



Powerful and Frictionless Storage Administration



SoftNAS™ Cloud Installation & User Guide

©2012-2017 SoftNAS, Inc.

Table of Contents

Getting Started.....	5
Legal	7
Release Notes	9
SoftNAS Cloud® Features and Benefits	32
Support.....	34
Deployment Checklist.....	36
SoftNAS Cloud Performance Best Practices	37
Performance Considerations	38
RAID Considerations	42
Software RAID Considerations.....	43
Hardware RAID Considerations	45
Amazon EBS RAID Considerations	46
Common Performance Use Cases	47
S3 Cloud Disk Best Practices	48
Networking	51
Security	53
Launching SoftNAS Cloud® Platforms.....	56
Amazon Web Services (AWS)	57
Amazon EC2 Cloud Disk Overview	60
AWS EC2 System Requirements.....	61
Configuring AWS Identity and Access Management: Role and User.....	63
Creating the IAM Role for SoftNAS Cloud®	64
Specifying the IAM User for SoftNAS Cloud®	69
Regions and Availability Zones for Amazon Machine Images	73
Elastic and Virtual IP Addresses.....	75
Allocating New Elastic IP Addresses	77
Associating and Disassociating an Address	79
Amazon EC2 Setup and Performance Considerations.....	81
Create and Configure an Instance in AWS.....	82
AWS Instances	91
Accessing SoftNAS Cloud® for EC2.....	94
Adding Amazon EBS Disks.....	95
Managing EC2 instances in AWS	99
Creating an EC2 Volume.....	101
Managing Volumes	104
EBS Volumes and Device Mapping	106
Status Checks & Alarms	109
Connecting to an Instance via SSH from the EC2 Console.....	112
SoftNAS Cloud® Configuration	115
Accessing SoftNAS StorageCenter	116
Getting Started Checklist.....	118
Changing Default Passwords	120
Updating to the Latest Version.....	122
Activating SoftNAS Cloud® License	124
SoftNAS Cloud® S3 Disk Overview.....	127
Adding Cloud Disk Extenders	129
Importing S3 Disks	138
Storage Pools Overview.....	140
Partitioning Disks	142
Create a Storage Pool.....	143

Sharing Volumes over a Network.....	146
Create & Configure Volumes.....	147
Creating a CIFS Share.....	150
Creating NFS Share.....	161
Creating an AFP (Apple Filing Protocol) Share.....	169
iSCSI LUNs and Targets.....	176
iSCSI CHAP Authentication.....	185
Snapshots in StorageCenter.....	187
Advanced/Performance Configuration.....	191
MTU 9000.....	192
Active Directory Configuration.....	196
Adding Domain Controllers as DNS Server for SoftNAS.....	202
Configuring Kerberos to Connect to Active Directory.....	206
Configuring Read Cache and Write Log.....	209
How to Migrate Data Disks to a New SoftNAS VM.....	212
Setting Up SnapReplicate and SNAP HA™.....	214
SnapReplicate.....	216
SNAP HA™.....	223
Registering SoftNAS Cloud®.....	226
Microsoft Azure.....	228
Microsoft Azure System Requirements.....	230
Create & Configure a Virtual Machine in Azure.....	232
Adding Administrative Accounts.....	239
Generating SSH Keys.....	246
Managing Network Settings.....	250
Adding Storage in Microsoft Azure.....	253
Creating Storage Accounts.....	254
Hot and Cool Storage.....	257
Adding Disks via the Microsoft Azure Portal.....	260
Adding Block Storage via the SoftNAS UI.....	264
Adding Object Storage via the SoftNAS UI.....	267
High Availability in Azure SoftNAS.....	270
Azure Availability Sets.....	271
SnapReplicate™ on Azure.....	278
SNAP HA on Azure.....	282
Connecting to the SoftNAS StorageCenter.....	284
CenturyLink.....	287
Setting up SoftNAS on Century Link.....	290
VMware vSphere.....	300
Preparing a VMWare Hardware Environment.....	302
VMware vSphere Networking Considerations.....	304
VMware vSphere Disk Device Considerations.....	305
VMware vSphere Guidance for Storage Enclosures.....	308
VMware vSphere System Requirements.....	309
Update VMware Tools.....	312
Deploying your SoftNAS Instance in VMware vSphere.....	313
Configuring the Network Using SoftNAS Console.....	318
Customizing the System.....	322
Configuring VM Settings.....	334
Logging on to VM.....	335
Performance Tuning for VMware vSphere.....	338

Allocating Disk Storage Devices	341
Add RAW Device Mapping in VMware	343
VMWare HA Considerations.....	348
Advanced Configuration Notes for SoftNAS Cloud®	349
SnapReplicate iSCSI Volume Sync.....	350
Changing Monitoring Notification Frequency	351
Networking Tips	353
Applying CHAP Authentication to iSCSI ACLs	354

Getting Started

SoftNAS™ Cloud is a network attached storage (NAS) virtual appliance. Our products are commercial-grade storage management solutions for businesses that require high-speed, reliable storage at affordable prices.

SoftNAS Cloud® supports the following platforms:

- Cloud computing platforms such as **Amazon EC2®** and **Microsoft® Azure™**
- On-premise Computing Infrastructure such as **VMware vSphere®**.

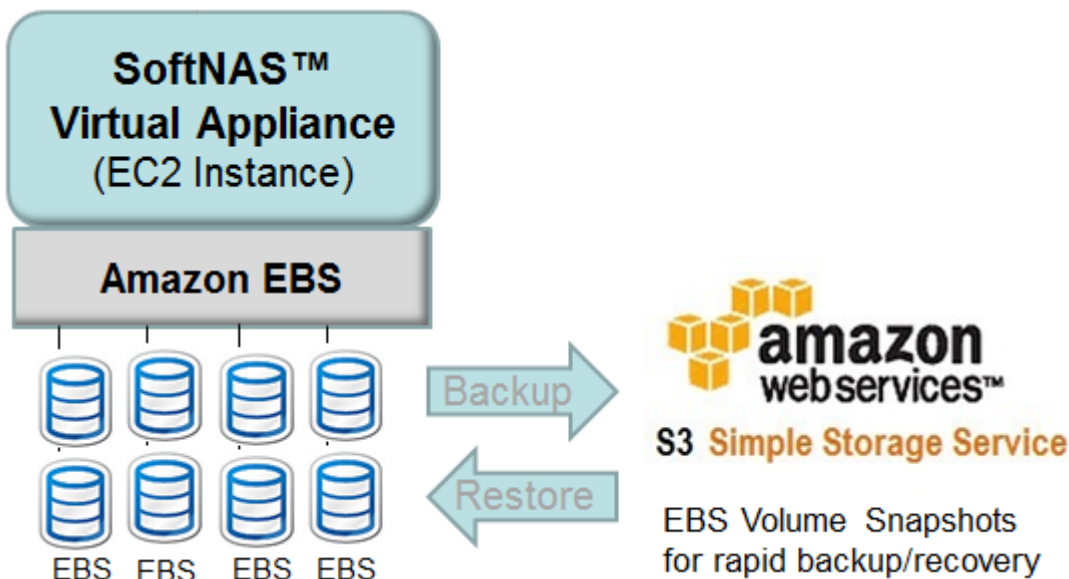
Architecture and Technology

SoftNAS Cloud® runs as a **Linux®**-based, 64-bit **CentOS** redistribution guest OS treated as a VM in a virtual server environment. In many use cases, storage devices are attached to the physical hardware layer, then presented to **SoftNAS Cloud®** as a VM running Linux.

