONTAP Mediator download page](#)

2. Confirm that the Mediator installation package is in the target directory:

```
ls
```

```
[root@mediator-host ~]#ls
ontap-mediator
```

If you are at a location without access to the internet, you must ensure that the installer has access to the required packages.

3. If necessary, move the Mediator installation package from the download directory to the installation directory on the Linux Mediator host.

== Install the ONTAP Mediator installation package

## About this task

- Beginning with ONTAP Mediator 1.4, the Secure Boot mechanism is enabled on UEFI systems. When Secure Boot is enabled, you must take additional steps to register the security key after installation:
  - Follow instructions in the README file:  
`/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-signing`  
to sign the SCST kernel module.
  - Locate the required keys:  
`/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys`



After installation, the README files and key location are also provided in the system output.

## Step

1. Install the Mediator installation package and respond to the prompts as required:

```
./ontap-mediator
```

The installation process proceeds to create the required accounts and install required packages. If you have a previous version of Mediator installed on the host, you will be prompted to confirm that you want to upgrade.

```
[root@scs000065018 ~]# ./ontap-mediator
ONTAP Mediator: Self Extracting Installer
ONTAP Mediator requires two user accounts. One for the service (netapp),
and one for use by ONTAP to the mediator API (mediatoradmin).
Would you like to use the default account names: netapp + mediatoradmin?
(Y(es)/n(o)): y
Enter ONTAP Mediator user account (mediatoradmin) password:
Re-Enter ONTAP Mediator user account (mediatoradmin) password:
Checking if SELinux is in enforcing mode
Checking for default Linux firewall
Linux firewall is running. Open ports 31784 and 3260? y(es)/n(o): y
success
success

Preparing for installation of ONTAP Mediator packages.
Do you wish to continue? Y(es)/n(o): y
+ Installing required packages.
Last metadata expiration check: 1:56:17 ago on Thu 07 Apr 2022 11:35:42 AM
EDT.
Package openssl-1:1.1.1k-6.el8_5.x86_64 is already installed.
Package openssl-devel-1:1.1.1k-6.el8_5.x86_64 is already installed.
```

```
.
.
.
.

Dependencies resolved.
Nothing to do.
Complete!
OS package installations finished
+ Installing ONTAP Mediator. (Log: /tmp/ontap_mediator.5gmxnI/ontap-
mediator/install_20220407133105.log)
    This step will take several minutes. Use the log file to view
progress.
Sudo include verified
ONTAP Mediator logging enabled
+ Install successful. (Moving log to
/opt/netapp/lib/ontap_mediator/log/install_20220407133105.log)
+ WARNING: This system supports UEFI
    Secure Boot (SB) is currently enabled on this system.
    The following action need be taken:
    Using the keys in
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys follow
instructions in
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-
signing
    to sign the SCST kernel module. Note that reboot will be
needed.
    SCST will not start automatically when Secure Boot is enabled and not
configured properly.
+ Note: ONTAP Mediator uses a kernel module compiled specifically for the
current
    system OS. Using 'yum update' to upgrade the kernel may cause a
service
    interruption.
    For more information, see /opt/netapp/lib/ontap_mediator/README
[root@scs000065018 ~]#
```

== Verify the installation

### Steps

1. Run the following commands to view the status of the ONTAP Mediator services:

a. Run: `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service;
enabled; vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1
weeks 0 days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi
--ini /opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi
--ini /opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
└─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi
--ini /opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

b. Run: `systemctl status mediator-scst`



```
[root@scspr1915530002 ~]# systemctl status mediator-scst
Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
Main PID: 286662 (iscsi-scstd)
Tasks: 1 (limit: 49473)
Memory: 1.2M
CGroup: /system.slice/mediator-scst.service
└─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

## 2. Confirm the ports the ONTAP Mediator service is using: netstat

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'
```

tcp	0	0	0.0.0.0:31784	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:3260	0.0.0.0:*	LISTEN
tcp6	0	0	:::3260	:::*	LISTEN

### == Result

The ONTAP Mediator service is now installed and running. Further configuration must be performed in the ONTAP storage system to use the Mediator features:

- To use the ONTAP Mediator service in a MetroCluster IP configuration, see [Configuring the ONTAP Mediator service from a MetroCluster IP configuration](#)
- To use SnapMirror Business Continuity, see [Install ONTAP Mediator Service and confirm the ONTAP cluster configuration](#)

### = Manage the ONTAP mediator service

:icons: font

:relative\_path: ./mediator/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

After you have installed ONTAP Mediator service, you may change the user name or password. You may also uninstall the ONTAP Mediator Service.

### == Change the user name

### About these tasks

This task is performed on the Linux host on which the ONTAP Mediator service is installed.

If you are unable to reach this command, you might need to run the command using the full path as shown in the following example:

```
/usr/local/bin/mediator_username
```

### Procedure

Change the username by choosing one of the following options:

- Run the command `mediator_change_user` and respond to the prompts as shown in the following example:

```
[root@mediator-host ~]# mediator_change_user
Modify the Mediator API username by entering the following values:
  Mediator API User Name: mediatoradmin
                        Password:
New Mediator API User Name: mediator
The account username has been modified successfully.
[root@mediator-host ~]#
```

- Run the following command:

```
MEDIATOR_USERNAME=mediator MEDIATOR_PASSWORD=mediator2
MEDIATOR_NEW_USERNAME=mediatoradmin mediator_change_user
```

```
[root@mediator-host ~]# MEDIATOR_USERNAME= mediator
MEDIATOR_PASSWORD='mediator2' MEDIATOR_NEW_USERNAME= mediatoradmin
mediator_change_user
The account username has been modified successfully.
[root@mediator-host ~]#
```

== Change the password

### About this task

This task is performed on the Linux host on which the ONTAP Mediator service is installed.

If you are unable to reach this command, you might need to run the command using the full path as shown in the following example:

```
/usr/local/bin/mediator_change_password
```

### Procedure

Change the password by choosing one of the following options:

- Run the `mediator_change_password` command and respond to the prompts as shown in the following example:

```
[root@mediator-host ~]# mediator_change_password
Change the Mediator API password by entering the following values:
  Mediator API User Name: mediatoradmin
    Old Password:
    New Password:
    Confirm Password:
The password has been updated successfully.
[root@mediator-host ~]#
```

- Run the following command:

```
MEDIATOR_USERNAME= mediatoradmin MEDIATOR_PASSWORD=mediator1
MEDIATOR_NEW_PASSWORD=mediator2 mediator_change_password
```

The example shows the password is changed from "mediator1" to "mediator2".

```
[root@mediator-host ~]# MEDIATOR_USERNAME=mediatoradmin
MEDIATOR_PASSWORD=mediator1 MEDIATOR_NEW_PASSWORD=mediator2
mediator_change_password
The password has been updated successfully.
[root@mediator-host ~]#
```

== Uninstall the ONTAP Mediator service

### Before you begin

If necessary, you can remove the ONTAP Mediator service. The Mediator must be disconnected from ONTAP before you remove the Mediator service.

### About this task

This task is performed on the Linux host on which the ONTAP Mediator service is installed.

If you are unable to reach this command, you might need to run the command using the full path as shown in the following example:

```
/usr/local/bin/uninstall_ontap_mediator
```

### Step

1. Uninstall the ONTAP Mediator service:

```
uninstall_ontap_mediator
```

```
[root@mediator-host ~]# uninstall_ontap_mediator

ONTAP Mediator: Self Extracting Uninstaller

+ Removing ONTAP Mediator. (Log:
/tmp/ontap_mediator.GmRGdA/uninstall_ontap_mediator/remove.log)
+ Remove successful.
[root@mediator-host ~]#
```

= Manage MetroCluster sites with System Manager

= MetroCluster site management overview with System Manager

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.8, you can use System Manager as a simplified interface for managing a configuration of a MetroCluster setup.

A MetroCluster configuration allows two clusters to mirror data to each other so if one cluster goes down, the data isn't lost.

Typically, an organization sets up the clusters in two separate geographical locations. An administrator at each location sets up a cluster and configures it. Then one of the administrators can set up the peering between the clusters so that they can share data.

The organization can also install an ONTAP Mediator in a third location. The ONTAP Mediator service monitors the status of each cluster. When one of the clusters detects that it cannot communicate with the partner cluster, it queries the monitor to determine if the error is a problem with the cluster system or with the network connection.

If the problem is with the network connection, the system administrator performs troubleshooting methods to correct the error and reconnect. If the partner cluster is down, the other cluster initiates a switchover process to control the data I/O for both clusters.

You can also perform a switchover to bring down one of the cluster systems for planned maintenance. The partner cluster handles all data I/O operations for both clusters until you bring up the cluster on which you performed maintenance and perform a switchback operation.

You can manage the following operations:

- [Set up an IP MetroCluster site](#)
- [Set up IP MetroCluster peering](#)
- [Configure an IP MetroCluster site](#)
- [Perform IP MetroCluster switchover and switchback](#)

- [Troubleshoot problems with IP MetroCluster configurations](#)
- [Upgrade ONTAP on MetroCluster clusters](#)

= Set up an IP MetroCluster site

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.8, you can use System Manager to set up an IP configuration of a MetroCluster site.

A MetroCluster site consists of two clusters. Typically, the clusters are located in different geographical locations.

### Before you start

- Your system should already be installed and cabled according to the [Installation and Setup Instructions](#) that came with the system.
- Cluster network interfaces should be configured on each node of each cluster for intra-cluster communication.

== Assign a node-management IP address

=== Windows System

You should connect your Windows computer to the same subnet as the controllers. This will automatically assign a node-management IP address to your system.

### Steps

1. From the Windows system, open the **Network** drive to discover the nodes.
2. Double-click the node to launch the cluster setup wizard.

=== Other systems

You should configure the node-management IP address for one of the nodes in your cluster. You can use this node-management IP address to launch the cluster set up wizard.

See [Creating the cluster on the first node](#) for information about assigning a node-management IP address.

== Initialize and configure the cluster

You initialize the cluster by setting an administrative password for the cluster and setting up the cluster management and node management networks. You can also configure services like a DNS server to resolve host names and an NTP server to synchronize time.

### Steps

1. On a web browser, enter the node-management IP address that you have configured: "https://node-management-IP"

System Manager automatically discovers the remaining nodes in the cluster.

2. In the **Initialize Storage System** window, perform the following:
  - a. Enter cluster management network configuration data.
  - b. Enter Node management IP addresses for all the nodes.
  - c. Provide domain name servers (DNS) details.
  - d. In the **Other** section, select the check box labeled **Use time service (NTP)** to add the time servers.

When you click **Submit**, wait for the cluster to be created and configured. Then, a validation process occurs.

### What's Next?

After both clusters have been set up, initialized, and configured, perform the following procedure:

- [Set up IP MetroCluster peering](#)

== Configure ONTAP on a new cluster video



= Set up IP MetroCluster peering

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.8, you can manage an IP configuration of a MetroCluster operation with System Manager. After setting up two clusters, you set up peering between them.

## Before you start

You should have completed the following procedure to set up two clusters:

- [Set up an IP MetroCluster site](#)

Certain steps of this process are performed by different system administrators located at the geographical sites of each cluster. For the purposes of explaining this process, the clusters are called "Site A cluster" and "Site B cluster".

== Performing the peering process from Site A

This process is performed by a system administrator at Site A.

### Steps

1. Log in to Site A cluster.
2. In System Manager, select **Dashboard** from the left navigation column to display the cluster overview.

The dashboard shows the details for this cluster (Site A). In the **MetroCluster** section, Site A cluster is shown on the left.

3. Click **Attach Partner Cluster**.
4. Enter the details of the network interfaces that allow the nodes in Site A cluster to communicate with the nodes in Site B cluster.
5. Click **Save and Continue**.
6. On the **Attach Partner Cluster** window, select **I do not have a passphrase**, which lets you generate a passphrase.
7. Copy the generated passphrase and share it with the system administrator at Site B.
8. Select **Close**.

== Performing the peering process from Site B

This process is performed by a system administrator at Site B.

### Steps

1. Log in to Site B cluster.
2. In System Manager, select **Dashboard** to display the cluster overview.

The dashboard shows the details for this cluster (Site B). In the MetroCluster section, Site B cluster is shown on the left.

3. Click **Attach Partner Cluster** to start the peering process.
4. Enter the details of the network interfaces that allow the nodes in Site B cluster to communicate with the nodes in Site A cluster.
5. Click **Save and Continue**.
6. On the **Attach Partner Cluster** window, select **I have a passphrase**, which lets you enter the passphrase that you received from the system administrator at Site A.
7. Select **Peer** to complete the peering process.

**What's next?**

After the peering process is successfully completed, you configure the clusters. See [Configure an IP MetroCluster site](#).

= Configure an IP MetroCluster site

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.8, you can manage an IP configuration of a MetroCluster operation with System Manager. After setting up two clusters and peering them, you configure each cluster.

### Before you start

You should have completed the following procedures:

- [Set up an IP MetroCluster site](#)
- [Set up IP MetroCluster peering](#)

== Configure the connection between clusters

### Steps

1. Log in to System Manager on one of the sites, and select **Dashboard**.

In the **MetroCluster** section, the graphic shows the two clusters that you set up and peered for the MetroCluster sites. The cluster you are working from (local cluster) is shown on the left.

2. Click **Configure MetroCluster**. From this window, you can perform the following tasks:
  - a. The nodes for each cluster in the MetroCluster configuration are shown. Use the drop-down lists to select which nodes in the local cluster will be disaster recovery partners with which nodes in the remote cluster.
  - b. Click the check box if you want to configure an ONTAP Mediator service. See [\[Configure the ONTAP Mediator service\]](#).
  - c. If both clusters have a license to enable encryption, the **Encryption** section is displayed.

To enable encryption, enter a passphrase.

- d. Click the check box if you want to configure MetroCluster with shared layer 3 network.



The HA partner nodes and network switches connecting to the nodes must have a matching configuration.

3. Click **Save** to configure the MetroCluster sites.

On the **Dashboard**, in the **MetroCluster** section, the graphic shows a check mark on the link between the two clusters, indicating a healthy connection.

== Configure the ONTAP Mediator service




The ONTAP Mediator service is typically installed at a geographic location separate from either location of the clusters. The clusters communicate regularly with the service to indicate that they are up and running. If one of the clusters in the MetroCluster configuration detects that the communication with its partner cluster is down, it checks with the ONTAP Mediator to determine if the partner cluster itself is down.

### Before you start

Both clusters at the MetroCluster sites should be up and peered.

### Steps

1. In System Manager in ONTAP 9.8, select **Cluster > Settings**.
2. In the **Mediator** section, click .
3. On the **Configure Mediator** window, click **Add+**.
4. Enter the configuration details for the ONTAP Mediator.

= Perform IP MetroCluster switchover and switchback

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can switch over control from one IP MetroCluster site to the other to perform maintenance or recover from an issue.



Switchover and switchback procedures are supported only for IP MetroCluster configurations.

== Overview of switchover and switchback

A switchover can occur in two instances:

- **A planned switchover**

This switchover is initiated by a system administrator using System Manager. The planned switchover allows a system administrator of a local cluster to switch control so that the data services of the remote cluster are handled by the local cluster. Then, a system administrator at the remote cluster location can perform maintenance on the remote cluster.

- **An unplanned switchover**

In some cases, when a MetroCluster cluster goes down or the connections between the clusters are down, ONTAP will automatically initiate a switchover procedure so that the cluster that is still running handles the data handling responsibilities of the down cluster.

At other times, when ONTAP cannot determine the status of one of the clusters, the system administrator of the site that is working initiates the switchover procedure to take control of the data handling responsibilities of the other site.

For any type of switchover procedure, the data servicing capability is returned to the cluster by using a *switchback* process.

You perform different switchover and switchback processes for ONTAP 9.7 and 9.8:

- [Use System Manager in ONTAP 9.7 for switchover and switchback](#)
- [Use System Manager in ONTAP 9.8 for switchover and switchback](#)

== Use System Manager in ONTAP 9.7 for switchover and switchback

### Steps

1. Log in to System Manager in ONTAP 9.7.
2. Click **(Return to classic version)**.
3. Click **Configuration > MetroCluster**.


System Manager verifies whether a negotiated switchover is possible.

4. Perform one of the following substeps when the validation process has completed:
  - a. If validation fails, but Site B is up, then an error has occurred. For example, there might be a problem with a subsystem, or NVRAM mirroring might not be synchronized.
    - i. Fix the issue that is causing the error, click **Close**, and then start again at Step 2.
    - ii. Halt the Site B nodes, click **Close**, and then perform the steps in [Performing an unplanned switchover](#).
  - b. If validation fails, and Site B is down, then most likely there is a connection problem. Verify that Site B is really down, then perform the steps in [Performing an unplanned switchover](#).
5. Click **Switchover from Site B to Site A** to initiate the switchover process.
6. Click **Switch to the new experience**.

== Use System Manager in ONTAP 9.8 for switchover and switchback

=== Perform a planned switchover (ONTAP 9.8)

### Steps

1. Log in to System Manager in ONTAP 9.8.
2. Select **Dashboard**. In the **MetroCluster** section, the two clusters are shown with a connection.
3. In the local cluster (shown on the left), click , and select **Take control of remote site**.

After the switchover request is validated, control is transferred from the remote site to the local site, which performs data service requests for both clusters.

The remote cluster reboots, but the storage components are not active, and the cluster does not service data requests. It is now available for planned maintenance.



The remote cluster should not be used for data servicing until you perform a switchback.

=== Perform an unplanned switchover (ONTAP 9.8)

An unplanned switchover might be initiated automatically by ONTAP. If ONTAP cannot determine if a switchback is needed, the system administrator of the MetroCluster site that is still running initiates the switchover with the following steps:

### Steps

1. Log in to System Manager in ONTAP 9.8.
2. Select **Dashboard**.

In the **MetroCluster** section, the connection between the two clusters is shown with an "X" on it, meaning a connection cannot be detected. Either the connections or the cluster is down.

3. In the local cluster (shown on the left), click , and select **Take control of remote site**.

After the switchover request is validated, control is transferred from the remote site to the local site, which performs data service requests for both clusters.

The cluster must be repaired before it is brought online again.



After the remote cluster is brought online again, it should not be used for data servicing until you perform a switchback.

=== Perform a switchback (ONTAP 9.8)


### Before you start

Whether the remote cluster was down due to planned maintenance or due to a disaster, it should now be up and running and waiting for the switchback.


### Steps

1. On the local cluster, log in to System Manager in ONTAP 9.8.
2. Select **Dashboard**.

In the **MetroCluster** section, the two clusters are shown.

3. In the local cluster (shown on the left), click , and select **Take back control**.

The data is *healed* first, to ensure data is synchronized and mirrored between both clusters.

4. When the data healing is complete, click , and select **Initiate switchback**.

When the switchback is complete, both clusters are active and servicing data requests. Also, the data is being mirrored and synchronized between the clusters.

= Modify address, netmask, and gateway in a MetroCluster IP

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.10.1, you can change the following properties of a MetroCluster IP interface: IP address and mask, and gateway. You can use any combination of parameters to update.

You might need to update these properties, for example, if a duplicate IP address is detected or if a gateway needs to change in the case of a layer 3 network due to router configuration changes. You can

only change one interface at a time. There will be traffic disruption on that interface until the other interfaces are updated and connections are reestablished.



You must make the changes on each port. Similarly, network switches also need to update their configuration. For example, if the gateway is updated, ideally it is changed on both nodes of an HA pair, since they are same. Plus the switch connected to those nodes also needs to update its gateway.

### Step

Update the IP address, netmask, and gateway for a each node and interface.

= Troubleshoot problems with IP MetroCluster configurations

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.8, System Manager monitors the health of IP MetroCluster configurations and helps you identify and correct problems that might occur.

== Overview of the MetroCluster Health Check

System Manager periodically checks the health of your IP MetroCluster configuration. When you view the MetroCluster section in the Dashboard, usually the message is "MetroCluster systems are healthy."

However, when a problem occurs, the message will show the number of events. You can click on that message and view the results of the health check for the following components:

- Node
- Network Interface
- Tier (Storage)
- Cluster
- Connection
- Volume
- Configuration Replication

The **Status** column identifies which components have problems, and the **Details** column suggests how to correct the problem.

== MetroCluster troubleshooting

### Steps

1. In System Manager, select **Dashboard**.
2. In the **MetroCluster** section, notice the message.
  - a. If the message indicates that your MetroCluster configuration is healthy, and the connections between the clusters and the ONTAP Mediator are healthy (shown with check marks), then you have no problems to correct.

- b. If the message lists the number of events, or the connections have gone down (shown with an "X"), then continue to the next step.
3. Click the message that shows the number of events.

The MetroCluster Health Report displays.

4. Troubleshoot the problems that appear in the report using the suggestions in the **Details** column.
5. When all the problems have been corrected, click **Check MetroCluster Health**.



The MetroCluster Health Check uses an intensive amount of resources, so it is recommended that you perform all your troubleshooting tasks before running the check.

The MetroCluster Health Check runs in the background. You can work on other tasks while you wait for it to finish.

= Data protection using tape backup

= Tape backup of FlexVol volumes overview

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

ONTAP supports tape backup and restore through Network Data Management Protocol (NDMP). NDMP allows you to back up data in storage systems directly to tape, resulting in efficient use of network bandwidth. ONTAP supports both dump and SMTape engines for tape backup.

You can perform a dump or SMTape backup or restore by using NDMP-compliant backup applications. Only NDMP version 4 is supported.

== Tape backup using dump

Dump is a Snapshot copy based backup in which your file system data is backed up to tape. The ONTAP dump engine backs up files, directories, and the applicable access control list (ACL) information to tape. You can back up an entire volume, an entire qtree, or a subtree that is not an entire volume or an entire qtree. Dump supports baseline, differential, and incremental backups.

== Tape backup using SMTape

SMTape is a Snapshot copy based disaster recovery solution from ONTAP that backs up blocks of data to tape. You can use SMTape to perform volume backups to tapes. However, you cannot perform a backup at the qtree or subtree level. SMTape supports baseline, differential, and incremental backups.

= Tape backup and restore workflow

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can perform tape backup and restore operations by using an NDMP-enabled backup application.

## About this task

The tape backup and restore workflow provides an overview of the tasks that are involved in performing tape backup and restore operations. For detailed information about performing a backup and restore operation, see the backup application documentation.

## Steps

1. Set up a tape library configuration by choosing an NDMP-supported tape topology.
2. Enable NDMP services on your storage system.

You can enable the NDMP services either at the node level or at the storage virtual machine (SVM) level. This depends on the NDMP mode in which you choose to perform the tape backup and restore operation.

3. Use NDMP options to manage NDMP on your storage system.

You can use NDMP options either at the node level or at the SVM level. This depends on the NDMP mode in which you choose to perform the tape backup and restore operation.

You can modify the NDMP options at the node level by using the `system services ndmp modify` command and at the SVM level by using the `vserver services ndmp modify` command. For more information about these commands, see the man pages.

4. Perform a tape backup or restore operation by using an NDMP-enabled backup application.

ONTAP supports both dump and SMTape engines for tape backup and restore.

For more information about using the backup application (also called *Data Management Applications* or *DMAs*) to perform backup or restore operations, see your backup application documentation.

## Related information

[Common NDMP tape backup topologies](#)

[Understanding dump engine for FlexVol volumes](#)

= Use cases for choosing a tape backup engine

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

ONTAP supports two backup engines: SMTape and dump. You should be aware of the use cases for the SMTape and dump backup engines to help you choose the backup engine to perform tape backup and restore operations.

Dump can be used in the following cases:

- Direct Access Recovery (DAR) of files and directories
- Backup of a subset of subdirectories or files in a specific path
- Excluding specific files and directories during backups
- Preserving backup for long durations

SMTape can be used in the following cases:

- Disaster recovery solution
- Preserving deduplication savings and deduplication settings on the backed up data during a restore operation
- Backup of large volumes

= Manage tape drives

= Manage tape drives overview

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can verify tape library connections and view tape drive information before performing a tape backup or restore operation. You can use a nonqualified tape drive by emulating this to a qualified tape drive. You can also assign and remove tape aliases in addition to viewing existing aliases.

When you back up data to tape, the data is stored in tape files. File marks separate the tape files, and the files have no names. You specify a tape file by its position on the tape. You write a tape file by using a tape device. When you read the tape file, you must specify a device that has the same compression type that you used to write that tape file.

= Commands for managing tape drives, media changers, and tape drive operations

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

There are commands for viewing information about tape drives and media changers in a cluster, bringing a tape drive online and taking it offline, modifying the tape drive cartridge position, setting and clearing tape drive alias name, and resetting a tape drive. You can also view and reset tape drive statistics.

If you want to...	Use this command...
Bring a tape drive online	<code>storage tape online</code>
Clear an alias name for tape drive or media changer	<code>storage tape alias clear</code>
Enable or disable a tape trace operation for a tape drive	<code>storage tape trace</code>
Modify the tape drive cartridge position	<code>storage tape position</code>
Reset a tape drive	<code>storage tape reset</code>

This command is available only at the advanced privilege level.

a|  
Set an alias name for tape drive or media changer  
a|  
storage tape alias set  
a|  
Take a tape drive offline  
a|  
storage tape offline  
a|  
View information about all tape drives and media changers  
a|  
storage tape show  
a|  
View information about tape drives attached to the cluster  
a|

- storage tape show-tape-drive
- system node hardware tape drive show

a|  
View information about media changers attached to the cluster  
a|  
storage tape show-media-changer  
a|  
View error information about tape drives attached to the cluster  
a|  
storage tape show-errors  
a|  
View all ONTAP qualified and supported tape drives attached to each node in the cluster  
a|  
storage tape show-supported-status  
a|  
View aliases of all tape drives and media changers attached to each node in the cluster  
a|  
storage tape alias show  
a|  
Reset the statistics reading of a tape drive to zero  
a|  
storage stats tape zero tape\_name

You must use this command at the nodeshell.

a|  
View tape drives supported by ONTAP  
a|  
storage show tape supported [-v]

You must use this command at the nodeshell. You can use the `-v` option to view more details about each tape drive.

a|  
View tape device statistics to understand tape performance and check usage pattern



a|

```
storage stats tape tape_name
```

You must use this command at the nodeshell.

For more information about these commands, see the man pages.

= Use a nonqualified tape drive  
:icons: font  
:relative\_path: ./tape-backup/  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

[.lead]

You can use a nonqualified tape drive on a storage system if it can emulate a qualified tape drive. It is then treated like a qualified tape drive. To use a nonqualified tape drive, you must first determine whether it emulates any of the qualified tape drives.

.About this task

A nonqualified tape drive is one that is attached to the storage system, but not supported or recognized by ONTAP.

.Steps

. View the nonqualified tape drives attached to a storage system by using the `storage tape show-supported-status` command.

+

The following command displays tape drives attached to the storage system and the support and qualification status of each tape drive. The nonqualified tape drives are also listed.

`tape_drive_vendor_name` is a nonqualified tape drive attached to the storage system, but not supported by ONTAP.

+

----

```
cluster1::> storage tape show-supported-status -node Node1
```

persistent

off}\*`

+

`scsi` selects the SCSI Reserve/Release mechanism.

+

`persistent` selects SCSI Persistent Reservations.

+

`off` disables tape reservations.

.Related information

[What tape reservations are](#)

= Commands for verifying tape library connections

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

[.lead]

You can view information about the connection path between a storage system and a tape library configuration attached to the storage system. You can use this information to verify the connection path to the tape library configuration or for troubleshooting issues related to the connection paths.

You can view the following tape library details to verify the tape library connections after adding or creating a new tape library, or after restoring a failed path in a single-path or multipath access to a tape library. You can also use this information while troubleshooting path-related errors or if access to a tape library fails.

\* Node to which the tape library is attached

\* Device ID

\* NDMP path

\* Tape library name

| If you want to...| Use this command...

a|

View information about a tape library in a cluster

a|

system node hardware tape library show

a|

View path information for a tape library

a|

storage tape library path show

a|

View path information for a tape library for every initiator port

a|

storage tape library path show-by-initiator

a|

View connectivity information between a storage tape library and cluster

a|

storage tape library config show

For more information about these commands, see the man pages.

:leveloffset: -1

= About tape drives

:leveloffset: +1

= Qualified tape drives overview

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

[.lead]

You must use a qualified tape drive that has been tested and found to work properly on a storage system. You can follow tape aliasing and also enable tape reservations to ensure that only one storage system accesses a tape drive at any particular time.

A qualified tape drive is a tape drive that has been tested and found to work properly on storage systems. You can qualify tape drives for existing ONTAP releases by using the tape configuration file.

= Format of the tape configuration file

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

[.lead]

The tape configuration file format consists of fields such as vendor ID, product ID, and details of compression types for a tape drive. This file also consists of optional fields for enabling the autoloading feature of a tape drive and changing the command timeout values of a tape drive.

The following table displays the format of the tape configuration file:

[options="header"]

Item	Size	Description
------	------	-------------

a		
---	--	--

vendor_id	(string)	
-----------	----------	--

a		
---	--	--

up to 8 bytes		
---------------	--	--

a		
---	--	--

The vendor ID as reported by the SCSI Inquiry command.		
--	--	--

a		
---	--	--

product_id	(string)	
------------	----------	--

a|  
up to 16 bytes  
a|  
The product ID as reported by the SCSI Inquiry command.

a|  
id\_match\_size(number)

a|  
The number of bytes of the product ID to be used for matching to detect the tape drive to be identified, beginning with the first character of the product ID in the Inquiry data.

a|  
vendor\_pretty (string)

a|  
up to 16 bytes

a|  
If this parameter is present, it is specified by the string displayed by the command, `storage tape show -device-names`; otherwise, `INQ_VENDOR_ID` is displayed.

a|  
product\_pretty(string)

a|  
up to 16 bytes

a|  
If this parameter is present, it is specified by the string displayed by the command, `storage tape show -device-names`; otherwise, `INQ_PRODUCT_ID` is displayed.

[NOTE]

The `vendor_pretty` and `product_pretty` fields are optional, but if one of these fields has a value, the other must also have a value.

The following table explains the description, density code, and compression algorithm for the various compression types, such as l, m, h, and a:

Item	Size	Description
{l   m   h   a}_description=(string)	up to 24 bytes	The string to print for the nodeshell command, <code>sysconfig -t</code> , that describes characteristics of the particular density setting.
{l   m   h   a}_density=(hex codes)		The density code to be set in the SCSI mode page block descriptor corresponding to the desired density code for l, m, h, or a.
{l   m   h   a}_algorithm=(hex codes)		The compression algorithm to be set in the SCSI Compression Mode Page corresponding to the density code and the desired density characteristic.

The following table describes the optional fields available in the tape configuration file:

Field	Description
autoload=(Boolean yes/no)	This field is set to <code>yes</code> if the tape drive has an automatic loading feature; that is, after tape cartridge is inserted, the tape drive becomes ready without the need to execute a SCSI <code>load (start/stop unit)</code> command. The default for this field is <code>no</code> .
cmd_timeout_0x	Individual timeout value. You must use this field only if you want to specify a different timeout value from the one being used as a default by the tape driver. The sample file lists the default SCSI command timeout values used by the tape drive. The timeout value can be expressed in minutes (m), seconds (s), or milliseconds (ms).

You should not change this field.



You can download and view the tape configuration file from the NetApp Support Site.

.Example of a tape configuration file format

The tape configuration file format for the HP LTO5 ULTRIUM tape drive is as follows:

```
vendor_id="HP"

product_id="Ultrium 5-SCSI"

id_match_size=9

vendor_pretty="Hewlett-Packard"

product_pretty="LTO-5"

l_description="LTO-3(ro)/4 4/800GB"

l_density=0x00

l_algorithm=0x00

m_description="LTO-3(ro)/4 8/1600GB cmp"

m_density=0x00

m_algorithm=0x01

h_description="LTO-5 1600GB"

h_density=0x58

h_algorithm=0x00

a_description="LTO-5 3200GB cmp"

a_density=0x58

a_algorithm=0x01

autoload="yes"
```

.Related information

[NetApp Tools: Tape Device Configuration Files](#)

= How the storage system qualifies a new tape drive dynamically

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/



If you record a tape using a no-rewind device, you must rewind the tape before you read it.

st is the standard designation for a tape drive.

alias\_number is the alias that ONTAP assigns to the tape drive. When ONTAP detects a new tape drive, ONTAP assigns an alias to the tape drive.

compression\_type is a drive-specific code for the density of data on the tape and the type of compression.

The following list describes the various values for compression\_type:

- a  
Highest compression
- h  
High compression
- m  
Medium compression
- l  
Low compression

### Examples

nrst0a specifies a no-rewind device on tape drive 0 using the highest compression.

### Example of a listing of tape devices

The following example shows the tape devices associated with HP Ultrium 2-SCSI:

```
                Tape drive (fc202_6:2.126L1)  HP          Ultrium 2-SCSI
rst01 - rewind device,          format is: HP (200GB)
nrst01 - no rewind device,      format is: HP (200GB)
urst01 - unload/reload device,  format is: HP (200GB)
rst0m - rewind device,          format is: HP (200GB)
nrst0m - no rewind device,      format is: HP (200GB)
urst0m - unload/reload device,  format is: HP (200GB)
rst0h - rewind device,          format is: HP (200GB)
nrst0h - no rewind device,      format is: HP (200GB)
urst0h - unload/reload device,  format is: HP (200GB)
rst0a - rewind device,          format is: HP (400GB w/comp)
nrst0a - no rewind device,      format is: HP (400GB w/comp)
urst0a - unload/reload device,  format is: HP (400GB w/comp)
```

The following list describes the abbreviations in the preceding example:

- GB—Gigabytes; this is the capacity of the tape.

- w/comp—With compression; this shows the tape capacity with compression.

= Supported number of simultaneous tape devices

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

ONTAP supports a maximum of 64 simultaneous tape drive connections, 16 medium changers, and 16 bridge or router devices for each storage system (per node) in any mix of Fibre Channel, SCSI, or SAS attachments.

Tape drives or medium changers can be devices in physical or virtual tape libraries or stand-alone devices.

Although a storage system can detect 64 tape drive connections, the maximum number of backup and restore sessions that can be performed simultaneously depends upon the scalability limits of the backup engine.

### Related information

[Scalability limits for dump backup and restore sessions](#)

= Tape aliasing

= Tape aliasing overview

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Aliasing simplifies the process of device identification. Aliasing binds a physical path name (PPN) or a serial number (SN) of a tape or a medium changer to a persistent, but modifiable alias name.

The following table describes how tape aliasing enables you to ensure that a tape drive (or tape library or medium changer) is always associated with a single alias name:

Scenario	Reassigning of the alias
When the system reboots	The tape drive is automatically reassigned its previous alias.
When a tape device moves to another port	The alias can be adjusted to point to the new address.
When more than one system uses a particular tape device	The user can set the alias to be the same for all the systems.

When you upgrade from Data ONTAP 8.1.x to Data ONTAP 8.2.x, the tape alias feature of Data ONTAP 8.2.x modifies the existing tape alias names. In such a case you might have to update the tape alias names in the backup application.

Assigning tape aliases provides a correspondence between the logical names of backup devices (for example, st0 or mc1) and a name permanently assigned to a port, a tape drive, or a medium changer.

st0 and st00 are different logical names.

Logical names and serial numbers are used only to access a device. After the device is accessed, it returns all error messages by using the physical path name.

There are two types of names available for aliasing: physical path name and serial number.

= What physical path names are

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Physical path names (PPNs) are the numerical address sequences that ONTAP assigns to tape drives and tape libraries based on the SCSI-2/3 adapter or switch (specific location) they are connected to the storage system. PPNs are also known as electrical names.

PPNs of direct-attached devices use the following format: `host_adapter.device_id_lun`

The LUN value is displayed only for tape and medium changer devices whose LUN values are not zero; that is, if the LUN value is zero the `lun` part of the PPN is not displayed.

For example, the PPN 8.6 indicates that the host adapter number is 8, the device ID is 6, and the logical unit number (LUN) is 0.

SAS tape devices are also direct-attached devices. For example, the PPN 5c.4 indicates that in a storage system, the SAS HBA is connected in slot 5, SAS tape is connected to port C of the SAS HBA, and the device ID is 4.

PPNs of Fibre Channel switch-attached devices use the following format: `switch:port_id.device_id_lun`

For example, the PPN MY\_SWITCH:5.3L2 indicates that the tape drive connected to port 5 of a switch called MY\_SWITCH is set with device ID 3 and has the LUN 2.

The LUN (logical unit number) is determined by the drive. Fibre Channel, SCSI tape drives and libraries, and disks have PPNs.

PPNs of tape drives and libraries do not change unless the name of the switch changes, the tape drive or library moves, or the tape drive or library is reconfigured. PPNs remain unchanged after reboot. For example, if a tape drive named MY\_SWITCH:5.3L2 is removed and a new tape drive with the same device ID and LUN is connected to port 5 of the switch MY\_SWITCH, the new tape drive would be accessible by using MY\_SWITCH:5.3L2.

= What serial numbers are

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

**A serial number (SN) is a unique identifier for a tape drive or a medium changer. ONTAP generates aliases based on SN instead of the WWN.**

Since the SN is a unique identifier for a tape drive or a medium changer, the alias remains the same regardless of the multiple connection paths to the tape drive or medium changer. This helps storage systems to track the same tape drive or medium changer in a tape library configuration.

The SN of a tape drive or a medium changer does not change even if you rename the Fibre Channel switch to which the tape drive or medium changer is connected. However, in a tape library if you replace an existing tape drive with a new one, then ONTAP generates new aliases because the SN of the tape drive changes. Also, if you move an existing tape drive to a new slot in a tape library or remap the tape drive's LUN, ONTAP generates a new alias for that tape drive.

You must update the backup applications with the newly generated aliases.

The SN of a tape device uses the following format: SN[xxxxxxxxxxx]L[X]

x is an alphanumeric character and LX is the LUN of the tape device. If the LUN is 0, the LX part of the string is not displayed.

Each SN consists of up to 32 characters; the format for the SN is not case-sensitive.

= Considerations when configuring multipath tape access

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can configure two paths from the storage system to access the tape drives in a tape library. If one path fails, the storage system can use the other paths to access the tape drives without having to immediately repair the failed path. This ensures that tape operations can be restarted.