SoftNAS Cloud® operates on an industry-standard Linux platform, and uses a derivative of the **Zettabyte File System® (ZFS)**, an open-source project originally released on **OpenSolaris®** by **Sun Microsystems, Inc.** This makes **SoftNAS Cloud®** able to leverage many **ZFS** features and add layers of functionality for NAS solutions in virtual computing and cloud computing.

An Apache webserver provides robust, secure access along with **Secure Shell® (SSH)**. Storage is accessible via **TCP/IP** protocols including **NFS v3**, **NFS v4**, **SMB/CIFS (Microsoft® Windows File Shares)**, and **iSCSI**.

SoftNAS Cloud® is packaged with a primary administration interface called **SoftNAS StorageCenter™**, which provides commercial-grade storage administration and management functionalities for businesses of all sizes.



Cloud Computing:

SoftNAS Cloud® provides the highly-available network storage backbone needed for business-critical cloud applications in the following environments:

[Amazon EC2](#)

[Microsoft Azure](#)

Premise-Based Computing:

SoftNAS Cloud® installs from a download to act as a virtual server appliance. Run as many instances of **SoftNAS Cloud® VM** as are needed in any of the following environments:



[VMware vSphere](#)

SoftNAS Cloud®™, **SoftNAS StorageCenter™**, **SnapReplicate™**, and **SNAP HA™** are trademarks of **SoftNAS Inc.** All other trademarks referred to in this guide are owned by their respective companies.

Legal

No Downtime Guarantee

The SoftNAS SNAP HA™ No Storage Downtime Guarantee Program guarantees 99.999% uptime for SoftNAS Cloud software and storage services, when operated with production workloads under SoftNAS best practices, or we will credit one-calendar month of SoftNAS service fees. By implementing SoftNAS SNAP HA™ in a high-availability configuration, you will realize 99.999% uptime of your storage infrastructure.

Who Qualifies?

New or existing SoftNAS customers running production applications or workloads on SoftNAS supported third party platforms who have also registered the product.

How do you qualify?

Deploy SoftNAS Cloud and successfully run SNAP HA™ high-availability storage following guidelines in the SoftNAS High-Availability Guide and the Technical Requirements described below. Then, register the product from the product registration form, accessible from StorageCenter™.

What is guaranteed?

NFS, CIFS/SMB or iSCSI storage connectivity will be available and operational 99.999% in any given one-calendar month period. This guarantee applies if:

storage connectivity outage is due to a simultaneous SoftNAS software failure of both SoftNAS Cloud controllers; or storage connectivity outage is due to a SoftNAS software failure of SoftNAS SNAP HA™ to maintain continuous NFS, CIFS/SMB and/or iSCSI access from at least one controller.

How do you file a claim?

Open a support ticket by going to <https://www.softnas.com/helpdesk/index.php?/Tickets/Submit>, complete the required outage information, and provide remote access into both controllers of the failed system. The support ticket must be submitted within 10 days after the end of the month in which the claimed outage or failure occurred. SoftNAS personnel must be provided with all requested log files and reasonable access to inspect the failed SoftNAS SNAP HA™ instances before a claim will be processed. Approval of the credit is at the discretion of SoftNAS, dependent upon the results of the check and inspection performed by SoftNAS. third-party reports, data or log files may not be used for determination. Upon SoftNAS' verification of the outage due solely to SoftNAS Cloud or SoftNAS SNAP HA™ operational failure and such outage is beyond the SoftNAS SNAP HA™ No Storage Downtime Guarantee Program, SoftNAS will issue a credit within 30 days of such determination.

How much is the credit and how is it applied?

The credit is equal to the monthly payment for the month in which the failure or outage occurred. If quarterly, semi-annual or annual payments are made, then such payment will be prorated on a monthly basis to determine the credit amount. Credits are applied towards future payments owed to SoftNAS only and are not issued as refunds.

SoftNAS Patents

The following SoftNAS products are covered by patents and pending patent applications in the United States. Additionally, there are one or more pending international applications. The below notification serves to provide virtual patent marking under 35 U.S.C. § 287(a).

SoftNAS Product	Patent Number (or Patent Pending)
SoftNAS Cloud	U.S. Pat. Nos. 9,378,262; 9,584,363.
SNAP HA™	
SnapReplicate™	
DeltaSync™	
FlexFiles™	

Ultrafast™	
------------	--

Disclaimers

Release Notes

Presented below for your convenience and information are the release notes of the latest releases.

WARNING: If updating from an older version, such as 3.4.9.4, your update can take up to 2 hours for the update to complete. Do NOT terminate the update while in progress else errors may occur. If you feel that your update is taking longer than 2 hours, please contact SoftNAS support for assistance and do not reboot your instance.

Note: SoftNAS will not prompt for a reboot post-update. Reboot will occur automatically. Schedule update to coincide with maintenance downtime.

Note: As of version 3.4.8 SoftNAS does not support launching SoftNAS Cloud VMs on the Azure Classic Portal. The Azure Resource Manager (ARM) is the only supported platform on Azure.

Note: As of version 3.4.9.7, the technical requirements for our No Downtime Guarantee have changed. In particular, the following minimum requirements must be met:

- Software version must be 3.4.9.7 or above.
- Software updates must be applied within 30 days of availability.

For more details on our No Downtime Guarantee, click [here](#).

Note: We have also updated our sizing guidance for SoftNAS instances on both Azure and AWS platforms.

General Purpose: For General Purpose workloads, the below sizes are a good starting point with regards to memory and CPU resources. The recommended instances are suited to handle processing and caching for workloads with minimal requirements for network bandwidth:

- **AWS:** M4.2Xlarge
- **Azure:** DS4_v2

High Performance: Workloads that are read intensive will benefit from larger memory-based read cache. The additional CPU resources will also provide better performance when deduplication, encryption, compression and/or RAID are enabled:

- **AWS:** M4.4Xlarge
- **Azure:** DS5_v2

Extreme Performance: The below options are ideal for heavier workloads that require a very high speed network connection due to the amount of data transferred over a network. In addition to the very high speed network, this level of VM gives you additional storage, CPU and memory:

- **AWS:** M4.10Xlarge
- **Azure:** DS15_v2

SoftNAS Cloud 3.4.9.7 Release - March 27, 2017

Overview

SoftNAS Cloud® 3.4.9.7 is a maintenance release containing fixes, and improvements. Version 3.4.9.7 is compatible with all editions of SoftNAS Cloud®.

Upgrading

Upgrading from 3.4.0 through 3.4.9.5

Reboot Required for AWS and VMware instances if updating from 3.4.9.5 or earlier. No reboot required for upgrades from 3.4.9.6

Upgrading from 3.3.3 or 3.3.4

Reboot Required for AWS and VMware instances if updating from 3.4.9.5 or earlier. No reboot required for upgrades from 3.4.9.6.

Follow instructions to upgrade a highly available SNAP HA™ pair.

Upgrading from versions prior to 3.3.3

1-click upgrades are not supported from versions older than 3.3.3. Follow instructions to migrate, or Contact SoftNAS Support to schedule an upgrade session.

New in SoftNAS Cloud® 3.4.9.7

Instance support update - New instance sizes supported in the AWS Marketplace.

Fixed in SoftNAS Cloud® 3.4.9.7

Improved Disk Status Reporting for HA failover - Failover is now triggered if an individual pool becomes unavailable, rather than only during a node failure.

Update Warning - Language added to beginning of update process logs reminding customers that an update can take up to two hours, and not to reboot system.

SoftNAS Cloud 3.4.9.6 Release - March 03, 2017

Overview

SoftNAS Cloud® 3.4.9.6 is a maintenance release containing fixes, and improvements. Version 3.4.9.6 is compatible with all editions of SoftNAS Cloud®.

Upgrading

Upgrading from 3.4.0 through 3.4.9.5

Reboot required for AWS and VMware instances.

Upgrading from 3.3.3 or 3.3.4

Reboot Required for AWS and VMware instances.

Follow instructions to upgrade a highly available SNAP HA™ pair.

Upgrading from versions prior to 3.3.3

1-click upgrades are not supported from versions older than 3.3.3. Follow instructions to migrate, or Contact SoftNAS Support to schedule an upgrade session.

Fixed in SoftNAS Cloud® 3.4.9.6

High Availability IP re-assignment issue - Fixed an issue in which the virtual IP address would not reassign itself to the primary node after a hard failover (ie, shut-down of primary node) and node recovery. This resulted in being unable to connect to CIFS and NFS shares post failover.

SoftNAS Cloud 3.4.9.5 Release - Feb 21, 2017

Overview

SoftNAS Cloud® 3.4.9.5 is a maintenance release containing fixes, and improvements. Version 3.4.9.5 is compatible with all editions of SoftNAS Cloud®.

Upgrading

Upgrading from 3.4.0 through 3.4.9.4

Reboot required for AWS and VMware instances.

WARNING: Due to the size of the 3.4.9.5 update, it can take up to 2 hours for the update to complete. Do NOT terminate the update while in progress else errors may occur. If you feel that your update is taking longer than 2 hours, please contact SoftNAS support for assistance and do not reboot your instance.

Upgrading from 3.3.3 or 3.3.4

Reboot Required for AWS and VMware instances.

Follow instructions to upgrade a highly available SNAP HA™ pair.

WARNING: Due to the size of the 3.4.9.5 update, it can take up to 2 hours for the update to complete. Do NOT terminate the update while in progress else errors may occur. If you feel that your update is taking longer than 2 hours, please contact SoftNAS support for assistance and do not reboot your instance.

Upgrading from versions prior to 3.3.3

1-click upgrades are not supported from versions older than 3.3.3. Follow instructions to migrate, or Contact SoftNAS Support to schedule an upgrade session.

New in SoftNAS Cloud® 3.4.9.5

Improved Disk Status Reporting for HA failover - Failover is now triggered if an individual pool becomes unavailable, rather than only during a node failure.

Sipcalc included in installation package - This allows SoftNAS HA to operate in isolated environments (without access to the internet) without needing to connect externally for sipcalc download.

SnapReplicate Throttling Improvements - Throttling now operates on all streams, rather than a per stream basis, ensuring that total outbound replication is throttled, rather than per individual volumes. Throttling levels update according to available bandwidth based on iptables. Throttling can be enabled and disabled through settings.

Improved logging/support reports - Additional log files added to default list of log files submitted when a support report is generated and sent to SoftNAS support, to make troubleshooting easier.

Fixed in SoftNAS Cloud® 3.4.9.5

NFS Bind Issue causing Client Mount hang fixed - An issue that caused client mounts to hang, and resulted in "stale file handle" errors. This has now been resolved.

Deletion of Disks in Active Pool Prevented - A "loophole" in which it was possible to accidentally delete a disk in an active pool has now been prevented.

Kerberos DNS issue fixed - Fixed an issue hard-coding Kerberos to a single KDC/Admin Server, rather than using DNS lookup to find a KDC/Admin server. This eliminates KDC/Admin Server as a single point of failure.

Hosts File Issue corrected - Fixed a bug in which the etc/hosts file would not return with correct values after a reboot in some cases.

Volume Naming Issue corrected - Users can now create volumes of the same name on different pools.

Snapclone Volume Mount issue fixed - A bug in which volumes created from Snapclones within the UI (but not if mounted from command line) would appear but without data has been resolved.

Consumption-based licensing persistent billing error message resolved - An issue in which the "Can not connect to AWS Billing" error would persist even after connectivity issues were fixed has now been eliminated.

Replication Hang Issue Resolved - Fixed an issue where replication could hang for lengthy periods without an error or notification.

Samba/NFS Failover issue - After a failover, Delta-Sync by design temporarily shuts down Samba and NFS to prevent data loss during a transfer. The ability to restart the service immediately has been introduced.

Premium Disk Raid 0 Pool Creation Error fixed - An erroneous error when creating a RAID 0 pool from P20 512GB Azure disks has been resolved.

Delta-Sync File-mapping issue fixed - An issue in which failures could occur due to Delta-Sync failing to map files correctly to .CSV has been resolved.

VIP mapping failure upon reboot fixed - An issue was occurring when a reboot was performed when HA was deactivated resulting in loss of the VIP(becomes unassigned). This has now been resolved.

Ensured that a reboot prompt is provided after each update.

Log verbiage fix - Improved instructions matching the user interface have been introduced in log messages to resolve SnapReplicate failures.

S3 bucket name fix - Numerical values can now be applied to bucket names.

Errata for SoftNAS Cloud® 3.4.9.5

If updating a SnapReplicate™ pairing to 3.4.9.5 according to the instructions found here, you may run across an error in which SoftNAS Cloud falsely reports SnapReplicate™ as still active, but with the deactivate button to continue the process grayed out.

Recommended Action: If the above occurs, switch to the SnapReplicate/Snap HA tab, and activate and deactivate replication, then return to the update process.

SoftNAS Cloud 3.4.9.4 Release - Dec 21, 2016

Overview

SoftNAS Cloud® 3.4.9.4 is a maintenance release containing fixes, and improvements. Version 3.4.9.4 is compatible with all editions of SoftNAS Cloud®.

Upgrading

Upgrading from 3.4.0 through 3.4.9.2

A reboot is required for any users leveraging cloud disks.

Upgrading from 3.3.3 or 3.3.4

A reboot is required for any users leveraging cloud disks.
Follow instructions to upgrade a highly available SNAP HA™ pair.

Upgrading from versions prior to 3.3.3

1-click upgrades are not supported from versions older than 3.3.3. Follow instructions to migrate, or Contact SoftNAS Support to schedule an upgrade session.

Fixed in SoftNAS Cloud® 3.4.9.4

Auto Failover Issue – Fixed an issue where in some cases auto-failover did not assign the VIP address to the proper interface.

SoftNAS Cloud 3.4.9.3 Release - Nov 21, 2016

Overview

SoftNAS Cloud® 3.4.9.3 is a maintenance release containing fixes, and improvements. Version 3.4.9.3 is compatible with all editions of SoftNAS Cloud®.

Upgrading

Upgrading from 3.4.0 through 3.4.9.2

A reboot is required for any users leveraging cloud disks.

Upgrading from 3.3.3 or 3.3.4

A reboot is required for any users leveraging cloud disks.
Follow instructions to upgrade a highly available SNAP HA™ pair.

Upgrading from versions prior to 3.3.3

1-click upgrades are not supported from versions older than 3.3.3. Follow instructions to migrate, or Contact SoftNAS Support to schedule an upgrade session.

Fixed in SoftNAS Cloud® 3.4.9.2

License Validation bug fix - Fixed an issue in which large storage volumes misrepresented terabytes as gigabytes, resulting in an error mistakenly stating the customer had exceeded his license limit.

SoftNAS Cloud 3.4.9.2 Release - Nov 15, 2016

Overview

SoftNAS Cloud® 3.4.9.2 is a maintenance release containing fixes, and improvements. Version 3.4.9.2 is compatible with all editions of SoftNAS Cloud®.

Upgrading

Upgrading from 3.4.0 through 3.4.9.1

A reboot is required for any users leveraging cloud disks.