You must consider the following when configuring multipath tape access from your storage system:

- In tape libraries that support LUN mapping, for multipath access to a LUN group, LUN mapping must be symmetrical on each path.

Tape drives and media changers are assigned to LUN groups (set of LUNs that share the same initiator path set) in a tape library. All tape drives of a LUN group must be available for backup and restore operations on all multiple paths.

- A maximum of two paths can be configured from the storage system to access the tape drives in a tape library.
- Multipath tape access supports load balancing. Load balancing is disabled by default.

In the following example, the storage system accesses LUN group 0 through two initiator paths: 0b and 0d. In both these paths, the LUN group has the same LUN number, 0, and LUN count, 5. The storage system accesses LUN group 1 through only one initiator path, 3d.

```
STSW-3070-2_cluster::> storage tape library config show

Node                LUN Group  LUN Count  Library Name  Library
Target Port  Initiator
-----
-----
STSW-3070-2_cluster-01      0      5      IBM 3573-TL_1
510a09800000412d      0b

0d

50050763124b4d6f      3d      2      IBM 3573-TL_2

3 entries were displayed
```

For more information, see the man pages.

= How you add tape drives and libraries to storage systems

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can add tape drives and libraries to storage system dynamically (without taking the storage system offline).

When you add a new medium changer, the storage system detects its presence and adds it to the configuration. If the medium changer is already referenced in the alias information, no new logical names are created. If the library is not referenced, the storage system creates a new alias for the medium changer.

In a tape library configuration, you must configure a tape drive or medium changer on LUN 0 of a target port for ONTAP to discover all medium changers and tape drives on that target port.

= What tape reservations are

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Multiple storage systems can share access to tape drives, medium changers, bridges, or tape libraries. Tape reservations ensure that only one storage system accesses a device at any particular time by enabling either the SCSI Reserve/Release mechanism or SCSI Persistent Reservations for all tape drives, medium changers, bridges, and tape libraries.

All the systems that share devices in a library, whether switches are involved or not, must use the same reservation method.

The SCSI Reserve/Release mechanism for reserving devices works well under normal conditions. However, during interface error recovery procedures, reservations can be lost. If this occurs, initiators other than the reserved owner can access the device.

Reservations made with SCSI Persistent Reservations are not affected by error recovery mechanisms, such as loop reset or target reset; however, not all devices implement SCSI Persistent Reservations correctly.

= Transfer data using ndmcopy

= Transfer data using ndmcopy overview

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

The `ndmcopy` nodeshell command transfers data between storage systems that support NDMP v4. You can perform both full and incremental data transfers. You can transfer full or partial volumes, qtrees, directories, or individual files.

### About this task

Using ONTAP 8.x and earlier releases, incremental transfers are limited to a maximum of two levels (one full and up to two incremental backups).

Beginning with ONTAP 9.0 and later releases, incremental transfers are limited to a maximum of nine levels (one full and up to nine incremental backups).

You can run `ndmcopy` at the nodeshell command line of the source and destination storage systems, or a storage system that is neither the source nor the destination of the data transfer. You can also run `ndmcopy` on a single storage system that is both the source and the destination of the data transfer.

You can use IPv4 or IPv6 addresses of the source and destination storage systems in the `ndmcopy` command. The path format is `/vserver_name/volume_name \[path\]`.

### Steps

1. Enable NDMP service on the source and destination storage systems:

<b>If you are performing data transfer at the source or destination in...</b>	<b>Use the following command...</b>
SVM-scoped NDMP mode	<code>vserver services ndmp on</code>

For NDMP authentication in the admin SVM, the user account is `admin` and the user role is `admin` or `backup`. In the data SVM, the user account is `vsadmin` and the user role is `vsadmin` or `vsadmin-backup` role.



```

a|
Node-scoped NDMP mode
a|
system services ndmp on

```

<p>. Transfer data within a storage system or between storage systems using the <code>ndmpcopy</code> command at the nodeshell:</p> <pre> + `*::&gt; system node run -node &lt;node_name&gt; &lt; ndmpcopy [options] source_IP:source_path destination_IP:destinatio n_path [-mcs {inet </pre>	<pre> inet6}} [-mcd {inet </pre>	<pre> inet6}} [-md {inet </pre>	<pre> inet6}}*` + [NOTE] </pre>
--	----------------------------------	---------------------------------	---------------------------------

DNS names are not supported in `ndmpcopy`. You must provide the IP address of the source and the destination. The loopback address (127.0.0.1) is not supported for the source IP address or the destination IP address.

- The `ndmcopy` command determines the address mode for control connections as follows:
  - The address mode for control connection corresponds to the IP address provided.
  - You can override these rules by using the `-mcs` and `-mcd` options.
- If the source or the destination is the ONTAP system, then depending on the NDMP mode (node-scoped or SVM-scoped), use an IP address that allows access to the target volume.
- `source_path` and `destination_path` are the absolute path names till the granular level of volume, `qtree`, directory or file.
- `-mcs` specifies the preferred addressing mode for the control connection to the source storage system.

`inet` indicates an IPv4 address mode and `inet6` indicates an IPv6 address mode.

- `-mcd` specifies the preferred addressing mode for the control connection to the destination storage system.

`inet` indicates an IPv4 address mode and `inet6` indicates an IPv6 address mode.

- `-md` specifies the preferred addressing mode for data transfers between the source and the destination storage systems.

`inet` indicates an IPv4 address mode and `inet6` indicates an IPv6 address mode.

If you do not use the `-md` option in the `ndmcopy` command, the addressing mode for the data connection is determined as follows:

- If either of the addresses specified for the control connections is an IPv6 address, the address mode for the data connection is IPv6.
- If both the addresses specified for the control connections are IPv4 addresses, the `ndmcopy` command first attempts an IPv6 address mode for the data connection.

If that fails, the command uses an IPv4 address mode.

An IPv6 address, if specified, must be enclosed within square brackets.

+

This sample command migrates data from a source path (`source_path`) to a destination path (`destination_path`).

+

```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password>
  -st md5 -dt md5 192.0.2.129:/<src_svm>/<src_vol>
192.0.2.131:/<dst_svm>/<dst_vol>
```

+

This sample command explicitly sets the control connections and the data connection to use IPv6 address mode:

+

```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password> -st md5
-dt md5 -mcs inet6 -mcd inet6 -md
  inet6 [2001:0db8:1:1:209:6bff:feae:6d67]:/<src_svm>/<src_vol>
[2001:0ec9:1:1:200:7cgg:gfd7:7e78]:/<dst_svm>/<dst_vol>
```

= Options for the `ndmpcopy` command

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You should understand the options available for the `ndmpcopy` `nodeshell` command to successfully transfer data.

The following table lists the available options. For more information, see the `ndmpcopy` man pages available through the `nodeshell`.

Option	Description
<code>-sa username:[password]</code>	<p>This option sets the source authentication user name and password for connecting to the source storage system. This is a mandatory option.</p> <p>For a user without admin privilege, you must specify the user's system-generated NDMP-specific password. The system-generated password is mandatory for both admin and non-admin users.</p>

Option	Description
-da username:[password]	This option sets the destination authentication user name and password for connecting to the destination storage system. This is a mandatory option.
-st {md5 text}	This option sets the source authentication type to be used when connecting to the source storage system. This is a mandatory option and therefore the user should provide either the <code>text</code> or <code>md5</code> option.
-dt {md5 text}	This option sets the destination authentication type to be used when connecting to the destination storage system.
-l	This option sets the dump level used for the transfer to the specified value of level. Valid values are 0, 1, to 9, where 0 indicates a full transfer and 1 to 9 specifies an incremental transfer. The default is 0.
-d	This option enables generation of ndmpcopy debug log messages. The ndmpcopy debug log files are located in the <code>/mroot/etc/log</code> root volume. The ndmpcopy debug log file names are in the <code>ndmpcopy.yyyymmdd</code> format.
-f	This option enables the forced mode. This mode enables system files to be overwritten in the <code>/etc</code> directory on the root of the 7-Mode volume.
-h	This option prints the help message.
-p	This option prompts you to enter the password for source and destination authorization. This password overrides the password specified for <code>-sa</code> and <code>-da</code> options.

You can use this option only when the command is running in an interactive console.

a|

-exclude

a|

This option excludes specified files or directories from the path specified for data transfer. The value can be a comma-separated list of directory or file names such as **.pst** or **.txt**.

:leveloffset: -1

= NDMP for FlexVol volumes

:leveloffset: +1

= About NDMP for FlexVol volumes

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

[.lead]

The Network Data Management Protocol (NDMP) is a standardized protocol for controlling backup, recovery, and other types of data transfer between primary and secondary storage devices, such as storage systems and tape libraries.

By enabling NDMP support on a storage system, you enable that storage system to communicate with NDMP-enabled network-attached backup applications (also called *Data Management Applications* or *DMAs*), data servers, and tape servers participating in backup or recovery operations. All network communications occur over TCPIP or TCP/IPv6 network. NDMP also provides low-level control of tape drives and medium changers.

You can perform tape backup and restore operations in either node-scoped NDMP mode or storage virtual machine (SVM) scoped NDMP mode.

You must be aware of the considerations that you have to take into account while using NDMP, list of environment variables, and supported NDMP tape backup topologies. You can also enable or disable the enhanced DAR functionality. The two authentication methods supported by ONTAP for authenticating NDMP access to a storage system are: plaintext and challenge.

.Related information

[Environment variables supported by ONTAP](#)

= About NDMP modes of operation

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

[.lead]

You can choose to perform tape backup and restore operations either at the node level as you have been doing until now or at the storage virtual machine (SVM) level. To perform these operations successfully at the SVM level, NDMP service must be enabled on the SVM.

If you upgrade from Data ONTAP 8.2 to Data ONTAP 8.3, the NDMP mode of operation used in 8.2 will continue to be retained post the upgrade from 8.2 to 8.3.

This mode is deprecated and will be removed in a future major release.

### Related information

[Managing node-scoped NDMP mode for FlexVol volumes](#)

= What SVM-scoped NDMP mode is

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can perform tape backup and restore operations at the storage virtual machine (SVM) level successfully if the NDMP service is enabled on the SVM. You can back up and restore all volumes hosted across different nodes in the SVM of a cluster if the backup application supports the CAB extension.

An NDMP control connection can be established on different LIF types. In the SVM-scoped NDMP mode, these LIFs belong to either the data SVM or admin SVM. The connection can be established on a LIF only if the NDMP service is enabled on the SVM that owns this LIF.

A data LIF belongs to the data SVM and the intercluster LIF, node-management LIF, and cluster-management LIF belong to the admin SVM.

In the SVM-scoped NDMP mode, the availability of volumes and tape devices for backup and restore operations depends on the LIF type on which the NDMP control connection is established and the status of the CAB extension. If your backup application supports the CAB extension and a volume and the tape device share the same affinity, then the backup application can perform a local backup or restore operation, instead of a three-way backup or restore operation.

### Related information

[Managing SVM-scoped NDMP mode for FlexVol volumes](#)

= Considerations when using NDMP

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You must take into account a number of considerations when starting the NDMP service on your storage system.

- Each node supports a maximum of 16 concurrent backups, restores, or combination of the two using connected tape drives.
- NDMP services can generate file history data at the request of NDMP backup applications.

File history is used by backup applications to enable optimized recovery of selected subsets of data from a backup image. File history generation and processing might be time-consuming and CPU-intensive for both the storage system and the backup application.

SMTape does not support file history.

+

If your data protection is configured for disaster recovery—where the entire backup image will be recovered—you can disable file history generation to reduce backup time. See your backup application documentation to determine whether it is possible to disable NDMP file history generation.

- Firewall policy for NDMP is enabled by default on all LIF types.
- In node-scoped NDMP mode, backing up a FlexVol volume requires that you use the backup application to initiate a backup on a node that owns the volume.

However, you cannot back up a node root volume.

- You can perform NDMP backup from any LIF as permitted by the firewall policies.

If you use a data LIF, you must select a LIF that is not configured for failover. If a data LIF fails over during an NDMP operation, the NDMP operation fails and must be run again.

- In node-scoped NDMP mode and storage virtual machine (SVM) scoped NDMP mode with no CAB extension support, the NDMP data connection uses the same LIF as the NDMP control connection.
- During LIF migration, ongoing backup and restore operations are disrupted.

You must initiate the backup and restore operations after the LIF migration.

- The NDMP backup path is of the format `/vserver_name/volume_name/path_name`.

`path_name` is optional, and specifies the path of the directory, file, or Snapshot copy.

- When a SnapMirror destination is backed up to tape by using the dump engine, only the data in the volume is backed up.

However, if a SnapMirror destination is backed up to tape using SMTape, then the metadata is also backed up. The SnapMirror relationships and the associated metadata are not backed up to tape. Therefore, during restore, only the data on that volume is restored, but the associated SnapMirror relationships are not restored.

## Related information

[What Cluster Aware Backup extension does](#)

[ONTAP concepts](#)

[System administration](#)

= Environment variable

= Environment variables overview

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Environment variables are used to communicate information about a backup or restore operation between an NDMP-enabled backup application and a storage system.



For example, if a user specifies that a backup application should back up `/vserver1/vol1/dir1`, the backup application sets the `FILESYSTEM` environment variable to `/vserver1/vol1/dir1`. Similarly, if a user specifies that a backup should be a level 1 backup, the backup application sets the `LEVEL` environment variable to 1 (one).

The setting and examining of environment variables are typically transparent to backup administrators; that is, the backup application sets them automatically.

A backup administrator rarely specifies environment variables; however, you might want to change the value of an environment variable from that set by the backup application to characterize or work around a functional or performance problem. For example, an administrator might want to temporarily disable file history generation to determine if the backup application's processing of file history information is contributing to performance issues or functional problems.

Many backup applications provide a means to override or modify environment variables or to specify additional environment variables. For information, see your backup application documentation.

= Environment variables supported by ONTAP

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Environment variables are used to communicate information about a backup or restore operation between an NDMP-enabled backup application and a storage system. ONTAP supports environment variables, which have an associated default value. However, you can manually modify these default values.

If you manually modify the values set by the backup application, the application might behave unpredictably. This is because the backup or restore operations might not be doing what the backup application expected them to do. But in some cases, judicious modification might help in identifying or working around problems.

The following tables list the environment variables whose behavior is common to dump and SMTape and those variables that are supported only for dump and SMTape. These tables also contain descriptions of how the environment variables that are supported by ONTAP work if they are used:

In most cases, variables that have the value, `Y` also accept `T` and `N` also accept `F`.

== Environment variables supported for dump and SMTape

Environment variable	Valid values	Default	Description
DEBUG	Y or N	N	Specifies that debugging information is printed.
FILESYSTEM	string	none	Specifies the path name of the root of the data that is being backed up.
NDMP_VERSION	return_only	none	<p>You should not modify the NDMP_VERSION variable. Created by the backup operation, the NDMP_VERSION variable returns the NDMP version.</p> <p>ONTAP sets the NDMP_VERSION variable during a backup for internal use and to pass to a backup application for informational purposes. The NDMP version of an NDMP session is not set with this variable.</p>
PATHNAME_SEPARATOR	return_value	none	<p>Specifies the path name separator character.</p> <p>This character depends on the file system being backed up. For ONTAP, the character "/" is assigned to this variable. The NDMP server sets this variable before starting a tape backup operation.</p>
TYPE	dump or smtape	dump	Specifies the type of backup supported to perform tape backup and restore operations.

Environment variable	Valid values	Default	Description
VERBOSE	Y or N	N	Increases the log messages while performing a tape backup or restore operation.

== Environment variables supported for dump

Environment variable	Valid values	Default	Description
ACL_START	return_only	none	<p>Created by the backup operation, the ACL_START variable is an offset value used by a direct access restore or restartable NDMP backup operation.</p> <p>The offset value is the byte offset in the dump file where the ACL data (Pass V) begins and is returned at the end of a backup. For a direct access restore operation to correctly restore backed-up data, the ACL_START value must be passed to the restore operation when it begins. An NDMP restartable backup operation uses the ACL_START value to communicate to the backup application where the nonrestartable portion of the backup stream begins.</p>

Environment variable	Valid values	Default	Description
BASE_DATE	0, -1, or DUMP_DATE value	-1	<p>Specifies the start date for incremental backups.</p> <p>When set to -1, the BASE_DATE incremental specifier is disabled. When set to 0 on a level 0 backup, incremental backups are enabled. After the initial backup, the value of the DUMP_DATE variable from the previous incremental backup is assigned to the BASE_DATE variable.</p> <p>These variables are an alternative to the LEVEL/UPDATE based incremental backups.</p>
DIRECT	Y or N	N	<p>Specifies that a restore should fast-forward directly to the location on the tape where the file data resides instead of scanning the entire tape.</p> <p>For direct access recovery to work, the backup application must provide positioning information. If this variable is set to Y, the backup application specifies the file or directory names and the positioning information.</p>
DMP_NAME	string	none	<p>Specifies the name for a multiple subtree backup.</p> <p>This variable is mandatory for multiple subtree backups.</p>

Environment variable	Valid values	Default	Description
DUMP_DATE	return_value	none	<p>You do not change this variable directly. It is created by the backup if the BASE_DATE variable is set to a value other than -1.</p> <p>The DUMP_DATE variable is derived by prepending the 32-bit level value to a 32-bit time value computed by the dump software. The level is incremented from the last level value passed into the BASE_DATE variable. The resulting value is used as the BASE_DATE value on a subsequent incremental backup.</p>

Environment variable	Valid values	Default	Description
ENHANCED_DAR_ENABLED	Y or N	N	<p>Specifies whether enhanced DAR functionality is enabled. Enhanced DAR functionality supports directory DAR and DAR of files with NT Streams. It provides performance improvements.</p> <p>Enhanced DAR during restore is possible only if the following conditions are met:</p> <ul style="list-style-type: none"> <li>• ONTAP supports enhanced DAR.</li> <li>• File history is enabled (HIST=Y) during the backup.</li> <li>• The <code>ndmpd.offset_map.enable</code> option is set to on.</li> <li>• ENHANCED_DAR_ENABLED variable is set to Y during restore.</li> </ul>

Environment variable	Valid values	Default	Description
EXCLUDE	pattern_string	none	<p>Specifies files or directories that are excluded when backing up data.</p> <p>The exclude list is a comma-separated list of file or directory names. If the name of a file or directory matches one of the names in the list, it is excluded from the backup.</p> <p>The following rules apply while specifying names in the exclude list:</p> <ul style="list-style-type: none"> <li>• The exact name of the file or directory must be used.</li> <li>• The asterisk (*), a wildcard character, must be either the first or the last character of the string.</li> </ul> <p>Each string can have up to two asterisks.</p> <ul style="list-style-type: none"> <li>• A comma in a file or directory name must be preceded with a backslash.</li> <li>• The exclude list can contain up to 32 names.</li> </ul>

Files or directories specified to be excluded for backup are not excluded if you set NON\_QUOTA\_TREE to *y* simultaneously.

a|  
EXTRACT

a|  
Y, N, or E

a|

N

a|

Specifies that subtrees of a backed-up data set are to be restored.

The backup application specifies the names of the subtrees to be extracted. If a file specified matches a directory whose contents were backed up, the directory is recursively extracted.

To rename a file, directory, or qtree during restore without using DAR, you must set the EXTRACT environment variable to E.

a|  
EXTRACT\_ACL

a|

Y or N

a|

Y

a|

Specifies that ACLs from the backed up file are restored on a restore operation.

The default is to restore ACLs when restoring data, except for DARs (DIRECT=Y).

a|  
FORCE

a|

Y or N

a|

N

a|

Determines if the restore operation must check for volume space and inode availability on the destination volume.

Setting this variable to Y causes the restore operation to skip checks for volume space and inode availability on the destination path.

If enough volume space or inodes are not available on the destination volume, the restore operation recovers as much data allowed by the destination volume space and inode availability. The restore operation stops when volume space or inodes are not available.

a|  
HIST

a|

Y or N

a|

N

a|

Specifies that file history information is sent to the backup application.

Most commercial backup applications set the HIST variable to Y. If you want to increase the speed of a



backup operation, or you want to troubleshoot a problem with the file history collection, you can set this variable to N.

You should not set the HIST variable to Y if the backup application does not support file history.

a|  
IGNORE\_CTIME

a|  
Y or N

a|  
N

a|

Specifies that a file is not incrementally backed up if only its ctime value has changed since the previous incremental backup.

Some applications, such as virus scanning software, change the ctime value of a file within the inode, even though the file or its attributes have not changed. As a result, an incremental backup might back up files that have not changed. The IGNORE\_CTIME variable should be specified only if incremental backups are taking an unacceptable amount of time or space because the ctime value was modified.

The NDMP `dump` command sets IGNORE\_CTIME to `false` by default. Setting it to `true` can result in the following data loss:

1. If IGNORE\_CTIME is set to `true` with a volume level incremental `ndmcopy`, it results in the deleting of files, which are moved across qtrees on source.
2. If IGNORE\_CTIME is set to `true` during a volume level incremental dump, it results in the deleting of files, which are moved across qtrees on source during incremental restore.

To avoid this problem, IGNORE\_CTIME must be set to `false` during volume level NDMP dumps or `ndmcopy`.

a|  
IGNORE\_QTREES

a|  
Y or N

a|

N

a|

Specifies that the restore operation does not restore qtree information from backed-up qtrees.

a|  
LEVEL

a|

0-31

a|

0

a|

Specifies the backup level.

Level 0 copies the entire data set. Incremental backup levels, specified by values above 0, copy all files (new or modified) since the last incremental backup. For example, a level 1 backs up new or modified files since the level 0 backup, a level 2 backs up new or modified files since the level 1 backup, and so on.

a|  
LIST

a|

Y or N

a|

N

a|

Lists the backed-up file names and inode numbers without actually restoring the data.

a|  
LIST\_QTREES

a|

Y or N

a|

N

a|

Lists the backed-up qtrees without actually restoring the data.

a|  
MULTI\_SUBTREE\_NAMES

a|

string

a|

none

a|

Specifies that the backup is a multiple subtree backup.

Multiple subtrees are specified in the string, which is a newline-separated, null-terminated list of subtree names. Subtrees are specified by path names relative to their common root directory, which must be specified as the last element of the list.

If you use this variable, you must also use the DMP\_NAME variable.

a|  
NDMP\_UNICODE\_FH

a|  
Y or N

a|  
N

a|  
Specifies that a Unicode name is included in addition to the NFS name of the file in the file history information.

This option is not used by most backup applications and should not be set unless the backup application is designed to receive these additional file names. The HIST variable must also be set.

a|  
NO\_ACLS

a|  
Y or N

a|  
N

a|  
Specifies that ACLs must not be copied when backing up data.

a|  
NON\_QUOTA\_TREE

a|  
Y or N

a|  
N

a|  
Specifies that files and directories in qtrees must be ignored when backing up data.

When set to Y, items in qtrees in the data set specified by the FILESYSTEM variable are not backed up. This variable has an effect only if the FILESYSTEM variable specifies an entire volume. The NON\_QUOTA\_TREE variable only works on a level 0 backup and does not work if the MULTI\_SUBTREE\_NAMES variable is specified.

Files or directories specified to be excluded for backup are not excluded if you set NON\_QUOTA\_TREE to Y simultaneously.

a|  
NOWRITE

a|  
Y or N

a|

N

a|

Specifies that the restore operation must not write data to the disk.

This variable is used for debugging.

a|  
RECURSIVE

a|  
Y or N

a|

Y

a|

Specifies that directory entries during a DAR restore be expanded.

The `DIRECT` and `ENHANCED_DAR_ENABLED` environment variables must be enabled (set to `Y`) as well. If the `RECURSIVE` variable is disabled (set to `N`), only the permissions and ACLs for all the directories in the original source path are restored from tape, not the contents of the directories. If the `RECURSIVE` variable is set to `N` or the `RECOVER_FULL_PATHS` variable is set to `Y`, the recovery path must end with the original path.

If the `RECURSIVE` variable is disabled and if there is more than one recovery path, all of the recovery paths must be contained within the longest of the recovery paths. Otherwise, an error message is displayed.

For example, the following are valid recovery paths because all of the recovery paths are within foo/dir1/deepdir/myfile:

- /foo
- /foo/dir
- /foo/dir1/deepdir
- /foo/dir1/deepdir/myfile

The following are invalid recovery paths:

- /foo
- /foo/dir
- /foo/dir1/myfile
- /foo/dir2
- /foo/dir2/myfile

a|  
RECOVER\_FULL\_PATHS

a|  
Y or N

a|  
N

a|  
Specifies that the full recovery path will have their permissions and ACLs restored after the DAR.

DIRECT and ENHANCED\_DAR\_ENABLED must be enabled (set to Y) as well. If RECOVER\_FULL\_PATHS is set to Y, the recovery path must end with the original path. If directories already exist on the destination volume, their permissions and ACLs will not be restored from tape.

a|  
UPDATE

a|  
Y or N

a|  
Y

a|  
Updates the metadata information to enable LEVEL based incremental backup.

== Environment variables supported for SMTape

[options="header"]

| Environment variable| Valid values| Default| Description

a|  
BASE\_DATE

a|  
DUMP\_DATE

a|

-1

a|

Specifies the start date for incremental backups.

BASE\_DATE is a string representation of the reference Snapshot identifiers. Using the BASE\_DATE string, SMTape locates the reference Snapshot copy.

BASE\_DATE is not required for baseline backups. For an incremental backup, the value of the DUMP\_DATE variable from the previous baseline or incremental backup is assigned to the BASE\_DATE variable.

The backup application assigns the DUMP\_DATE value from a previous SMTape baseline or incremental backup.

a|

DUMP\_DATE

a|

return\_value

a|

none

a|

At the end of an SMTape backup, DUMP\_DATE contains a string identifier that identifies the Snapshot copy used for that backup. This Snapshot copy could be used as the reference Snapshot copy for a subsequent incremental backup.

The resulting value of DUMP\_DATE is used as the BASE\_DATE value for subsequent incremental backups.

a|

SMTAPE\_BACKUP\_SET\_ID

a|

string

a|

none

a|

Identifies the sequence of incremental backups associated with the baseline backup.

Backup set ID is a 128-bit unique ID that is generated during a baseline backup. The backup application assigns this ID as the input to the SMTAPE\_BACKUP\_SET\_ID variable during an incremental backup.

a|

SMTAPE\_SNAPSHOT\_NAME

a|

Any valid Snapshot copy that is available in the volume

a|

Invalid

a|

When the SMTAPE\_SNAPSHOT\_NAME variable is set to a Snapshot copy, that Snapshot copy and its older Snapshot copies are backed up to tape.

For incremental backup, this variable specifies incremental Snapshot copy. The BASE\_DATE variable provides the baseline Snapshot copy.

a|

## SMTAPE\_DELETE\_SNAPSHOT

a|

Y or N

a|

N

a|

For a Snapshot copy created automatically by SMTape, when the SMTAPE\_DELETE\_SNAPSHOT variable is set to Y, then after the backup operation is complete, SMTape deletes this Snapshot copy. However, a Snapshot copy created by the backup application will not be deleted.

a|

## SMTAPE\_BREAK\_MIRROR

a|

Y or N

a|

N

a|

When the SMTAPE\_BREAK\_MIRROR variable is set to Y, the volume of type DP is changed to a RW volume after a successful restore.

:leveloffset: -1

= Common NDMP tape backup topologies

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

[.lead]

NDMP supports a number of topologies and configurations between backup applications and storage systems or other NDMP servers providing data (file systems) and tape services.

== Storage system-to-local-tape

In the simplest configuration, a backup application backs up data from a storage system to a tape subsystem attached to the storage system. The NDMP control connection exists across the network boundary. The NDMP data connection that exists within the storage system between the data and tape services is called an NDMP local configuration.

== Storage system-to-tape attached to another storage system

A backup application can also back up data from a storage system to a tape library (a medium changer with one or more tape drives) attached to another storage system. In this case, the NDMP data connection between the data and tape services is provided by a TCP or TCP/IPv6 network connection. This is called an NDMP three-way storage system-to-storage system configuration.

== Storage system-to-network-attached tape library

NDMP-enabled tape libraries provide a variation of the three-way configuration. In this case, the tape library attaches directly to the TCP/IP network and communicates with the backup application and the storage system through an internal NDMP server.

== Storage system-to-data server-to-tape or data server-to-storage system-to-tape

NDMP also supports storage system-to-data-server and data-server-to-storage system three-way configurations, although these variants are less widely deployed. Storage system-to-server allows storage system data to be backed up to a tape library attached to the backup application host or to another data server system. The server-to-storage system configuration allows server data to be backed up to a storage system-attached tape library.

= Supported NDMP authentication methods

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

[.lead]

You can specify an authentication method to allow NDMP connection requests. ONTAP supports two methods for authenticating NDMP access to a storage system: plaintext and challenge.

In node-scoped NDMP mode, both challenge and plaintext are enabled by default. However, you cannot



This extension is supported only in the SVM-scoped NDMP mode.

- Connection Address Extension (CAE) for IPv6 support
- Extension class 0x2050

This extension supports restartable backup operations and Snapshot Management Extensions.

The `NDMP_SNAP_RECOVER` message, which is part of the Snapshot Management Extensions, is used to initiate a recovery operation and to transfer the recovered data from a local Snapshot copy to a local file system location. In ONTAP, this message allows the recovery of volumes and regular files only.

The `NDMP_SNAP_DIR_LIST` message enables you to browse through the Snapshot copies of a volume. If a nondisruptive operation takes place while a browsing operation is in progress, the backup application must reinitiate the browsing operation.

= NDMP restartable backup extension for a dump supported by ONTAP

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the NDMP restartable backup extension (RBE) functionality to restart a backup from a known checkpoint in the data stream before the failure.

= What enhanced DAR functionality is

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the enhanced direct access recovery (DAR) functionality for directory DAR and DAR of files and NT streams. By default, enhanced DAR functionality is enabled.

Enabling enhanced DAR functionality might impact the backup performance because an offset map has to be created and written onto tape. You can enable or disable enhanced DAR in both the node-scoped and storage virtual machine (SVM)-scoped NDMP modes.

= Scalability limits for NDMP sessions

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You must be aware of the maximum number of NDMP sessions that can be established simultaneously on storage systems of different system memory capacities. This maximum number depends on the system memory of a storage system.

The limits mentioned in the following table are for the NDMP server. The limits mentioned in the section “Scalability limits for dump backup and restore sessions” are for the dump and restore session.

#### Scalability limits for dump backup and restore sessions

System memory of a storage system	Maximum number of NDMP sessions
Less than 16 GB	8
Greater than or equal to 16 GB but less than 24 GB	20
Greater than or equal to 24 GB	36

You can obtain the system memory of your storage system by using the `sysconfig -a` command (available through the nodeshell). For more information about using this command, see the man pages.

= About NDMP for FlexGroup volumes

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.7, NDMP is supported on FlexGroup volumes.

Beginning with ONTAP 9.7, the `ndmcopy` command is supported for data transfer between FlexVol and FlexGroup volumes.

If you revert from ONTAP 9.7 to an earlier version, the incremental transfer information of the previous transfers is not retained and therefore, you must perform a baseline copy after reverting.

Beginning with ONTAP 9.8, the following NDMP features are supported on FlexGroup volumes:

- The `NDMP_SNAP_RECOVER` message in the extension class `0x2050` can be used for recovering individual files in a FlexGroup volume.
- NDMP restartable backup extension (RBE) is supported for FlexGroup volumes.
- Environment variables `EXCLUDE` and `MULTI_SUBTREE_NAMES` are supported for FlexGroup volumes.

= About NDMP with SnapLock volumes

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Creating multiple copies of regulated data provides you with redundant recovery scenarios, and by using NDMP dump and restore, it's possible to preserve the write once, read many (WORM) characteristics of source files on a SnapLock volume.

WORM attributes on the files in a SnapLock volume are preserved when backing up, restoring and copying data; however, WORM attributes are enforced only when restoring to a SnapLock volume. If a backup from a SnapLock volume is restored to a volume other than a SnapLock volume, the WORM attributes are preserved but are ignored and are not enforced by ONTAP.

= Manage node-scoped NDMP mode for FlexVol volumes

= Manage node-scoped NDMP mode for FlexVol volumes overview

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can manage NDMP at the node level by using NDMP options and commands. You can modify the NDMP options by using the `options` command. You must use NDMP-specific credentials to access a storage system to perform tape backup and restore operations.

For more information about the `options` command, see the man pages.

#### Related information

[Commands for managing node-scoped NDMP mode](#)

[What node-scoped NDMP mode is](#)

= Commands for managing node-scoped NDMP mode

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the `system services ndmp` commands to manage NDMP at a node level. Some of these commands are deprecated and will be removed in a future major release.

You can use the following NDMP commands only at the advanced privilege level:

- `system services ndmp service terminate`
- `system services ndmp service start`
- `system services ndmp service stop`
- `system services ndmp log start`
- `system services ndmp log stop`

If you want to...	Use this command...
Enable NDMP service	<code>system services ndmp on*</code>
Disable NDMP service	<code>system services ndmp off*</code>
Display NDMP configuration	<code>system services ndmp show*</code>
Modify NDMP configuration	<code>system services ndmp modify*</code>
Display the default NDMP version	<code>system services ndmp version*</code>
Display NDMP service configuration	<code>system services ndmp service show</code>
Modify NDMP service configuration	<code>system services ndmp service modify</code>
Display all NDMP sessions	<code>system services ndmp status</code>
Display detailed information about all NDMP sessions	<code>system services ndmp probe</code>
Terminate the specified NDMP session	<code>system services ndmp kill</code>
Terminate all NDMP sessions	<code>system services ndmp kill-all</code>
Change the NDMP password	<code>system services ndmp password*</code>

If you want to...	Use this command...
Enable node-scoped NDMP mode	<code>system services ndmp node-scope-mode on*</code>
Disable node-scoped NDMP mode	<code>system services ndmp node-scope-mode off*</code>
Display the node-scoped NDMP mode status	<code>system services ndmp node-scope-mode status*</code>
Forcefully terminate all NDMP sessions	<code>system services ndmp service terminate</code>
Start the NDMP service daemon	<code>system services ndmp service start</code>
Stop the NDMP service daemon	<code>system services ndmp service stop</code>
Start logging for the specified NDMP session	<code>system services ndmp log start*</code>
Stop logging for the specified NDMP session	<code>system services ndmp log stop*</code>

- These commands are deprecated and will be removed in a future major release.

For more information about these commands, see the man pages for the `system services ndmp` commands.

= User authentication in a node-scoped NDMP mode

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

In the node-scoped NDMP mode, you must use NDMP specific credentials to access a storage system in order to perform tape backup and restore operations.

The default user ID is “root”. Before using NDMP on a node, you must ensure that you change the default NDMP password associated with the NDMP user. You can also change the default NDMP user ID.

### Related information

[Commands for managing node-scoped NDMP mode](#)

= Manage SVM-scoped NDMP mode for FlexVol volumes

= Manage SVM-scoped NDMP mode for FlexVol volumes overview

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can manage NDMP on a per SVM basis by using the NDMP options and

commands. You can modify the NDMP options by using the `vserver services ndmp modify` command. In the SVM-scoped NDMP mode, user authentication is integrated with the role-based access control mechanism.

You can add NDMP in the allowed or disallowed protocols list by using the `vserver modify` command. By default, NDMP is in the allowed protocols list. If NDMP is added to the disallowed protocols list, NDMP sessions cannot be established.

You can control the LIF type on which an NDMP data connection is established by using the `-preferred-interface-role` option. During an NDMP data connection establishment, NDMP chooses an IP address that belongs to the LIF type as specified by this option. If the IP addresses do not belong to any of these LIF types, then the NDMP data connection cannot be established. For more information about the `-preferred-interface-role` option, see the man pages.

For more information about the `vserver services ndmp modify` command, see the man pages.

### Related information

[Commands for managing SVM-scoped NDMP mode](#)

[What Cluster Aware Backup extension does](#)

[ONTAP concepts](#)

[What SVM-scoped NDMP mode is](#)

[System administration](#)

= Commands for managing SVM-scoped NDMP mode

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the `vserver services ndmp` commands to manage NDMP on each storage virtual machine (SVM, formerly known as Vserver).

If you want to...	Use this command...
Enable NDMP service	<code>vserver services ndmp on</code>

NDMP service must always be enabled on all nodes in a cluster. You can enable NDMP service on a node by using the `system services ndmp on` command. By default, NDMP service is always enabled on a node.

a|  
Disable NDMP service  
a|  
vserver services ndmp off  
a|  
Display NDMP configuration  
a|  
vserver services ndmp show  
a|  
Modify NDMP configuration  
a|  
vserver services ndmp modify  
a|  
Display default NDMP version  
a|  
vserver services ndmp version  
a|  
Display all NDMP sessions  
a|  
vserver services ndmp status  
a|  
Display detailed information about all NDMP sessions  
a|  
vserver services ndmp probe  
a|  
Terminate a specified NDMP session  
a|  
vserver services ndmp kill  
a|  
Terminate all NDMP sessions  
a|  
vserver services ndmp kill-all  
a|  
Generate the NDMP password  
a|  
vserver services ndmp generate-password  
a|  
Display NDMP extension status  
a|  
vserver services ndmp extensions show

This command is available at the advanced privilege level.

a|  
Modify (enable or disable) NDMP extension status  
a|  
vserver services ndmp extensions modify

This command is available at the advanced privilege level.

a|  
Start logging for the specified NDMP session  
a|

```
vserver services ndmp log start
```

This command is available at the advanced privilege level.

a|

Stop logging for the specified NDMP session

a|

```
vserver services ndmp log stop
```

This command is available at the advanced privilege level.



For more information about these commands, see the man pages for the `vserver services ndmp` commands.

= What Cluster Aware Backup extension does

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

[.lead]

CAB (Cluster Aware Backup) is an NDMP v4 protocol extension. This extension enables the NDMP server to establish a data connection on a node that owns a volume. This also enables the backup application to determine if volumes and tape devices are located on the same node in a cluster.

To enable the NDMP server to identify the node that owns a volume and to establish a data connection on such a node, the backup application must support the CAB extension. CAB extension requires the backup application to inform the NDMP server about the volume to be backed up or restored prior to establishing the data connection. This allows the NDMP server to determine the node that hosts the volume and appropriately establish the data connection.