Upgrading from 3.3.3 or 3.3.4

A reboot is required for any users leveraging cloud disks.
Follow instructions to upgrade a highly available SNAP HA™ pair.

Upgrading from versions prior to 3.3.3

1-click upgrades are not supported from versions older than 3.3.3. Follow instructions to migrate, or Contact SoftNAS Support to schedule an upgrade session.

New in SoftNAS Cloud® 3.4.9.2

Getting Started Checklist Change - To more accurately reflect the requirement of an email address for notifications and alerts, guidance is changed to create a 'notification email', rather than 'admin email'.

Fixed in SoftNAS Cloud® 3.4.9.2

AWS Directory Service Integration Fix - Fixed bug resulting in Ajax communication error as well as errors in authenticating group permissions.

Errata for SoftNAS Cloud® 3.4.9.2

Error Creating HA Controller - Fixed an issue where the longer instance ID lengths were preventing creation of the HA controller.

SoftNAS Cloud 3.4.9.1 Release - Oct 25, 2016

Overview

SoftNAS Cloud® 3.4.9.1 is a maintenance release containing fixes, and improvements. Version 3.4.9.1 is compatible with all editions of SoftNAS Cloud®.

Upgrading

Upgrading from 3.4.0 through 3.4.9

A reboot is required for any users leveraging cloud disks.

Upgrading from 3.3.3 or 3.3.4

A reboot is required for any users leveraging cloud disks.
Follow instructions to upgrade a highly available SNAP HA™ pair.

Upgrading from versions prior to 3.3.3

1-click upgrades are not supported from versions older than 3.3.3. Follow instructions to migrate, or Contact SoftNAS Support to schedule an upgrade session.

New in SoftNAS Cloud® 3.4.9.1

Ephemeral Disks as Cache for Azure - SoftNAS Cloud can now leverage ephemeral disks as read cache to improve performance on Azure instances.

Case Sensitivity Option/Volume Creation - A checkbox has been provided to allow users to determine whether to apply case sensitivity to a pool.

Selectable Software Updates - Software Updates now shows up to 3 of the latest release versions available for upgrade (if the user has not updated for more than 3 releases), and allows the user to select from between them, based on linked release notes.

Self-Configured Disk Authentication Version Option - In the Add Cloud Disk Extender wizard for Self-Configured Disks, users can now specify the authentication version (v2 or v4) used for the object storage in question.

AWS Billing Gateway Failure to Connect Alert added - FCP customers will now be alerted if the connection to the AWS Billing Gateway fails, and provided a timer in order to know when services will be disconnected.

Support for AWS US East Ohio Region - The AWS/Ohio region is now accessible from within StorageCenter's Add Devices wizard, allowing users to create S3 disks from this region.

HA Validation Pre-Checks - Validations have been added to ensure key HA requirements are all configured prior to SNAP HA setup. These include:

- Access to S3
- Access to a NTP server
- Two ENIs (one for replication traffic, one for heartbeat)
- Checking that each ENI is set to a different subnet
- IAM permissions
- Admin email is validated

Fixed in SoftNAS Cloud® 3.4.9.1

Email Notifications Fix - SoftNAS Cloud no longer attempts to send email notifications to the default email example address of admin@example.com.

Etc./Hosts File Fix - Duplicate 127.0.0.1 entries no longer appear in the hosts file after a reboot.

Importing S3 Disk Fix - If importing an S3 volume and the user specified an incorrect volume size (ie; a smaller size than it was created as), StorageCenter did not alert the user of the issue. This has been corrected.

Email Notification Fix - An unnecessary alert email generated when checking for updates, regardless of whether updates are available, has been downgraded to info status, and will be logged rather than generating an alert email.

Errata for SoftNAS Cloud® 3.4.9.1

On a SnapReplicate pairing of proxy SoftNAS instances, exclusions for the source and target now populate automatically. However, upon deletion of Replication, the source entry should be removed from target exclusion list. This does not occur.

Recommended Action: If deleting replication on a proxied SoftNAS instance, remove source entry exclusion from target manually.

Due to persistent display issues with header elements in Microsoft Edge, we no longer support the browser.

Recommended Action: Open the instance in a supported browser, such as Internet Explorer or Chrome.

In the Available Devices panel of Disk Devices, the Make and Model column presents SoftNAS created Azure disks as "Msft Virtual Disks" rather than "SoftNAS, Azure Virtual Disk". This will be corrected in a later release.

Recommended Action: None

During software update, the Progress Bar may go to 102% for a few seconds prior to completion.

Recommended Action: None.

SoftNAS Cloud 3.4.9 Release - Sept 15, 2016

Overview

Version 3.4.9 is a maintenance release containing critical fixes and improvements. Version 3.4.9 is compatible with all editions of SoftNAS Cloud.

Upgrading

Upgrading from 3.4.0 through 3.4.9

No reboot is required.

Upgrading from 3.3.3 or 3.3.4

No reboot is required.

Follow instructions to upgrade a highly available SNAP HA™ pair.

Upgrading from versions prior to 3.3.3

1-click upgrades are not supported from versions older than 3.3.3. Follow instructions to migrate, or Contact SoftNAS Support to schedule an upgrade session.

Fixed in SoftNAS Cloud® 3.4.9

Fixed NFSv4 bind issue - NFS was not mounting correctly after HA failover events leading to stale file handle errors. This issue has been fixed.

SoftNAS Cloud 3.4.8 Release - Sept 1, 2016

Overview

SoftNAS Cloud® 3.4.8 is a maintenance release containing feature additions, fixes, and improvements. Version 3.4.8 is compatible with all editions of SoftNAS Cloud.

Upgrading

Upgrading from 3.4.0 through 3.4.8

A reboot is required for any users leveraging cloud disks.

Upgrading from 3.3.3 or 3.3.4

A reboot is required for any users leveraging cloud disks.

Follow instructions to upgrade a highly available SNAP HA™ pair.

Upgrading from versions prior to 3.3.3

1-click upgrades are not supported from versions older than 3.3.3. Follow instructions to migrate, or Contact SoftNAS Support to schedule an upgrade session.

New in SoftNAS Cloud® 3.4.8

Azure

Azure Blob Object Storage Support – SoftNAS Cloud® frontends the object based scalable storage provided by Azure Blob Storage to present NFS, CIFS/SMB, iSCSI or AFP file sharing protocols for enterprise workloads. SoftNAS Cloud allows easy workload migrations to the Azure cloud without changing existing application data structures or workflows. Scale NAS deployments to Azure Blob Storage from gigabytes to petabytes.

Azure storage backends for SoftNAS Cloud:

- **Azure Premium Storage** – SSD based block storage for high-performance, I/O intensive workloads.
- **Azure General Purpose Storage** – HDD based block storage for general purpose workloads.
- **Azure Hot Blob Storage** - Object storage optimized for frequent I/O data.
- **Azure Cool Blob Storage** - Object storage optimized for low I/O and low cost (safe-keeping of less frequently accessed file data).

SNAP HA™ – now on Azure – SoftNAS' patent-pending SNAP HA™ allows easy high-availability (HA) and cluster configuration for robust non-stop application operation with automatic failover and seamless transfer across controllers. SNAP HA, combined with Azure availability sets, makes the unique SoftNAS No Storage Downtime Guarantee available for customers using SoftNAS Cloud for Microsoft Azure.

Role-based Access Control (RBAC) – Ensure greater security and control for organizations with multiple users or systems on Microsoft Azure. RBAC allows management of users, roles and permissions to provide defined parameters for delegated administration.

Support Change: As of 3.4.8 softnas does not support launching vms on the Classic Portal. The Azure Resource Manager (ARM) is the only supported platform. Prominent SoftNAS features (notably high availability) will not function on VMs using Classic Portal.

All Platforms

DeltaSync™ – Reduces the Recovery Time Objective (RTO) from days to hours for cluster recovery from a high-availability (HA) failover event.

Fixed in SoftNAS Cloud® 3.4.8

Fixed SnapClone/HA issue - Replicating SnapClones no longer results in an HA degraded state.

False error message removed - The false error message when restoring a pool with LUKS encryption enabled is eliminated.

Fix to SNAP HA wizard on proxy instances - EIP option no longer displays if creating a SNAP HA pairing on a proxy enabled SoftNAS instance.

Error Message fixed - If entering a non-existent pool name into the Create Volume wizard, an error message reading "Creating volume: No such pool: r0_dfaf" will be generated.

S3 Import failure display issue fixed - A disk with 0 bytes no longer displays upon a failed S3 import.

'Total Space Used' stat fixed - Space calculations for block based volumes now display correctly.

Self-Configured Disk bucket error fixed - A bucket error occurring when rebooting a proxy instance using self-configured disks has been eliminated.

Fixed Proxy exclusion list- source and target exclusions for replication now auto-populate correctly before and after replication is disabled/re-enabled.

Fixed Display Issues in Microsoft Edge - Scroll bars within UI elements now display and function properly.

Fixed UI Issue - Text overlapping radial button in LDAP server settings workspace is now correctly placed.

Errata for SoftNAS Cloud® 3.4.8

Errors may occur importing S3 disks that are members of a Storage Pool composed of multiple S3 disks.

Recommended Action: Contact SoftNAS Support to assist if it is necessary to import Storage Pools that span multiple S3 disks.

1 click upgrade feature for versions below 3.3.3 is not functioning in Internet Explorer.

Recommended Action: Perform the operation in Mozilla or Firefox. (3174)

On a SnapReplicate pairing of proxy SoftNAS instances, exclusions for the source and target now populate automatically. However, upon deletion of Replication, the source entry should be removed from target exclusion list. This does not occur.

Recommended Action: If deleting replication on a proxied SoftNAS instance, remove source entry exclusion from target manually.

Due to SSL certificate renewal process, after software update, a failed request error may appear due to browser calling up cached content. Alternatively, the software update complete message may appear twice, followed by a white web page.

Recommended Action: For either issue, refresh the browser (Ctrl +f5) to return to login.

Azure AD password expiry can cause HA and Add Disk failures.

Recommended Action: To disable password expiry, see Azure Documentation.

When importing a deleted pool, the import pool dialog box may not disappear, though the pool imports successfully.

Recommended Action: Verify pool import, and close the dialog box.

Table headers for Disk Devices, Volumes and LUNS, Storage Pool panels may shift out of position/out of sight if you navigate to another area while a task (create/delete) is in process.

Recommended Action: Refresh browser, or log out/log in if this occurs.

SoftNAS login screen can intermittently appear in SoftNAS UI panel rather than in browser if session expires.

Recommended Action: Refresh your browser, login as usual.

Deleting an Azure Blob Disk from an instance via the Azure Portal can cause your SoftNAS instance to become unstable/unresponsive.

Recommended Action: Delete Azure Blob disks from within the SoftNAS UI.

Currently, displayed pool or volume graphs are proportional, which can result in small pools being nearly invisible if presented along with large pools or volumes (for example a 10 GB volume next to a 100 terabyte volume).

SoftNAS Cloud 3.4.7.4 Release - Aug 19, 2016

Overview

Version 3.4.7.4 is a maintenance release containing critical fixes and improvements. Version 3.4.7.4 is compatible with all editions of SoftNAS Cloud. Upgrading to this release is highly recommended for anyone leveraging Cloud Disks.

Upgrading

Upgrading from 3.4.0 through 3.4.7

A reboot is required for any users leveraging cloud disks.

Upgrading from 3.3.3 or 3.3.4

A reboot is required for any users leveraging cloud disks.
Follow instructions to upgrade a highly available SNAP HA™ pair.

Upgrading from versions prior to 3.3.3

1-click upgrades are not supported from versions older than 3.3.3. Follow instructions to migrate, or Contact SoftNAS Support to schedule an upgrade session.

Fixed in SoftNAS Cloud® 3.4.7.4

S3 Cloud Disk Fix - A modification to S3 Cloud disks allows for proper response when the underlying object storage returns a 500 or 503 error.

SoftNAS Cloud 3.4.7.3 Release - Aug 2, 2016

Overview

Version 3.4.7.3 is a maintenance release containing critical fixes and improvements. Version 3.4.7.3 is compatible with all editions of SoftNAS Cloud.

Upgrading

Upgrading from 3.4.0 through 3.4.7

No reboot is required.

Upgrading from 3.3.3 or 3.3.4

No reboot is required.
Follow instructions to upgrade a highly available SNAP HA™ pair.

Upgrading from versions prior to 3.3.3

1-click upgrades are not supported from versions older than 3.3.3. Follow instructions to migrate, or Contact SoftNAS Support to schedule an upgrade session.

Fixed in SoftNAS Cloud® 3.4.7.3

Fix to default settings - Disabled Linux Memory Overcommit.

SoftNAS Cloud 3.4.7.2 Release - June 13, 2016

Overview

Version 3.4.7.2 is a maintenance release containing critical fixes and improvements. Version 3.4.7.2 is compatible with all editions of SoftNAS Cloud.

Upgrading

Upgrading from 3.4.0 through 3.4.7

No reboot is required.

Upgrading from 3.3.3 or 3.3.4

No reboot is required.

Follow instructions to upgrade a highly available SNAP HA™ pair.

Upgrading from versions prior to 3.3.3

1-click upgrades are not supported from versions older than 3.3.3. Follow instructions to migrate, or Contact SoftNAS Support to schedule an upgrade session.

Fixed in SoftNAS Cloud® 3.4.7.2

Fix to Ajax errors - resolved an issue specific to 3.4.7 in which Ajax errors would result when rejoining a domain.

Fix to NFS Exports Functionality - When creating NFS exports, the option to make the export available to everyone was not functioning correctly. This has been resolved.

Fix to NFS Exports bind entries - An issue with NFSv4 bind entries overwriting required entries for NFSv3 compatibility has been fixed.

Fix to AWS VIP routing table - When failing over in an HA setting, an error would occur upon required update of the AWS VIP routing table. This has been resolved.

Fix to SNAP HA deletion error - An error that would occur when attempting to delete a SNAP HA pairing has been resolved.

Fix to Century Link Regional S3 Bucket location error - S3 Buckets placed in US East region would be misplaced to another region. This has been resolved.

SoftNAS Cloud 3.4.7.1 Release - May 23, 2016

Overview

Version 3.4.7.1 is a maintenance release containing critical fixes and improvements. Version 3.4.7.1 is compatible with all editions of SoftNAS Cloud.

Upgrading

Upgrading from 3.4.0 through 3.4.7

No reboot is required.

Upgrading from 3.3.3 or 3.3.4

No reboot is required.

Follow instructions to upgrade a highly available SNAP HA™ pair.

Upgrading from versions prior to 3.3.3

1-click upgrades are not supported from versions older than 3.3.3. Follow instructions to migrate, or Contact SoftNAS Support to schedule an upgrade session.

Fixed in SoftNAS Cloud® 3.4.7.1

VMware S3 Disk Device Errors - Fixed an issue in which S3 disks introduced to VMware instances upgraded to 3.4.7 would result in errors, or would hang. Pre-existing S3 disks (from prior to upgrade) sometimes did not display in the Volumes Table. These issues have been resolved.