With the CAB extension supported by the backup application, the NDMP server provides affinity information about volumes and tape devices. Using this affinity information, the backup application can perform a local backup instead of a three-way backup if a volume and tape device are located on the same node in a cluster.

= Availability of volumes and tape devices for backup and restore on different LIF types

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

[.lead]

You can configure a backup application to establish an NDMP control connection on any of the LIF types in a cluster. In the storage virtual machine (SVM)-scoped NDMP mode, you can determine the availability of volumes and tape devices for backup and restore operations depending upon these LIF types and the status of the CAB extension.

The following tables show the availability of volumes and tape devices for NDMP control connection LIF types and the status of the CAB extension:

== Availability of volumes and tape devices when CAB extension is not supported by the backup application

[options="header"]

NDMP control connection LIF type	Volumes available for backup or restore	Tape devices available for backup or restore
----------------------------------	---	--

a		
---	--	--

Node-management LIF		
---------------------	--	--

a		
---	--	--

All volumes hosted by a node

a|

Tape devices connected to the node hosting the node-management LIF

a|

Data LIF

a|

Only volumes that belong to the SVM hosted by a node that hosts the data LIF

a|

None

a|

Cluster-management LIF

a|

All volumes hosted by a node that hosts the cluster-management LIF

a|

None

a|

Intercluster LIF

a|

All volumes hosted by a node that hosts the intercluster LIF

a|

Tape devices connected to the node hosting the intercluster LIF

== Availability of volumes and tape devices when CAB extension is supported by the backup application

[options="header"]

| NDMP control connection LIF type| Volumes available for backup or restore| Tape devices available for backup or restore

a|

Node-management LIF

a|

All volumes hosted by a node

a|

Tape devices connected to the node hosting the node-management LIF

a|

Data LIF

a|

All volumes that belong to the SVM that hosts the data LIF

a|

None

a|

Cluster-management LIF

a|

All volumes in the cluster

a|

All tape devices in the cluster

a|

Intercluster LIF

a|

All volumes in the cluster

a|

All tape devices in the cluster

= What affinity information is  
:icons: font  
:relative\_path: ./tape-backup/  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

[.lead]  
With the backup application being CAB aware, the NDMP server provides unique location information about volumes and tape devices. Using this affinity information, the backup application can perform a local backup instead of a three-way backup if a volume and a tape device share the same affinity.

If the NDMP control connection is established on a node management LIF, cluster management LIF, or an intercluster LIF, the backup application can use the affinity information to determine if a volume and tape device are located on the same node and then perform either a local or a three-way backup or restore operation. If the NDMP control connection is established on a data LIF, then the backup application always performs a three-way backup.

== Local NDMP backup and Three-way NDMP backup

image:::./media/local\_and\_three-way\_backup\_in\_vserver\_aware\_ndmp\_mode.png[ocal and three way back up diagrams]

Using the affinity information about volumes and tape devices, the DMA (backup application) performs a local NDMP backup on the volume and tape device located on Node 1 in the cluster. If the volume moves from Node 1 to Node 2, affinity information about the volume and tape device changes. Hence, for a subsequent backup the DMA performs a three-way NDMP backup operation. This ensures continuity of the backup policy for the volume irrespective of the node to which the volume is moved to.

.Related information

[What Cluster Aware Backup extension does](#)

= NDMP server supports secure control connections in SVM-scoped mode  
:icons: font

false]` command.

= NDMP data connection types  
:icons: font  
:relative\_path: ./tape-backup/  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

[.lead]  
In the storage virtual machine (SVM)-scoped NDMP mode, the supported NDMP data connection types depend on the NDMP control connection LIF type and the status of the CAB extension. This NDMP data connection type indicates whether you can perform a local or a three-way NDMP backup or restore operation.

You can perform a three-way NDMP backup or restore operation over a TCP or TCP/IPv6 network. The following tables show the NDMP data connection types based on the NDMP control connection LIF type and the status of the CAB extension.

== NDMP data connection type when CAB extension is supported by the backup application

[options="header"]

| NDMP control connection LIF type| NDMP data connection type

a|  
Node-management LIF  
a|  
LOCAL, TCP, TCP/IPv6  
a|  
Data LIF  
a|  
TCP, TCP/IPv6  
a|  
Cluster-management LIF  
a|  
LOCAL, TCP, TCP/IPv6  
a|  
Intercluster LIF  
a|  
LOCAL, TCP, TCP/IPv6

== NDMP data connection type when CAB extension is not supported by the backup application

[options="header"]

| NDMP control connection LIF type| NDMP data connection type

a|  
Node-management LIF  
a|  
LOCAL, TCP, TCP/IPv6  
a|  
Data LIF  
a|  
TCP, TCP/IPv6  
a|  
Cluster-management LIF  
a|  
TCP, TCP/IPv6  
a|  
Intercluster LIF  
a|  
LOCAL, TCP, TCP/IPv6

.Related information

[What Cluster Aware Backup extension does](#)

[Network management](#)

= User authentication in the SVM-scoped NDMP mode

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

[.lead]

In the storage virtual machine (SVM)-scoped NDMP mode, NDMP user authentication is integrated with role-based access control. In the SVM context, the NDMP user must have either the “vsadmin” or “vsadmin-backup” role. In a cluster context, the NDMP user must have either the “admin” or “backup” role.

Apart from these pre-defined roles, a user account associated with a custom role can also be used for NDMP authentication provided that the custom role has the “vserver services ndmp” folder in its command directory and the access level of the folder is not “none”. In this mode, you must generate an NDMP password for a given user account, which is created through role-based access control. Cluster users in an admin or backup role can access a node-management LIF, a cluster-management LIF, or an intercluster LIF. Users in a vsadmin-backup or vsadmin role can access only the data LIF for that SVM. Therefore, depending on the role of a user, the availability of volumes and tape devices for backup and restore operations vary.

This mode also supports user authentication for NIS and LDAP users. Therefore, NIS and LDAP users can access multiple SVMs with a common user ID and password. However, NDMP authentication does not support Active Directory users.

In this mode, a user account must be associated with the SSH application and the “User password” authentication method.

.Related information

[Commands for managing SVM-scoped NDMP mode](#)

[System administration](#)

[ONTAP concepts](#)

= Generate an NDMP-specific password for NDMP users

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

[.lead]

In the storage virtual machine (SVM)-scoped NDMP mode, you must generate a password for a specific

From the storage virtual machine (SVM, formerly known as Vserver) context, you can generate NDMP passwords for users belonging only to that SVM.

+

The following example shows how to generate an NDMP-specific password for a user ID user1:

+

```
cluster1::vserver services ndmp> generate-password -vserver vs1 -user
user1

Vserver: vs1
User: user1
Password: jWZiNt57huPOoD8d
```

1. If you change the password to your regular storage system account, repeat this procedure to obtain your new NDMP-specific password.

= How tape backup and restore operations are affected during disaster recovery in MetroCluster configuration

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can perform tape backup and restore operations simultaneously during disaster recovery in a MetroCluster configuration. You must understand how these operations are affected during disaster recovery.

If tape backup and restore operations are performed on a volume of anSVM in a disaster recovery relationship, then you can continue performing incremental tape backup and restore operations after a switchover and switchback.

= About dump engine for FlexVol volumes

= About dump engine for FlexVol volumes

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Dump is a Snapshot copy based backup and recovery solution from ONTAP that helps you to back up files and directories from a Snapshot copy to a tape device and restore the backed up data to a storage system.

You can back up your file system data, such as directories, files, and their associated security settings, to a tape device by using the dump backup. You can back up an entire volume, an entire qtree, or a subtree that is neither an entire volume nor an entire qtree.

You can perform a dump backup or restore by using NDMP-compliant backup applications.

When you perform a dump backup, you can specify the Snapshot copy to be used for a backup. If you do not specify a Snapshot copy for the backup, the dump engine creates a Snapshot copy for the backup. After the backup operation is completed, the dump engine deletes this Snapshot copy.

You can perform level-0, incremental, or differential backups to tape by using the dump engine.

After reverting to a release earlier than Data ONTAP 8.3, you must perform a baseline backup operation before performing an incremental backup operation.

### Related information

[Upgrade, revert, or downgrade](#)

= How a dump backup works

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

A dump backup writes file system data from disk to tape using a predefined process. You can back up a volume, a qtree, or a subtree that is neither an entire volume nor an entire qtree.

The following table describes the process that ONTAP uses to back up the object indicated by the dump path:

Stage	Action
1	For less than full volume or full qtree backups, ONTAP traverses directories to identify the files to be backed up. If you are backing up an entire volume or qtree, ONTAP combines this stage with Stage 2.
2	For a full volume or full qtree backup, ONTAP identifies the directories in the volumes or qtrees to be backed up.
3	ONTAP writes the directories to tape.
4	ONTAP writes the files to tape.
5	ONTAP writes the ACL information (if applicable) to tape.

The dump backup uses a Snapshot copy of your data for the backup. Therefore, you do not have to take the volume offline before initiating the backup.

The dump backup names each Snapshot copy it creates as `snapshot_for_backup.n`, where `n` is an integer starting at 0. Each time the dump backup creates a Snapshot copy, it increments the integer by 1. The integer is reset to 0 after the storage system is rebooted. After the backup operation is completed, the dump engine deletes this Snapshot copy.

When ONTAP performs multiple dump backups simultaneously, the dump engine creates multiple Snapshot copies. For example, if ONTAP is running two dump backups simultaneously, you find the following Snapshot copies in the volumes from which data is being backed up:

`snapshot_for_backup.0` and `snapshot_for_backup.1`.

When you are backing up from a Snapshot copy, the dump engine does not create an additional Snapshot



copy.

= Types of data that the dump engine backs up

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

The dump engine enables you to back up data to tape to guard against disasters or controller disruptions. In addition to backing up data objects such as a files, directories, qtrees, or entire volumes, the dump engine can back up many types of information about each file. Knowing the types of data that the dump engine can back up and the restrictions to take into consideration can help you plan your approach to disaster recovery.

In addition to backing up data in files, the dump engine can back up the following information about each file, as applicable:

- UNIX GID, owner UID, and file permissions
- UNIX access, creation, and modification time
- File type
- File size
- DOS name, DOS attributes, and creation time
- Access control lists (ACLs) with 1,024 access control entries (ACEs)
- Qtree information
- Junction paths

Junction paths are backed up as symbolic links.

- LUN and LUN clones

You can back up an entire LUN object; however, you cannot back up a single file within the LUN object. Similarly, you can restore an entire LUN object but not a single file within the LUN.

The dump engine backs up LUN clones as independent LUNs.

- VM-aligned files

Backup of VM-aligned files is not supported in releases earlier than Data ONTAP 8.1.2.

When a snapshot-backed LUN clone is transitioned from Data ONTAP operating in 7-Mode to ONTAP, it becomes an inconsistent LUN. The dump engine does not back up inconsistent LUNs.

When you restore data to a volume, client I/O is restricted on the LUNs being restored. The LUN restriction is removed only when the dump restore operation is complete. Similarly, during a SnapMirror single file or LUN restore operation, client I/O is restricted on both files and LUNs being restored. This restriction is removed only when the single file or LUN restore operation is complete. If a dump backup is performed on a volume on which a dump restore or SnapMirror single file or LUN restore operation is being performed, then the files or LUNs that have client I/O restriction are not included in the backup. These files or LUNs are included in a subsequent backup operation if the client I/O restriction is removed.

A LUN running on Data ONTAP 8.3 that is backed up to tape can be restored only to 8.3 and later releases and not to an earlier release. If the LUN is restored to an earlier release, then the LUN is restored as a file.

When you back up a SnapVault secondary volume or a volume SnapMirror destination to tape, only the data on the volume is backed up. The associated metadata is not backed up. Therefore, when you try to restore the volume, only the data on that volume is restored. Information about the volume SnapMirror relationships is not available in the backup and therefore is not restored.

If you dump a file that has only Windows NT permissions and restore it to a UNIX-style qtree or volume, the file gets the default UNIX permissions for that qtree or volume.

If you dump a file that has only UNIX permissions and restore it to an NTFS-style qtree or volume, the file gets the default Windows permissions for that qtree or volume.

Other dumps and restores preserve permissions.

You can back up VM-aligned files and the `vm-align-sector` option. For more information about VM-aligned files, see [Logical storage management](#).

= What increment chains are

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

An increment chain is a series of incremental backups of the same path. Because you can specify any level of backup at any time, you must understand increment chains to be able to perform backups and restores effectively. You can perform 31 levels of incremental backup operations.

There are two types of increment chains:

- A consecutive increment chain, which is a sequence of incremental backups that starts with level 0 and is raised by 1 at each subsequent backup.
- A nonconsecutive increment chain, where incremental backups skip levels or have levels that are out of sequence, such as 0, 2, 3, 1, 4, or more commonly 0, 1, 1, 1 or 0, 1, 2, 1, 2.

Incremental backups are based on the most recent lower-level backup. For example, the sequence of backup levels 0, 2, 3, 1, 4 provides two increment chains: 0, 2, 3 and 0, 1, 4. The following table explains the bases of the incremental backups:

Backup order	Increment level	Increment chain	Base	Files backed up
1	0	Both	Files on the storage system	All files in the backup path
2	2	0, 2, 3	Level-0 backup	Files in the backup path created since the level-0 backup
3	3	0, 2, 3	Level-2 backup	Files in the backup path created since the level-2 backup

Backup order	Increment level	Increment chain	Base	Files backed up
4	1	0, 1, 4	Level-0 backup, because this is the most recent level that is lower than the level-1 backup	Files in the backup path created since the level-0 backup, including files that are in the level-2 and level-3 backups
5	4	0, 1, 4	The level-1 backup, because it is a lower level and is more recent than the level-0, level-2, or level-3 backups	Files created since the level-1 backup

= What the blocking factor is

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

A tape block is 1,024 bytes of data. During a tape backup or restore, you can specify the number of tape blocks that are transferred in each read/write operation. This number is called the *blocking factor*.

You can use a blocking factor from 4 to 256. If you plan to restore a backup to a system other than the system that did the backup, the restore system must support the blocking factor that you used for the backup. For example, if you use a blocking factor of 128, the system on which you restore that backup must support a blocking factor of 128.

During an NDMP backup, the `MOVER_RECORD_SIZE` determines the blocking factor. ONTAP allows a maximum value of 256 KB for `MOVER_RECORD_SIZE`.

= When to restart a dump backup

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

A dump backup sometimes does not finish because of internal or external errors, such as tape write errors, power outages, accidental user interruptions, or internal inconsistency on the storage system. If your backup fails for one of these reasons, you can restart it.

You can choose to interrupt and restart a backup to avoid periods of heavy traffic on the storage system or to avoid competition for other limited resources on the storage system, such as a tape drive. You can interrupt a long backup and restart it later if a more urgent restore (or backup) requires the same tape drive. Restartable backups persist across reboots. You can restart an aborted backup to tape only if the following conditions are true:

- The aborted backup is in phase IV.

- All of the associated Snapshot copies that were locked by the dump command are available.
- The file history must be enabled.

When such a dump operation is aborted and left in a restartable state, the associated Snapshot copies are locked. These Snapshot copies are released after the backup context is deleted. You can view the list of backup contexts by using the `vserver services ndmp restartable backup show` command.

```
cluster::> vserver services ndmp restartable-backup show
Vserver      Context Identifier          Is Cleanup Pending?
-----
vserver1 330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1 481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2 5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.
```

```
cluster::> vserver services ndmp restartable-backup show -vserver
vserver1 -context-id 330e6739-0179-11e6-a299-005056bb4bc9

          Vserver: vserver1
    Context Identifier: 330e6739-0179-11e6-a299-005056bb4bc9
      Volume Name: /vserver1/vol1
    Is Cleanup Pending?: false
    Backup Engine Type: dump
Is Snapshot Copy Auto-created?: true
      Dump Path: /vol/vol1
Incremental Backup Level ID: 0
      Dump Name: /vserver1/vol1
Context Last Updated Time: 1460624875
      Has Offset Map?: true
      Offset Verify: true
    Is Context Restartable?: true
      Is Context Busy?: false
      Restart Pass: 4
      Status of Backup: 2
      Snapshot Copy Name: snapshot_for_backup.1
    State of the Context: 7

cluster::>"
```

= How a dump restore works

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

A dump restore writes file system data from tape to disk using a predefined process.

The process in the following table shows how the dump restore works:

Stage	Action
1	ONTAP catalogs the files that need to be extracted from the tape.
2	ONTAP creates directories and empty files.
3	ONTAP reads a file from tape, writes it to disk, and sets the permissions (including ACLs) on it.
4	ONTAP repeats stages 2 and 3 until all the specified files are copied from the tape.

= Types of data that the dump engine restores

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

When a disaster or controller disruption occurs, the dump engine provides multiple methods for you to recover all of the data that you backed up, from single files, to file attributes, to entire directories. Knowing the types of data that dump engine can restore and when to use which method of recovery can help minimize downtime.

You can restore data to an online mapped LUN. However, host applications cannot access this LUN until the restore operation is complete. After the restore operation is complete, the host cache of the LUN data should be flushed to provide coherency with the restored data.

The dump engine can recover the following data:

- Contents of files and directories
- UNIX file permissions
- ACLs

If you restore a file that has only UNIX file permissions to an NTFS qtree or volume, the file has no Windows NT ACLs. The storage system uses only the UNIX file permissions on this file until you create a Windows NT ACL on it.

If you restore ACLs backed up from storage systems running Data ONTAP 8.2 to storage systems running Data ONTAP 8.1.x and earlier that have an ACE limit lower than 1,024, a default ACL is restored.

- Qtree information

Qtree information is used only if a qtree is restored to the root of a volume. Qtree information is not used if a qtree is restored to a lower directory, such as `/vs1/vol1/subdir/lowerdir`, and it ceases to be a qtree.

- All other file and directory attributes
- Windows NT streams
- LUNs

- A LUN must be restored to a volume level or a qtree level for it to remain as a LUN.

If it is restored to a directory, it is restored as a file because it does not contain any valid metadata.

- A 7-Mode LUN is restored as a LUN on an ONTAP volume.
- A 7-Mode volume can be restored to an ONTAP volume.
- VM-aligned files restored to a destination volume inherit the VM-align properties of the destination volume.
- The destination volume for a restore operation might have files with mandatory or advisory locks.

While performing restore operation to such a destination volume, the dump engine ignores these locks.

= Considerations before restoring data

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can restore backed-up data to its original path or to a different destination. If you are restoring backed-up data to a different destination, you must prepare the destination for the restore operation.

Before restoring data either to its original path or to a different destination, you must have the following information and meet the following requirements:

- The level of the restore
- The path to which you are restoring the data
- The blocking factor used during the backup
- If you are doing an incremental restore, all tapes must be in the backup chain
- A tape drive that is available and compatible with the tape to be restored from

Before restoring data to a different destination, you must perform the following operations:

- If you are restoring a volume, you must create a new volume.
- If you are restoring a qtree or a directory, you must rename or move files that are likely to have the same names as files you are restoring.

In ONTAP 9, qtree names support the Unicode format. The earlier releases of ONTAP do not support this

format. If a qtree with Unicode names in ONTAP 9 is copied to an earlier release of ONTAP using the `ndmpcopy` command or through restoration from a backup image in a tape, the qtree is restored as a regular directory and not as a qtree with Unicode format.

If a restored file has the same name as an existing file, the existing file is overwritten by the restored file. However, the directories are not overwritten.

To rename a file, directory, or qtree during restore without using DAR, you must set the `EXTRACT` environment variable to `E`.

== Required space on the destination storage system

You require about 100 MB more space on the destination storage system than the amount of data to be restored.

The restore operation checks for volume space and inode availability on the destination volume when the restore operation starts. Setting the `FORCE` environment variable to `Y` causes the restore operation to skip the checks for volume space and inode availability on the destination path. If there is not enough volume space or inodes available on the destination volume, the restore operation recovers as much data allowed by the destination volume space and inode availability. The restore operation stops when there is no more volume space or inodes left.

= Scalability limits for dump backup and restore sessions

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You must be aware of the maximum number of dump backup and restore sessions that can be performed simultaneously on storage systems of different system memory capacities. This maximum number depends on the system memory of a storage system.

The limits mentioned in the following table are for the dump or restore engine. The limits mentioned in the scalability limits for NDMP sessions are for the NDMP server, which are higher than the engine limits.

System memory of a storage system	Total number of dump backup and restore sessions
Less than 16 GB	4
Greater than or equal to 16 GB but less than 24 GB	16
Greater than or equal to 24 GB	32

If you use `ndmpcopy` command to copy data within storage systems, two NDMP sessions are established, one for dump backup and the other for dump restore.



You can obtain the system memory of your storage system by using the `sysconfig -a` command (available through the nodeshell). For more information about using this command, see the man pages.

### Related information

[Scalability limits for NDMP sessions](#)

= Tape backup and restore support between Data ONTAP operating in 7-Mode and ONTAP

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can restore data backed up from a storage system operating in 7-Mode or running ONTAP to a storage system either operating in 7-Mode or running ONTAP.

The following tape backup and restore operations are supported between Data ONTAP operating in 7-Mode and ONTAP:

- Backing up a 7-Mode volume to a tape drive connected to a storage system running ONTAP
- Backing up an ONTAP volume to a tape drive connected to a 7-Mode system
- Restoring backed-up data of a 7-Mode volume from a tape drive connected to a storage system running ONTAP
- Restoring backed-up data of an ONTAP volume from a tape drive connected to a 7-Mode system
- Restoring a 7-Mode volume to an ONTAP volume

- A 7-Mode LUN is restored as a LUN on an ONTAP volume.
- You should retain the ONTAP LUN identifiers when restoring a 7-Mode LUN to an existing ONTAP LUN.

- Restoring an ONTAP volume to a 7-Mode volume

An ONTAP LUN is restored as a regular file on a 7-Mode volume.

= Delete restartable contexts

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

If you want to start a backup instead of restarting a context, you can delete the context.

### About this task

You can delete a restartable context using the `vserver services ndmp restartable-backup delete` command by providing the SVM name and the context ID.

### Steps

1. Delete a restartable context:

```
vserver services ndmp restartable-backup delete -vserver vserver-name  
-context-id context_identifier.
```

```
cluster::> vserver services ndmpd restartable-backup show
Vserver      Context Identifier          Is Cleanup Pending?
-----
vserver1     330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1     481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2     5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>
cluster::> vserver services ndmp restartable-backup delete -vserver
vserver1 -context-id 481025c1-0179-11e6-a299-005056bb4bc9

cluster::> vserver services ndmpd restartable-backup show
Vserver      Context Identifier          Is Cleanup Pending?
-----
vserver1     330e6739-0179-11e6-a299-005056bb4bc9 false
vserver2     5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>"
```

= How dump works on a SnapVault secondary volume

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can perform tape backup operations on data that is mirrored on the SnapVault secondary volume. You can back up only the data that is mirrored on the SnapVault

secondary volume to tape, and not the SnapVault relationship metadata.

When you break the data protection mirror relationship (`snapmirror break`) or when a SnapMirror resynchronization occurs, you must always perform a baseline backup.

= How dump works with storage failover and ARL operations

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Before you perform dump backup or restore operations, you should understand how these operations work with storage failover (takeover and giveback) or aggregate relocation (ARL) operations. The `-override-vetoes` option determines the behavior of dump engine during a storage failover or ARL operation.

When a dump backup or restore operation is running and the `-override-vetoes` option is set to `false`, a user-initiated storage failover or ARL operation is stopped. However, if the `-override-vetoes` option is set to `true`, then the storage failover or ARL operation is continued and the dump backup or restore operation is aborted. When a storage failover or ARL operation is automatically initiated by the storage system, an active dump backup or restore operation is always aborted. You cannot restart dump backup and restore operations even after storage failover or ARL operations complete.

== Dump operations when CAB extension is supported

If the backup application supports CAB extension, you can continue performing incremental dump backup and restore operations without reconfiguring backup policies after a storage failover or ARL operation.

== Dump operations when CAB extension is not supported

If the backup application does not support CAB extension, you can continue performing incremental dump backup and restore operations if you migrate the LIF configured in the backup policy to the node that hosts the destination aggregate. Otherwise, after the storage failover and ARL operation, you must perform a baseline backup prior to performing the incremental backup operation.

For storage failover operations, the LIF configured in the backup policy must be migrated to the partner node.

## Related information

[ONTAP concepts](#)

[High Availability](#)

= How dump works with volume move

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Tape backup and restore operations and volume move can run in parallel until the final cutover phase is attempted by the storage system. After this phase, new tape backup and restore operations are not allowed on the volume that is being moved. However, the current operations continue to run until completion.

The following table describes the behavior of tape backup and restore operations after the volume move operation:

<b>If you are performing tape backup and restore operations in the...</b>	<b>Then...</b>
storage virtual machine (SVM) scoped NDMP mode when CAB extension is supported by the backup application	You can continue performing incremental tape backup and restore operations on read/write and read-only volumes without reconfiguring backup policies.
SVM-scoped NDMP mode when CAB extension is not supported by the backup application	You can continue performing incremental tape backup and restore operations on read/write and read-only volumes if you migrate the LIF configured in the backup policy to the node that hosts the destination aggregate. Otherwise, after the volume move, you must perform a baseline backup before performing the incremental backup operation.

When a volume move occurs, if the volume belonging to a different SVM on the destination node has the same name as that of the moved volume, then you cannot perform incremental backup operations of the moved volume.

## Related information

### [ONTAP concepts](#)

= How dump works when a FlexVol volume is full

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Before performing an incremental dump backup operation, you must ensure that there is sufficient free space in the FlexVol volume.

If the operation fails, you must increase the free space in the Flex Vol volume either by increasing its size or by deleting the Snapshot copies. Then perform the incremental backup operation again.

= How dump works when volume access type changes

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

When a SnapMirror destination volume or a SnapVault secondary volume changes state from read/write to read-only or from read-only to read/write, you must perform a baseline tape backup or restore operation.

SnapMirror destination and SnapVault secondary volumes are read-only volumes. If you perform tape backup and restore operations on such volumes, you must perform a baseline backup or restore operation whenever the volume changes state from read-only to read/write or from read/write to read-only.

## Related information

### [ONTAP concepts](#)

= How dump works with SnapMirror single file or LUN restore

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Before you perform dump backup or restore operations on a volume to which a single file or LUN is restored by using SnapMirror technology, you must understand how dump operations work with a single file or LUN restore operation.

During a SnapMirror single file or LUN restore operation, client I/O is restricted on the file or LUN being restored. When the single file or LUN restore operation finishes, the I/O restriction on the file or LUN is removed. If a dump backup is performed on a volume to which a single file or LUN is restored, then the file or LUN that has client I/O restriction is not included in the dump backup. In a subsequent backup operation, this file or LUN is backed up to tape after the I/O restriction is removed.

You cannot perform a dump restore and a SnapMirror single file or LUN restore operation simultaneously on the same volume.

= How dump backup and restore operations are affected in MetroCluster configurations

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Before you perform dump backup and restore operations in a MetroCluster configuration, you must understand how dump operations are affected when a switchover or switchback operation occurs.

== Dump backup or restore operation followed by switchover

Consider two clusters: cluster 1 and cluster 2. During a dump backup or restore operation on cluster 1, if a switchover is initiated from cluster 1 to cluster 2, then the following occurs:

- If the value of the `override-vetoes` option is `false`, then the switchover is aborted and the backup or restore operation continues.
- If the value of the option is `true`, then the dump backup or restore operation is aborted and the switchover continues.

== Dump backup or restore operation followed by switchback

A switchover is performed from cluster 1 to cluster 2 and a dump backup or restore operation is initiated on cluster 2. The dump operation backs up or restores a volume that is located on cluster 2. At this point, if a switchback is initiated from cluster 2 to cluster 1, then the following occurs:

- If the value of the `override-vetoes` option is `false`, then the switchback is cancelled and the backup or restore operation continues.
- If the value of the option is `true`, then the backup or restore operation is aborted and the switchback continues.

== Dump backup or restore operation initiated during a switchover or switchback

During a switchover from cluster 1 to cluster 2, if a dump backup or restore operation is initiated on cluster 1, then the backup or restore operation fails and the switchover continues.

During a switchback from cluster 2 to cluster 1, if a dump backup or restore operation is initiated from cluster 2, then the backup or restore operation fails and the switchback continues.

= About SMTape engine for FlexVol volumes

= About SMTape engine for FlexVol volumes

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

SMTape is a disaster recovery solution from ONTAP that backs up blocks of data to tape. You can use SMTape to perform volume backups to tapes. However, you cannot perform a backup at the `qtree` or `subtree` level. SMTape supports baseline, differential, and incremental backups. SMTape does not require a license.

You can perform an SMTape backup and restore operation by using an NDMP-compliant backup application. You can choose SMTape to perform backup and restore operations only in the storage virtual machine (SVM) scoped NDMP mode.

Reversion process is not supported when an SMTape backup or restore session is in progress. You must wait

until the session finishes or you must abort the NDMP session.

Using SMTape, you can back up 255 Snapshot copies. For subsequent baseline, incremental, or differential backups, you must delete older backed-up Snapshot copies.

Before performing a baseline restore, the volume to which data is being restored must be of type `DP` and this volume must be in the restricted state. After a successful restore, this volume is automatically online. You can perform subsequent incremental or differential restores on this volume in the order in which the backups were performed.

= Use Snapshot copies during SMTape backup

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You should understand how Snapshot copies are used during an SMTape baseline backup and an incremental backup. There are also considerations to keep in mind while performing a backup using SMTape.

== Baseline backup

While performing a baseline backup, you can specify the name of the Snapshot copy to be backed up to tape. If no Snapshot copy is specified, then depending on the access type of the volume (read/write or read-only), either a Snapshot copy is created automatically or existing Snapshot copies are used. When you specify a Snapshot copy for the backup, all the Snapshot copies older than the specified Snapshot copy are also backed up to tape.

If you do not specify a Snapshot copy for the backup, the following occurs:

- For a read/write volume, a Snapshot copy is created automatically.

The newly created Snapshot copy and all the older Snapshot copies are backed up to tape.

- For a read-only volume, all the Snapshot copies, including the latest Snapshot copy, are backed up to tape.

Any new Snapshot copies created after the backup is started are not backed up.

== Incremental backup

For SMTape incremental or differential backup operations, the NDMP-compliant backup applications create and manage the Snapshot copies.

You must always specify a Snapshot copy while performing an incremental backup operation. For a successful incremental backup operation, the Snapshot copy backed up during the previous backup operation (baseline or incremental) must be on the volume from which the backup is performed. To ensure that you use this backed-up Snapshot copy, you must consider the Snapshot policy assigned on this volume while configuring the backup policy.

== Considerations on SMTape backups on SnapMirror destinations

- A data protection mirror relationship creates temporary Snapshot copies on the destination volume for replication.

You should not use these Snapshot copies for SMTape backup.



- If a SnapMirror update occurs on a destination volume in a data protection mirror relationship during an SMTape backup operation on the same volume, then the Snapshot copy that is backed up by SMTape must not be deleted on the source volume.

During the backup operation, SMTape locks the Snapshot copy on the destination volume and if the corresponding Snapshot copy is deleted on the source volume, then the subsequent SnapMirror update operation fails.

- You should not use these Snapshot copies during incremental backup.

= SMTape capabilities

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

SMTape capabilities such as backup of Snapshot copies, incremental and differential backups, preservation of deduplication and compression features on restored volumes, and tape seeding help you optimize your tape backup and restore operations.

SMTape provides the following capabilities:

- Provides a disaster recovery solution
- Enables incremental and differential backups
- Backs up Snapshot copies
- Enables backup and restore of deduplicated volumes and preserves deduplication on the restored volumes
- Backs up compressed volumes and preserves compression on the restored volumes
- Enables tape seeding

SMTape supports the blocking factor in multiples of 4 KB, in the range of 4 KB through 256 KB.

You can restore data to volumes created across up to two major consecutive ONTAP releases only.

= Features not supported in SMTape

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

**SMTape does not support restartable backups and verification of backed-up files.**

= Scalability limits for SMTape backup and restore sessions

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

While performing SMTape backup and restore operations through NDMP or CLI (tape seeding), you must be aware of the maximum number of SMTape backup and restore sessions that can be performed simultaneously on storage systems with different system memory capacities. This maximum number depends on the system memory of a storage system.

SMTape backup and restore sessions scalability limits are different from NDMP session limits and dump session limits.

System memory of the storage system	Total number of SMTape backup and restore sessions
Less than 16 GB	6
Greater than or equal to 16 GB but less than 24 GB	16
Greater than or equal to 24 GB	32

You can obtain the system memory of your storage system by using the `sysconfig -a` command (available through the nodeshell). For more information about using this command, see the man pages.

### Related information

[Scalability limits for NDMP sessions](#)

[Scalability limits for dump backup and restore sessions](#)

= What tape seeding is

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Tape seeding is an SMTape functionality that helps you initialize a destination FlexVol volume in a data protection mirror relationship.

Tape seeding enables you to establish a data protection mirror relationship between a source system and a destination system over a low-bandwidth connection.

Incremental mirroring of Snapshot copies from the source to the destination is feasible over a low bandwidth connection. However, an initial mirroring of the base Snapshot copy takes a long time over a low-bandwidth connection. In such cases, you can perform an SMTape backup of the source volume to a tape and use the tape to transfer the initial base Snapshot copy to the destination. You can then set up incremental SnapMirror updates to the destination system using the low-bandwidth connection.

### Related information

[ONTAP concepts](#)

= How SMTape works with storage failover and ARL operations

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Before you perform SMTape backup or restore operations, you should understand how these operations work with storage failover (takeover and giveback) or aggregate relocation (ARL) operation. The `-override-vetoes` option determines the behavior of SMTape engine during a storage failover or ARL operation.

When an SMTape backup or restore operation is running and the `-override-vetoes` option is set to `false`, a user-initiated storage failover or ARL operation is stopped and the backup or restore operation complete. If the backup application supports CAB extension, then you can continue performing

incremental SMTape backup and restore operations without reconfiguring backup policies. However, if the `-override-vetoes` option is set to `true`, then the storage failover or ARL operation is continued and the SMTape backup or restore operation is aborted.

#### Related information

[Network management](#)

[High Availability](#)

= How SMTape works with volume move

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

SMTape backup operations and volume move operations can run in parallel until the storage system attempts the final cutover phase. After this phase, new SMTape backup operations cannot run on the volume that is being moved. However, the current operations continue to run until completion.

Before the cutover phase for a volume is started, the volume move operation checks for active SMTape backup operations on the same volume. If there are active SMTape backup operations, then the volume move operation moves into a cutover deferred state and allows the SMTape backup operations to complete. After these backup operations are completed, you must manually restart the volume move operation.

If the backup application supports CAB extension, you can continue performing incremental tape backup and restore operations on read/write and read-only volumes without reconfiguring backup policies.

Baseline restore and volume move operations cannot be performed simultaneously; however, incremental restore can run in parallel with volume move operations, with the behavior similar to that of SMTape backup operations during volume move operations.

#### Related information

[ONTAP concepts](#)

= How SMTape works with volume rehost operations

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

SMTape operations cannot commence when a volume rehost operation is in progress on a volume. When a volume is involved in a volume rehost operation, SMTape sessions should not be started on that volume.

If any volume rehost operation is in progress, then SMTape backup or restore fails. If an SMTape backup or restore is in progress, then volume rehost operations fail with an appropriate error message. This condition applies to both NDMP-based and CLI-based backup or restore operations.

= How NDMP backup policy are affected during ADB

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

When the automatic data balancer (ADB) is enabled, the balancer analyzes the usage statistics of aggregates to identify the aggregate that has exceeded the configured high-threshold usage percentage.

After identifying the aggregate that has exceeded the threshold, the balancer identifies a volume that can be moved to aggregates residing in another node in the cluster and attempts to move that volume. This situation affects the backup policy configured for this volume because if the data management application (DMA) is not CAB aware, then the user has to reconfigure the backup policy and run the baseline backup operation.

If the DMA is CAB aware and the backup policy has been configured using specific interface, then the ADB is not affected.

= How SMTape backup and restore operations are affected in MetroCluster configurations

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Before you perform SMTape backup and restore operations in a MetroCluster configuration, you must understand how SMTape operations are affected when a switchover or switchback operation occurs.

== SMTape backup or restore operation followed by switchover

Consider two clusters: cluster 1 and cluster 2. During an SMTape backup or restore operation on cluster 1, if a switchover is initiated from cluster 1 to cluster 2, then the following occurs:

- If the value of the `-override-vetoes` option is `false`, then the switchover process is aborted and the backup or restore operation continues.
- If the value of the option is `true`, then the SMTape backup or restore operation is aborted and the switchover process continues.

== SMTape backup or restore operation followed by switchback

A switchover is performed from cluster 1 to cluster 2 and an SMTape backup or restore operation is initiated on cluster 2. The SMTape operation backs up or restores a volume that is located on cluster 2. At this point, if a switchback is initiated from cluster 2 to cluster 1, then the following occurs:

- If the value of the `-override-vetoes` option is `false`, then the switchback process is aborted and the backup or restore operation continues.
- If the value of the option is `true`, then the backup or restore operation is aborted and the switchback process continues.

== SMTape backup or restore operation initiated during a switchover or switchback

During a switchover process from cluster 1 to cluster 2, if an SMTape backup or restore operation is initiated on cluster 1, then the backup or restore operation fails and the switchover continues.

During a switchback process from cluster 2 to cluster 1, if an SMTape backup or restore operation is initiated from cluster 2, then the backup or restore operation fails and the switchback continues.

= Monitor tape backup and restore operations for FlexVol volumes

= Monitor tape backup and restore operations for FlexVol volumes overview

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can view the event log files to monitor the tape backup and restore operations. ONTAP automatically logs significant backup and restore events and the time at which they occur in a log file named `backup` in the controller's `/etc/log/` directory. By default, event logging is set to `on`.

You might want to view event log files for the following reasons:

- Checking whether a nightly backup was successful
- Gathering statistics on backup operations
- For using the information in past event log files to help diagnose problems with backup and restore operations

Once every week, the event log files are rotated. The `/etc/log/backup` file is renamed to `/etc/log/backup.0`, the `/etc/log/backup.0` file is renamed to `/etc/log/backup.1`, and so on. The system saves the log files for up to six weeks; therefore, you can have up to seven message files (`/etc/log/backup.[0-5]` and the current `/etc/log/backup` file).