SoftNAS Cloud 3.4.7 Release - May 16, 2016

Overview

Version 3.4.7 is a maintenance release containing critical fixes and improvements. Version 3.4.7 is compatible with all editions of SoftNAS Cloud® NAS.

Upgrading

Upgrading from 3.4.0 through 3.4.7

A reboot is required in order to see the benefits of the fixes added in this release. Existing functionality will not be affected pending reboot. SoftNAS recommends upgrading during a maintenance window.

Upgrading from 3.3.3 or 3.3.4

A reboot is required in order to see the benefits of the fixes added in this release. Existing functionality will not be affected pending reboot. SoftNAS recommends upgrading during a maintenance window.

Follow instructions to upgrade a highly available SNAP HA™ pair.

Upgrading from versions prior to 3.3.3

1-click upgrades are not supported from versions older than 3.3.3. Follow instructions to migrate, or [Contact SoftNAS Support](#) to schedule an upgrade session.

HA Patch in SoftNAS Cloud® 3.4.7

HA Hotfix Release to Prevent Spontaneous Failovers and Improve Logging

3.4.7 includes new logic and logging to address an issue seen in previous releases where brief losses of communication between AWS and SoftNAS instances have resulted in unnecessary failovers. These measures will both prevent the unnecessary failovers, and aid SoftNAS in determining root cause.

Fixed in SoftNAS Cloud® 3.4.7

LUN Target Deletion Issue Fixed - Fixed an issue where a deleted target would result in the LUN detaching from other targets.

CIFS Samba Configuration issue fixed - Fixed an issue with user level authentication for CIFS and Active Directory integration.

AWS key error on Proxy instances - Fixed an issue in which EBS and S3 disks added to a SoftNAS instance that was protected by a proxy server would result in an AWS error message. Bucket errors on S3 when connected to a proxy were also resolved.

Software Update via Proxy - Fixed an issue where software updates could not be installed when connected via a proxy.

License Authentication/Proxy issue - Fixed an issue with activating licenses of SoftNAS instances that are installed behind a proxy.

Updates Functionality in Webmin Panel - Users can now perform OS Yum updates from within the Webmin Panel.

Log Message Classification Change - Fixed an HA failure message in SoftNAS logs which was misclassified as a "Warning" rather than an "Error". The message has been changed to:

"Error ---> HA controller is not configured! Using SnapReplicate role instead of HA Controller as authoritative."

Fix to CLI Created Disks - Fixed an issue where disks created in CLI would default to a setting of sync=disabled.

NFS Server Default Thread Count Value- Default thread count logic is improved, and is now based on the amount of available RAM, rather than a set default.

Improved NFS Export Functionality - Users can now add multiple hosts via our Webmin Panel with comma separated values.

Exports and Shares Displaying after Pool Deletion - Fixed an issue in which NFS Exports and AFP Volume Shares would continue to display after a pool was deleted.

Importing S3 disks from Frankfurt Region Resolved - Errata issue identified in 3.4.6 is now resolved. Users can now import S3 disks from Frankfurt without issue.

SMTP Server Authentication - Fixed an issue with SMTP Authentication where windows domain and username were not recognized as valid credentials (ie: domain/username).

Errata for SoftNAS Cloud® 3.4.7

Elastic IP addresses will not work when using a proxy. This option will be removed from the HA configuration wizard in a later release, if a proxy setup is detected.

Recommended Action: If planning to establish high availability and use a proxy server, plan your configuration to make use of Virtual IP addresses in your configuration.

As we are doing a yum update as part of the 3.4.7 update, it could take time to complete. The time varies depending on Instance or VM resources.

Recommended Action: Plan the update for a maintenance window.

A misleading error message is generated if the wrong name is typed into the storage pool field when creating a volume - the error message reads 'Creating Volume: Not enough space at pool test.' It will be changed in an upcoming release to state that the pool specified does not exist.

S3 volumes created and attached as iSCSI LUNs are not displaying the disk use percentage in the Volumes table.

Recommended action: Monitor iSCSI Volumes in the Overview section to avoid running out of disk space.

After upgrading your instance, your instance will refresh. A prompt should appear telling you to reboot your instance. It currently does not.

Recommended Action: Reboot your instance after upgrade.

If running your SoftNAS instance behind a proxy, you may run into issues with running a Yum update on your SoftNAS instance. Certain mirror lists may return a 404 error (not found).

Recommended Action: In the command shell, run the 'yum clean all' command, and then 'yum update' in order to resolve the issue.

If running a SnapReplicate SoftNAS pairing, for replication to occur, the IPs of both paired instances must be added to the proxy's exclusion list manually.

SoftNAS Cloud 3.4.6.2 Release - March 30, 2016

Overview

Version 3.4.6.2 is a maintenance release containing critical fixes and improvements. Version 3.4.6.2 is compatible with all editions of SoftNAS Cloud.

Upgrading

Upgrading from 3.4.0 through 3.4.6

No reboot is required.

Upgrading from 3.3.3 or 3.3.4

No reboot is required.

[Follow instructions to upgrade](#) a highly available SNAP HA™ pair.

Upgrading from versions prior to 3.3.3

1-click upgrades are not supported from versions older than 3.3.3. [Follow instructions to migrate](#), or [Contact SoftNAS Support](#) to schedule an upgrade session.

Fixed in SoftNAS Cloud® 3.4.6.2

AWS JAVA SDK update- Added support for a new reporting API resulting in a minor change to a usage reporting structure.

Version Numbering enhancement - Added support for four-digit version numbers within SoftNAS.

SoftNAS Cloud 3.4.6.1 Release - March 21, 2016

Overview

Version 3.4.6.1 is an optional maintenance release containing upgrades that allow use of AWS' new Flexible Consumption Pricing model. If not switching to the Flexible Consumption Pricing model, this upgrade can be skipped. Version 3.4.6.1 is compatible with all editions of SoftNAS Cloud® NAS.

Upgrading

Upgrading from 3.4.0 through 3.4.6

No reboot is required.

Upgrading from 3.3.3 or 3.3.4

No reboot is required.

[Follow instructions to upgrade](#) a highly available SNAP HA™ pair.

Upgrading from versions prior to 3.3.3

1-click upgrades are not supported from versions older than 3.3.3. [Follow instructions to migrate](#), or [Contact SoftNAS Support](#) to schedule an upgrade session.

Fixed in SoftNAS Cloud® 3.4.6.1

Flexible Consumption Pricing Added- SoftNAS is one of four vendors chosen to be part of the AWS flexible consumption pricing (FCP) launch. This new pricing model, only available via the AWS Marketplace, allows you to scale your software usage up or down without modifying your SoftNAS EC2-based instance and still pay through your AWS Marketplace bill. When your usage changes, your hourly charge changes to match. This means you only pay for the amount of software you need to operate your workloads.

SoftNAS Cloud 3.4.6 Release - March 08, 2016

Overview

Version 3.4.6 is a maintenance release containing critical fixes and improvements. Version 3.4.6 is compatible with all editions of SoftNAS Cloud® NAS.

Upgrading

Upgrading from 3.4.0 through 3.4.6

A number of S3 improvements are included as part of the upgrade. To take full advantage of the S3 improvements, a reboot is required. S3 Cloud Disks will continue to function without a reboot, but at the pre-upgrade level of functionality.

Upgrading from 3.3.3 or 3.3.4

A number of S3 improvements are included as part of the upgrade. To take full advantage of the S3 improvements, a reboot is required. S3 Cloud Disks will continue to function without a reboot, but at the pre-upgrade level of functionality.