= Access the event log files

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can access the event log files for tape backup and restore operations in the `/etc/log/` directory by using the `rdfile` command at the nodeshell. You can view these event log files to monitor tape backup and restore operations.

### About this task

With additional configurations, such as an access-control role with access to the `spi` web service or a user account set up with the `http` access method, you can also use a web browser to access these log files.

### Steps

1. To access the nodeshell, enter the following command:

```
node run -node node_name
```

`node_name` is the name of the node.

2. To access the event log files for tape backup and restore operations, enter the following command:

```
rdfile /etc/log/backup
```

### Related information

[System administration](#)

[ONTAP concepts](#)

= What the dump and restore event log message format is

= Dump and restore event log message format overview

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

For each dump and restore event, a message is written to the backup log file.

The format of the dump and restore event log message is as follows:

`type timestamp identifier event (event_info)`

The following list describes the fields in the event log message format:

- Each log message begins with one of the type indicators described in the following table:

Type	Description
log	Logging event
dmp	Dump event
rst	Restore event

- `timestamp` shows the date and time of the event.
- The `identifier` field for a dump event includes the dump path and the unique ID for the dump. The `identifier` field for a restore event uses only the restore destination path name as a unique identifier. Logging-related event messages do not include an `identifier` field.

= What logging events are

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

The event field of a message that begins with a log specifies the beginning of a logging or the end of a logging.

It contains one of the events shown in the following table:

Event	Description
Start_Logging	Indicates the beginning of logging or that logging has been turned back on after being disabled.
Stop_Logging	Indicates that logging has been turned off.

= What dump events are

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

The event field for a dump event contains an event type followed by event-specific information within parentheses.

The following table describes the events, their descriptions, and the related event information that might be recorded for a dump operation:



<b>Event</b>	<b>Description</b>	<b>Event information</b>
Start	NDMP dump is started	Dump level and the type of dump
End	Dumps completed successfully	Amount of data processed
Abort	The operation is cancelled	Amount of data processed
Options	Specified options are listed	All options and their associated values, including NDMP options
Tape_open	The tape is open for read/write	The new tape device name
Tape_close	The tape is closed for read/write	The tape device name
Phase-change	A dump is entering a new processing phase	The new phase name
Error	A dump has encountered an unexpected event	Error message
Snapshot	A Snapshot copy is created or located	The name and time of the Snapshot copy
Base_dump	A base dump entry in the internal metafile has been located	The level and time of the base dump (for incremental dumps only)

= What restore events are

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

The event field for a restore event contains an event type followed by event-specific information in parentheses.

The following table provides information about the events, their descriptions, and the related event information that can be recorded for a restore operation:

<b>Event</b>	<b>Description</b>	<b>Event information</b>
Start	NDMP restore is started	Restore level and the type of restore
End	Restores completed successfully	Number of files and amount of data processed

Event	Description	Event information
Abort	The operation is cancelled	Number of files and amount of data processed
Options	Specified options are listed	All options and their associated values, including NDMP options
Tape_open	The tape is open for read/write	The new tape device name
Tape_close	The tape is closed for read/write	The tape device name
Phase-change	Restore is entering a new processing phase	The new phase name
Error	Restore encounters an unexpected event	Error message

= Enabling or disabling event logging

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can turn the event logging on or off.

### Steps

1. To enable or disable event logging, enter the following command at the clustershell:

```
options -option_name backup.log.enable -option-value {on | off}
```

`on` turns event logging on.

`off` turns event logging off.

Event logging is turned on by default.

= Error messages for tape backup and restore of FlexVol volumes

= Backup and restore error messages

= Resource limitation: no available thread

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Resource limitation: no available thread

- **Cause**

The maximum number of active local tape I/O threads is currently in use. You can have a maximum of 16 active local tape drives.

- **Corrective action**

Wait for some tape jobs to finish before starting a new backup or restore job.

= Tape reservation preempted

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Tape reservation preempted

- **Cause**

The tape drive is in use by another operation or the tape has been closed prematurely.

- **Corrective action**

Ensure that the tape drive is not in use by another operation and that the DMA application has not aborted the job and then retry.

= Could not initialize media

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Could not initialize media

- **Cause**

You might get this error for one of the following reasons:

- The tape drive used for the backup is corrupt or damaged.
- The tape does not contain the complete backup or is corrupt.
- The maximum number of active local tape I/O threads is currently in use.

You can have a maximum of 16 active local tape drives.

- **Corrective action**

- If the tape drive is corrupt or damaged, retry the operation with a valid tape drive.
- If the tape does not contain the complete backup or is corrupt, you cannot perform the restore operation.
- If tape resources are not available, wait for some of the backup or restore jobs to finish and then retry the operation.

= Maximum number of allowed dumps or restores (maximum session limit) in progress

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Maximum number of allowed dumps or restores (*maximum session limit*) in progress

- **Cause**

The maximum number of backup or restore jobs is already running.

- **Corrective action**

Retry the operation after some of the currently running jobs have finished.

= Media error on tape write

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Media error on tape write

- **Cause**

The tape used for the backup is corrupted.

- **Corrective action**

Replace the tape and retry the backup job.

= Tape write failed

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Tape write failed

- **Cause**

The tape used for the backup is corrupted.

- **Corrective action**

Replace the tape and retry the backup job.

= Tape write failed - new tape encountered media error

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Tape write failed - new tape encountered media error

- **Cause**

The tape used for the backup is corrupted.

- **Corrective action**

Replace the tape and retry the backup.

= Tape write failed - new tape is broken or write protected

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Tape write failed - new tape is broken or write protected

- **Cause**

The tape used for the backup is corrupted or write-protected.

- **Corrective action**

Replace the tape and retry the backup.

= Tape write failed - new tape is already at the end of media

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Tape write failed - new tape is already at the end of media

- **Cause**

There is not enough space on the tape to complete the backup.

- **Corrective action**

Replace the tape and retry the backup.

= Tape write error

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Tape write error - The previous tape had less than the required minimum capacity, size MB, for this tape operation, The operation should be restarted from the beginning

- **Cause**

The tape capacity is insufficient to contain the backup data.

- **Corrective action**

Use tapes with larger capacity and retry the backup job.

= Media error on tape read

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Media error on tape read

- **Cause**

The tape from which data is being restored is corrupted and might not contain the complete backup data.

- **Corrective action**

If you are sure that the tape has the complete backup, retry the restore operation. If the tape does not contain the complete backup, you cannot perform the restore operation.

= Tape read error

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Tape read error

- **Cause**

The tape drive is damaged or the tape does not contain the complete backup.

- **Corrective action**

If the tape drive is damaged, use another tape drive. If the tape does not contain the complete backup, you cannot restore the data.

= Already at the end of tape

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Already at the end of tape

- **Cause**

The tape does not contain any data or must be rewound.

- **Corrective action**

If the tape does not contain data, use the tape that contains the backup and retry the restore job. Otherwise, rewind the tape and retry the restore job.

= Tape record size is too small. Try a larger size.

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Tape record size is too small. Try a larger size.

- **Cause**

The blocking factor specified for the restore operation is smaller than the blocking factor that was used during the backup.

- **Corrective action**

Use the same blocking factor that was specified during the backup.

= Tape record size should be block\_size1 and not block\_size2

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Tape record size should be block\_size1 and not block\_size2

- **Cause**

The blocking factor specified for the local restore is incorrect.

- **Corrective action**

Retry the restore job with `block_size1` as the blocking factor.

= Tape record size must be in the range between 4KB and 256KB

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Tape record size must be in the range between 4KB and 256KB

- **Cause**

The blocking factor specified for the backup or restore operation is not within the permitted range.

- **Corrective action**

Specify a blocking factor in the range of 4 KB to 256 KB.

= NDMP error messages

= Network communication error

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Network communication error

- **Cause**

Communication to a remote tape in an NDMP three-way connection has failed.

- **Corrective action**

Check the network connection to the remote mover.

= Message from Read Socket: error\_string

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Message from Read Socket: error\_string



- **Cause**

Restore communication from the remote tape in NDMP 3-way connection has errors.

- **Corrective action**

Check the network connection to the remote mover.

= Message from Write Dirnet: error\_string

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Message from Write Dirnet: error\_string

- **Cause**

Backup communication to a remote tape in an NDMP three-way connection has an error.

- **Corrective action**

Check the network connection to the remote mover.

= Read Socket received EOF

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Read Socket received EOF

- **Cause**

Attempt to communicate with a remote tape in an NDMP three-way connection has reached the End Of File mark. You might be attempting a three-way restore from a backup image with a larger block size.

- **Corrective action**

Specify the correct block size and retry the restore operation.

= ndmpd invalid version number: version\_number ``

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

ndmpd invalid version number: version\_number

- **Cause**

The NDMP version specified is not supported by the storage system.

- **Corrective action**

Specify NDMP version 4.

```
= ndmpd session session_ID not active
:icons: font
:relative_path: ./tape-backup/
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/
```

- **Message**

```
ndmpd session session_ID not active
```

- **Cause**

The NDMP session might not exist.

- **Corrective action**

Use the `ndmpd status` command to view the active NDMP sessions.

```
= Could not obtain vol ref for Volume volume_name
:icons: font
:relative_path: ./tape-backup/
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/
```

- **Message**

```
Could not obtain vol ref for Volume vol_name
```

- **Cause**

The volume reference could not be obtained because the volume might be in use by other operations.

- **Corrective action**

Retry the operation later.

```
= Data connection type ["NDMP4_ADDR_TCP"|"NDMP4_ADDR_TCP_IPv6"] not supported for
["IPv6"|"IPv4"] control connections
:icons: font
:relative_path: ./tape-backup/
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/
```

- **Message**

```
Data connection type ["NDMP4_ADDR_TCP"|"NDMP4_ADDR_TCP_IPv6"] not supported
for ["IPv6"|"IPv4"] control connections
```

- **Cause**

In node-scoped NDMP mode, the NDMP data connection established must be of the same network address type (IPv4 or IPv6) as the NDMP control connection.

- **Corrective action**

Contact your backup application vendor.

= DATA LISTEN: CAB data connection prepare precondition error

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

```
DATA LISTEN: CAB data connection prepare precondition error
```

- **Cause**

NDMP data listen fails when the backup application has negotiated the CAB extension with the NDMP server and there is a mismatch in the specified NDMP data connection address type between the NDMP\_CAB\_DATA\_CONN\_PREPARE and the NDMP\_DATA\_LISTEN messages.

- **Corrective action**

Contact your backup application vendor.

= DATA CONNECT: CAB data connection prepare precondition error

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

```
DATA CONNECT: CAB data connection prepare precondition error
```

- **Cause**

NDMP data connect fails when the backup application has negotiated the CAB extension with the NDMP server and there is a mismatch in the specified NDMP data connection address type between the NDMP\_CAB\_DATA\_CONN\_PREPARE and the NDMP\_DATA\_CONNECT messages.

- **Corrective action**

Contact your backup application vendor.

= Error:show failed: Cannot get password for user '<username>'

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

```
Error: show failed: Cannot get password for user '<username>'
```

- **Cause**

Incomplete user account configuration for NDMP

- **Corrective action**

Ensure that the user account is associated with the SSH access method and the authentication method is user password.

= Dump error messages

= Destination volume is read-only

```
:icons: font
```

```
:relative_path: ./tape-backup/
```

```
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/
```

- **Message**

```
Destination volume is read-only
```

- **Cause**

The path to which the restore operation is attempted to is read-only.

- **Corrective action**

Try restoring the data to a different location.

= Destination qtree is read-only

```
:icons: font
```

```
:relative_path: ./tape-backup/
```

```
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/
```

- **Message**

```
Destination qtree is read-only
```

- **Cause**

The qtree to which the restore is attempted to is read-only.

- **Corrective action**

Try restoring the data to a different location.

= Dumps temporarily disabled on volume, try again

```
:icons: font
```

```
:relative_path: ./tape-backup/
```

```
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/
```

- **Message**

Dumps temporarily disabled on volume, try again

- **Cause**

NDMP dump backup is attempted on a SnapMirror destination volume that is part of either a `snapmirror break` or a `snapmirror resync` operation.

- **Corrective action**

Wait for the `snapmirror break` or `snapmirror resync` operation to finish and then perform the dump operation.

Whenever the state of a SnapMirror destination volume changes from read/write to read-only or from read-only to read/write, you must perform a baseline backup.

= NFS labels not recognized

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Error: Aborting: dump encountered NFS security labels in the file system

- **Cause**

NFS security labels are supported Beginning with ONTAP 9.9.1 when NFSv4.2 is enabled. However, NFS security labels are not currently recognized by the dump engine. If it encounters any NFS security labels on the files, directories, or any special files in any format of dump, the dump fails.

- **Corrective action**

Verify that no files or directories have NFS security labels.

= No files were created

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

No files were created

- **Cause**

A directory DAR was attempted without enabling the enhanced DAR functionality.

- **Corrective action**

Enable the enhanced DAR functionality and retry the DAR.

= Restore of the file <file name> failed

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Restore of the file file name failed

- **Cause**

When a DAR (Direct Access Recovery) of a file whose file name is the same as that of a LUN on the destination volume is performed, then the DAR fails.

- **Corrective action**

Retry DAR of the file.

= Truncation failed for src inode <inode number>...

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Truncation failed for src inode <inode number>. Error <error number>. Skipping inode.

- **Cause**

Inode of a file is deleted when the file is being restored.

- **Corrective action**

Wait for the restore operation on a volume to complete before using that volume.

= Unable to lock a snapshot needed by dump

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Unable to lock a snapshot needed by dump

- **Cause**

The Snapshot copy specified for the backup is not available.

- **Corrective action**

Retry the backup with a different Snapshot copy.

Use the `snap list` command to see the list of available Snapshot copies.

= Unable to locate bitmap files

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Unable to locate bitmap files

- **Cause**

The bitmap files required for the backup operation might have been deleted. In this case, the backup cannot be restarted.

- **Corrective action**

Perform the backup again.

= Volume is temporarily in a transitional state

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Volume is temporarily in a transitional state

- **Cause**

The volume being backed up is temporarily in an unmounted state.

- **Corrective action**

Wait for some time and perform the backup again.

= SMTape error messages

= Chunks out of order

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Chunks out of order

- **Cause**

The backup tapes are not being restored in the correct sequence.

- **Corrective action**

Retry the restore operation and load the tapes in the correct sequence.

= Chunk format not supported

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Chunk format not supported

- **Cause**

The backup image is not of SMTape.

- **Corrective action**

If the backup image is not of SMTape, retry the operation with a tape that has the SMTape backup.

= Failed to allocate memory



:icons: font  
:relative\_path: ./tape-backup/  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Failed to allocate memory

- **Cause**

The system has run out of memory.

- **Corrective action**

Retry the job later when the system is not too busy.

= Failed to get data buffer

:icons: font  
:relative\_path: ./tape-backup/  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Failed to get data buffer

- **Cause**

The storage system ran out of buffers.

- **Corrective action**

Wait for some storage system operations to finish and then retry the job.

= Failed to find snapshot

:icons: font  
:relative\_path: ./tape-backup/  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Failed to find snapshot

- **Cause**

The Snapshot copy specified for the backup is unavailable.

- **Corrective action**

Check if the specified Snapshot copy is available. If not, retry with the correct Snapshot copy.

= Failed to create snapshot

:icons: font  
:relative\_path: ./tape-backup/  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Failed to create snapshot

- **Cause**

The volume already contains the maximum number of Snapshot copies.

- **Corrective action**

Delete some Snapshot copies and then retry the backup operation.

= Failed to lock snapshot

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Failed to lock snapshot

- **Cause**

The Snapshot copy is either in use or has been deleted.

- **Corrective action**

If the Snapshot copy is in use by another operation, wait for that operation to finish and then retry the backup. If the Snapshot copy has been deleted, you cannot perform the backup.

= Failed to delete snapshot

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Failed to delete snapshot

- **Cause**

The auto Snapshot copy could not be deleted because it is in use by other operations.

- **Corrective action**

Use the `snap` command to determine the status of the Snapshot copy. If the Snapshot copy is not required, delete it manually.

= Failed to get latest snapshot

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Failed to get latest snapshot

- **Cause**

The latest Snapshot copy might not exist because the volume is being initialized by SnapMirror.

- **Corrective action**

Retry after initialization is complete.

= Failed to load new tape

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Failed to load new tape

- **Cause**

Error in tape drive or media.

- **Corrective action**

Replace the tape and retry the operation.

= Failed to initialize tape

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Failed to initialize tape

- **Cause**

You might get this error message for one of the following reasons:

- The backup image is not of SMTape.
- The tape blocking factor specified is incorrect.
- The tape is corrupt or damaged.
- The wrong tape is loaded for restore.

- **Corrective action**

- If the backup image is not of SMTape, retry the operation with a tape that has SMTape backup.
- If the blocking factor is incorrect, specify the correct blocking factor and retry the operation.
- If the tape is corrupt, you cannot perform the restore operation.

- If the wrong tape is loaded, retry the operation with the correct tape.

= Failed to initialize restore stream

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Failed to initialize restore stream

- **Cause**

You might get this error message for one of the following reasons:

- The backup image is not of SMTape.
- The tape blocking factor specified is incorrect.
- The tape is corrupt or damaged.
- The wrong tape is loaded for restore.

- **Corrective action**

- If the backup image is not of SMTape, retry the operation with a tape that has the SMTape backup.
- If the blocking factor is incorrect, specify the correct blocking factor and retry the operation.
- If the tape is corrupt, you cannot perform the restore operation.
- If the wrong tape is loaded, retry the operation with the correct tape.

= Failed to read backup image

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Failed to read backup image

- **Cause**

The tape is corrupt.

- **Corrective action**

If the tape is corrupt, you cannot perform the restore operation.

= Image header missing or corrupted

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Image header missing or corrupted

- **Cause**

The tape does not contain a valid SMTape backup.

- **Corrective action**

Retry with a tape containing a valid backup.

= Internal assertion

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Internal assertion

- **Cause**

There is an internal SMTape error.

- **Corrective action**

Report the error and send the `etc/log/backup` file to technical support.

= Invalid backup image magic number

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Invalid backup image magic number

- **Cause**

The backup image is not of SMTape.

- **Corrective action**

If the backup image is not of SMTape, retry the operation with a tape that has the SMTape backup.

= Invalid backup image checksum

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Invalid backup image checksum

- **Cause**

The tape is corrupt.

- **Corrective action**

If the tape is corrupt, you cannot perform the restore operation.

= Invalid input tape

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Invalid input tape

- **Cause**

The signature of the backup image is not valid in the tape header. The tape has corrupted data or does not contain a valid backup image.

- **Corrective action**

Retry the restore job with a valid backup image.

= Invalid volume path

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Invalid volume path

- **Cause**

The specified volume for the backup or restore operation is not found.

- **Corrective action**

Retry the job with a valid volume path and volume name.

= Mismatch in backup set ID

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Mismatch in backup set ID

- **Cause**

The tape loaded during a tape change is not a part of the backup set.

- **Corrective action**

Load the correct tape and retry the job.

= Mismatch in backup time stamp

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Mismatch in backup time stamp

- **Cause**

The tape loaded during a tape change is not a part of the backup set.

- **Corrective action**

Use the `smtape restore -h` command to verify the header information of a tape.

= Job aborted due to shutdown

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Job aborted due to shutdown

- **Cause**

The storage system is being rebooted.

- **Corrective action**

Retry the job after the storage system reboots.

= Job aborted due to Snapshot autodelete

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Job aborted due to Snapshot autodelete

- **Cause**

The volume does not have enough space and has triggered the automatic deletion of Snapshot copies.

- **Corrective action**

Free up space in the volume and retry the job.

= Tape is currently in use by other operations

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Tape is currently in use by other operations

- **Cause**

The tape drive is in use by another job.

- **Corrective action**

Retry the backup after the currently active job is finished.

= Tapes out of order

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Tapes out of order

- **Cause**

The first tape of the tape sequence for the restore operation does not have the image header.

- **Corrective action**

Load the tape with the image header and retry the job.

= Transfer failed (Aborted due to MetroCluster operation)

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Transfer failed (Aborted due to MetroCluster operation)

- **Cause**

The SMTape operation is aborted because of a switchover or switchback operation.

- **Corrective action**

Perform the SMTape operation after the switchover or switchback operation finishes.

= Transfer failed (ARL initiated abort)

:icons: font

:relative\_path: ./tape-backup/



:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Transfer failed (ARL initiated abort)

- **Cause**

While an SMTape operation is in progress if an aggregate relocation is initiated, then the SMTape operation is aborted.

- **Corrective action**

Perform the SMTape operation after the aggregate relocation operation finishes.

= Transfer failed (CFO initiated abort)

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Transfer failed (CFO initiated abort)

- **Cause**

The SMTape operation is aborted because of a storage failover (takeover and giveback) operation of a CFO aggregate.

- **Corrective action**

Perform the SMTape operation after the storage failover of the CFO aggregate finishes.

= Transfer failed (SFO initiated abort)

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Transfer failed (SFO initiated abort)

- **Cause**

The SMTape operation is aborted because of a storage failover (takeover and giveback) operation.

- **Corrective action**

Perform the SMTape operation after the storage failover (takeover and giveback) operation finishes.

= Underlying aggregate under migration

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Underlying aggregate under migration

- **Cause**

If an SMTape operation is initiated on an aggregate that is under migration (storage failover or aggregate relocation), then the SMTape operation fails.

- **Corrective action**

Perform the SMTape operation after the aggregate migration finishes.

= Volume is currently under migration

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Volume is currently under migration

- **Cause**

Volume migration and SMTape backup cannot run simultaneously.

- **Corrective action**

Retry the backup job after the volume migration is complete.

= Volume offline

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Volume offline

- **Cause**

The volume being backed up is offline.

- **Corrective action**

Bring the volume online and retry the backup.

= Volume not restricted

:icons: font

:relative\_path: ./tape-backup/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

- **Message**

Volume not restricted

- **Cause**

The destination volume to which data is being restored is not restricted.

- **Corrective action**

Restrict the volume and retry the restore operation.

= NDMP configuration

= NDMP configuration overview

:icons: font

:relative\_path: ./ndmp/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can quickly configure an ONTAP 9 cluster to use the Network Data Management Protocol (NDMP) to back up data directly to tape using a third-party backup application.

Configure NDMP in the following circumstances:

- The cluster is running ONTAP 9.
- You have a third-party backup application (also called a Data Management Application or DMA).
- You are a cluster administrator.
- You want to perform backup operations either at the cluster level (using the admin storage virtual machine (SVM)) or node level.
- Tape devices and an optional media server are installed.
- Tape devices are connected to the cluster through a Fibre Channel (FC) switch and not directly attached.
- At least one tape device has a logical unit number (LUN) of 0.

#### **Related information**

[Data protection using tape backup.](#)

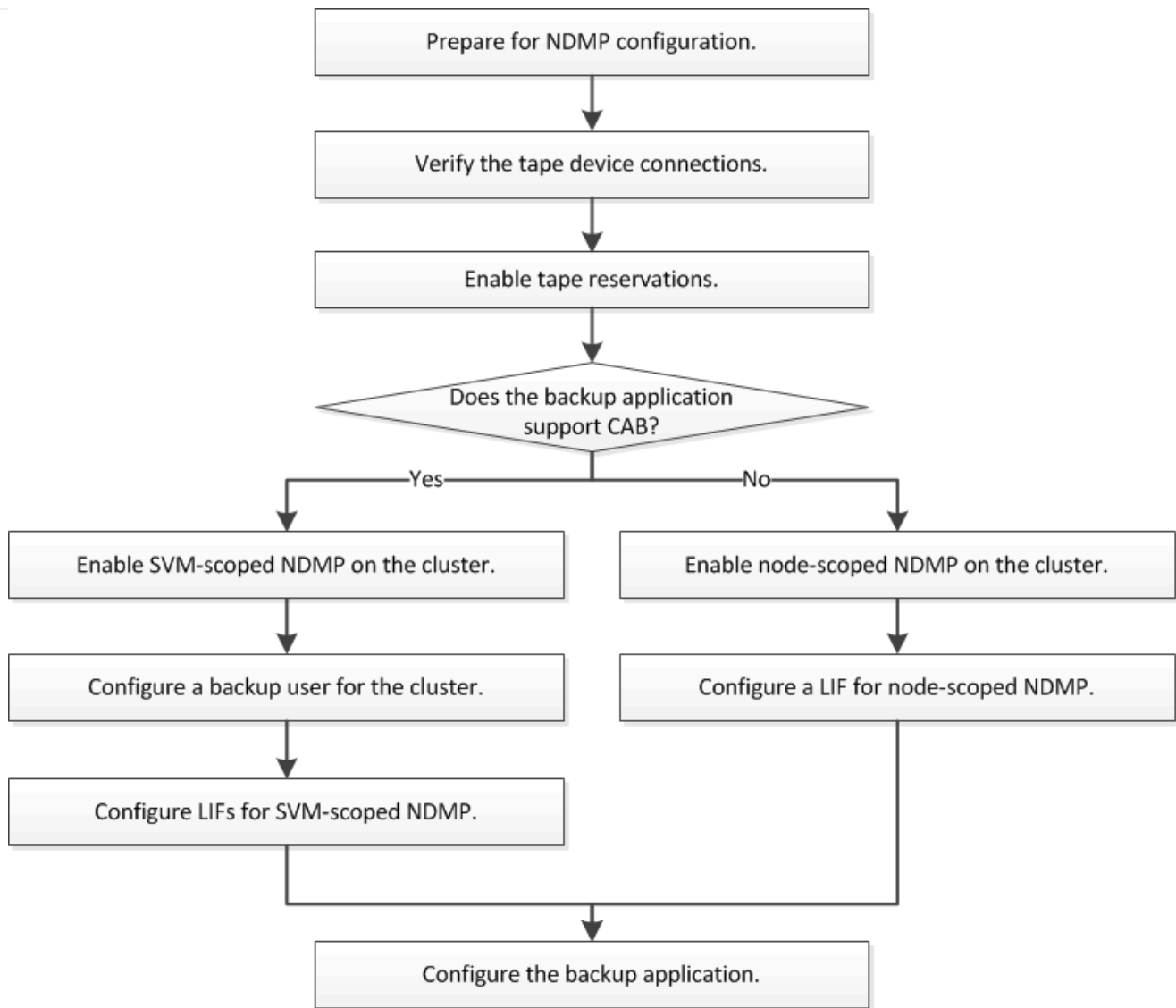
= NDMP configuration workflow

:icons: font

:relative\_path: ./ndmp/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Setting up tape backup over NDMP involves preparing for NDMP configuration, verifying the tape device connections, enabling tape reservations, configuring NDMP at the SVM or node level, enabling NDMP on the cluster, configuring a backup user, configuring LIFs, and configuring the backup application.



= Prepare for NDMP configuration

:icons: font

:relative\_path: ./ndmp/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Before you configure tape backup access over Network Data Management Protocol (NDMP), you must verify that the planned configuration is supported, verify that your tape drives are listed as qualified drives on each node, verify that all nodes have intercluster LIFs, and identify whether the backup application supports the Cluster Aware Backup (CAB) extension.

### Steps

1. Refer to your backup application provider's compatibility matrix for ONTAP support (NetApp does not qualify third-party backup applications with ONTAP or NDMP).

You should verify that the following NetApp components are compatible:

- The version of ONTAP 9 that is running on the cluster.
- The backup application vendor and version: for example, Veritas NetBackup 8.2 or CommVault.

- The tape devices details, such as the manufacturer, model, and interface of the tape drives: for example, IBM Ultrium 8 or HPe StoreEver Ultrium 30750 LTO-8.
- The platforms of the nodes in the cluster: for example, FAS8700 or A400.



You can find legacy ONTAP compatibility support matrices for backup applications in the [NetApp Interoperability Matrix Tool](#).

2. Verify that your tape drives are listed as qualified drives in each node's built-in tape configuration file:

- On the command line-interface, view the built-in tape configuration file by using the `storage tape show-supported-status` command.

```
cluster1::> storage tape show-supported-status

Node: cluster1-1

Tape Drives                                Is
-----                                -
Support Status

-----
Certance Ultrium 2                          true      Dynamically Qualified
Certance Ultrium 3                          true      Dynamically Qualified
Digital DLT2000                             true      Qualified
```

- Compare your tape drives to the list of qualified drives in the output.

The names of the tape devices in the output might vary slightly from the names on the device label or in the Interoperability Matrix. For example, Digital DLT2000 can also be known as DLT2k. You can ignore these minor naming differences.

- a. If a device is not listed as qualified in the output even though the device is qualified according to the Interoperability Matrix, download and install an updated configuration file for the device using the instructions on the NetApp Support Site.

### NetApp Downloads: Tape Device Configuration Files

A qualified device might not be listed in the built-in tape configuration file if the tape device was qualified after the node was shipped.

. Verify that every node in the cluster has an intercluster LIF:

- b. View the intercluster LIFs on the nodes by using the `network interface show -role intercluster` command.

```
cluster1::> network interface show -role intercluster
```

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
-----	-----	-----	-----	-----
cluster1	IC1	up/up	192.0.2.65/24	cluster1-1
e0a	true			

- c. If an intercluster LIF does not exist on any node, create an intercluster LIF by using the `network interface create` command.

```
cluster1::> network interface create -vserver cluster1 -lif IC2
-role intercluster
-home-node cluster1-2 -home-port e0b -address 192.0.2.68 -netmask
255.255.255.0
-status-admin up -failover-policy local-only -firewall-policy
intercluster
```

```
cluster1::> network interface show -role intercluster
```

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
cluster1	IC1	up/up	192.0.2.65/24	cluster1-1
e0a	true			
cluster1	IC2	up/up	192.0.2.68/24	cluster1-2
e0b	true			

### Network management

. Identify whether the backup application supports Cluster Aware Backup (CAB) by using the documentation provided with the backup application.

+

CAB support is a key factor in determining the type of backup you can perform.

= Verify tape device connections

:icons: font

:relative\_path: ./ndmp/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You must ensure that all drives and media changers are visible in ONTAP as devices.

### Steps

1. View information about all drives and media changers by using the `storage tape show` command.

```
cluster1::> storage tape show
```

```
Node: cluster1-01
```

Device ID	Device Type	Description
sw4:10.11	tape drive	HP LTO-3
0b.125L1	media changer	HP MSL G3 Series
0d.4	tape drive	IBM LTO 5 ULT3580
0d.4L1	media changer	IBM 3573-TL

normal  
normal  
normal  
normal  
...

2. If a tape drive is not displayed, troubleshoot the problem.
3. If a media changer is not displayed, view information about media changers by using the `storage tape show-media-changer` command, and then troubleshoot the problem.

```
cluster1::> storage tape show-media-changer
```

```
Media Changer: sw4:10.11L1
```

```
Description: PX70-TL
```

```
WWNN: 2:00a:000e11:10b919
```

```
WWPN: 2:00b:000e11:10b919
```

```
Serial Number: 00FRU7800000_LL1
```

```
Errors: -
```

```
Paths:
```

Node	Initiator	Alias	Device State
------	-----------	-------	--------------

Status			
--------	--	--	--

cluster1-01	2b	mc0	in-use
-------------	----	-----	--------

normal

...

= Enable tape reservations

:icons: font

:relative\_path: ./ndmp/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/



You must ensure that tape drives are reserved for use by backup applications for NDMP backup operations.

### About this task

The reservation settings vary in different backup applications, and these settings must match the backup application and the nodes or servers using the same drives. See the vendor documentation of the backup application for the correct reservation settings.

### Steps

1. Enable reservations by using the options `-option-name tape.reservations -option -value persistent` command.

The following command enables reservations with the `persistent` value:

```
cluster1::> options -option-name tape.reservations -option-value
persistent
2 entries were modified.
```

2. Verify that reservations are enabled on all nodes by using the `options tape.reservations` command, and then review the output.

```
cluster1::> options tape.reservations

cluster1-1
  tape.reservations           persistent

cluster1-2
  tape.reservations           persistent
2 entries were displayed.
```

= Configure NDMP at the SVM level or the node level

= Configure NDMP at the SVM level or the node level overview

:icons: font

:relative\_path: ./ndmp/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

If the backup application supports Cluster Aware Backup (CAB), you can configure NDMP as SVM-scoped at the cluster (admin SVM) level, which enables you to back up all volumes hosted across different nodes of the cluster. Otherwise, you can configure node-scoped NDMP, which enables you to back up all the volumes hosted on that node.

= Configure SVM-scoped NDMP

= Configure SVM-scoped NDMP overview

:icons: font

```
:relative_path: ./ndmp/  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/
```

If the DMA supports the Cluster Aware Backup (CAB) extension, you can back up all the volumes hosted across different nodes in a cluster by enabling SVM-scoped NDMP, configuring a backup user account, and configuring LIFs for data and control connection.

### What you'll need

The CAB extension must be supported by the DMA.

= Enable SVM-scoped NDMP on the cluster

```
:icons: font
```

```
:relative_path: ./ndmp/
```

```
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/
```

You can configure SVM-scoped NDMP on the cluster by enabling SVM-scoped NDMP mode and NDMP service on the cluster (admin SVM).

### About this task

Turning off node-scoped NDMP mode enables SVM-scoped NDMP mode on the cluster.

### Steps

1. Enable SVM-scoped NDMP mode by using the `system services ndmp` command with the `node-scope-mode` parameter.

```
cluster1::> system services ndmp node-scope-mode off  
NDMP node-scope-mode is disabled.
```

2. Enable NDMP service on the admin SVM by using the `vserver services ndmp on` command.

```
cluster1::> vserver services ndmp on -vserver cluster1
```

The authentication type is set to `challenge` by default and plaintext authentication is disabled.

For secure communication, you should keep plaintext authentication disabled.

1. Verify that NDMP service is enabled by using the `vserver services ndmp show` command.

```
cluster1::> vserver services ndmp show

Vserver      Enabled  Authentication type
-----
cluster1     true     challenge
vs1          false    challenge
```

= Configure a backup user for the cluster

:icons: font

:relative\_path: ./ndmp/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

To authenticate NDMP from the backup application, you must create a local backup user, or an NIS or LDAP user for the cluster with the admin or backup role, and generate an NDMP password for the backup user.

### What you'll need

If you are using an NIS or LDAP user, the user must be created on the respective server. You cannot use an Active Directory user.

### Steps

1. Create a backup user with the admin or backup role by using the `security login create` command.

You can specify a local backup user name or an NIS or LDAP user name for the `-user-or-group -name` parameter.

The following command creates the backup user `backup_admin1` with the `backup` role:

```
cluster1::> security login create -user-or-group-name backup_admin1
-application ssh
-authmethod password -role backup

Please enter a password for user 'backup_admin1':
Please enter it again:
```

2. Generate a password for the admin SVM by using the `vserver services ndmp generate password` command.

The generated password must be used to authenticate the NDMP connection by the backup application.

```
cluster1::> vserver services ndmp generate-password -vserver
cluster1 -user backup_admin1
```

```
Vserver: cluster1
User: backup_admin1
Password: qG5CqQHYxw7tE57g
```

= Configure LIFs

:icons: font

:relative\_path: ./ndmp/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You must identify the LIFs that will be used for establishing a data connection between the data and tape resources, and for control connection between the admin SVM and the backup application. After identifying the LIFs, you must verify that firewall and failover policies are set for the LIFs, and specify the preferred interface role.

Beginning with ONTAP 9.10.1, firewall policies are deprecated and wholly replaced with LIF service policies. For more information, see [LIFs and service policies in ONTAP 9.6 and later](#).

### Steps

1. Identify the intercluster, cluster-management, and node-management LIFs by using the `network interface show` command with the `-role` parameter.

The following command displays the intercluster LIFs:

```
cluster1::> network interface show -role intercluster
```

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
	-----	-----	-----	
	-----	-----	-----	
cluster1	IC1	up/up	192.0.2.65/24	
cluster1-1	e0a true			
cluster1	IC2	up/up	192.0.2.68/24	
cluster1-2	e0b true			

The following command displays the cluster-management LIF:

```
cluster1::> network interface show -role cluster-mgmt
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
cluster1	cluster_mgmt	up/up	192.0.2.60/24	
cluster1-2	e0M true			

The following command displays the node-management LIFs:

```
cluster1::> network interface show -role node-mgmt
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
cluster1	cluster1-1_mgmt1	up/up	192.0.2.69/24	
cluster1-1	e0M true			
	cluster1-2_mgmt1	up/up	192.0.2.70/24	
cluster1-2	e0M true			

2. Ensure that the firewall policy is enabled for NDMP on the intercluster, cluster-management (cluster-mgmt), and node-management (node-mgmt) LIFs:

- a. Verify that the firewall policy is enabled for NDMP by using the `system services firewall policy show` command.

The following command displays the firewall policy for the cluster-management LIF:

```
cluster1::> system services firewall policy show -policy cluster
```

Vserver	Policy	Service	Allowed
cluster	cluster	dns	0.0.0.0/0
		http	0.0.0.0/0
		https	0.0.0.0/0
		** ndmp	0.0.0.0/0**
		ndmps	0.0.0.0/0
		ntp	0.0.0.0/0
		rsh	0.0.0.0/0
		snmp	0.0.0.0/0
		ssh	0.0.0.0/0
		telnet	0.0.0.0/0

10 entries were displayed.

The following command displays the firewall policy for the intercluster LIF:

```
cluster1::> system services firewall policy show -policy intercluster
```

Vserver	Policy	Service	Allowed
cluster1	intercluster	dns	-
		http	-
		https	-
		**ndmp	0.0.0.0/0, ::/0**
		ndmps	-
		ntp	-
		rsh	-
		ssh	-
		telnet	-

9 entries were displayed.

The following command displays the firewall policy for the node-management LIF:

```
cluster1::> system services firewall policy show -policy mgmt
```

Vserver	Policy	Service	Allowed
cluster1-1	mgmt	dns	0.0.0.0/0, ::/0
		http	0.0.0.0/0, ::/0
		https	0.0.0.0/0, ::/0
		**ndmp	0.0.0.0/0, ::/0**
		ndmps	0.0.0.0/0, ::/0
		ntp	0.0.0.0/0, ::/0
		rsh	-
		snmp	0.0.0.0/0, ::/0
		ssh	0.0.0.0/0, ::/0
		telnet	-

10 entries were displayed.

- b. If the firewall policy is not enabled, enable the firewall policy by using the `system services firewall policy modify` command with the `-service` parameter.

The following command enables firewall policy for the intercluster LIF:

```
cluster1::> system services firewall policy modify -vserver  
cluster1 -policy intercluster -service ndmp 0.0.0.0/0
```

3. Ensure that the failover policy is set appropriately for all the LIFs:

- a. Verify that the failover policy for the cluster-management LIF is set to `broadcast-domain-wide`, and the policy for the intercluster and node-management LIFs is set to `local-only` by using the `network interface show -failover` command.

The following command displays the failover policy for the cluster-management, intercluster, and node-management LIFs:

```

cluster1::> network interface show -failover

          Logical                Home                Failover
Failover
Vserver  Interface                Node:Port        Policy
Group
-----
-----
cluster  cluster1_clus1          cluster1-1:e0a  local-only
cluster
                                                Failover
Targets:
                                                .....

**cluster1  cluster_mgmt          cluster1-1:e0m  broadcast-
domain-wide Default**
                                                Failover
Targets:
                                                .....

          **IC1                cluster1-1:e0a  local-only
Default**
                                                Failover
Targets:
          **IC2                cluster1-1:e0b  local-only
Default**
                                                Failover
Targets:

**cluster1-1 cluster1-1_mgmt1    cluster1-1:e0m  local-only
Default**
                                                Failover
Targets:

**cluster1-2 cluster1-2_mgmt1    cluster1-2:e0m  local-only
Default**
                                                Failover
Targets:
                                                .....

```

- b. If the failover policies are not set appropriately, modify the failover policy by using the `network interface modify` command with the `-failover-policy` parameter.

```

cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only

```



4. Specify the LIFs that are required for data connection by using the `vserver services ndmp modify` command with the `preferred-interface-role` parameter.

```
cluster1::> vserver services ndmp modify -vserver cluster1
-preferred-interface-role intercluster,cluster-mgmt,node-mgmt
```

5. Verify that the preferred interface role is set for the cluster by using the `vserver services ndmp show` command.

```
cluster1::> vserver services ndmp show -vserver cluster1

                Vserver: cluster1
                NDMP Version: 4
                .....
                .....
                Preferred Interface Role: intercluster, cluster-mgmt,
node-mgmt
```

= Configure node-scoped NDMP

= Enable node-scoped NDMP on the cluster

:icons: font

:relative\_path: ./ndmp/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can back up volumes hosted on a node by enabling node-scoped NDMP, setting up the password for the root user, and configuring a LIF for data and control connection.

You can configure node-scoped NDMP by enabling node-scoped NDMP on the cluster and NDMP service on all nodes of the cluster. You must also configure the `root` user for NDMP when enabling the NDMP service.

### Steps

1. Enable node-scoped NDMP mode by using the `system services ndmp` command with the `node-scope-mode` parameter.

```
cluster1::> system services ndmp node-scope-mode on
NDMP node-scope-mode is enabled.
```

2. Enable NDMP service on all nodes in the cluster by using the `system services ndmp on` command.

Using the wildcard `“*”` enables NDMP service on all nodes at the same time.

You must specify a password for authentication of the NDMP connection by the backup application.

```
cluster1::> system services ndmp on -node *
```

```
Please enter password:
```

```
Confirm password:
```

```
2 entries were modified.
```

3. Disable the `-clear-text` option for secure communication of the NDMP password by using the `system services ndmp modify` command.

Using the wildcard "\*" disables the `-clear-text` option on all nodes at the same time.

```
cluster1::> system services ndmp modify -node * -clear-text false
2 entries were modified.
```

4. Verify that NDMP service is enabled and the `-clear-text` option is disabled by using the `system services ndmp show` command.

```
cluster1::> system services ndmp show
Node                Enabled  Clear text  User Id
-----
cluster1-1         true    false      root
cluster1-2         true    false      root
2 entries were displayed.
```

= Configure a LIF

:icons: font

:relative\_path: ./ndmp/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You must identify a LIF that will be used for establishing a data connection and control connection between the node and the backup application. After identifying the LIF, you must verify that firewall and failover policies are set for the LIF.

#### Steps

1. Identify the intercluster LIF hosted on the nodes by using the `network interface show` command with the `-role` parameter.

```
cluster1::> network interface show -role intercluster
```

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
cluster1	IC1	up/up	192.0.2.65/24	cluster1-1
e0a	true			
cluster1	IC2	up/up	192.0.2.68/24	cluster1-2
e0b	true			

2. Ensure that the firewall policy is enabled for NDMP on the intercluster LIFs:

- Verify that the firewall policy is enabled for NDMP by using the `system services firewall policy show` command.

The following command displays the firewall policy for the intercluster LIF:

```
cluster1::> system services firewall policy show -policy
intercluster
```

Vserver	Policy	Service	Allowed
cluster1	intercluster	dns	-
		http	-
		https	-
		**ndmp	0.0.0.0/0, ::/0**
		ndmps	-
		ntp	-
		rsh	-
		ssh	-
		telnet	-

9 entries were displayed.

- If the firewall policy is not enabled, enable the firewall policy by using the `system services firewall policy modify` command with the `-service` parameter.

The following command enables firewall policy for the intercluster LIF:

```
cluster1::> system services firewall policy modify -vserver
cluster1 -policy intercluster -service ndmp 0.0.0.0/0
```

3. Ensure that the failover policy is set appropriately for the intercluster LIFs:

- a. Verify that the failover policy for the intercluster LIFs is set to `local-only` by using the `network interface show -failover` command.

```
cluster1::> network interface show -failover
          Logical          Home          Failover
Failover
Vserver   Interface          Node:Port          Policy          Group
-----
-----
cluster1  **IC1              cluster1-1:e0a    local-only
Default**
                                     Failover
Targets:
                                     .....
          **IC2              cluster1-2:e0b    local-only
Default**
                                     Failover
Targets:
                                     .....
cluster1-1 cluster1-1_mgmt1 cluster1-1:e0m    local-only
Default
                                     Failover
Targets:
                                     .....

```

- b. If the failover policy is not set appropriately, modify the failover policy by using the `network interface modify` command with the `-failover-policy` parameter.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

= Configure the backup application

:icons: font

:relative\_path: ./ndmp/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

After the cluster is configured for NDMP access, you must gather information from the cluster configuration and then configure the rest of the backup process in the backup application.

**Steps**

1. Gather the following information that you configured earlier in ONTAP:
  - The user name and password that the backup application requires to create the NDMP connection

- The IP addresses of the intercluster LIFs that the backup application requires to connect to the cluster
2. In ONTAP, display the aliases that ONTAP assigned to each device by using the `storage tape alias show` command.

The aliases are often useful in configuring the backup application.

```
cluster1::> storage tape show -alias

Device ID: 2a.0
Device Type: tape drive
Description: Hewlett-Packard LTO-5

Node                Alias      Mapping
-----
stsw-3220-4a-4b-02  st2       SN[HU19497WVR]
...
```

3. In the backup application, configure the rest of the backup process by using the backup application's documentation.

**After you finish**

If a data mobility event occurs, such as a volume move or LIF migration, you must be prepared to reinitialize any interrupted backup operations.

= Replication between NetApp Element software and ONTAP

= Replication between NetApp Element software and ONTAP overview

:icons: font

:relative\_path: ./element-replication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can ensure business continuity on an Element system by using SnapMirror to replicate Snapshot copies of an Element volume to an ONTAP destination. In the event of a disaster at the Element site, you can serve data to clients from the ONTAP system, and then reactivate the Element system when service is restored.

Beginning with ONTAP 9.4, you can replicate Snapshot copies of a LUN created on an ONTAP node back to an Element system. You might have created a LUN during an outage at the Element site, or you might be using a LUN to migrate data from ONTAP to Element software.

You should work with Element to ONTAP backup if the following apply:

- You want to use best practices, not explore every available option.
- You want to use the ONTAP command-line interface (CLI), not System Manager or an automated scripting tool.
- You are using iSCSI to serve data to clients.

If you require additional configuration or conceptual information, see the following documentation:

- Element configuration

[NetApp Element software documentation](#)

- SnapMirror concepts and configuration

[Data protection overview](#)

== About replication between Element and ONTAP

Beginning with ONTAP 9.3, you can use SnapMirror to replicate Snapshot copies of an Element volume to an ONTAP destination. In the event of a disaster at the Element site, you can serve data to clients from the ONTAP system, then reactivate the Element source volume when service is restored.

Beginning with ONTAP 9.4, you can replicate Snapshot copies of a LUN created on an ONTAP node back to an Element system. You might have created a LUN during an outage at the Element site, or you might be using a LUN to migrate data from ONTAP to Element software.

=== Types of data protection relationship

SnapMirror offers two types of data protection relationship. For each type, SnapMirror creates a Snapshot copy of the Element source volume before initializing or updating the relationship:

- In a *disaster recovery (DR)* data protection relationship, the destination volume contains only the Snapshot copy created by SnapMirror, from which you can continue to serve data in the event of a catastrophe at the primary site.
- In a *long-term retention* data protection relationship, the destination volume contains point-in-time Snapshot copies created by Element software, as well as the Snapshot copy created by SnapMirror. You might want to retain monthly Snapshot copies created over a 20-year span, for example.

=== Default policies

The first time you invoke SnapMirror, it performs a *baseline transfer* from the source volume to the destination volume. The *SnapMirror policy* defines the contents of the baseline and any updates.

You can use a default or custom policy when you create a data protection relationship. The *policy type* determines which Snapshot copies to include and how many copies to retain.

The table below shows the default policies. Use the `MirrorLatest` policy to create a traditional DR relationship. Use the `MirrorAndVault` or `Unified7year` policy to create a unified replication relationship, in which DR and long-term retention are configured on the same destination volume.

Policy	Policy Type	Update behavior
MirrorLatest	async-mirror	Transfer the Snapshot copy created by SnapMirror.
MirrorAndVault	mirror-vault	Transfer the Snapshot copy created by SnapMirror and any less recent Snapshot copies made since the last update, provided they have SnapMirror labels “daily” or “weekly”.

Unified7year	mirror-vault	Transfer the Snapshot copy created by SnapMirror and any less recent Snapshot copies made since the last update, provided they have SnapMirror labels “daily”, “weekly”, or “monthly”.
--------------	--------------	--

For complete background information on SnapMirror policies, including guidance on which policy to use, see [Data Protection](#).

### === Understanding SnapMirror labels

Every policy with the “mirror-vault” policy type must have a rule that specifies which Snapshot copies to replicate. The rule “daily”, for example, indicates that only Snapshot copies assigned the SnapMirror label “daily” should be replicated. You assign the SnapMirror label when you configure Element Snapshot copies.

### === Replication from an Element source cluster to an ONTAP destination cluster

You can use SnapMirror to replicate Snapshot copies of an Element volume to an ONTAP destination system. In the event of a disaster at the Element site, you can serve data to clients from the ONTAP system, then reactivate the Element source volume when service is restored.

An Element volume is roughly equivalent to an ONTAP LUN. SnapMirror creates a LUN with the name of the Element volume when a data protection relationship between Element software and ONTAP is initialized. SnapMirror replicates data to an existing LUN if the LUN meets the requirements for Element to ONTAP replication.

Replication rules are as follows:

- An ONTAP volume can contain data from one Element volume only.
- You cannot replicate data from an ONTAP volume to multiple Element volumes.

### === Replication from an ONTAP source cluster to an Element destination cluster

Beginning with ONTAP 9.4, you can replicate Snapshot copies of a LUN created on an ONTAP system back to an Element volume:

- If a SnapMirror relationship already exists between an Element source and an ONTAP destination, a LUN created while you are serving data from the destination is automatically replicated when the source is reactivated.
- Otherwise, you must create and initialize a SnapMirror relationship between the ONTAP source cluster and the Element destination cluster.

Replication rules are as follows:

- The replication relationship must have a policy of type “async-mirror”.

Policies of type “mirror-vault” are not supported.

- Only iSCSI LUNs are supported.
- You cannot replicate more than one LUN from an ONTAP volume to an Element volume.
- You cannot replicate a LUN from an ONTAP volume to multiple Element volumes.

### === Prerequisites

You must have completed the following tasks before configuring a data protection relationship between Element and ONTAP:

- The Element cluster must be running NetApp Element software version 10.1 or later.
- The ONTAP cluster must be running ONTAP 9.3 or later.



- SnapMirror must have been licensed on the ONTAP cluster.
- You must have configured volumes on the Element and ONTAP clusters that are large enough to handle anticipated data transfers.
- If you are using the “mirror-vault” policy type, a SnapMirror label must have been configured for the Element Snapshot copies to be replicated.

You can perform this task in the Element software web UI only. For more information, see the [NetApp Element software documentation](#)

- You must have ensured that port 5010 is available.
- If you foresee that you might need to move a destination volume, you must have ensured that full-mesh connectivity exists between the source and destination. Every node on the Element source cluster must be able to communicate with every node on the ONTAP destination cluster.

### === Support details

The following table shows support details for Element to ONTAP backup.

Resource or feature	Support details
SnapMirror	<ul style="list-style-type: none"> <li>• The SnapMirror restore feature is not supported.</li> <li>• The <code>MirrorAllSnapshots</code> and <code>XDPDefault</code> policies are not supported.</li> <li>• The “vault” policy type is not supported.</li> <li>• The system-defined rule “all_source_snapshots” is not supported.</li> <li>• The “mirror-vault” policy type is supported only for replication from Element software to ONTAP. Use “async-mirror” for replication from ONTAP to Element software.</li> <li>• The <code>-schedule</code> and <code>-prefix</code> options for <code>snapmirror policy add-rule</code> are not supported.</li> <li>• The <code>-preserve</code> and <code>-quick-resync</code> options for <code>snapmirror resync</code> are not supported.</li> <li>• Storage efficiency is not preserved.</li> <li>• Fan-out and cascade data protection deployments are not supported.</li> </ul>
ONTAP	<ul style="list-style-type: none"> <li>• ONTAP Select is supported beginning with ONTAP 9.4 and Element 10.3.</li> <li>• Cloud Volumes ONTAP is supported beginning with ONTAP 9.5 and Element 11.0.</li> </ul>
Element	<ul style="list-style-type: none"> <li>• Volume size limit is 8 TiB.</li> <li>• Volume block size must be 512 bytes. A 4K byte block size is not supported.</li> <li>• Volume size must be a multiple of 1 MiB.</li> <li>• Volume attributes are not preserved.</li> <li>• Maximum number of Snapshot copies to be replicated is 30.</li> </ul>
Network	<ul style="list-style-type: none"> <li>• A single TCP connection is allowed per transfer.</li> <li>• The Element node must be specified as an IP address. DNS hostname lookup is not supported.</li> <li>• IPspaces are not supported.</li> </ul>
SnapLock	SnapLock volumes are not supported.

FlexGroup	FlexGroup volumes are not supported.
SVM DR	ONTAP volumes in an SVM DR configuration are not supported.
MetroCluster	ONTAP volumes in a MetroCluster configuration are not supported.

= Workflow for replication between Element and ONTAP

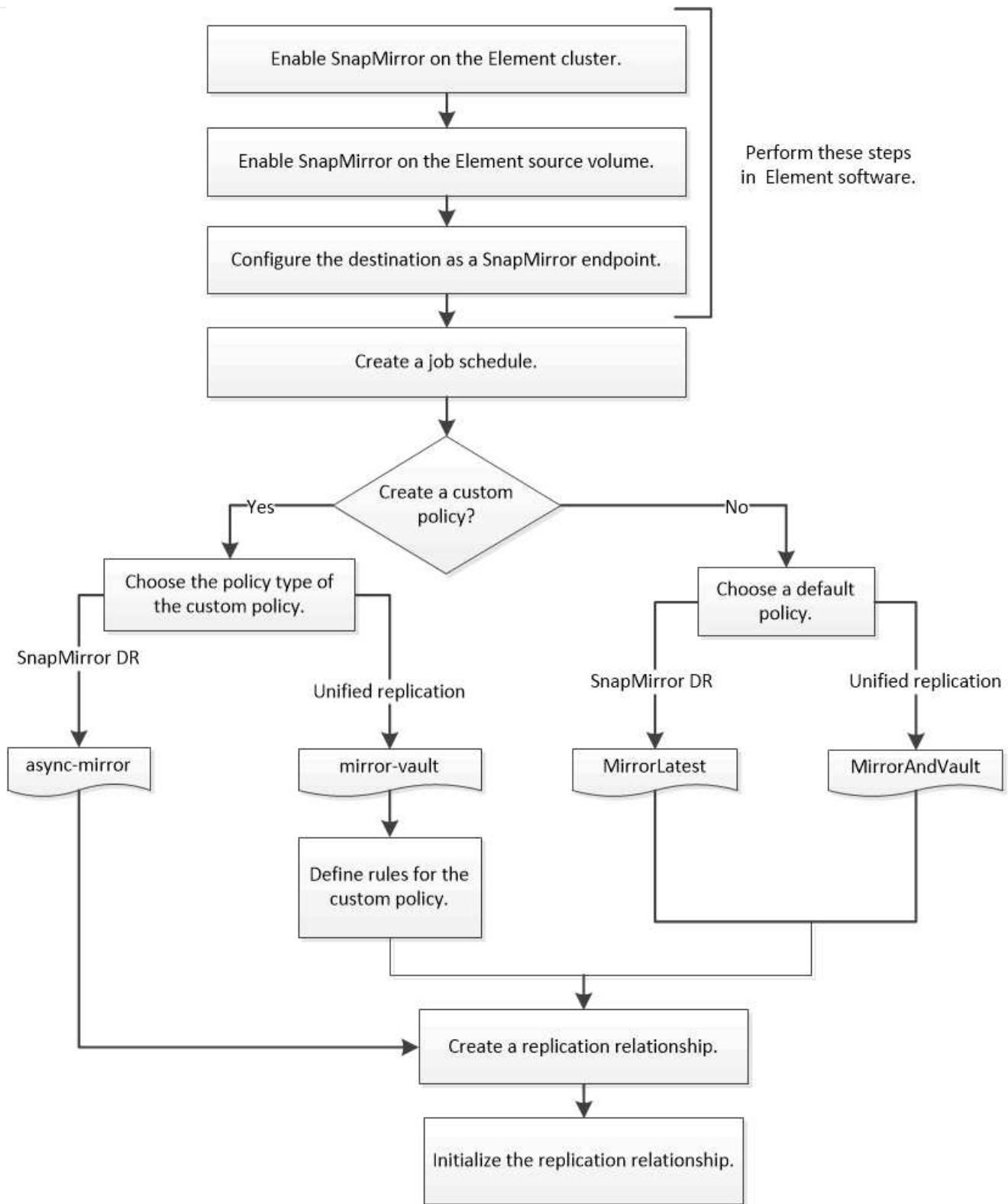
:icons: font

:relative\_path: ./element-replication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Whether you are replicating data from Element to ONTAP or from ONTAP to Element, you need to configure a job schedule, specify a policy, and create and initialize the relationship. You can use a default or custom policy.

The workflow assumes that you have completed the prerequisite tasks listed in [Prerequisites](#). For complete background information on SnapMirror policies, including guidance on which policy to use, see [Data protection](#).



= Enable SnapMirror in Element software

= Enable SnapMirror on the Element cluster

:icons: font

:relative\_path: ./element-replication/

:imagesdir: /tmp/d20221026-17026-1injpo/source/./encryption-at-rest/./media/

You must enable SnapMirror on the Element cluster before you can create a

replication relationship. You can perform this task in the Element software web UI only.

**Before you begin**

- The Element cluster must be running NetApp Element software version 10.1 or later.
- SnapMirror can only be enabled for Element clusters used with NetApp ONTAP volumes.

**About this task**

The Element system comes with SnapMirror disabled by default. SnapMirror is not automatically enabled as part of a new installation or upgrade.

Once enabled, SnapMirror cannot be disabled. You can only disable the SnapMirror feature and restore the default settings by returning the cluster to the factory image.

## Steps

1. Click **Clusters > Settings**.
2. Find the cluster-specific settings for SnapMirror.
3. Click **Enable SnapMirror**.

= Enable SnapMirror on the Element source volume

:icons: font

:relative\_path: ./element-replication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You must enable SnapMirror on the Element source volume before you can create a replication relationship. You can perform this task in the Element software web UI only.


## Before you begin

- You must have enabled SnapMirror on the Element cluster.
- The volume block size must be 512 bytes.
- The volume must not be participating in Element remote replication.
- The volume access type must not be “Replication Target”.

## About this task

The procedure below assumes the volume already exists. You can also enable SnapMirror when you create or clone a volume.

## Steps

1. Click **Management > Volumes**.
2. Click the  button for the volume.
3. In the drop-down menu, select **Edit**.
4. In the **Edit Volume** dialog, select **Enable SnapMirror**.
5. Click **Save Changes**.

= Create a SnapMirror endpoint

:icons: font

:relative\_path: ./element-replication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You must create a SnapMirror endpoint before you can create a replication relationship. You can perform this task in the Element software web UI only.

## Before you begin

You must have enabled SnapMirror on the Element cluster.

## Steps

1. Click **Data Protection > SnapMirror Endpoints**.
2. Click **Create Endpoint**.
3. In the **Create a New Endpoint** dialog, enter the ONTAP cluster management IP address.

4. Enter the user ID and password of the ONTAP cluster administrator.

5. Click **Create Endpoint**.

= Configure a replication relationship

= Create a replication job schedule

:icons: font

:relative\_path: ./element-replication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Whether you are replicating data from Element to ONTAP or from ONTAP to Element, you need to configure a job schedule, specify a policy, and create and initialize the relationship. You can use a default or custom policy.

You can use the `job schedule cron create` command to create a replication job schedule. The job schedule determines when SnapMirror automatically updates the data protection relationship to which the schedule is assigned.

### About this task

You assign a job schedule when you create a data protection relationship. If you do not assign a job schedule, you must update the relationship manually.

### Step

1. Create a job schedule:

```
job schedule cron create -name job_name -month month -dayofweek day_of_week
-day day_of_month -hour hour -minute minute
```

For `-month`, `-dayofweek`, and `-hour`, you can specify `all` to run the job every month, day of the week, and hour, respectively.

Beginning with ONTAP 9.10.1, you can include the Vserver for your job schedule:

```
job schedule cron create -name job_name -vserver Vserver_name -month month
-dayofweek day_of_week -day day_of_month -hour hour -minute minute
```

The following example creates a job schedule named `my_weekly` that runs on Saturdays at 3:00 a.m.:

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

= Customize a replication policy

= Create a custom replication policy

:icons: font

:relative\_path: ./element-replication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use a default or custom policy when you create a replication relationship. For

a custom unified replication policy, you must define one or more *rules* that determine which Snapshot copies are transferred during initialization and update.

You can create a custom replication policy if the default policy for a relationship is not suitable. You might want to compress data in a network transfer, for example, or modify the number of attempts SnapMirror makes to transfer Snapshot copies.

### About this task

The *policy type* of the replication policy determines the type of relationship it supports. The table below shows the available policy types.

Policy type	Relationship type
async-mirror	SnapMirror DR
mirror-vault	Unified replication

### Step

1. Create a custom replication policy:

```
snapmirror policy create -vserver SVM -policy policy -type async-  
mirror|mirror-vault -comment comment -tries transfer_tries -transfer  
-priority low|normal -is-network-compression-enabled true|false
```

For complete command syntax, see the man page.

Beginning with ONTAP 9.5, you can specify the schedule for creating a common Snapshot copy schedule for SnapMirror Synchronous relationships by using the `-common-snapshot-schedule` parameter. By default, the common Snapshot copy schedule for SnapMirror Synchronous relationships is one hour. You can specify a value from 30 minutes to two hours for the Snapshot copy schedule for SnapMirror Synchronous relationships.

The following example creates a custom replication policy for SnapMirror DR that enables network compression for data transfers:

```
cluster_dst::> snapmirror policy create -vserver svml -policy  
DR_compressed -type async-mirror -comment "DR with network  
compression enabled" -is-network-compression-enabled true
```

The following example creates a custom replication policy for unified replication:

```
cluster_dst::> snapmirror policy create -vserver svml -policy  
my_unified -type mirror-vault
```

### After you finish

For "mirror-vault" policy types, you must define rules that determine which Snapshot copies are transferred during initialization and update.



Use the `snapmirror policy show` command to verify that the SnapMirror policy was created. For complete command syntax, see the man page.

= Define a rule for a policy

:icons: font

:relative\_path: ./element-replication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

For custom policies with the “mirror-vault” policy type, you must define at least one rule that determines which Snapshot copies are transferred during initialization and update. You can also define rules for default policies with the “mirror-vault” policy type.

### About this task

Every policy with the “mirror-vault” policy type must have a rule that specifies which Snapshot copies to replicate. The rule “bi-monthly”, for example, indicates that only Snapshot copies assigned the SnapMirror label “bi-monthly” should be replicated. You assign the SnapMirror label when you configure Element Snapshot copies.

Each policy type is associated with one or more system-defined rules. These rules are automatically assigned to a policy when you specify its policy type. The table below shows the system-defined rules.

System-defined rule	Used in policy types	Result
sm_created	async-mirror, mirror-vault	A Snapshot copy created by SnapMirror is transferred on initialization and update.
daily	mirror-vault	New Snapshot copies on the source with the SnapMirror label “daily” are transferred on initialization and update.
weekly	mirror-vault	New Snapshot copies on the source with the SnapMirror label “weekly” are transferred on initialization and update.
monthly	mirror-vault	New Snapshot copies on the source with the SnapMirror label “monthly” are transferred on initialization and update.

You can specify additional rules as needed, for default or custom policies. For example:

- For the default `MirrorAndVault` policy, you might create a rule called “bi-monthly” to match Snapshot copies on the source with the “bi-monthly” SnapMirror label.
- For a custom policy with the “mirror-vault” policy type, you might create a rule called “bi-weekly” to match Snapshot copies on the source with the “bi-weekly” SnapMirror label.

### Step

## 1. Define a rule for a policy:

```
snapmirror policy add-rule -vserver SVM -policy policy_for_rule -snapmirror  
-label snapmirror-label -keep retention_count
```

For complete command syntax, see the man page.

The following example adds a rule with the SnapMirror label `bi-monthly` to the default `MirrorAndVault` policy:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy  
MirrorAndVault -snapmirror-label bi-monthly -keep 6
```

The following example adds a rule with the SnapMirror label `bi-weekly` to the custom `my_snapvault` policy:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy  
my_snapvault -snapmirror-label bi-weekly -keep 26
```

The following example adds a rule with the SnapMirror label `app_consistent` to the custom `Sync` policy:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy Sync  
-snapmirror-label app_consistent -keep 1
```

You can then replicate Snapshot copies from the source cluster that match this SnapMirror label:

```
cluster_src::> snapshot create -vserver vs1 -volume vol1 -snapshot  
snapshot1 -snapmirror-label app_consistent
```

= Create a replication relationship

= Create a relationship from an Element source to an ONTAP destination

```
:icons: font
```

```
:relative_path: ./element-replication/
```

```
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/
```

The relationship between the source volume in primary storage and the destination volume in secondary storage is called a *data protection relationship*. You can use the `snapmirror create` command to create a data protection relationship from an Element source to an ONTAP destination, or from an ONTAP source to an Element destination.

You can use SnapMirror to replicate Snapshot copies of an Element volume to an ONTAP destination system. In the event of a disaster at the Element site, you can serve data to clients from the ONTAP

system, then reactivate the Element source volume when service is restored.

**Before you begin**

- The Element node containing the volume to be replicated must have been made accessible to ONTAP.
- The Element volume must have been enabled for SnapMirror replication.
- If you are using the “mirror-vault” policy type, a SnapMirror label must have been configured for the Element Snapshot copies to be replicated.

You can perform this task in the Element software web UI only. For more information, see the [Element documentation](#).

## About this task

You must specify the Element source path in the form `hostip:/lun/name`, where “lun” is the actual string “lun” and `name` is the name of the Element volume.

An Element volume is roughly equivalent to an ONTAP LUN. SnapMirror creates a LUN with the name of the Element volume when a data protection relationship between Element software and ONTAP is initialized. SnapMirror replicates data to an existing LUN if the LUN meets the requirements for replicating from Element software to ONTAP.

Replication rules are as follows:

- An ONTAP volume can contain data from one Element volume only.
- You cannot replicate data from an ONTAP volume to multiple Element volumes.

In ONTAP 9.3 and earlier, a destination volume can contain up to 251 Snapshot copies. In ONTAP 9.4 and later, a destination volume can contain up to 1019 Snapshot copies.

## Step

1. From the destination cluster, create a replication relationship from an Element source to an ONTAP destination:

```
snapmirror create -source-path hostip:/lun/name -destination-path  
SVM:volume|cluster://SVM/volume -type XDP -schedule schedule -policy policy
```

For complete command syntax, see the man page.

The following example creates a SnapMirror DR relationship using the default `MirrorLatest` policy:

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily  
-policy MirrorLatest
```

The following example creates a unified replication relationship using the default `MirrorAndVault` policy:

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily  
-policy MirrorAndVault
```

The following example creates a unified replication relationship using the `Unified7year` policy:

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily  
-policy Unified7year
```

The following example creates a unified replication relationship using the custom `my_unified` policy:

```
cluster_dst::> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy my_unified
```

### After you finish

Use the `snapmirror show` command to verify that the SnapMirror relationship was created. For complete command syntax, see the man page.

= Create a relationship from an ONTAP source to an Element destination

:icons: font

:relative\_path: ./element-replication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.4, you can use SnapMirror to replicate Snapshot copies of a LUN created on an ONTAP source back to an Element destination. You might be using the LUN to migrate data from ONTAP to Element software.

### Before you begin

- The Element destination node must have been made accessible to ONTAP.
- The Element volume must have been enabled for SnapMirror replication.

### About this task

You must specify the Element destination path in the form `hostip:/lun/name`, where “lun” is the actual string “lun” and `name` is the name of the Element volume.

Replication rules are as follows:

- The replication relationship must have a policy of type “async-mirror”.

You can use a default or custom policy.

- Only iSCSI LUNs are supported.
- You cannot replicate more than one LUN from an ONTAP volume to an Element volume.
- You cannot replicate a LUN from an ONTAP volume to multiple Element volumes.

### Step

1. Create a replication relationship from an ONTAP source to an Element destination:

```
snapmirror create -source-path SVM:volume|cluster://SVM/volume -destination
-path hostip:/lun/name -type XDP -schedule schedule -policy policy
```

For complete command syntax, see the man page.

The following example creates a SnapMirror DR relationship using the default `MirrorLatest` policy:

```
cluster_dst::> snapmirror create -source-path svm_1:volA_dst
-destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
-policy MirrorLatest
```

The following example creates a SnapMirror DR relationship using the custom `my_mirror` policy:

```
cluster_dst::> snapmirror create -source-path svm_1:volA_dst
-destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
-policy my_mirror
```

### After you finish

Use the `snapmirror show` command to verify that the SnapMirror relationship was created. For complete command syntax, see the man page.

= Initialize a replication relationship

:icons: font

:relative\_path: ./element-replication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

For all relationship types, initialization performs a *baseline transfer*: it makes a Snapshot copy of the source volume, then transfers that copy and all the data blocks it references to the destination volume.

### Before you begin

- The Element node containing the volume to be replicated must have been made accessible to ONTAP.
- The Element volume must have been enabled for SnapMirror replication.
- If you are using the “mirror-vault” policy type, a SnapMirror label must have been configured for the Element Snapshot copies to be replicated.

### About this task

You must specify the Element source path in the form `hostip:/lun/name`, where “lun” is the actual string “lun” and `name` is the name of the Element volume.

Initialization can be time-consuming. You might want to run the baseline transfer in off-peak hours.

If initialization of a relationship from an ONTAP source to an Element destination fails for any reason, it will continue to fail even after you have corrected the problem (an invalid LUN name, for example). The workaround is as follows:

1. Delete the relationship.
2. Delete the Element destination volume.
3. Create a new Element destination volume.
4. Create and initialize a new relationship from the ONTAP source to the Element destination volume.

## Step

1. Initialize a replication relationship:

```
snapmirror initialize -source-path hostip:/lun/name -destination-path  
SVM:volume|cluster://SVM/volume
```

For complete command syntax, see the man page.

The following example initializes the relationship between the source volume 0005 at IP address 10.0.0.11 and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst:> snapmirror initialize -source-path  
10.0.0.11:/lun/0005 -destination-path svm_backup:volA_dst
```

= Serve data from a SnapMirror DR destination volume

= Make the destination volume writeable

:icons: font

:relative\_path: ./element-replication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

When disaster disables the primary site for a SnapMirror DR relationship, you can serve data from the destination volume with minimal disruption. You can reactivate the source volume when service is restored at the primary site.

You need to make the destination volume writeable before you can serve data from the volume to clients. You can use the `snapmirror quiesce` command to stop scheduled transfers to the destination, the `snapmirror abort` command to stop ongoing transfers, and the `snapmirror break` command to make the destination writeable.

### About this task

You must specify the Element source path in the form `hostip:/lun/name`, where “lun” is the actual string “lun” and `name` is the name of the Element volume.

### Steps

1. Stop scheduled transfers to the destination:

```
snapmirror quiesce -source-path hostip:/lun/name -destination-path  
SVM:volume|cluster://SVM/volume
```

For complete command syntax, see the man page.

The following example stops scheduled transfers between the source volume 0005 at IP address 10.0.0.11 and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst:> snapmirror quiesce -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst
```

## 2. Stop ongoing transfers to the destination:

```
snapmirror abort -source-path hostip:/lun/name -destination-path  
SVM:volume|cluster://SVM/volume
```

For complete command syntax, see the man page.

The following example stops ongoing transfers between the source volume 0005 at IP address 10.0.0.11 and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror abort -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst
```

## 3. Break the SnapMirror DR relationship:

```
snapmirror break -source-path hostip:/lun/name -destination-path  
SVM:volume|cluster://SVM/volume
```

For complete command syntax, see the man page.

The following example breaks the relationship between the source volume 0005 at IP address 10.0.0.11 and the destination volume `volA_dst` on `svm_backup` and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror break -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst
```

= Configure the destination volume for data access

:icons: font

:relative\_path: ./element-replication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

After making the destination volume writeable, you must configure the volume for data access. SAN hosts can access the data from the destination volume until the source volume is reactivated.

1. Map the Element LUN to the appropriate initiator group.
2. Create iSCSI sessions from the SAN host initiators to the SAN LIFs.
3. On the SAN client, perform a storage re-scan to detect the connected LUN.

= Reactivate the original source volume

:icons: font

:relative\_path: ./element-replication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can reestablish the original data protection relationship between the source and destination volumes when you no longer need to serve data from the destination.



## About this task

The procedure below assumes that the baseline in the original source volume is intact. If the baseline is not intact, you must create and initialize the relationship between the volume you are serving data from and the original source volume before performing the procedure.

You must specify the Element source path in the form `hostip:/lun/name`, where “lun” is the actual string “lun” and `name` is the name of the Element volume.

Beginning with ONTAP 9.4, Snapshot copies of a LUN created while you are serving data from the ONTAP destination are automatically replicated when the Element source is reactivated.

Replication rules are as follows:

- Only iSCSI LUNs are supported.
- You cannot replicate more than one LUN from an ONTAP volume to an Element volume.
- You cannot replicate a LUN from an ONTAP volume to multiple Element volumes.

## Steps

1. Delete the original data protection relationship:

```
snapmirror delete -source-path SVM:volume|cluster://SVM/volume -destination  
-path hostip:/lun/name -policy policy
```

For complete command syntax, see the man page.

The following example deletes the relationship between the original source volume, 0005 at IP address 10.0.0.11, and the volume you are serving data from, volA\_dst on svm\_backup:

```
cluster_dst::> snapmirror delete -source-path 10.0.0.11:/lun/0005  
-policy MirrorLatest -destination-path svm_backup:volA_dst
```

2. Reverse the original data protection relationship:

```
snapmirror resync -source-path SVM:volume|cluster://SVM/volume -destination  
-path hostip:/lun/name -policy policy
```

For complete command syntax, see the man page.

Although resync does not require a baseline transfer, it can be time-consuming. You might want to run the resync in off-peak hours.

The following example reverses the relationship between the original source volume, 0005 at IP address 10.0.0.11, and the volume you are serving data from, volA\_dst on svm\_backup:

```
cluster_dst::> snapmirror resync -source-path svm_backup:volA_dst  
-destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
```

3. Update the reversed relationship:

```
snapmirror update -source-path SVM:volume|cluster://SVM/volume -destination  
-path hostip:/lun/name
```

For complete command syntax, see the man page.

The command fails if a common Snapshot copy does not exist on the source and destination. Use `snapmirror initialize` to re-initialize the relationship.

+

The following example updates the relationship between the volume you are serving data from, volA\_dst on svm\_backup, and the original source volume, 0005 at IP address 10.0.0.11:

+

```
cluster_dst:> snapmirror update -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

### 1. Stop scheduled transfers for the reversed relationship:

```
snapmirror quiesce -source-path SVM:volume|cluster://SVM/volume
-destination-path hostip:/lun/name
```

For complete command syntax, see the man page.

The following example stops scheduled transfers between the volume you are serving data from, volA\_dst on svm\_backup, and the original source volume, 0005 at IP address 10.0.0.11:

```
cluster_dst:> snapmirror quiesce -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

### 2. Stop ongoing transfers for the reversed relationship:

```
snapmirror abort -source-path SVM:volume|cluster://SVM/volume -destination
-path hostip:/lun/name
```

For complete command syntax, see the man page.

The following example stops ongoing transfers between the volume you are serving data from, volA\_dst on svm\_backup, and the original source volume, 0005 at IP address 10.0.0.11:

```
cluster_dst:> snapmirror abort -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

### 3. Break the reversed relationship:

```
snapmirror break -source-path SVM:volume|cluster://SVM/volume -destination
-path hostip:/lun/name
```

For complete command syntax, see the man page.

The following example breaks the relationship between the volume you are serving data from, volA\_dst on svm\_backup, and the original source volume, 0005 at IP address 10.0.0.11:

```
cluster_dst::> snapmirror break -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

#### 4. Delete the reversed data protection relationship:

```
snapmirror delete -source-path SVM:volume|cluster://SVM/volume -destination
-path hostip:/lun/name -policy policy
```

For complete command syntax, see the man page.