[Follow instructions to upgrade](#) a highly available SNAP HA™ pair.

Upgrading from versions prior to 3.3.3

1-click upgrades are not supported from versions older than 3.3.3. [Follow instructions to migrate](#), or [Contact SoftNAS Support](#) to schedule an upgrade session.

Security Patch in SoftNAS Cloud® 3.4.6

Hotfix Release to Resolve Linux Glibc Library Vulnerability

On February 16th, a serious defect was found in the getaddrinfo() library call in glibc. This issue, labelled CVE-2015-7547, allows an attacker to cause buffer overflow to occur, creating the possibility of remote code execution in some circumstances. In order to ensure that SoftNAS instances are not vulnerable to this potentially serious security issue, a hotfix has been created in order to eliminate this risk. If this hotfix has not already been applied, we recommend applying it immediately after your update to 3.4.6, as both the hotfix and update will require a reboot. Performing a single reboot for both patch and update will save significant time. See [\[SoftNAS KB\]: Installing Hotfix for CVE-2015-7547](#) for update instructions.

Fixed in SoftNAS Cloud® 3.4.6

Improvements to the implementation of S3 Cloud Disk Extender: A new High-Performance S3 Block Cache has been implemented that improves performance drastically by caching changes in RAM, then synchronously flushing to S3 media in concert with ZFS filesystem to ensure data integrity. The High-Performance S3 Block Cache replaces the earlier “Block Cache File”, which is deprecated and no longer used or required.

After upgrading to 3.4.6 (or later) and rebooting, it is recommended to delete any unused "s3cachepool" pools that were previously assigned for the block cache file storage, as they are no longer used. The block devices used for these pools can be reassigned as read cache, write log, or decommissioned.

Additionally, after upgrading to 3.4.6, it is necessary to reboot the instance in order for all of the improvements to be installed. S3 Cloud Disks will continue to function, but until the system is rebooted not all of the improvements will have been applied. Reboot is expected to take some time as the software updates are applied, particularly for S3 customers. The time required for the reboot to complete is dependent on the amount of data in the cache, and the speed of your network connection. See **Errata** for more details.

Frankfurt Region HA issue: Fixed an authentication issue preventing HA setup from functioning in the Frankfurt region.

Erroneous Dialog Windows: Fixed an issue in which HA installation would display several unnecessary dialog windows.

AD Domain Field Character Limit: Increased the previously restrictive character limit to 255 characters.

Editing Volumes: Fixed an issue in which if a user attempted to edit a volume, modifying the volume would not complete.

Errata for SoftNAS Cloud® 3.4.6

As stated above, a reboot is required to obtain the improvements to S3 performance. Under certain conditions, this reboot can take a great deal of time. The reboot process performs three basic steps - applying the update,

flushing the cache, then the reboot itself. If using S3 over a slow network connection, flushing the cache can take a long time. It is important NOT to interrupt this process (ie. by a hard boot) or you may lose valuable data.

Recommended Action: To avoid a lengthy reboot process, stop i/o, and wait for the cache to flush prior to performing your reboot. You can determine the amount of data in your cache by opening SoftNAS' dashboard, and viewing **Cache Memory** under the **Performance** tab. Alternatively, monitor the network writes traffic in the **I/O Throughput** panel. When this activity subsides, your reboot should take far less time.

When running a software update on platforms other than AWS an error may be shown in the log: "**curl: (7) couldn't connect to host**".

Recommended Action: It is safe to ignore this error, and the update will complete successfully.

An issue may occur when deleting SoftNAS Cloud Extender disks where the disk continues to appear in the disk devices panel and the Storage Center user interface is unable to be displayed.

Recommended Action: The issue will resolve itself and Storage Center will provide full functionality when the delete operation completes.

The **SoftNAS Dashboard > Performance Panel** does not include all types of filesystem activity in the throughput graph.

Errors may occur importing S3 disks that are members of a Storage Pool composed of multiple S3 disks. SoftNAS Support can assist if it is necessary to import Storage Pools that span multiple S3 disks.

If configured in a SNAP HATM/SnapReplicate configuration, volumes deleted from the primary node are not deleted from the secondary. A takeover initiated from the target node will replicate the volume again.

Recommended Action: If you need to remove the volume and its data permanently, delete the volume from both nodes.

iSCSI targets reconnect after a reboot, but disk devices may not show as available, due to a delay to the start of ZFS services.

Recommended Action: Refresh after a minute or two, and the disks will reappear.

If restoring a pool with LUKS encryption enabled, a false error message may be generated in the logs. The restoration process will successfully restore the selected pool and data.

Recommended Action: No action required, disregard error message.

S3 Imports to the Frankfurt AWS region fail when initiated from the UI.

Recommended Action: If you have the need to import an S3 Bucket in Frankfurt please contact SoftNAS Support.

SoftNAS Cloud 3.4.5 Release - January 13, 2016

Overview

Version 3.4.5 is a maintenance release containing critical fixes and improvements. Version 3.4.5 is compatible with all editions of SoftNAS Cloud® NAS.

Upgrading

Upgrading from 3.4.0 through 3.4.5

No reboot is required.

Upgrading from 3.3.3 or 3.3.4

No reboot is required.

[Follow instructions to upgrade](#) a highly available SNAP HATM pair.

Upgrading from versions prior to 3.3.3

1-click upgrades are not supported from versions older than 3.3.3. [Follow instructions to migrate](#), or [Contact SoftNAS Support](#) to schedule an upgrade session.

Fixed in SoftNAS Cloud® 3.4.5

Nuisance alerts and log messages fixed - A minor issue with SNAP HA™ resulted in unnecessary log messages and nuisance email alerts from the target node has been resolved.

NFS Bind on reboot fixed - A critical issue with remounting NFS bind mounts on reboot has been resolved.

Errata for SoftNAS Cloud® 3.4.5

If updating an instance that has as yet never been updated, there is a known issue where updating from 3.4.4 or earlier to 3.4.5 will hang at 82%, and will seemingly not update.

Recommended Action: The update completes just fine, however you will need to reboot the system, or alternatively, go to Webmin, run the command "service httpd restart", then refresh the browser to see the changes.

Note: Instances newer than 3.4.6 will not see this issue. This issue will also not be seen if the update process has previously been run, for example, if you previously updated from 3.4.3 to 3.4.4. The above issue has also been seen in VMware instances.

SoftNAS Cloud 3.4.4 Release - December 22, 2015

Overview

Version 3.4.4 is a maintenance release containing critical fixes and improvements. Version 3.4.4 is compatible with all editions of SoftNAS® Cloud NAS.

Upgrading

Upgrading from 3.4.0 through 3.4.4

No reboot is required.

Upgrading from 3.3.3 or 3.3.4

No reboot is required.

[Follow instructions to upgrade](#) a highly available SNAP HA™ pair.

Upgrading from versions prior to 3.3.3

1-click upgrades are not supported from versions older than 3.3.3. [Follow instructions to migrate](#), or [Contact SoftNAS Support](#) to schedule an upgrade session.

Fixed in SoftNAS Cloud® 3.4.4

S3 Cloud Disk data integrity fixes - Issues addressed that may result in a degradation of data integrity for S3 Cloud Disks through reboots, upgrades, and power-loss scenarios. All customers using S3 Cloud Disks are strongly encouraged to apply the following steps. Steps 1-3 are required for data integrity. #4 is a performance improvement.