The following example deletes the reversed relationship between the original source volume, 0005 at IP address 10.0.0.11, and the volume you are serving data from, volA\_dst on svm\_backup:

```
cluster_src::> snapmirror delete -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
```

#### 5. Reestablish the original data protection relationship:

```
snapmirror resync -source-path hostip:/lun/name -destination-path
SVM:volume|cluster://SVM/volume
```

For complete command syntax, see the man page.

The following example reestablishes the relationship between the original source volume, 0005 at IP address 10.0.0.11, and the original destination volume, volA\_dst on svm\_backup:

```
cluster_dst::> snapmirror resync -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst
```

### After you finish

Use the `snapmirror show` command to verify that the SnapMirror relationship was created. For complete command syntax, see the man page.

= Update a replication relationship manually

:icons: font

:relative\_path: ./element-replication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You might need to update a replication relationship manually if an update fails because of a network error.

### About this task

You must specify the Element source path in the form `hostip:/lun/name`, where “lun” is the actual string “lun” and `name` is the name of the Element volume.

### Steps

1. Update a replication relationship manually:

```
snapmirror update -source-path hostip:/lun/name -destination-path  
SVM:volume|cluster://SVM/volume
```

For complete command syntax, see the man page.

The command fails if a common Snapshot copy does not exist on the source and destination. Use `snapmirror initialize` to re-initialize the relationship.

+

The following example updates the relationship between the source volume 0005 at IP address 10.0.0.11 and the destination volume `volA_dst` on `svm_backup`:

+

```
cluster_src::> snapmirror update -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst
```

= Resynchronize a replication relationship

:icons: font

:relative\_path: ./element-replication/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You need to resynchronize a replication relationship after you make a destination volume writeable, after an update fails because a common Snapshot copy does not exist on the source and destination volumes, or if you want to change the replication policy for the relationship.

#### About this task

Although `resync` does not require a baseline transfer, it can be time-consuming. You might want to run the `resync` in off-peak hours.

You must specify the Element source path in the form `hostip:/lun/name`, where “lun” is the actual string “lun” and `name` is the name of the Element volume.

#### Step

1. Resync the source and destination volumes:

```
snapmirror resync -source-path hostip:/lun/name -destination-path
SVM:volume|cluster://SVM/volume -type XDP -schedule schedule -policy policy
```

For complete command syntax, see the man page.

The following example resyncs the relationship between the source volume 0005 at IP address 10.0.0.11 and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path 10.0.0.11:/lun/0005
-policy MirrorLatest -destination-path svm_backup:volA_dst
```

= Event and performance monitoring

:hardbreaks:

:linkattrs:

:relative\_path: ./event-performance-monitoring/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

= View cluster performance with System Manager

= Cluster performance overview with System Manager

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

The topics in this section show you how to manage cluster health and performance with System Manager in ONTAP 9.7 and later releases.

The System Manager Dashboard provides the following performance information:

- **Health:** You can monitor the health of a cluster. Alerts are shown when problems arise.
- **Capacity:** System Manager shows you the available capacity on the cluster.
- **Performance:** You can monitor how well the cluster is performing, based on latency, IOPS, and throughput. The metrics are graphed every 15 seconds by hour, day, week, month, or year.
- **Network:** You can view how the network is configured with hosts and storage objects. You can view the number of ports that are available and the interfaces and storage VMs that are associated with them.

= View performance on cluster dashboard

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Use the dashboard to make informed decisions about workloads you might want to add or move. You can also look at peak usage times to plan for potential changes.

The performance values refresh every 3 seconds and the performance graph refreshes every 15 seconds.

### Steps

1. Click **Dashboard**.
2. Under **Performance**, select the interval.

= Identify hot volumes and other objects

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Accelerate your cluster performance by identifying the frequently accessed volumes

(hot volumes) and data (hot objects).

### Steps

1. Click **Storage > Volumes**.
2. Filter the IOPS, latency, and throughput columns to view the frequently accessed volumes and data.

= Modify QoS

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font


:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process. You can also modify QoS after your storage has been provisioned.

### Steps

1. In System Manager, click **Storage** and select **Volumes**.
2. Next to the volume for which you want to modify QoS, click  and select **Edit**.

= Monitor cluster performance using System Manager

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can monitor cluster performance by viewing information about your system on the System Manager Dashboard.

The Dashboard displays information about important alerts and notifications, the efficiency and capacity of storage tiers and volumes, the nodes that are available in a cluster, the status of the nodes in an HA pair, the most active applications and objects, and the performance metrics of a cluster or a node.

The Dashboard lets you determine the following information:

- **Health:** How healthy is the cluster?
- **Capacity:** What capacity is available on the cluster?
- **Performance:** How well is the cluster performing, based on latency, IOPS, and throughput?
- **Network:** How is the network configured with hosts and storage objects, such as ports, interfaces, and storage VMs?

In the Health and Capacity overviews, you can click  to view additional information and perform tasks.

In the Performance overview, you can view metrics based on the hour, the day, the week, the month, or the year.



In the Network overview, the number of each object in the network is displayed (for example, "8 NVMe/FC ports"). You can click on the numbers to view details about each network object.

= Performance monitoring setup with the CLI

= Performance monitoring overview

:icons: font

:relative\_path: ./performance-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can quickly install and configure Active IQ Unified Manager (formerly OnCommand Unified Manager), perform basic monitoring tasks, and identify performance issues.

You should use these procedure to monitor cluster performance, if the following assumptions apply to your situation:

- You want to use best practices, not explore every available option.
- You want to install Unified Manager by using a virtual appliance, instead of a Linux or Windows-based installation.
- You're willing to use a static configuration rather than DHCP to install the software.
- You are a cluster administrator with the "admin" role.

#### Related information

If these assumptions are not correct for your situation, you should see the following resources:

- [Active IQ Unified Manager 9.8 Installation](#)
- [System administration](#)

= Performance monitoring

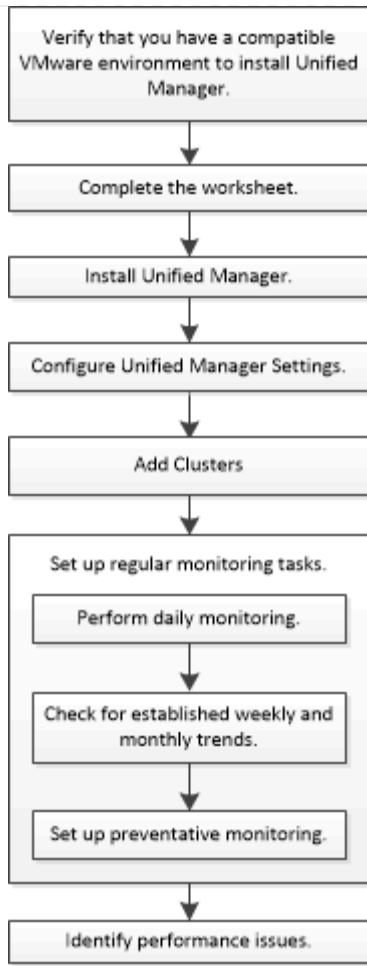
= Performance monitoring workflow

:icons: font

:relative\_path: ./performance-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Monitoring cluster performance involves installing Active IQ Unified Manager software, setting up basic monitoring tasks, and identifying performance issues.



= Verify that your VMware environment is supported

:icons: font

:relative\_path: ./performance-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

For successful installation of Active IQ Unified Manager, you must verify that your VMware environment meets the necessary requirements.

### Steps

1. Verify that your VMware infrastructure meets the sizing requirements for the installation of Unified Manager.
2. Go to the Interoperability Matrix to verify that you have a supported combination of the following components:
  - ONTAP version
  - ESXi operating system version
  - VMware vCenter Server version
  - VMware Tools version
  - Browser type and version

The [Interoperability Matrix](#) lists the supported configurations for Unified Manager.

+

. Click the configuration name for the selected configuration.

+

Details for that configuration are displayed in the Configuration Details window.

1. Review the information in the following tabs:

- Notes

Lists important alerts and information that are specific to your configuration.

- Policies and Guidelines

Provides general guidelines for all configurations.

= Active IQ Unified Manager worksheet

:icons: font

:relative\_path: ./performance-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Before you install, configure, and connect Active IQ Unified Manager, you should have specific information about your environment readily available. You can record the information in the worksheet.

== Unified Manager installation information

Virtual machine on which software is deployed	Your value
ESXi server IP address	
Host fully qualified domain name	
Host IP address	
Network mask	
Gateway IP address	
Primary DNS address	
Secondary DNS address	
Search domains	
Maintenance user name	
Maintenance user password	

== Unified Manager configuration information

Setting	Your value
Maintenance user email address	
NTP server	
SMTP server host name or IP address	
SMTP user name	
SMTP password	
SMTP default port	25 (Default value)
Email from which alert notifications are sent	
LDAP bind distinguished name	
LDAP bind password	

== Cluster information

Capture the following information for each cluster on Unified Manager.

Cluster 1 of N	Your value
Host name or cluster-management IP address	

The administrator must have been assigned the "admin" role.

a|

a|

ONTAP administrator password

a|

a|

Protocol (HTTP or HTTPS)

a|

.Related information

## Administrator authentication and RBAC

= Install Active IQ Unified Manager

:leveloffset: +1

= Download and deploy Active IQ Unified Manager

:icons: font

:relative\_path: ../performance-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

[.lead]

To install the software, you must download the virtual appliance (VA) installation file and then use a VMware vSphere Client to deploy the file to a VMware ESXi server. The VA is available in an OVA file.

.Steps

. Go to the **NetApp Support Site Software Download** page and locate Active IQ Unified Manager.

+

<https://mysupport.netapp.com/products/index.html>

. Select **VMware vSphere** in the **Select Platform** drop-down menu and click **Go!**

. Save the OVA file to a local or network location that is accessible to your VMware vSphere Client.

. In VMware vSphere Client, click **File > Deploy OVF Template**.

. Locate the OVA file and use the wizard to deploy the virtual appliance on the ESXi server.

+

You can use the **Properties** tab in the wizard to enter your static configuration information.

. Power on the VM.

. Click the **Console** tab to view the initial boot process.

. Follow the prompt to install VMware Tools on the VM.

. Configure the time zone.

. Enter a maintenance user name and password.

. Go to the URL displayed by the VM console.

= Configure initial Active IQ Unified Manager settings

:icons: font

:relative\_path: ../performance-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

[.lead]

The Active IQ Unified Manager Initial Setup dialog box appears when you first access the web UI, which enables you to configure some initial settings and to add clusters.

.Steps

To disable alerts from being sent for certain types of events, you must clear all of the check boxes in an event category. This action does not stop events from appearing in the user interface.

## Steps

1. In the left navigation pane, select **Storage Management > Alert Setup**.

The Alert Setup page is displayed.

2. Click **Add** and configure the appropriate settings for each of the event types.

To have email alerts sent to multiple users, enter a comma between each email address.

3. Click **Save**.

= Identify performance issues in Active IQ Unified Manager

:icons: font

:relative\_path: ./performance-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

If a performance event occurs, you can locate the source of the issue within Active IQ Unified Manager and use other tools to fix it. You might receive an email notification of an event or notice the event during daily monitoring.

## Steps

1. Click the link in the email notification, which takes you directly to the storage object having a performance event.

If you...	Then...
Receive an email notification of an event	Click the link to go directly to the event details page.
Notice the event while analyzing the Event Inventory page	Select the event to go directly to the event details page.

2. If the event has crossed a system-defined threshold, follow the suggested actions in the UI to troubleshoot the issue.
3. If the event has crossed a user-defined threshold, analyze the event to determine if you need to take action.
4. If the issue persists, check the following settings:
  - Protocol settings on the storage system
  - Network settings on any Ethernet or fabric switches
  - Network settings on the storage system
  - Disk layout and aggregate metrics on the storage system
5. If the issue persists, contact technical support for assistance.

= Use Active IQ Digital Advisor to view system performance

:icons: font

:relative\_path: ./performance-config/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/



For any ONTAP system that sends AutoSupport telemetry to NetApp, you can view extensive performance and capacity data. Active IQ shows system performance over a longer period than you can see in System Manager.

You can view graphs of CPU utilization, latency, IOPS, IOPS by protocol, and network throughput. You can also download this data in .csv format for analysis in other tools.

In addition to this performance data, Active IQ can show you storage efficiency by workload and compare that efficiency to the expected efficiency for that type of workload. You can view capacity trends and see an estimate of how much additional storage you might need to add in a given timeframe

- Storage Efficiency is available at the customer, cluster, and node level on the left-hand-side of the main dashboard.
- Performance is available at the cluster and node level on the left-hand-side of the main dashboard.

## Related information

[Active IQ Digital Advisor documentation](#)

[Active IQ Digital Advisor video playlist](#)

[Active IQ Web Portal](#)

= Performance management with the CLI

= Performance management overview

:icons: font

:relative\_path: ./performance-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can set up basic performance management tasks identify and resolve common performance issues.

You can use these procedures to monitor cluster performance if the following assumptions apply to your situation:

- You want to use best practices, not explore every available option.
- You do not want to read a lot of conceptual background.
- You want to display system status and alerts, monitor cluster performance, and perform root-cause analysis by using Active IQ Unified Manager (formerly OnCommand Unified Manager), in addition to the ONTAP command-line interface.
- You are using the ONTAP command-line interface to configure storage quality of service (QoS).

QoS is also available in System Manager, NSLM, WFA, VSC (VMware Plug-in), and APIs.

- You want to install Unified Manager by using a virtual appliance, instead of a Linux or Windows-based installation.
- You're willing to use a static configuration rather than DHCP to install the software.
- You can access ONTAP commands at the advanced privilege level.
- You are a cluster administrator with the "admin" role.

## Related information

If these assumptions are not correct for your situation, you should see the following resources:

- [Active IQ Unified Manager 9.8 Installation](#)
- [System administration](#)
- [Performance monitoring setup](#)

= Monitor performance

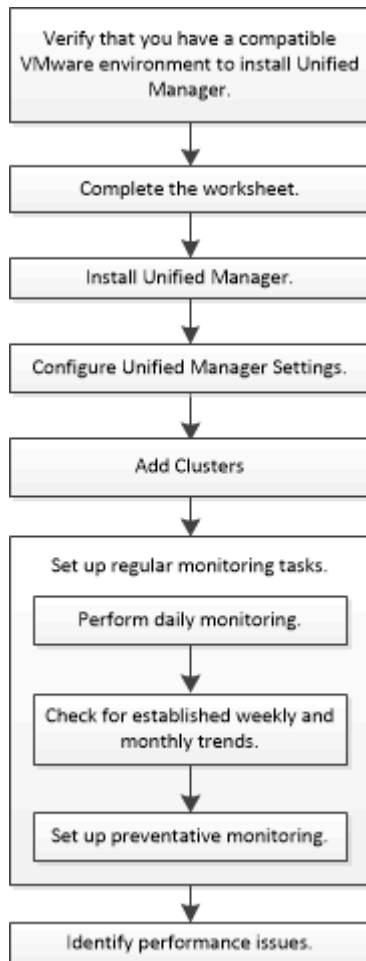
= Performance monitoring workflow overview

:icons: font

:relative\_path: ./performance-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Monitoring cluster performance involves installing Active IQ Unified Manager software, setting up basic monitoring tasks, and identifying performance issues.



= Verify that your VMware environment is supported

:icons: font

:relative\_path: ./performance-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

For successful installation of Active IQ Unified Manager, you must verify that your VMware environment meets the necessary requirements.

### Steps

1. Verify that your VMware infrastructure meets the sizing requirements for the installation of Unified Manager.
2. Go to the [Interoperability Matrix](#) to verify that you have a supported combination of the following components:
  - ONTAP version
  - ESXi operating system version
  - VMware vCenter Server version
  - VMware Tools version
  - Browser type and version

The [Interoperability Matrix](#) lists the supported configurations for Unified Manager.

1. Click the configuration name for the selected configuration.

Details for that configuration are displayed in the Configuration Details window.

2. Review the information in the following tabs:

- Notes

Lists important alerts and information that are specific to your configuration.

- Policies and Guidelines

Provides general guidelines for all configurations.

= Active IQ Unified Manager worksheet

:icons: font

:relative\_path: ./performance-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Before you install, configure, and connect Active IQ Unified Manager, you should have specific information about your environment readily available. You can record the information in the worksheet.

== Unified Manager installation information

Virtual machine on which software is deployed	Your value
ESXi server IP address	
Host fully qualified domain name	
Host IP address	
Network mask	
Gateway IP address	
Primary DNS address	
Secondary DNS address	
Search domains	
Maintenance user name	
Maintenance user password	

== Unified Manager configuration information

Setting	Your value
Maintenance user email address	
NTP server	
SMTP server host name or IP address	
SMTP user name	
SMTP password	
SMTP default port	25 (Default value)
Email from which alert notifications are sent	
LDAP bind distinguished name	
LDAP bind password	
Active Directory administrator name	
Active Directory password	
Authentication server base distinguished name	
Authentication server host name or IP address	

== Cluster information

Capture the following information for each cluster on Unified Manager.

Cluster 1 of N	Your value
Host name or cluster-management IP address	

The administrator must have been assigned the "admin" role.

a|

a|

ONTAP administrator password

a|

a|

Protocol (HTTP or HTTPS)

a|

.Related information

## Administrator authentication and RBAC

= Install Active IQ Unified Manager

:leveloffset: +1

= Download and deploy Active IQ Unified Manager

:icons: font

:relative\_path: ../performance-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

[.lead]

To install the software, you must download the virtual appliance (VA) installation file and then use a VMware vSphere Client to deploy the file to a VMware ESXi server. The VA is available in an OVA file.

.Steps

. Go to the **NetApp Support Site Software Download** page and locate Active IQ Unified Manager.

+

<https://mysupport.netapp.com/products/index.html>

. Select **VMware vSphere** in the **Select Platform** drop-down menu and click **Go!**

. Save the OVA file to a local or network location that is accessible to your VMware vSphere Client.

. In VMware vSphere Client, click **File > Deploy OVF Template**.

. Locate the OVA file and use the wizard to deploy the virtual appliance on the ESXi server.

+

You can use the **Properties** tab in the wizard to enter your static configuration information.

. Power on the VM.

. Click the **Console** tab to view the initial boot process.

. Follow the prompt to install VMware Tools on the VM.

. Configure the time zone.

. Enter a maintenance user name and password.

. Go to the URL displayed by the VM console.

= Configure initial Active IQ Unified Manager settings

:icons: font

:relative\_path: ../performance-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

[.lead]

The Active IQ Unified Manager Initial Setup dialog box appears when you first access the web UI, which enables you to configure some initial settings and to add clusters.

.Steps



To select more than one event, press the Ctrl key while you make your selections.

1. Click **Actions**, and select the users that you want to notify, choose the notification frequency, choose whether an SNMP trap will be sent to the trap receiver, and assign a script to be executed when an alert is generated.

If you modify the email address that is specified for the user and reopen the alert for editing, the Name field appears blank because the modified email address is no longer mapped to the user that was previously selected. Also, if you modified the email address of the selected user from the Users page, the modified email address is not updated for the selected user.

+

You can also choose to notify users through SNMP traps.

1. Click **Save**.

### Example of adding an alert

This example shows how to create an alert that meets the following requirements:

- Alert name: HealthTest
- Resources: includes all volumes whose name contains "abc" and excludes all volumes whose name contains "xyz"
- Events: includes all critical health events
- Actions: includes "[sample@domain.com](mailto:sample@domain.com)", a "Test" script, and the user has to be notified every 15 minutes

Perform the following steps in the Add Alert dialog box:

1. Click **Name**, and enter `HealthTest` in the **Alert Name** field.
2. Click **Resources**, and in the Include tab, select **Volumes** from the drop-down list.
  - a. Enter `abc` in the **Name contains** field to display the volumes whose name contains "abc".
  - b. Select **<<All Volumes whose name contains 'abc'>>** from the Available Resources area, and move it to the Selected Resources area.
  - c. Click **Exclude**, and enter `xyz` in the **Name contains** field, and then click **Add**.
3. Click **Events**, and select **Critical** from the Event Severity field.
4. Select **All Critical Events** from the Matching Events area, and move it to the Selected Events area.
5. Click **Actions**, and enter `sample@domain.com` in the Alert these users field.
6. Select **Remind every 15 minutes** to notify the user every 15 minutes.

You can configure an alert to repeatedly send notifications to the recipients for a specified time. You should determine the time from which the event notification is active for the alert.

7. In the Select Script to Execute menu, select **Test** script.
8. Click **Save**.

= Identify performance issues in Active IQ Unified Manager

:icons: font

:relative\_path: ./performance-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

If a performance event occurs, you can locate the source of the issue within Active IQ Unified Manager and use other tools to fix it. You might receive an email notification of an event or notice the event during daily monitoring.

### Steps

1. Click the link in the email notification, which takes you directly to the storage object having a performance event.

If you...	Then...
Receive an email notification of an event	Click the link to go directly to the event details page.
Notice the event while analyzing the Event Inventory page	Select the event to go directly to the event details page.

2. If the event has crossed a system-defined threshold, follow the suggested actions in the UI to troubleshoot the issue.
3. If the event has crossed a user-defined threshold, analyze the event to determine if you need to take action.
4. If the issue persists, check the following settings:
  - Protocol settings on the storage system
  - Network settings on any Ethernet or fabric switches
  - Network settings on the storage system
  - Disk layout and aggregate metrics on the storage system
5. If the issue persists, contact technical support for assistance.

= Use Active IQ Digital Advisor to view system performance

:icons: font

:relative\_path: ./performance-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

For any ONTAP system that sends AutoSupport telemetry to NetApp, you can view extensive performance and capacity data. Active IQ shows system performance over a longer period than you can see in System Manager.

You can view graphs of CPU utilization, latency, IOPS, IOPS by protocol, and network throughput. You can also download this data in .csv format for analysis in other tools.

In addition to this performance data, Active IQ can show you storage efficiency by workload and compare that efficiency to the expected efficiency for that type of workload. You can view capacity trends and see an estimate of how much additional storage you might need to add in a given timeframe

- Storage Efficiency is available at the customer, cluster, and node level on the left-hand-side of the main dashboard.
- Performance is available at the cluster and node level on the left-hand-side of the main dashboard.

## Related information

[Active IQ Digital Advisor documentation](#)

[Active IQ Digital Advisor video playlist](#)

[Active IQ Web Portal](#)

= Manage performance issues

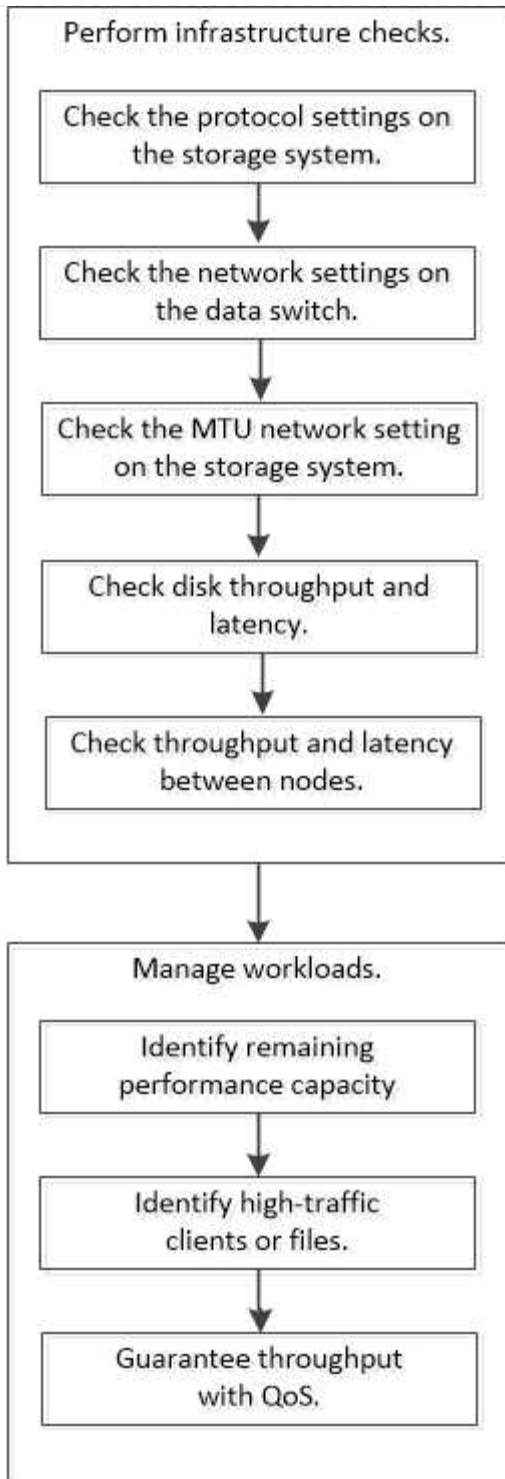
= Performance management workflow

:icons: font

:relative\_path: ./performance-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Once you have identified a performance issue, you can conduct some basic diagnostic checks of your infrastructure to rule out obvious configuration errors. If those don't pinpoint the problem, you can start looking at workload management issues.



= Perform basic infrastructure checks

= Check protocol settings on the storage system

= Check the NFS TCP maximum transfer size

:icons: font

:relative\_path: ./performance-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

For NFS, you can check whether the TCP maximum transfer size for reads and

writes might be causing a performance issue. If you think the size is slowing performance, you can increase it.

#### What you'll need

- You must have cluster administrator privileges to perform this task.
- You must use advanced privilege level commands for this task.

#### Steps

1. Change to the advanced privilege level:

```
set -privilege advanced
```

2. Check the TCP maximum transfer size:

```
vserver nfs show -vserver vserver_name -instance
```

3. If the TCP maximum transfer size is too small, increase the size:

```
vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer
```

4. Return to the administrative privilege level:

```
set -privilege admin
```

#### Example

The following example changes the TCP maximum transfer size of SVM1 to 1048576:

```
cluster1::*> vserver nfs modify -vserver SVM1 -tcp-max-xfer-size  
1048576
```

= Check the iSCSI TCP read/write size

:icons: font

:relative\_path: ./performance-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

For iSCSI, you can check the TCP read/write size to determine if the size setting is creating a performance issue. If the size is the source of an issue, you can correct it.

#### What you'll need

Advanced privilege level commands are required for this task.

#### Steps

1. Change to advanced privilege level:

```
set -privilege advanced
```

2. Check the TCP window size setting:

```
vserver iscsi show -vserver vserver_name -instance
```

### 3. Modify the TCP window size setting:

```
vserver iscsi modify -vserver vserver_name -tcp-window-size integer
```

### 4. Return to administrative privilege:

```
set -privilege admin
```

#### Example

The following example changes the TCP window size of SVM1 to 131,400 bytes:

```
cluster1::*> vserver iscsi modify -vserver vs1 -tcp-window-size 131400
```

= Check the CIFS multiplex settings

:icons: font

:relative\_path: ./performance-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

If slow CIFS network performance causes a performance issue, you can modify the multiplex settings to improve and correct it.

#### Steps

##### 1. Check the CIFS multiplex setting:

```
vserver cifs options show -vserver -vserver_name -instance
```

##### 2. Modify the CIFS multiplex setting:

```
vserver cifs options modify -vserver -vserver_name -max-mpx integer
```

#### Example

The following example changes the maximum multiplex count on SVM1 to 255:

```
cluster1:::> vserver cifs options modify -vserver SVM1 -max-mpx 255
```

= Check the FC adapter port speed

:icons: font

:relative\_path: ./performance-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

The adapter target port speed should match the speed of the device to which it connects, to optimize performance. If the port is set to autonegotiation, it can take longer to reconnect after a takeover and giveback or other interruption.

#### What you'll need

All LIFs that use this adapter as their home port must be offline.

#### Steps

1. Take the adapter offline:

```
network fcp adapter modify -node nodename -adapter adapter -state down
```

2. Check the maximum speed of the port adapter:

```
fcp adapter show -instance
```

3. Change the port speed, if necessary:

```
network fcp adapter modify -node nodename -adapter adapter -speed  
{1|2|4|8|10|16|auto}
```

4. Bring the adapter online:

```
network fcp adapter modify -node nodename -adapter adapter -state up
```

5. Bring all the LIFs on the adapter online:

```
network interface modify -vserver * -lif * { -home-node node1 -home-port  
e0c } -status-admin up
```

### Example

The following example changes the port speed of adapter 0d on node1 to 2 Gbps:

```
cluster1::> network fcp adapter modify -node node1 -adapter 0d -speed 2
```

= Check the network settings on the data switches

:icons: font

:relative\_path: ./performance-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Although you must maintain the same MTU settings on your clients, servers and storage systems (that is, network endpoints), intermediate network devices such as NICs and switches should be set to their maximum MTU values to ensure that performance is not impacted.

For best performance, all components in the network must be able to forward jumbo frames (9000 bytes IP, 9022 bytes including Ethernet). Data switches should be set to at least 9022 bytes, but a typical value of 9216 is possible with most switches.

### Procedure

For data switches, check that the MTU size is set to 9022 or higher.

For more information, see the switch vendor documentation.

= Check the MTU network setting on the storage system

:icons: font

:relative\_path: ./performance-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/



You can change the network settings on the storage system if they are not the same as on the client or other network endpoints. Whereas the management network MTU setting is set to 1500, the data network MTU size should be 9000.

== About this task

All ports within a broadcast-domain have the same MTU size, with the exception of the e0M port handling management traffic. If the port is part of a broadcast-domain, use the `broadcast-domain modify` command to change the MTU for all ports within the modified broadcast-domain.

Note that intermediate network devices such as NICs and data switches can be set to higher MTU sizes than network endpoints. For more information, see [Check the network settings on the data switches](#).

### Steps

1. Check the MTU port setting on the storage system:

```
network port show -instance
```

2. Change the MTU on the broadcast domain used by the ports:

```
network port broadcast-domain modify -ip-space ip-space -broadcast-domain  
broadcast-domain -mtu new_mtu
```

### Example

The following example changes the MTU port setting to 9000:

```
network port broadcast-domain modify -ip-space Cluster -broadcast-domain  
Cluster -mtu 9000
```

= Check disk throughput and latency

:icons: font

:relative\_path: ./performance-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can check the disk throughput and latency metrics for cluster nodes to assist you in troubleshooting.

### About this task

Advanced privilege level commands are required for this task.

### Steps

1. Change to advanced privilege level:

```
set -privilege advanced
```

2. Check the disk throughput and latency metrics:

```
statistics disk show -sort-key latency
```

### Example

The following example displays the totals in each user read or write operation for node2 on cluster1:

```
::*> statistics disk show -sort-key latency
cluster1 : 8/24/2015 12:44:15
```

Disk	Node	Busy (%)	Total Ops	Read Ops	Write Ops	Read (Bps)	Write (Bps)	*Latency (us)
1.10.20	node2	4	5	3	2	95232	367616	23806
1.10.8	node2	4	5	3	2	138240	386048	22113
1.10.6	node2	3	4	2	2	48128	371712	19113
1.10.19	node2	4	6	3	2	102400	443392	19106
1.10.11	node2	4	4	2	2	122880	408576	17713

= Check throughput and latency between nodes

:icons: font

:relative\_path: ./performance-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the `network test-path` command to identify network bottlenecks, or to prequalify network paths between nodes. You can run the command between intercluster nodes or intracluster nodes.

#### What you'll need

- You must be a cluster administrator to perform this task.
- Advanced privilege level commands are required for this task.
- For an intercluster path, the source and destination clusters must be peered.

#### About this task

Occasionally, network performance between nodes may not meet expectations for your path configuration. A 1 Gbps transmission rate for the kind of large data transfers seen in SnapMirror replication operations, for example, would not be consistent with a 10 GbE link between the source and destination clusters.

You can use the `network test-path` command to measure throughput and latency between nodes. You can run the command between intercluster nodes or intracluster nodes.

The test saturates the network path with data, so you should run the command when the system is not busy and when network traffic between nodes is not excessive. The test times out after ten seconds. The command can be run only between ONTAP 9 nodes.

The `session-type` option identifies the type of operation you are running over the network path—for example, "AsyncMirrorRemote" for SnapMirror replication to a remote destination. The type dictates the amount of data used in the test. The following table defines the session types:

Session Type	Description
AsyncMirrorLocal	Settings used by SnapMirror between nodes in the same cluster
AsyncMirrorRemote	Settings used by SnapMirror between nodes in different clusters (default type)
RemoteDataTransfer	Settings used by ONTAP for remote data access between nodes in the same cluster (for example, an NFS request to a node for a file stored in a volume on a different node)

### Steps

1. Change to advanced privilege level:

```
set -privilege advanced
```

2. Measure throughput and latency between nodes:

```
network test-path -source-node source_nodename |local -destination-cluster  
destination_clustername -destination-node destination_nodename -session  
-type  
Default|AsyncMirrorLocal|AsyncMirrorRemote|SyncMirrorRemote|RemoteDataTrans  
fer
```

The source node must be in the local cluster. The destination node can be in the local cluster or in a peered cluster. A value of "local" for `-source-node` specifies the node on which you are running the command.

The following command measures throughput and latency for SnapMirror-type replication operations between `node1` on the local cluster and `node3` on `cluster2`:

```
cluster1::> network test-path -source-node node1 -destination  
-cluster cluster2 -destination-node node3 -session-type  
AsyncMirrorRemote  
Test Duration:      10.88 secs  
Send Throughput:   18.23 MB/sec  
Receive Throughput: 18.23 MB/sec  
MB sent:           198.31  
MB received:       198.31  
Avg latency in ms: 2301.47  
Min latency in ms: 61.14  
Max latency in ms: 3056.86
```

### 3. Return to administrative privilege:

```
set -privilege admin
```

#### After you finish

If performance does not meet expectations for the path configuration, you should check node performance statistics, use available tools to isolate the problem in the network, check switch settings, and so forth.

= Manage workloads

= Identify remaining performance capacity

:icons: font

:relative\_path: ./performance-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Performance capacity, or *headroom*, measures how much work you can place on a node or an aggregate before performance of workloads on the resource begins to be affected by latency. Knowing the available performance capacity on the cluster helps you provision and balance workloads.

#### What you'll need

Advanced privilege level commands are required for this task.

#### About this task

You can use the following values for the `-object` option to collect and display headroom statistics:

- For CPUs, `resource_headroom_cpu`.
- For aggregates, `resource_headroom_aggr`.

You can also complete this task using System Manager and Active IQ Unified Manager.

#### Steps

##### 1. Change to advanced privilege level:

```
set -privilege advanced
```

##### 2. Start real-time headroom statistics collection:

```
statistics start -object resource_headroom_cpu|aggr
```

For complete command syntax, see the man page.

##### 3. Display real-time headroom statistics information:

```
statistics show -object resource_headroom_cpu|aggr
```

For complete command syntax, see the man page.

##### 4. Return to administrative privilege:

```
set -privilege admin
```

**Example**

The following example displays the average hourly headroom statistics for cluster nodes.

You can compute the available performance capacity for a node by subtracting the `current_utilization` counter from the `optimal_point_utilization` counter. In this example, the utilization capacity for `CPU_sti2520-213` is -14% (72%-86%), which suggests that the CPU has been overutilized on average for the past hour.

You could have specified `ewma_daily`, `ewma_weekly`, or `ewma_monthly` to get the same information averaged over longer periods of time.

```
sti2520-2131454963690::*> statistics show -object resource_headroom_cpu
-raw -counter ewma_hourly
(statistics show)
```

```
Object: resource_headroom_cpu
Instance: CPU_sti2520-213
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-213
```

Counter	Value
-----	-----
ewma_hourly	-
current_ops	4376
current_latency	37719
current_utilization	86
optimal_point_ops	2573
optimal_point_latency	3589
optimal_point_utilization	72
optimal_point_confidence_factor	1

```
Object: resource_headroom_cpu
Instance: CPU_sti2520-214
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-214
```

Counter	Value
-----	-----
ewma_hourly	-
current_ops	0
current_latency	0
current_utilization	0
optimal_point_ops	0
optimal_point_latency	0
optimal_point_utilization	71
optimal_point_confidence_factor	1

2 entries were displayed.

= Identify high-traffic clients or files

:icons: font

:relative\_path: ./performance-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use ONTAP Active Objects technology to identify clients or files that are responsible for a disproportionately large amount of cluster traffic. Once you have

identified these "top" clients or files, you can rebalance cluster workloads or take other steps to resolve the issue.

### What you'll need

You must be a cluster administrator to perform this task.

### Steps

1. View the top clients accessing the cluster:

```
statistics top client show -node node_name -sort-key sort_column -interval  
seconds_between_updates -iterations iterations -max number_of_instances
```

For complete command syntax, see the man page.

The following command displays the top clients accessing cluster1:

```
cluster1::> statistics top client show  
  
cluster1 : 3/23/2016 17:59:10  
  
                                *Total  
      Client Vserver           Node Protocol      Ops  
-----
```

172.17.180.170	vs4	siderop1-vs4	nfs	668
172.17.180.169	vs3	siderop1-vs3	nfs	337
172.17.180.171	vs3	siderop1-vs3	nfs	142
172.17.180.170	vs3	siderop1-vs3	nfs	137
172.17.180.123	vs3	siderop1-vs3	nfs	137
172.17.180.171	vs4	siderop1-vs4	nfs	95
172.17.180.169	vs4	siderop1-vs4	nfs	92
172.17.180.123	vs4	siderop1-vs4	nfs	92
172.17.180.153	vs3	siderop1-vs3	nfs	0

2. View the top files accessed on the cluster:

```
statistics top file show -node node_name -sort-key sort_column -interval  
seconds_between_updates -iterations iterations -max number_of_instances
```

For complete command syntax, see the man page.

The following command displays the top files accessed on cluster1:

```
cluster1::> statistics top file show
```

```
cluster1 : 3/23/2016 17:59:10
```

```

                                *Total
                                Vserver      Node      Ops
-----
/vol/vol1/vm170-read.dat    vol1      vs4 siderop1-vs4 22
/vol/vol1/vm69-write.dat   vol1      vs3 siderop1-vs3 6
/vol/vol2/vm171.dat        vol2      vs3 siderop1-vs3 2
/vol/vol2/vm169.dat        vol2      vs3 siderop1-vs3 2
/vol/vol2/p123.dat         vol2      vs4 siderop1-vs4 2
/vol/vol2/p123.dat         vol2      vs3 siderop1-vs3 2
/vol/vol1/vm171.dat        vol1      vs4 siderop1-vs4 2
/vol/vol1/vm169.dat        vol1      vs4 siderop1-vs4 2
/vol/vol1/vm169.dat        vol1      vs4 siderop1-vs3 2
/vol/vol1/p123.dat         vol1      vs4 siderop1-vs4 2
```

= Guarantee throughput with QoS

= Guarantee throughput with QoS overview

:icons: font

:relative\_path: ./performance-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use storage quality of service (QoS) to guarantee that performance of critical workloads is not degraded by competing workloads. You can set a throughput *ceiling* on a competing workload to limit its impact on system resources, or set a throughput *floor* for a critical workload, ensuring that it meets minimum throughput targets, regardless of demand by competing workloads. You can even set a ceiling and floor for the same workload.

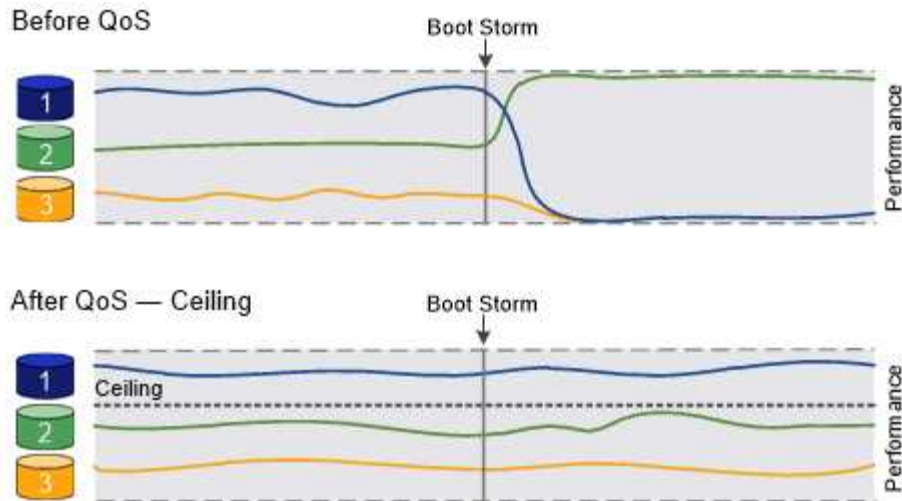
== About throughput ceilings (QoS Max)

A throughput ceiling limits throughput for a workload to a maximum number of IOPS or MBps, or IOPS and MBps. In the figure below, the throughput ceiling for workload 2 ensures that it does not "bully" workloads 1 and 3.

A *policy group* defines the throughput ceiling for one or more workloads. A workload represents the I/O operations for a *storage object*: a volume, file, qtree or LUN, or all the volumes, files, qtrees, or LUNs in an SVM. You can specify the ceiling when you create the policy group, or you can wait until after you monitor workloads to specify it.

Throughput to workloads might exceed the specified ceiling by up to 10%, especially if a workload experiences rapid changes in throughput. The ceiling might be exceeded by up to 50% to handle bursts. Bursts occur on single nodes when tokens accumulate up to 150%





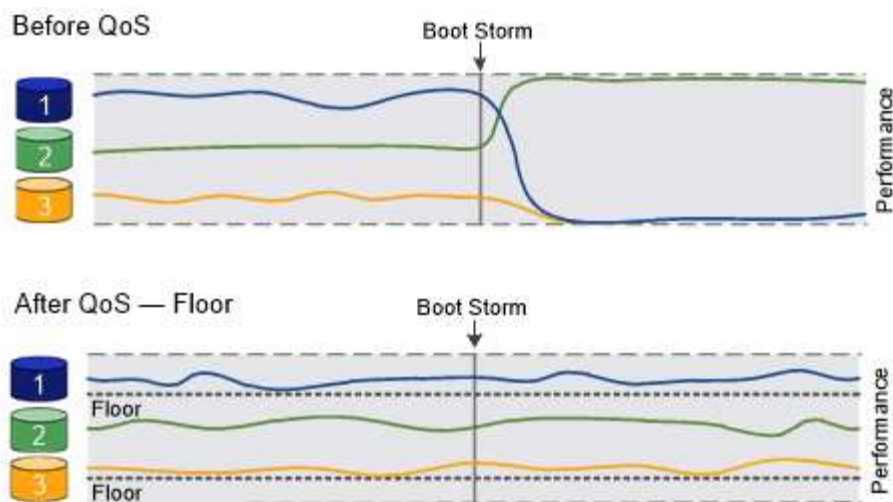
== About throughput floors (QoS Min)

A throughput floor guarantees that throughput for a workload does not fall below a minimum number of IOPS or MBps, or IOPS and MBps. In the figure below, the throughput floors for workload 1 and workload 3 ensure that they meet minimum throughput targets, regardless of demand by workload 2.

As the examples suggest, a throughput ceiling throttles throughput directly. A throughput floor throttles throughput indirectly, by giving priority to the workloads for which the floor has been set.

A policy group that defines a throughput floor cannot be applied to an SVM. You can specify the floor when you create the policy group, or you can wait until after you monitor workloads to specify it.

In releases before ONTAP 9.7, throughput floors are guaranteed when there is sufficient performance capacity available. In ONTAP 9.7 and later, throughput floors can be guaranteed even when there is insufficient performance capacity available. This new floor behavior is called floors v2. To meet the guarantees, floors v2 can result in higher latency on workloads without a throughput floor or on work that exceeds the floor settings. Floors v2 applies to both QoS and adaptive QoS. The option of enabling/disabling the new behavior of floors v2 is available in ONTAP 9.7P6 and later. A workload might fall below the specified floor during critical operations like `volume move trigger-cutover`. Even when sufficient capacity is available and critical operations are not taking place, throughput to a workload might fall below the specified floor by up to 5%. If floors are overprovisioned and there is no performance capacity, some workloads might fall below the specified floor.



== About shared and non-shared QoS policy groups

Beginning with ONTAP 9.4, you can use a *non-shared* QoS policy group to specify that the defined throughput ceiling or floor applies to each member workload individually. Behavior of *shared* policy groups depends on the policy type:

- For throughput ceilings, the total throughput for the workloads assigned to the shared policy group cannot exceed the specified ceiling.
- For throughput floors, the shared policy group can be applied to a single workload only.

== About adaptive QoS

Ordinarily, the value of the policy group you assign to a storage object is fixed. You need to change the value manually when the size of the storage object changes. An increase in the amount of space used on a volume, for example, usually requires a corresponding increase in the throughput ceiling specified for the volume.

*Adaptive QoS* automatically scales the policy group value to workload size, maintaining the ratio of IOPS to TBs|GBs as the size of the workload changes. That is a significant advantage when you are managing hundreds or thousands of workloads in a large deployment.

You typically use adaptive QoS to adjust throughput ceilings, but you can also use it to manage throughput floors (when workload size increases). Workload size is expressed as either the allocated space for the storage object or the space used by the storage object.

Used space is available for throughput floors in ONTAP 9.5 and later. It is not supported for throughput floors in ONTAP 9.4 and earlier.

- An *allocated space* policy maintains the IOPS/TB|GB ratio according to the nominal size of the storage object. If the ratio is 100 IOPS/GB, a 150 GB volume will have a throughput ceiling of 15,000 IOPS for as long as the volume remains that size. If the volume is resized to 300 GB, adaptive QoS adjusts the throughput ceiling to 30,000 IOPS.
- A *used space* policy (the default) maintains the IOPS/TB|GB ratio according to the amount of actual data stored before storage efficiencies. If the ratio is 100 IOPS/GB, a 150 GB volume that has 100 GB of data stored would have a throughput ceiling of 10,000 IOPS. As the amount of used space changes, adaptive QoS adjusts the throughput ceiling according to the ratio.

Beginning with ONTAP 9.5, you can specify an I/O block size for your application that enables a throughput limit to be expressed in both IOPS and MBps. The MBps limit is calculated from the block size multiplied by the IOPS limit. For example, an I/O block size of 32K for an IOPS limit of 6144IOPS/TB yields an MBps limit of 192MBps.

You can expect the following behavior for both throughput ceilings and floors:

- When a workload is assigned to an adaptive QoS policy group, the ceiling or floor is updated immediately.
- When a workload in an adaptive QoS policy group is resized, the ceiling or floor is updated in approximately five minutes.

Throughput must increase by at least 10 IOPS before updates take place.

Adaptive QoS policy groups are always non-shared: the defined throughput ceiling or floor applies to each member workload individually.

Beginning with ONTAP 9.6, throughput floors is supported on ONTAP Select premium with SSD.

== General support

The following table shows the differences in support for throughput ceilings, throughput floors, and adaptive QoS.

Resource or feature	Throughput ceiling	Throughput floor	Throughput floor v2	Adaptive QoS
ONTAP 9 version	All	9.2 and later	9.7 and later	9.3 and later
Platforms	All	<ul style="list-style-type: none"> <li>• AFF</li> <li>• C190 *</li> <li>• ONTAP Select premium with SSD *</li> </ul>	<ul style="list-style-type: none"> <li>• AFF</li> <li>• C190</li> <li>• ONTAP Select premium with SSD</li> </ul>	All
Protocols	All	All	All	All

FabricPool	Yes	Yes, if the tiering policy is set to "none" and no blocks are in the cloud.	Yes, if the tiering policy is set to "none" and no blocks are in the cloud.	Yes
SnapMirror Synchronous	Yes	No	No	Yes

\*C190 and ONTAP Select support started with the ONTAP 9.6 release.

== Supported workloads for throughput ceilings

The following table shows workload support for throughput ceilings by ONTAP 9 version. Root volumes, load-sharing mirrors, and data protection mirrors are not supported.

<b>Workload support - ceiling</b>	<b>9.0</b>	<b>9.1</b>	<b>9.2</b>	<b>9.3</b>	<b>9.4 and later</b>	<b>9.8 and later</b>
Volume	yes	yes	yes	yes	yes	yes
File	yes	yes	yes	yes	yes	yes
LUN	yes	yes	yes	yes	yes	yes
SVM	yes	yes	yes	yes	yes	yes
FlexGroup volume	no	no	no	yes	yes	yes
qtrees*	no	no	no	no	no	yes
Multiple workloads per policy group	yes	yes	yes	yes	yes	yes
Non-shared policy groups	no	no	no	no	yes	yes

\*Beginning with ONTAP 9.8, NFS access is supported in qtrees in FlexVol and FlexGroup volumes with NFS enabled. Beginning with ONTAP 9.9.1, SMB access is also supported in qtrees in FlexVol and FlexGroup volumes with SMB enabled.

== Supported workloads for throughput floors

The following table shows workload support for throughput floors by ONTAP 9 version. Root volumes, load-sharing mirrors, and data protection mirrors are not supported.

<b>Workload support - floor</b>	<b>9.2</b>	<b>9.3</b>	<b>9.4 and later</b>	<b>9.8 and later</b>
Volume	yes	yes	yes	yes
File	no	yes	yes	yes
LUN	yes	yes	yes	yes
SVM	no	no	no	no
FlexGroup volume	no	no	yes	yes
qtrees *	no	no	no	yes
Multiple workloads per policy group	no	no	yes	yes
Non-shared policy groups	no	no	yes	yes

\*Beginning with ONTAP 9.8, NFS access is supported in qtrees in FlexVol and FlexGroup volumes with NFS enabled. Beginning with ONTAP 9.9.1, SMB access is also supported in qtrees in FlexVol and FlexGroup volumes with SMB enabled.

== Supported workloads for adaptive QoS

The following table shows workload support for adaptive QoS by ONTAP 9 version. Root volumes, load-sharing mirrors, and data protection mirrors are not supported.

<b>Workload support - adaptive QoS</b>	<b>9.3</b>	<b>9.4 and later</b>
Volume	yes	yes
File	no	yes
LUN	no	yes
SVM	no	no
FlexGroup volume	no	yes
Multiple workloads per policy group	yes	yes
Non-shared policy groups	yes	yes

== Maximum number of workloads and policy groups

The following table shows the maximum number of workloads and policy groups by ONTAP 9 version.

Workload support	9.3 and earlier	9.4 and later
Maximum workloads per cluster	12,000	40,000
Maximum workloads per node	12,000	40,000
Maximum policy groups	12,000	12,000

= Enable or disable throughput floors v2

:icons: font

:relative\_path: ./performance-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can enable or disable throughput floors v2 on AFF. The default is enabled. With floors v2 enabled, throughput floors can be met when controllers are heavily used at the expense of higher latency on other workloads. Floors v2 applies to both QoS and Adaptive QoS.

### Steps

1. Change to advanced privilege level:

```
set -privilege advanced
```

2. Enter one of the following commands:

If you want to...	Use this command:
Disable floors v2	<pre>qos settings throughput-floors-v2 -enable false</pre>
Enable floors v2	<pre>qos settings throughput-floors-v2 -enable true</pre>

To disable throughput floors v2 in an MetroCluster cluster, you must run the

```
qos settings throughput-floors-v2 -enable false
```

command on both the source and destination clusters.

+

```
cluster1::*> qos settings throughput-floors-v2 -enable false
```

= Storage QoS workflow

:icons: font

:relative\_path: ./performance-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

If you already know the performance requirements for the workloads you want to manage with QoS, you can specify the throughput limit when you create the policy group. Otherwise, you can wait until after you monitor the workloads to specify the limit.

= Set a throughput ceiling with QoS

:icons: font

:relative\_path: ./performance-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the `max-throughput` field for a policy group to define a throughput ceiling for storage object workloads (QoS Max). You can apply the policy group when you create or modify the storage object.

#### What you'll need

- You must be a cluster administrator to create a policy group.
- You must be a cluster administrator to apply a policy group to an SVM.

#### About this task

- Beginning with ONTAP 9.4, you can use a *non-shared* QoS policy group to specify that the defined throughput ceiling applies to each member workload individually. Otherwise, the policy group is *shared*: the total throughput for the workloads assigned to the policy group cannot exceed the specified ceiling.

Set `-is-shared=false` for the `qos policy-group create` command to specify a non-shared policygroup.

- You can specify the throughput limit for the ceiling in IOPS, MB/s, or IOPS, MB/s. If you specify both IOPS and MB/s, whichever limit is reached first is enforced.

If you set a ceiling and a floor for the same workload, you can specify the throughput limit for the ceiling in IOPS only.

- A storage object that is subject to a QoS limit must be contained by the SVM to which the policy group belongs. Multiple policy groups can belong to the same SVM.
- You cannot assign a storage object to a policy group if its containing object or its child objects belong to the policy group.
- It is a QoS best practice to apply a policy group to the same type of storage objects.

## Steps

### 1. Create a policy group:

```
qos policy-group create -policy-group policy_group -vserver SVM -max
-throughput number_of_iops|Mb/S|iops,Mb/S -is-shared true|false
```

For complete command syntax, see the man page. You can use the `qos policy-group modify` command to adjust throughput ceilings.

The following command creates the shared policy group `pg-vs1` with a maximum throughput of 5,000 IOPS:

```
cluster1::> qos policy-group create -policy-group pg-vs1 -vserver
vs1 -max-throughput 5000iops -is-shared true
```

The following command creates the non-shared policy group `pg-vs3` with a maximum throughput of 100 IOPS and 400 Kb/S:

```
cluster1::> qos policy-group create -policy-group pg-vs3 -vserver
vs3 -max-throughput 100iops,400KB/s -is-shared false
```

The following command creates the non-shared policy group `pg-vs4` without a throughput limit:

```
cluster1::> qos policy-group create -policy-group pg-vs4 -vserver
vs4 -is-shared false
```

### 2. Apply a policy group to an SVM, file, volume, or LUN:

```
storage_object create -vserver SVM -qos-policy-group policy_group
```

For complete command syntax, see the man pages. You can use the `storage_object modify` command to apply a different policy group to the storage object.

The following command applies policy group `pg-vs1` to SVM `vs1`:

```
cluster1::> vserver create -vserver vs1 -qos-policy-group pg-vs1
```

The following commands apply policy group `pg-app` to the volumes `app1` and `app2`:



```
cluster1::> volume create -vserver vs2 -volume app1 -aggregate aggr1
-qos-policy-group pg-app
```

```
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
-qos-policy-group pg-app
```

### 3. Monitor policy group performance:

```
qos statistics performance show
```

For complete command syntax, see the man page.

Monitor performance from the cluster. Do not use a tool on the host to monitor performance.

+

The following command shows policy group performance:

+

```
cluster1::> qos statistics performance show
Policy Group           IOPS      Throughput  Latency
-----
-total-                12316     47.76MB/s  1264.00us
pg_vs1                 5008     19.56MB/s   2.45ms
_System-Best-Effort    62       13.36KB/s   4.13ms
_System-Background    30        0KB/s       0ms
```

### 1. Monitor workload performance:

```
qos statistics workload performance show
```

For complete command syntax, see the man page.

Monitor performance from the cluster. Do not use a tool on the host to monitor performance.

+

The following command shows workload performance:

+

```
cluster1::> qos statistics workload performance show
Workload          ID      IOPS      Throughput    Latency
-----
-total-          -      12320      47.84MB/s    1215.00us
appl-wid7967     7967    7219      28.20MB/s    319.00us
vs1-wid12279    12279    5026      19.63MB/s     2.52ms
_USERSPACE_APPS   14       55      10.92KB/s    236.00us
_Scan_Backgro... 5688     20         0KB/s         0ms
```

+

You can use the `qos statistics workload latency show` command to view detailed latency statistics for QoS workloads.

= Set a throughput floor with QoS

:icons: font

:relative\_path: ./performance-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use the `min-throughput` field for a policy group to define a throughput floor for storage object workloads (QoS Min). You can apply the policy group when you create or modify the storage object. Beginning with ONTAP 9.8, you can specify the throughput floor in IOPS or MBps, or IOPS and MBps.

### What you'll need

- You must be running ONTAP 9.2 or later. Throughput floors are available beginning with ONTAP 9.2.
- You must be a cluster administrator to create a policy group.

### About this task

- Beginning with ONTAP 9.4, you can use a *non-shared* QoS policy group to specify that the defined throughput floor be applied to each member workload individually. This is the only condition in which a policy group for a throughput floor can be applied to multiple workloads.

Set `-is-shared=false` for the `qos policy-group create` command to specify a non-shared policy group.

- Throughput to a workload might fall below the specified floor if there is insufficient performance capacity (headroom) on the node or aggregate.
- A storage object that is subject to a QoS limit must be contained by the SVM to which the policy group belongs. Multiple policy groups can belong to the same SVM.
- It is a QoS best practice to apply a policy group to the same type of storage objects.
- A policy group that defines a throughput floor cannot be applied to an SVM.

### Steps

1. Check for adequate performance capacity on the node or aggregate, as described in [permalink :identify-remaining-performance-capacity-task.html](#) [Identifying remaining performance capacity].
2. Create a policy group:

```
qos policy-group create -policy group policy_group -vserver SVM -min-throughput qos_target -is-shared true|false
```

For complete command syntax, see the man page for your ONTAP release. You can use the `qos policy-group modify` command to adjust throughput floors.

The following command creates the shared policy group `pg-vs2` with a minimum throughput of 1,000 IOPS:

```
cluster1::> qos policy-group create -policy group pg-vs2 -vserver vs2 -min-throughput 1000iops -is-shared true
```

The following command creates the non-shared policy group `pg-vs4` without a throughput limit:

```
cluster1::> qos policy-group create -policy group pg-vs4 -vserver
vs4 -is-shared false
```

### 3. Apply a policy group to a volume or LUN:

```
storage_object create -vserver SVM -qos-policy-group policy_group
```

For complete command syntax, see the man pages. You can use the `_storage_object_modify` command to apply a different policy group to the storage object.

The following command applies policy group `pg-app2` to the volume `app2`:

```
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
-qos-policy-group pg-app2
```

### 4. Monitor policy group performance:

```
qos statistics performance show
```

For complete command syntax, see the man page.

Monitor performance from the cluster. Do not use a tool on the host to monitor performance.

+

The following command shows policy group performance:

+

```
cluster1::> qos statistics performance show
Policy Group          IOPS      Throughput  Latency
-----
-total-              12316     47.76MB/s  1264.00us
pg_app2              7216     28.19MB/s   420.00us
_System-Best-Effort    62       13.36KB/s    4.13ms
_System-Background    30         0KB/s         0ms
```

### 1. Monitor workload performance:

```
qos statistics workload performance show
```

For complete command syntax, see the man page.

Monitor performance from the cluster. Do not use a tool on the host to monitor performance.

+

The following command shows workload performance:

+

```
cluster1::> qos statistics workload performance show
Workload          ID      IOPS      Throughput      Latency
-----
-total-          -      12320      47.84MB/s      1215.00us
app2-wid7967     7967    7219      28.20MB/s      319.00us
vs1-wid12279     12279   5026      19.63MB/s      2.52ms
_USERSPACE_APPS  14      55        10.92KB/s      236.00us
_Scan_Backgro... 5688    20        0KB/s          0ms
```

+

You can use the `qos statistics workload latency show` command to view detailed latency statistics for QoS workloads.

= Use adaptive QoS policy groups

:icons: font

:relative\_path: ./performance-admin/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can use an *adaptive* QoS policy group to automatically scale a throughput ceiling or floor to volume size, maintaining the ratio of IOPS to TBs|GBs as the size of the volume changes. That is a significant advantage when you are managing hundreds or thousands of workloads in a large deployment.

#### What you'll need

- You must be running ONTAP 9.3. Adaptive QoS policy groups are available beginning with ONTAP 9.3.
- You must be a cluster administrator to create a policy group.

#### About this task

A storage object can be a member of an adaptive policy group or a non-adaptive policy group, but not both. The SVM of the storage object and the policy must be the same. The storage object must be online.

Adaptive QoS policy groups are always non-shared: the defined throughput ceiling or floor applies to each member workload individually.

The ratio of throughput limits to storage object size is determined by the interaction of the following fields:

- `expected-iops` is the minimum expected IOPS per allocated TB|GB.

`expected-iops` is guaranteed on AFF platforms only. `expected-iops` is guaranteed for FabricPool only if

the tiering policy is set to "none" and no blocks are in the cloud. `expected-iops` is guaranteed for volumes that are not in a SnapMirror Synchronous relationship.

- `peak-iops` is the maximum possible IOPS per allocated or used TB|GB.
- `expected-iops-allocation` specifies whether allocated space (the default) or used space is used for `expected-iops`.

`expected-iops-allocation` is available in ONTAP 9.5 and later. It is not supported in ONTAP 9.4 and earlier.

- `peak-iops-allocation` specifies whether allocated space or used space (the default) is used for `peak-iops`.
- `absolute-min-iops` is the absolute minimum number of IOPS. You can use this field with very small storage objects. It overrides both `peak-iops` and/or `expected-iops` when `absolute-min-iops` is greater than the calculated `expected-iops`.

For example, if you set `expected-iops` to 1,000 IOPS/TB, and the volume size is less than 1 GB, the calculated `expected-iops` will be a fractional IOP. The calculated `peak-iops` will be an even smaller fraction. You can avoid this by setting `absolute-min-iops` to a realistic value.

- `block-size` specifies the application I/O block size. The default is 32K. Valid values are 8K, 16K, 32K, 64K, ANY. ANY means that the block size is not enforced.

Three default adaptive QoS policy groups are available, as shown in the following table. You can apply these policy groups directly to a volume.

Default policy group	Expected IOPS/TB	Peak IOPS/TB	Absolute Min IOPS
extreme	6,144	12,288	1000
performance	2,048	4,096	500
value	128	512	75

You cannot assign a storage object to a policy group if its containing object or its child objects belong to a policy group. The following table lists the restrictions.

If you assign the...	Then you cannot assign...
SVM to a policy group	Any storage objects contained by the SVM to a policy group
Volume to a policy group	The volume's containing SVM or any child LUNs to a policy group
LUN to a policy group	The LUN's containing volume or SVM to a policy group
File to a policy group	The file's containing volume or SVM to a policy group

## Steps

1. Create an adaptive QoS policy group:

```
qos adaptive-policy-group create -policy group policy_group -vserver SVM
-expected-iops number_of_iops/TB|GB -peak-iops number_of_iops/TB|GB
-expected-iops-allocation-space|used-space -peak-iops-allocation allocated-
space|used-space -absolute-min-iops number_of_iops -block-size
```

8K|16K|32K|64K|ANY

For complete command syntax, see the man page.

`-expected-iops-allocation` and `-block-size` is available in ONTAP 9.5 and later. These options are not supported in ONTAP 9.4 and earlier.



+

The following command creates adaptive QoS policy group `adpg-app1` with `-expected-iops` set to 300 IOPS/TB, `-peak-iops` set to 1,000 IOPS/TB, `-peak-iops-allocation` set to `used-space`, and `-absolute-min-iops` set to 50 IOPS:

+

```
cluster1::> qos adaptive-policy-group create -policy group adpg-app1
-vserver vs2 -expected-iops 300iops/tb -peak-iops 1000iops/TB -peak
-iops-allocation used-space -absolute-min-iops 50iops
```

#### 1. Apply an adaptive QoS policy group to a volume:

```
volume create -vserver SVM -volume volume -aggregate aggregate -size
number_of TB|GB -qos-adaptive-policy-group policy_group
```

For complete command syntax, see the man pages.

The following command applies adaptive QoS policy group `adpg-app1` to volume `app1`:

```
cluster1::> volume create -vserver vs1 -volume app1 -aggregate aggr1
-size 2TB -qos-adaptive-policy-group adpg-app1
```

The following commands apply the default adaptive QoS policy group `extreme` to the new volume `app4` and to the existing volume `app5`. The throughput ceiling defined for the policy group applies to volumes `app4` and `app5` individually:

```
cluster1::> volume create -vserver vs4 -volume app4 -aggregate aggr4
-size 2TB -qos-adaptive-policy-group extreme
```

```
cluster1::> volume modify -vserver vs5 -volume app5 -qos-adaptive
-policy-group extreme
```

= Monitor cluster performance with Unified Manager

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

With Active IQ Unified Manager, you can maximize availability and maintain control of your NetApp AFF and FAS storage infrastructure for improved scalability,

supportability, performance, and security.

Active IQ Unified Manager continuously monitors system health and send alerts, so your organization can free up IT staff resources. You can instantly view storage status from a single dashboard and quickly address issues through recommended actions.

Data management is simplified because you can discover, monitor, and receive notifications to proactively manage storage and quickly resolve issues. Admin efficiency is improved because you can monitor petabytes of data from a single dashboard and manage your data at scale.

With Active IQ Unified Manager, you can keep pace with fluctuating business demands, optimizing performance using performance data and advanced analytics. The reporting capabilities allow you to access standard reports or create custom operational reports to meet the specific needs of your business.

= Monitor cluster performance with Cloud Insights

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

NetApp Cloud Insights is a monitoring tool that gives you visibility into your complete infrastructure. With Cloud Insights, you can monitor, troubleshoot, and optimize all your resources including your public clouds and your private data centers.

== Cloud Insights comes in two editions

Cloud Insights Basic Edition is designed specifically to monitor and optimize your NetApp Data Fabric assets. It provides advanced analytics for the connections between all NetApp resources including HCI and All Flash FAS (AFF) within the environment free of charge.

Cloud Insights Standard Edition focuses not only on NetApp Data Fabric-enabled infrastructure components, but also on multi-vendor and multi-cloud environments. With its enriched capabilities, you can access support for over 100 services and resources.

In today's world, with resources in play from your on-premises data centers to multiple public clouds, it's crucial to have the complete picture from the application itself to the backend disk of the storage array. The additional support for application monitoring (like Kafka, MongoDB, and Nginx) gives you the information and knowledge you need to operate at the optimal level of utilization as well as with the perfect risk buffer.

Both editions (Basic and Standard) can integrate with NetApp Active IQ Unified Manager. Customers who use Active IQ Unified Manager will be able to see join information inside the Cloud Insights user interface. Notifications posted on Active IQ Unified Manager will not be overlooked and can now be correlated to events in Cloud Insights. In other words, you get the best of both worlds.

== Monitor, troubleshoot, and optimize all your resources

Cloud Insights helps you significantly reduce the time to resolve issues and prevent them from impacting end users. It also helps you reduce cloud infrastructure costs. Your exposure to insider threats is reduced by protecting your data with actionable intelligence.

Cloud Insights gives you visibility to your entire hybrid infrastructure in one place—from the public cloud to your data center. You can instantly create relevant dashboards that can be customized to your specific needs. You can also create targeted and conditional alerts that are specific and relevant to your organization's needs.

Advanced anomaly detection helps you proactively fix issues before they arise. You can view resource contention and degradation automatically to quickly restore impacted workloads. Troubleshooting goes more quickly with the automatically built hierarchy of relationships between the different components in your stack.

You can identify unused or abandoned resources across your environment, which helps you discover opportunities to right-size the infrastructure and optimize your entire spend.

Cloud Insights visualizes your system topology to gain an understanding of your Kubernetes architecture. You can monitor the health of your Kubernetes clusters, including which nodes are in trouble, and zoom in when you see a problem.

Cloud Insights helps you protect organizational data from being misused by malicious or compromised users through advanced machine learning and anomaly detection that gives you actionable intelligence on insider threats.

Cloud Insights helps you to visualize Kubernetes metrics so you can fully understand the relations between your pods, nodes, and clusters. You're able to assess the health of a cluster or a working pod, as well as the load it is currently processing—enabling you to take command of your K8S cluster and to control both the health and the cost of your deployment.

= File System Analytics

= File System Analytics overview

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

File System Analytics (FSA) was first introduced in ONTAP 9.8 to provide real-time visibility into file usage and storage capacity trends inside ONTAP FlexGroup or FlexVol volumes. This native capability eliminates the need for external tools and provides key insights into how your storage is utilized and whether there are opportunities to optimize the storage for your business needs.

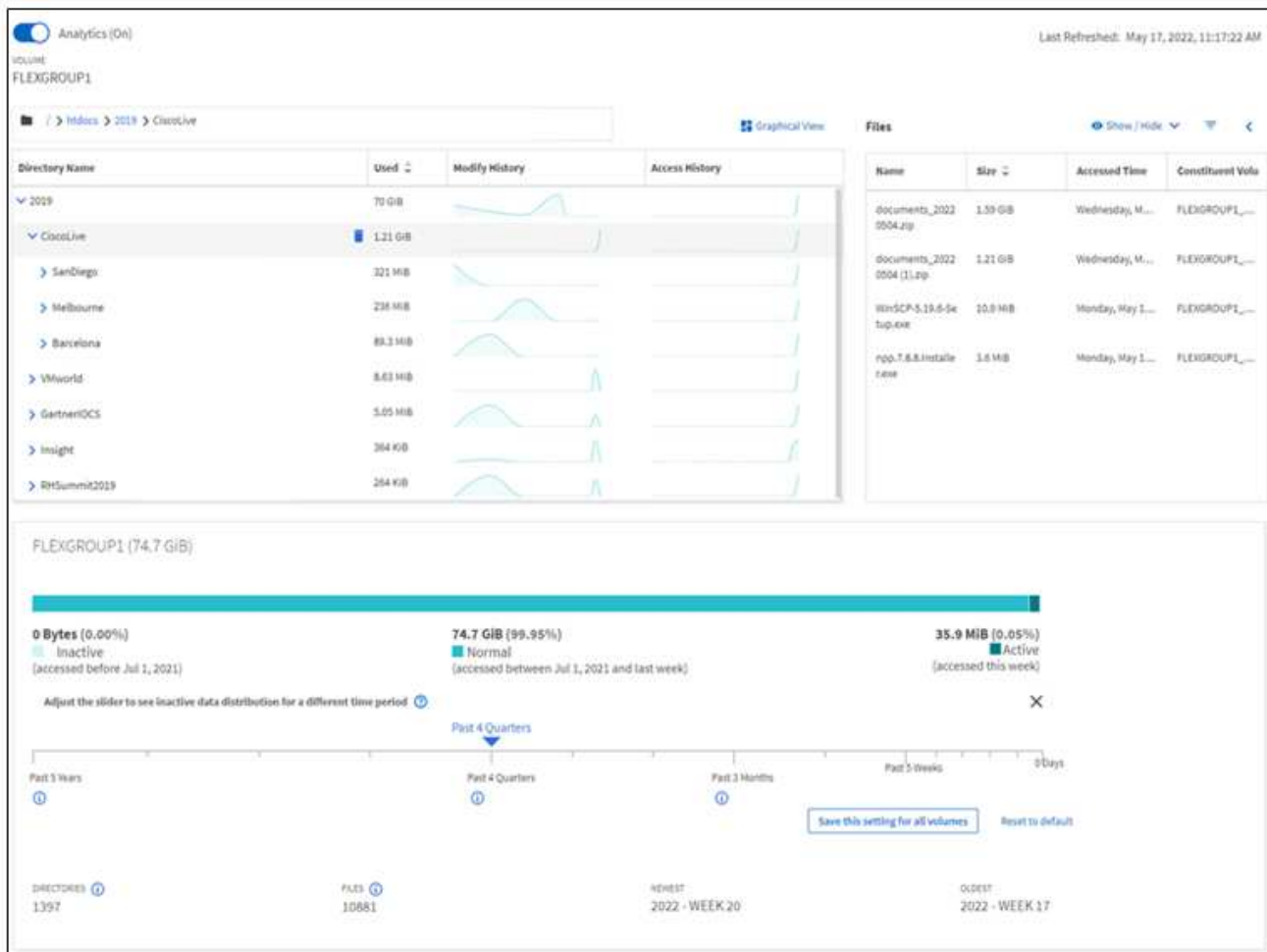
With FSA, you have visibility at all levels of a volume's file system hierarchy in NAS. For example, you can gain usage and capacity insights at the Storage VM (SVM), volume, directory, and file levels. You can use FSA to answer questions like:

- What is filling up my storage, and are there any large files I can move to another storage location?
- Which are my most active volumes, directories, and files? Is my storage performance optimized for the needs of my users?
- How much data was added in the last month?
- Who are my most active or least active storage users?

- How much inactive or dormant data is on my primary storage? Can I move that data to a lower cost cold tier?
- Will my planned quality-of-service changes negatively impact access to critical, frequently accessed files?

File System Analytics is integrated into ONTAP System Manager. Views within System Manager provide:

- Real-time visibility for effective data management and operation
- Real-time data collection and aggregation
- Subdirectory and file sizes and counts, together with associated performance profiles
- File age histograms for modify and access histories



== Supported volume types

File System Analytics is designed to provide visibility on volumes with active NAS data, with the exception of FlexCache caches and SnapMirror destination volumes.

== File System Analytics feature availability

Each ONTAP release expands the analytic scope of File System Analytics.

	ONTAP 9.11.1	ONTAP 9.10.1	ONTAP 9.9.1	ONTAP 9.8
Visualization in System Manager	X	X	X	X

Capacity analytics	X	X	X	X
Inactive data information	X	X	X	X
Support for volumes transitioned from Data ONTAP 7-Mode	X	X	X	
Ability to customize inactive period in System Manager	X	X	X	
Volume-level Activity Tracking	X	X		
Download Activity Tracking data to CSV	X	X		
SVM-level Activity Tracking	X			
Timeline	X			


== Learn more about File System Analytics

## ONTAP File System Analytics

Daniel Tennant  
Director of Software Engineering  
December 13, 2020

© 2020 NetApp, Inc. All rights reserved. — NETAPP CONFIDENTIAL —






### Further Reading

- [TR 4687: Best-practice guidelines for ONTAP File System Analytics](#)
- [Knowledge Base: High or fluctuating latency after turning on NetApp ONTAP File System Analytics](#)

= Enable File System Analytics

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

To collect and display usage data such as capacity analytics, you need to enable File

## System Analytics on a volume.

Beginning with ONTAP 9.8, you can enable File System Analytics on a new or existing volume. If you upgrade a system to ONTAP 9.8 or later, ensure that all upgrade processes have completed before you enable File System Analytics.

### Steps

Depending on the size and contents of the volume, enabling analytics may take time while ONTAP processes existing data in the volume. System Manager displays progress and presents analytics data when complete. If you need more precise information about initialization progress, you can use the ONTAP CLI command `volume analytics show`.

You can enable File System Analytics with ONTAP System Manager or the CLI.

### System Manager

In ONTAP 9.8 and 9.9.1	Beginning in ONTAP 9.10.1
<ol style="list-style-type: none"><li>1. Select <b>Storage &gt; Volumes</b>.</li><li>2. Select the desired volume, then select <b>Explorer</b>.</li><li>3. Select <b>Enable Analytics</b> or <b>Disable Analytics</b>.</li></ol>	<ol style="list-style-type: none"><li>1. Select <b>Storage &gt; Volumes</b>.</li><li>2. Select the desired volume. From the individual volume menu, select <b>File System &gt; Explorer</b>.</li><li>3. Select <b>Enable Analytics</b> or <b>Disable Analytics</b>.</li></ol>

### CLI

#### To enable File System Analytics with the CLI:

1. Run the following command:

```
volume analytics on -vserver svm_name -volume volume_name [-foreground {true|false}]
```

By default, the command runs in the foreground; ONTAP displays progress and presents analytics data when complete. If you need more precise information, you can run the command in the background by using the `-foreground false` option and then use the `volume analytics show` command to display initialization progress in the CLI.

2. After successfully enabling File System Analytics, use ONTAP System Manager to display the analytic data.

= View file system activity

:toc: macro

:toclevels: 1

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

After File System Analytics (FSA) is enabled, you can view the root directory contents of a selected volume sorted by the space used in each subtree.

Select any file system object to browse the file system and to display detailed information about each object in a directory. Information about directories can also be displayed graphically. Over time, historical data is displayed for each subtree. Space used is not sorted if there are more than 3000 directories.

== Explorer

The File System Analytics **Explorer** screen consists of three areas:

- Tree view of directories and subdirectories; expandable list showing name, size, modify history, and access history.
- Files; showing name, size, and accessed time for the object selected in the directory list.
- Active and inactive data comparison for the object selected in the directory list.

Beginning with ONTAP 9.9.1, you can customize the range to be reported. The default value is one year. Based on these customizations, you can take corrective actions, such as moving volumes and modifying the tiering policy.

Accessed time is shown by default. However, if the volume default has been altered from the CLI (by setting the `-atime-update` option to `false` with the `volume modify` command), then only last modified time is shown. For example:

- The tree view will not display the **access history**.
- The files view will be altered.
- The active/inactive data view will be based on modified time (`mtime`).

Using these displays, you can examine the following:

- File system locations consuming the most space
- Detailed information about a directory tree, including file and subdirectory count within directories and subdirectories
- File system locations that contain old data (for example, scratch, temp, or log trees)

Keep the following points in mind when interpreting FSA output:

- FSA show where and when your data is in use, not how much data is being processed. For example, large space consumption by recently accessed or modified files does not necessarily indicate high system processing loads.

- The way that the **Volume Explorer** tab calculates space consumption for FSA might differ from other tools. In particular, there could be significant differences compared to the consumption reported in the **Volume Overview** if the volume has storage efficiency features enabled. This is because the **Volume Explorer** tab does not include efficiency savings.
- Due to space limitations in the directory display, it is not possible to view a directory depth greater than 8 levels in the *List View*. To view directories more than 8 levels deep, you must switch to *Graphical View*, locate the desired directory, then switch back to *List View*. This will allow additional screen space in the display.

## Steps

1. View the root directory contents of a selected volume:

In ONTAP 9.8 and 9.9.1	Beginning in ONTAP 9.10.1
Click <b>Storage &gt; Volumes</b> , select the desired volume, then click <b>Explorer</b> .	Select <b>Storage &gt; Volumes</b> , select the desired volume. From the individual volume menu, select <b>File System &gt; Explorer</b> .

= Enable Activity Tracking

:icons: font

:relative\_path: ./file-system-analytics/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.10.1, File System Analytics includes an Activity Tracking feature that allows you to identify hot objects and download them as a CSV file.

Beginning with ONTAP 9.11.1, Activity Tracking is expanded to the SVM scope. Also beginning in ONTAP 9.11.1, System Manager features a timeline for Activity Tracking, allowing you to look through up to five minutes of Activity Tracking data.

Activity Tracking enables monitoring in four categories:

- Directories
- Files
- Clients
- Users

For each category monitored, Activity Tracking will display read IOPs, write IOPs, read throughputs, and write throughputs. Queries on Activity Tracking refresh every 10 to 15 seconds pertaining to hot spots seen in the system over the previous five-second interval.

Activity tracking information is approximate, and the accuracy of the data depends on the distribution of the incoming I/O traffic.

When viewing Activity Tracking in System Manager at the volume level, only the menu of the expanded volume will actively refresh. If the view of any volumes are collapsed, they will not refresh until the volume display is expanded. You can stop the refreshes with the **Pause Refresh** button. Activity data can be downloaded in a CSV format that will display all the point-in-time data captured for the selected volume.

With the timeline feature available beginning in ONTAP 9.11.1, you can keep a record of hotspot activity on a volume or SVM, continuously updating approximately every five seconds and retaining the previous five minutes of data. Timeline data is only retained for fields that are visible area of the page. If you



collapse a tracking category or scroll so the timeline is out of view, the timeline will stop collecting data. By default, timelines are disabled and will automatically be disabled when you navigate away from the Activity tab.

== Enable Activity Tracking for a single volume

You can enable Activity Tracking with ONTAP System Manager or the ONTAP CLI.

#### About this task

If you use RBAC with the ONTAP REST API or System Manager, you will need to create custom roles to manage access to Activity Tracking. See [\[Role-based access control \(RBAC\) and Activity Tracking\]](#) for this process.

## System Manager

### Steps

1. Select **Storage > Volumes**. Select the desired volume. From the individual volume menu, select File System and then select the Activity tab.
2. Ensure **Activity Tracking** is turned on to view individual reports on top directories, files, clients, and users.
3. To analyze data in greater depth without refreshes, select **Pause Refresh**. You can download the data to have a CSV record of the report as well.

## CLI

### Steps

1. Enable Activity Tracking:

```
volume activity-tracking on -vsverver svm_name -volume volume_name
```

2. You can check if the Activity Tracking state for a volume is on or off with the command:

```
volume activity-tracking show -vsverver svm_name -volume volume_name -state
```

3. Once enabled, use ONTAP System Manager or the ONTAP REST API to display Activity Tracking data.

== Enable Activity Tracking for multiple volumes

You can enable Activity Tracking for multiple volumes at once with System Manager.

#### About this task

If you use RBAC with the ONTAP REST API or System Manager, you will need to create custom roles to manage access to Activity Tracking. See [\[Role-based access control \(RBAC\) and Activity Tracking\]](#) for this process.

## For specific volumes

### Steps

1. Select **Storage > Volumes**. Select the desired volume. From the individual volume menu, select File System and then select the Activity tab.
2. Select the volumes that you want to enable Activity Tracking on. At the top of the volume list, select the **More Options** button. Select **Enable Activity Tracking**.

3. To view Activity Tracking at the SVM level, select the specific SVM you would like to view from **Storage > Volumes**. Navigate to the File System tab then Activity and you will see data for the volumes that have Activity Tracking enabled.

#### **For all volumes in an SVM**

##### **Steps**

1. Select **Storage > Volumes**. Select an SVM from the menu.
2. Navigate to the **File System** tab, choose the **More** tab to enable Activity Tracking on all volumes in the SVM.

## == Role-based access control (RBAC) and Activity Tracking

If you use [role-based access control \(RBAC\)](#) in System Manager or the ONTAP REST API, you will need to create a dedicated role to moderate access to Activity Tracking in File System Analytics.

### Steps

1. Create a default role to have access to all features.

This needs to be done before creating the restrictive role to ensure the role is only restrictive on the Activity Tracking:

```
security login role create -cmddirname DEFAULT -access all -role
storageAdmin
```

2. Create the restrictive role:

```
security login role create -cmddirname "volume file show-disk-usage"
-access none -role storageAdmin
```

3. Authorize roles to access the SVM's web services:

- `rest` for REST API calls
- `security` for password protection
- `sysmgr` for System Manager access

```
vserver services web access create -vserver svm-name -name_ -name rest
-role storageAdmin
```

```
vserver services web access create -vserver svm-name -name security
-role storageAdmin
```

```
vserver services web access create -vserver svm-name -name sysmgr -role
storageAdmin
```

4. Create a user.

You must issue a distinct create command for each application you would like to apply to the user. Calling create multiple times on the same user simply applies all the applications to that one user and does not create a new user each time. The `http` parameter for application type applies for the ONTAP REST API and System Manager.

```
security login create -user-or-group-name storageUser -authentication
-method password -application http -role storageAdmin
```

5. With the new user credentials, you can now log in to System Manager or use the ONTAP REST API to access File Systems Analytics data.

[Learn more about RBAC roles and the ONTAP REST API](#)

= Take corrective action based on analytics

:toc: macro

:toclevels: 1

:hardbreaks:  
:icons: font  
:linkattrs:  
:relative\_path: ./  
:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

Beginning with ONTAP 9.9.1, you can take corrective actions based on current data and desired outcomes directly from the File System Analytics displays.

When analytics are enabled, you can take the following actions:

- Delete directories and files

In the Explorer display, you can select directories or individual files to delete. Directories are deleted with low-latency fast directory delete functionality. (Fast directory delete is also available beginning in ONTAP 9.9.1 without analytics enabled.)

- Assign media cost in storage tiers to compare costs of inactive data storage locations


Media cost is a value that you assign based on your evaluation of storage costs, represented as your choice of currency per GB. When set, System Manager uses the assigned media cost to project estimated savings when you move volumes.


The media cost you set is not persistent; it can only be set for a single browser session.

- Move volumes to reduce storage costs

Based on analytics displays and media cost comparisons, you can move volumes to less expensive storage in local tiers.

Only one volume at a time can be compared and moved.

To perform this action...	Take these steps...
Delete directories or files	<ol style="list-style-type: none"><li>1. Click <b>Storage &gt; Volumes</b>, then click <b>Explorer</b>.</li></ol> <p>When you hover over a file or folder, the option to delete appears. You can only delete one object at a time.</p> <div data-bbox="850 1497 902 1549"></div> <p>When directories and files are deleted, the new storage capacity values are not displayed immediately.</p>

<p>Enable media cost comparison</p>	<ol style="list-style-type: none"> <li>1. Click <b>Storage &gt; Tiers</b>, then click <b>Set Media Cost</b> in the desired local tier (aggregate) tiles.  Be sure to select active and inactive tiers to enable comparison.</li> <li>2. Enter a currency type and amount.  When you enter or change the media cost, the change is made in all media types.</li> </ol>
<p>Move volumes to a less expensive tier</p>	<ol style="list-style-type: none"> <li>1. After enabling media cost display, click <b>Storage &gt; Tiers</b>, then click <b>Volumes</b>.</li> <li>2. To compare destination options for a volume, click  for the volume, then click <b>Move</b>.</li> <li>3. In the <b>Select Destination Local Tier</b> display, select destination tiers to display the estimated cost difference.</li> <li>4. After comparing options, select the desired tier and click <b>Move</b>.</li> </ol>

= Considerations for File System Analytics

:icons: font

:relative\_path: ./file-system-analytics/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You should be aware of certain usage limits and potential performance impacts associated with implementing File System Analytics.

== SVM-protected relationships

If you have enabled File System Analytics on volumes whose containing SVM is in a protection relationship, the analytics data is not replicated to the destination SVM. If the source SVM must be resynchronized in a recovery operation, you must manually reenables analytics on desired volumes after recovery.

== Performance considerations

In some cases, enabling File System Analytics could negatively impact performance during the initial metadata collection. This is most typically seen on systems that are at maximum utilization. To avoid enabling analytics on such systems, you can use ONTAP System Manager performance monitoring tools.

If you experience a notable increase in latency, refer to the Knowledge Base article [High or fluctuating latency after turning on NetApp ONTAP File System Analytics](#).

= EMS configuration

= EMS configuration overview

:icons: font

:relative\_path: ./error-messages/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./encryption-at-rest/./media/

You can quickly configure ONTAP 9 to send important EMS (Event Management System) event notifications directly to an email address, syslog server, Simple Management Network Protocol (SNMP) trap host, or REST API server so that you are immediately notified of system issues that require prompt attention.

To monitor the most important activities in your system, you must monitor the important EMS events.

Because important event notifications are not enabled by default, you must configure the EMS to send notifications to either an email address, a syslog server, an SNMP trap host, or REST API server.

Configure EMS event notifications for important events if the following are true:

- You are implementing one of the following scenarios:
  - You are setting up a new system running ONTAP 9 that does not have EMS configured.
  - You have an existing system running ONTAP 9 that does not have EMS configured.
  - You are upgrading to ONTAP 9 that does not have EMS configured.
  - You have just completed a transition from Data ONTAP operating in 7-Mode to ONTAP 9.
- You want to use best practices, not explore every available option.
- You do not want to read a lot of conceptual background.

You can find the EMS Event Catalog under More Resources on this page: [ONTAP 9 Product Library](#). See [Convert the legacy event route-based routing to event notifications](#) for more information on how to perform the notification-based model conversion. You can also refer to the [EMS reference](#).

= Configure EMS event notifications and filters with System Manager

You can use System Manager to configure how the Event Management System (EMS) delivers event notifications so that you can be notified of system issues that require your prompt attention.

ONTAP version	With System Manager, you can...
ONTAP 9.10.1	Configure email addresses, syslog servers, and webhook applications, as well as SNMP trap hosts.
ONTAP 9.7 to 9.10.0	Configure only SNMP trap hosts. You can configure other EMS destination with the ONTAP CLI. See <a href="#">EMS configuration overview</a> .

You can perform the following procedures:

- [\[add-ems-destination\]](#)
- [\[create-ems-filter\]](#)
- [\[edit-ems-destination\]](#)
- [\[edit-ems-filter\]](#)
- [\[delete-ems-destination\]](#)
- [\[delete-ems-filter\]](#)



## Related information

- [EMS Event Catalog](#)
- [Using the CLI to configure SNMP traphosts to receive event notifications](#)

== Add an EMS event notification destination

You can use System Manager to specify to where you want EMS messages sent.

## Steps

1. Click **Cluster > Settings**.
2. In the **Notifications Management** section, click , then click **View Event Destinations**.
3. On the **Notification Management** page, select the **Events Destinations** tab.
4. Click  **Add**.
5. Specify a name, an EMS destination type, and filters.



If needed, you can add a new filter. Click **Add a New Event Filter**.



6. Depending on the EMS destination type you selected, specify the following:

To configure...	Specify or select...
SNMP traphost	<ul style="list-style-type: none"><li>• Traphost name</li></ul>
Email (Beginning with 9.10.1)	<ul style="list-style-type: none"><li>• Destination email address</li><li>• Mail server</li><li>• From email address</li></ul>
Syslog server (Beginning with 9.10.1)	<ul style="list-style-type: none"><li>• Host name or IP address of the server</li></ul>
Webhook (Beginning with 9.10.1)	<ul style="list-style-type: none"><li>• Webhook URL</li><li>• Client authentication (select this option to specify a client certificate)</li></ul>

== Create a new EMS event notification filter

Beginning with ONTAP 9.10.1, you can use System Manager to define new customized filters that specify the rules for handling EMS notifications.

## Steps

1. Click **Cluster > Settings**.
2. In the **Notifications Management** section, click , then click **View Event Destinations**.
3. On the **Notification Management** page, select the **Event Filters** tab.
4. Click  **Add**.
5. Specify a name, and select whether you want to copy rules from an existing event filter or add new

rules.



6. Depending on your choice, perform the following steps:

If you choose....	Then, perform these steps...
<b>Copy rules from existing event filter</b>	<ol style="list-style-type: none"><li>1. Select an existing event filter.</li><li>2. Modify the existing rules.</li><li>3. Add other rules, if needed, by clicking <b>+ Add</b>.</li></ol>
<b>Add new rules</b>	Specify the type, name pattern, severities, and SNMP trap type for each new rule.

== Edit an EMS event notification destination

Beginning with ONTAP 9.10.1, you can use System Manager to change the event notification destination information.

### Steps

1. Click **Cluster > Settings**.
2. In the **Notifications Management** section, click , then click **View Event Destinations**.
3. On the **Notifications Management** page, select the **Events Destinations** tab.
4. Next to the name of the event destination, click , then click **Edit**.
5. Modify the event destination information, then click **Save**.



== Edit an EMS event notification filter

Beginning with ONTAP 9.10.1, you can use System Manager to modify customized filters to change how event notifications are handled.



You cannot modify system-defined filters.

### Steps

1. Click **Cluster > Settings**.
2. In the **Notifications Management** section, click , then click **View Event Destinations**.
3. On the **Notification Management** page, select the **Event Filters** tab.
4. Next to the name of the event filter, click , then click **Edit**.
5. Modify the event filter information, then click **Save**.

== Delete an EMS event notification destination

Beginning with ONTAP 9.10.1, you can use System Manager to delete an EMS event notification destination.





You cannot delete SNMP destinations.

### Steps

1. Click **Cluster > Settings**.



2. In the **Notifications Management** section, click , then click **View Event Destinations**.
3. On the **Notification Management** page, select the **Events Destinations** tab.
4. Next to the name of the event destination, click , then click **Delete**.



= Delete an EMS event notification filter

Beginning with ONTAP 9.10.1, you can use System Manager to delete customized filters.



You cannot delete system-defined filters.

### Steps

1. Click **Cluster > Settings**.
2. In the **Notifications Management** section, click , then click **View Event Destinations**.
3. On the **Notification Management** page, select the **Event Filters** tab.
4. Next to the name of the event filter, click , then click **Delete**.

= Configure EMS event notifications with the CLI

= EMS configuration workflow

:icons: font

:relative\_path: ./error-messages/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./error-messages/./media/

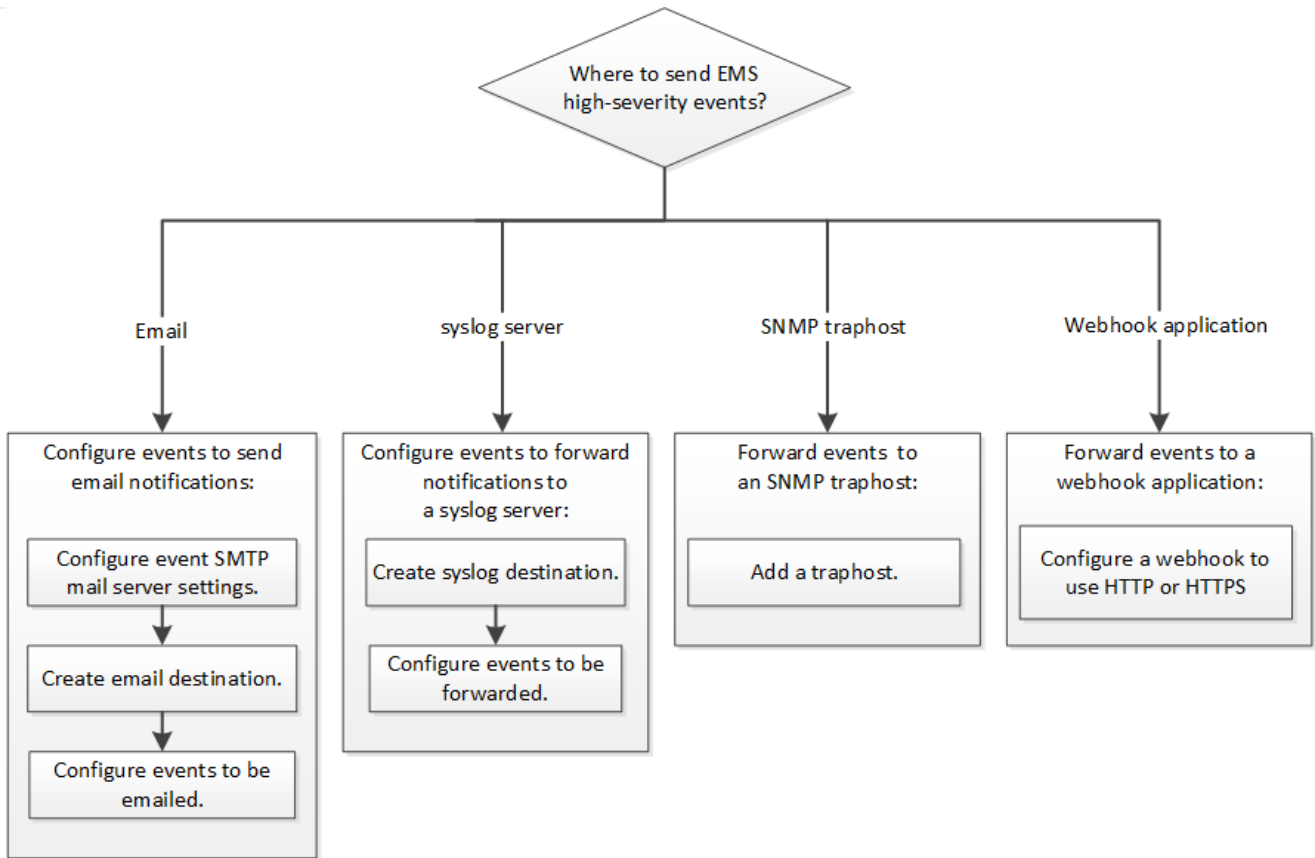
You must configure important EMS event notifications to be sent either as email, forwarded to a syslog server, forwarded to an SNMP trap host, or forwarded to a webhook application. This helps you to avoid system disruptions by taking corrective actions in a timely manner.

### About this task

If your environment already contains a syslog server for aggregating the logged events from other systems, such as servers and applications, then it is easier to use that syslog server also for important event notifications from storage systems.

If your environment does not already contain a syslog server, then it is easier to use email for important event notifications.

If you already forward event notifications to an SNMP trap host, then you might want to monitor that trap host for important events.



**Choices**

- Set EMS to send event notifications.

If you want...	Refer to this...
The EMS to send important event notifications to an email address	<a href="#">Configure important EMS events to send email notifications</a>
The EMS to forward important event notifications to a syslog server	<a href="#">Configure important EMS events to forward notifications to a syslog server</a>
If you want the EMS to forward event notifications to an SNMP traphost	<a href="#">Configure SNMP traphosts to receive event notifications</a>
If you want the EMS to forward event notifications to a webhook application	<a href="#">Configure important EMS events to forward notifications to a webhook application</a>

= Configure important EMS events to send email notifications

:icons: font

:relative\_path: ./error-messages/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./error-messages/./media/

To receive email notifications of the most important events, you must configure the EMS to send email messages for events that signal important activity.

### What you'll need

DNS must be configured on the cluster to resolve the email addresses.

### About this task

You can perform this task any time the cluster is running by entering the commands on the ONTAP command line.

### Steps

1. Configure the event SMTP mail server settings:

```
event config modify -mail-server mailhost.your_domain -mail-from  
cluster_admin@your_domain
```

2. Create an email destination for event notifications:

```
event notification destination create -name storage-admins -email  
your_email@your_domain
```

3. Configure the important events to send email notifications:

```
event notification create -filter-name important-events -destinations  
storage-admins
```

= Configuring important EMS events to forward notifications to a syslog server

:icons: font

:relative\_path: ./error-messages/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./error-messages/./media/

To log notifications of the most severe events on a syslog server, you must configure the EMS to forward notifications for events that signal important activity.

### What you'll need

DNS must be configured on the cluster to resolve the syslog server name.

### About this task

If your environment does not already contain a syslog server for event notifications, you must first create one. If your environment already contains a syslog server for logging events from other systems, then you might want to use that one for important event notifications.

You can perform this task any time the cluster is running by entering the commands on the ONTAP command line.

### Steps

1. Create a syslog server destination for important events:

```
event notification destination create -name syslog-ems -syslog syslog-  
server-address
```

2. Configure the important events to forward notifications to the syslog server:

```
event notification create -filter-name important-events -destinations  
syslog-ems
```

= Configure SNMP traphosts to receive event notifications

:icons: font

:relative\_path: ./error-messages/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./error-messages/./media/

To receive event notifications on an SNMP traphost, you must configure a traphost.

**What you'll need**

- SNMP and SNMP traps must be enabled on the cluster.

SNMP and SNMP traps are enabled by default.

- DNS must be configured on the cluster to resolve the traphost names.

### About this task

If you do not already have an SNMP traphost configured to receive event notifications (SNMP traps), you must add one.

You can perform this task any time the cluster is running by entering the commands on the ONTAP command line.

### Step

1. If your environment does not already have an SNMP traphost configured to receive event notifications, add one:

```
system snmp traphost add -peer-address snmp_traphost_name
```

All event notifications that are supported by SNMP by default are forwarded to the SNMP traphost.

= Configure important EMS events to forward notifications to a webhook application

:icons: font

:relative\_path: ./error-messages/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./error-messages/./media/

You can configure ONTAP to forward important event notifications to a webhook application. The configuration steps needed depend on the level of security you choose.

== Prepare to configure EMS event forwarding

There are several concepts and requirements you should consider before configuring ONTAP to forward event notifications to a webhook application.

=== Webhook application

You need a webhook application capable of receiving the ONTAP event notifications. A webhook is a user-defined callback routine that extends the capability of the remote application or server where it runs. Webhooks are called or activated by the client (in this case ONTAP) by sending an HTTP request to the destination URL. Specifically, ONTAP sends an HTTP POST request to the server hosting the webhook application along with the event notification details formatted in XML.

=== Security options

There are several security options available depending on how the Transport Layer Security (TLS) protocol is used. The option you choose determines the required ONTAP configuration.

TLS is a cryptographic protocol that is widely used on the internet. It provides privacy as well as data integrity and authentication using one or more public key certificates. The certificates are issued by trusted certificate authorities.

## HTTP

You can use HTTP to transport the event notifications. With this configuration, the connection is not secure. The identities of the ONTAP client and webhook application are not verified. Further, the network traffic is not encrypted or protected. See [Configure a webhook destination to use HTTP](#) for the configuration details.

## HTTPS

For additional security, you can install a certificate at the server hosting the webhook routine. The HTTPS protocol is used by ONTAP to verify the identity of the webhook application server as well as by both parties to ensure the privacy and integrity of the network traffic. See [Configure a webhook destination to use HTTPS](#) for the configuration details.

## HTTPS with mutual authentication

You can further enhance the HTTPS security by installing a client certificate at the ONTAP system issuing the webhook requests. In addition to ONTAP verifying the identity of the webhook application server and protecting the network traffic, the webhook application verifies the identity of the ONTAP client. This two-way peer authentication is known as *Mutual TLS*. See [Configure a webhook destination to use HTTPS with mutual authentication](#) for the configuration details.

## Related information

- [The Transport Layer Security \(TLS\) Protocol Version 1.3](#)

== Configure a webhook destination to use HTTP

You can configure ONTAP to forward event notifications to a webhook application using HTTP. This is the least secure option but the simplest to set up.

## Steps

1. Create a new destination `restapi-ems` to receive the events:

```
event notification destination create -name restapi-ems -rest-api-url
http://<webhook-application>
```

In the above command, you must use the **HTTP** scheme for the destination.

2. Create a notification linking the `important-events` filter with the `restapi-ems` destination:

```
event notification create -filter-name important-events -destinations
restapi-ems
```

== Configure a webhook destination to use HTTPS

You can configure ONTAP to forward event notifications to a webhook application using HTTPS. ONTAP uses the server certificate to confirm the identity of the webhook application as well as secure the network traffic.

## Before you begin

- Generate a private key and certificate for the webhook application server
- Have the root certificate available to install in ONTAP

## Steps

1. Install the appropriate server private key and certificates at the server hosting your webhook application. The specific configuration steps are dependent on the server.
2. Install the server root certificate in ONTAP:

```
security certificate install -type server-ca
```

The command will ask for the certificate.

3. Create the `restapi-ems` destination to receive the events:

```
event notification destination create -name restapi-ems -rest-api-url  
https://<webhook-application>
```

In the above command, you must use the **HTTPS** scheme for the destination.

4. Create the notification that links the `important-events` filter with the new `restapi-ems` destination:

```
event notification create -filter-name important-events -destinations  
restapi-ems
```

== Configure a webhook destination to use HTTPS with mutual authentication

You can configure ONTAP to forward event notifications to a webhook application using HTTPS with mutual authentication. With this configuration there are two certificates. ONTAP uses the server certificate to confirm the identity of the webhook application and secure the network traffic. In addition, the application hosting the webhook uses the client certificate to confirm the identity of the ONTAP client.

### Before you begin

You must do the following before configuring ONTAP:

- Generate a private key and certificate for the webhook application server
- Have the root certificate available to install in ONTAP
- Generate a private key and certificate for the ONTAP client

### Steps

1. Perform the first two steps in the task [Configure a webhook destination to use HTTPS](#) to install the server certificate so that ONTAP can verify the identity of the server.
2. Install the appropriate root and intermediate certificates at the webhook application to validate the client certificate.
3. Install the client certificate in ONTAP:

```
security certificate install -type client
```

The command will ask for the private key and certificate.

4. Create the `restapi-ems` destination to receive the events:

```
event notification destination create -name restapi-ems -rest-api-url  
https://<webhook-application> -certificate-authority <issuer of the client  
certificate> -certificate-serial <serial of the client certificate>
```

In the above command, you must use the **HTTPS** scheme for destination.

5. Create the notification that links the `important-events` filter with the new `restapi-ems` destination:

```
event notification create -filter-name important-events -destinations
restapi-ems
```

= Update deprecated EMS event mapping

= EMS event mapping models

:icons: font

:relative\_path: ./error-messages/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./error-messages/./media/

Prior to ONTAP 9.0, EMS events could only be mapped to event destinations based on event name pattern matching. The ONTAP command sets (`event destination`, `event route`) that use this model continue to be available in the latest versions of ONTAP, but they have been deprecated starting with ONTAP 9.0.

Beginning with ONTAP 9.0, the best practice for ONTAP EMS event destination mapping is to use the more scalable event filter model in which pattern matching is done on multiple fields, using the `event filter`, `event notification`, and `event notification destination` command sets.

If your EMS mapping is configured using the deprecated commands, you should update your mapping to use the `event filter`, `event notification`, and `event notification destination` command sets.

There are two types of event destinations:

1. **System-generated destinations:** There are five system-generated event destinations (created by default)

- `allevents`

- `asup`

- `criticals`

- `pager`

- `traphost`

Some of the system-generated destinations are for special purpose. For example, the `asup` destination routes `callhome.*` events to the AutoSupport module in ONTAP to generate AutoSupport messages.

2. **User-created destinations:** These are manually created using the `event destination create` command.



```
cluster-1::event*> destination show
```

```
Hide
Name          Mail Dest.      SNMP Dest.      Syslog Dest.
Params
-----
-----
allevents     -              -              -
false
asup          -              -              -
false
criticals    -              -              -
false
pager         -              -              -
false
traphost      -              -              -
false
```

```
5 entries were displayed.
```

```
+
```

```
cluster-1::event*> destination create -name test -mail test@xyz.com
```

```
This command is deprecated. Use the "event filter", "event
notification destination" and "event notification" commands,
instead.
```

```
+
```

```
cluster-1::event*> destination show
```

```
Hide
Name          Mail Dest.      SNMP Dest.      Syslog Dest.
Params
-----
-----
allevents     -              -              -
false
asup          -              -              -
false
criticals    -              -              -
false
pager         -              -              -
false
test          test@xyz.com    -              -
false
traphost      -              -              -
false
```

```
6 entries were displayed.
```

In the deprecated model, EMS events are individually mapped to a destination using the `event route add-destinations` command.

```
cluster-1::event*> route add-destinations -message-name raid.aggr.*
-add-destinations test
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
4 entries were acted on.

cluster-1::event*> route show -message-name raid.aggr.*
```

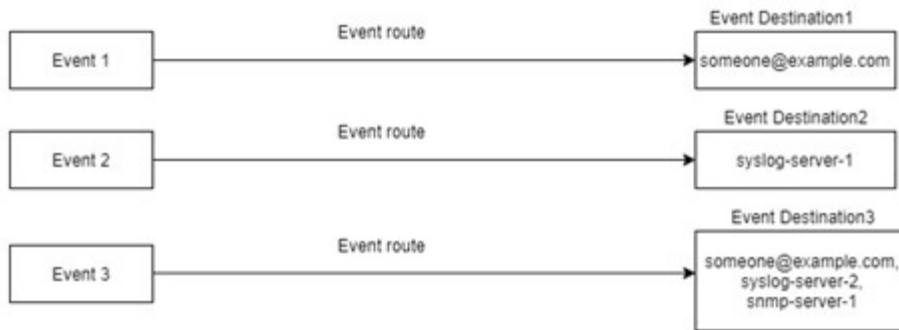
Time	Message	Severity	Destinations	Freq	Threshd
0	raid.aggr.autoGrow.abort	NOTICE	test	0	0
0	raid.aggr.autoGrow.success	NOTICE	test	0	0
0	raid.aggr.lock.conflict	INFORMATIONAL	test	0	0
0	raid.aggr.log.CP.count	DEBUG	test	0	0

```
4 entries were displayed.
```

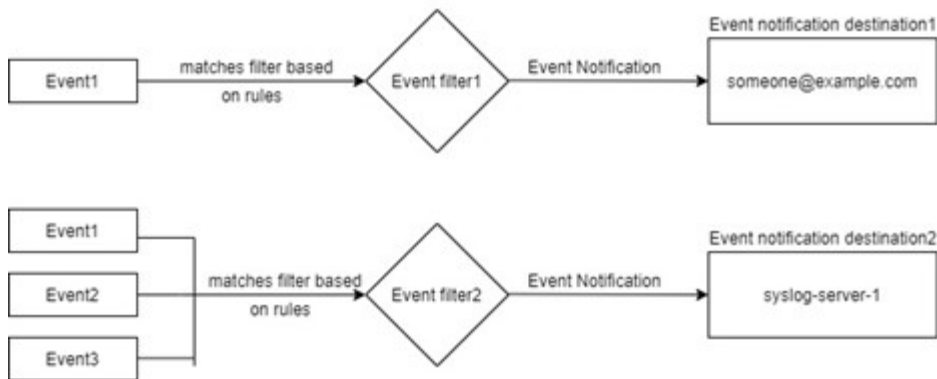
The new, more scalable EMS event notifications mechanism is based on event filters and event notification destinations. Refer to the following KB article for detailed information on the new event notification mechanism:

- [Overview of Event Management System for ONTAP 9](#)

### Legacy routing based model



### Event notification based model



= Update EMS event mapping from deprecated ONTAP commands

:icons: font

:relative\_path: ./error-messages/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./error-messages/./media/

If your EMS event mapping is currently configured using the deprecated ONTAP command sets (`event destination`, `event route`), you should follow this procedure to update your mapping to use the `event filter`, `event notification`, and `event notification destination` command sets.

#### Steps

1. List all the event destinations in the system using the `event destination show` command.

```
cluster-1::event*> destination show
```

```
Hide
Name          Mail Dest.      SNMP Dest.      Syslog Dest.
Params
-----
allevents     -              -              -
false
asup          -              -              -
false
criticals     -              -              -
false
pager         -              -              -
false
test          test@xyz.com    -              -
false
traphost      -              -              -
false
6 entries were displayed.
```

2. For each destination, list the events being mapped to it using the `event route show -destinations <destination name>` command.

```
cluster-1::event*> route show -destinations test
```

Time	Message	Severity	Destinations	Freq
Threshd	Threshd			
0	raid.aggr.autoGrow.abort	NOTICE	test	0
0	raid.aggr.autoGrow.success	NOTICE	test	0
0	raid.aggr.lock.conflict	INFORMATIONAL	test	0
0	raid.aggr.log.CP.count	DEBUG	test	0

```
4 entries were displayed.
```

3. Create a corresponding `event filter` which includes all these subsets of events. For example, if you want to include only the `raid.aggr.*` events, use a wildcard for the `message-name` parameter when creating the filter. You can also create filters for single events.



You can create up to 50 event filters.

```
cluster-1::event*> filter create -filter-name test_events

cluster-1::event*> filter rule add -filter-name test_events -type
include -message-name raid.aggr.*

cluster-1::event*> filter show -filter-name test_events
Filter Name Rule      Rule      Message Name      SNMP Trap Type
Severity
      Position Type
-----
test_events
      1      include  raid.aggr.*      *
*
      2      exclude  *                *
*
2 entries were displayed.
```

4. Create an event notification destination for each of the event destination endpoints (i.e., SMTP/SNMP/syslog)

```
cluster-1::event*> notification destination create -name dest1
-email test@xyz.com

cluster-1::event*> notification destination show
Name      Type      Destination
-----
dest1     email     test@xyz.com (via "localhost" from
"admin@localhost", configured in "event config")
snmp-traphost snmp      - (from "system snmp traphost")
2 entries were displayed.
```

5. Create an event notification by mapping the event filter to the event notification destination.

```

cluster-1::event*> notification create -filter-name asup_events
-destinations dest1

cluster-1::event*> notification show
ID    Filter Name                Destinations
----  -
1     default-trap-events         snmp-traphost
2     asup_events                 dest1
2 entries were displayed.

```

6. Repeat steps 1-5 for each event destination that has an event route mapping.



Events routed to SNMP destinations should be mapped to the snmp-traphost event notification destination. The SNMP traphost destination uses the system configured SNMP traphost.

```

cluster-1::event*> system snmp traphost add 10.234.166.135

cluster-1::event*> system snmp traphost show
      scspr2410142014.gdl.englab.netapp.com
(scsp2410142014.gdl.englab.netapp.com) <10.234.166.135>
Community: public

cluster-1::event*> notification destination show -name snmp-traphost

      Destination Name: snmp-traphost
      Type of Destination: snmp
      Destination: 10.234.166.135 (from "system snmp
traphost")
      Server CA Certificates Present?: -
      Client Certificate Issuing CA: -
      Client Certificate Serial Number: -
      Client Certificate Valid?: -

```

= ONTAP command reference

:icons: font

:relative\_path: ./concepts/

:imagesdir: /tmp/d20221026-17026-1injipo/source/./error-messages/./media/

:hardbreaks:

The ONTAP manual pages explain how to use ONTAP CLI commands. Man pages are available at the ONTAP command line with the `man` command.

== Command reference by version

## Supported ONTAP versions

- [ONTAP 9.11.1](#)
- [ONTAP 9.10.1](#)
- [ONTAP 9.9.1](#)
- [ONTAP 9.8](#)
- [ONTAP 9.7](#)
- [ONTAP 9.6](#)
- [ONTAP 9.5](#)
- [ONTAP 9.3](#)

Command reference for versions of ONTAP on limited support are available as PDFs:

## Archived command reference

- [ONTAP 9.4](#)
- [ONTAP 9.2](#)
- [ONTAP 9.1](#)
- [ONTAP 9.0](#)

== CLI comparison tool

You can learn about changes to the command-line interface (CLI) commands between ONTAP releases by using the CLI Comparison Tool on the [NetApp Support Site](#).

## Further Reading

- [Use the ONTAP command line interface](#)
- [Methods of navigating CLI command directories](#)

= Legal notices

:hardbreaks:

:icons: font

:linkattrs:

:relative\_path: ./

:imagesdir: /tmp/d20221026-17026-1injipo/source/./error-messages/./media/

Legal notices provide access to copyright statements, trademarks, patents, and more.

== Copyright

<http://www.netapp.com/us/legal/copyright.aspx>

== Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

== Patents

A current list of NetApp owned patents can be found at:

<https://www.netapp.com/us/media/patents-page.pdf>

== Privacy policy

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

== Open source

Provides information about third-party copyright and licenses used in this product.

[Notice for ONTAP 9.12.0](#)

[Notice for ONTAP 9.11.1](#)

[Notice for ONTAP 9.10.1](#)

[Notice for ONTAP 9.9.1](#)

[Notice for ONTAP 9.8](#)

[Notice for ONTAP 9.7](#)

[Notice for ONTAP 9.6](#)

[Notice for ONTAP 9.5](#)

[Notice for ONTAP 9.4](#)

[Notice for ONTAP 9.3](#)

[Notice for ONTAP 9.2](#)

[Notice for ONTAP 9.1](#)



## Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.