1. Upgrade to 3.4.4.
2. Configure all S3 Cloud Disks to utilize 1 GB block cache file. For new configuration follow directions in Add Cloud Disk Extenders in the Install Guide. For existing configurations [Contact SoftNAS Support](#).
3. Install [the S3 Hotfix](#) to ensure optimal performance and data integrity.
4. Follow [S3 Cloud Disk Best Practices](#) by using VPC Endpoints on AWS.

Resync of data after a high availability failover - A SNAP HA™ pair that had been failed, and repaired did not reliably replicate data to the new target node.

New in SoftNAS Cloud® 3.4.4

New - SoftNAS Cloud AMI is now available in the Korea region, without local Korea S3 bucket support (all other regions supported). Local Korea S3 bucket support coming in a future software update.

Errata for SoftNAS Cloud® 3.4.4

In a high availability configuration, with the Primary instance in a Degraded state, SNAP HA™ may not be able to be deleted through the Delete HA operation on first attempt.

Recommended Action: Log out of the StorageCenter UI. Log back in, and press Delete HA again. Successive Delete HA operations will succeed.

SoftNAS Cloud 3.4.3 Release - December 4, 2015

Overview

Version 3.4.3 fixes a licensing issue in 3.4.0-3.4.2 for SoftNAS Cloud Standard on AWS Marketplace. Version 3.4.3 is compatible with all editions of SoftNAS Cloud® NAS.

Upgrading

Upgrading from 3.4.0 through 3.4.2

No reboot is required.

Upgrading from 3.3.3 or 3.3.4

No reboot is required.

[Follow instructions to upgrade](#) a highly available SNAP HA™ pair.

Upgrading from versions prior to 3.3.3

1-click upgrades are not supported from versions older than 3.3.3. [Follow instructions to migrate](#), or [Contact SoftNAS Support](#) to schedule an upgrade session.

SoftNAS Cloud 3.4.2 Release - November 21, 2015

Overview

Versions 3.4.2 provides additional security to major release version 3.4.0. Version 3.4.2 for all editions of SoftNAS Cloud® NAS is available. Upgrading to version 3.4.2 is highly recommended to address critical feature and security enhancements.

Upgrading

Upgrading from 3.4.0 or 3.4.1

No reboot is required.

Upgrading from 3.3.3 or 3.3.4

No reboot is required.

[Follow instructions to upgrade](#) a highly available SNAP HA™ pair.

Upgrading from versions prior to 3.3.3

1-click upgrades are not supported from versions older than 3.3.3. [Follow instructions to migrate](#), or [Contact SoftNAS Support](#) to schedule an upgrade session.

Security Update in SoftNAS Cloud® 3.4.2

Security Update to Resolve Severe SoftNAS StorageCenter Security Vulnerability on Open Networks

This security update resolves a potentially severe security vulnerability in the SoftNAS StorageCenter Apache web server that could allow remote code execution when combined with other attacks over an unprotected network such as the Internet. An attacker who successfully exploited the vulnerability could run arbitrary commands on the storage appliance. Customers who have properly restricted Internet-based access to StorageCenter using the recommend best practices that limit StorageCenter access to a limited number of approved IP addresses or that isolate StorageCenter access to private networks, are less likely to be impacted than those who provide open Internet-based StorageCenter access (which is never recommended).

This security update addresses the vulnerability by closing exploits in Apache web server.

New in SoftNAS Cloud® 3.4.0

360-degree Encryption™ – Data encryption all the time—at rest and in flight. Data-at-rest is encrypted through open source Linux Unified Key Setup (LUKS). LUKS is accepted as the standard for encryption of stored data. Data-in-flight is encrypted for CIFS and NFS file protocols.

Apple File Protocol Support – Apple File Protocol (AFP) offers file services for Mac OS X. Now Mac users can consolidate time machine backups and search for files with Spotlight when using SoftNAS with AFP for centralized storage.

Dual Factor Authentication – Prevent unauthorized access to SoftNAS management console with two-step authentication for SoftNAS StorageCenter™ through Google Authenticator.

Login Protection from Bots – Human verification through Google reCAPTCHA prevents bots from programmatically gaining access to the SoftNAS management console.

Red Hat AMI on AWS – SoftNAS Cloud for Red Hat Enterprise Linux (RHEL) is now available as a separate RHEL 7 AMI on AWS Marketplace.

Hitachi Data Systems S3 Support – Easily add Hitachi Content Platform (HCP) within StorageCenter to provide file services for Hitachi object storage.

Active Directory Integration Improvements – Trusted Active Directory Domains, user searches and domains with up to 1.35 million objects now supported.

Fixed in SoftNAS Cloud® 3.4.0

Key fixes to improve the SoftNAS experience include:

- Alert system improved to decrease the number of generated emails
- Software upgrade fixed to work with HA
- 1-click software upgrade is restricted to version 3.3.0 and newer
- GUID Partition Tables (GPT) on S3 devices could have been corrupted when upgrading from versions older than 3.3.0.
- Adding 16TB EBS Volumes is now supported from StorageCenter
- IAM improved to be more restrictive
- Samba configuration file preserved across software updates
- Product Registration prompts 7 days after product launch
- NTP configurable for HA
- File permissions synchronize across CIFS shares and NFS exports
- StorageCenter no longer randomly logs out user sessions
- EULA “agree” button fixed to be accessible in FireFox 39.03

Errata for SoftNAS Cloud 3.4.0 - 3.4.2

Due to a number of factors, SoftNAS instances may increase resource consumption when moving from POC to Production. Planning for production instances should reflect this by planning for these higher resource requirements. Examples where higher resources are needed include: increased IO load, replacing local storage such as EBS with S3, enabling SnapReplication, scheduling backups.

Recommended Action: Plan scale-out to production by anticipating the need to use larger instances and more resources for the SoftNAS VM.

S3 based Storage Pools continue to grow over time, which can affect S3 bucket usage.

Recommended Action: Contact Support for the patch for Trim/Discard.

SnapReplicate does not replicate SnapClones. The Event Log reports not transferring SnapClones as an error.

Recommended Action: Be aware that SnapClone data is not protected with SnapReplication and HA.

Log files sent by Support Report can fail when too large. Failure is indicated by a pop-up status “Failure: Ajax communication failed”.

Recommended Action: Contact Support to transfer log files through FTP.

Users are allowed through StorageCenter UI to remove disk devices from newly created storage pools, even when files are stored in a pool.

Recommended Action: After creating a storage pool, close and reopen the Disk Devices tab before taking any action on devices in the tab.

EBS Volumes may be incorrectly shown as Internal Devices in the Disk Devices tab if created added from the AWS console while other devices are added from StorageCenter.

Recommended Action: Do not add disk devices from StorageCenter and AWS console at the same time.

Errant error message is shown for loading AFP in SnapReplicate event log. The errant message can be viewed in the Events section of Replication Control Panel, "ERROR: AFP Netatalk service failed to reload in remote node...".

Recommended Action: The message is invalid. Ignore.

Refreshing the SnapReplicate tab when connected through RDP will cause the UI frames to scroll to right.

Recommended Action: The issue is cosmetic only. Avoid continual refreshes of the SnapReplicate tab when connected to the UI through RDP.

UI has compatibility issues with FireFox version 41.0.1. A specific example is that the "Next" button on SnapReplicate wizard does not get enabled.

Recommended Action: Use earlier version of FireFox such as 40.0.3 or another browser such as Internet Explorer, Chrome, Safari.

In General System Settings, the webmin screen lists NFS Exports twice under Networking. NFS v4 and v3 are supported, and are shown here as separate selections.

Recommended Action: Select each NFS Exports option to find the version interested in.

In the CIFS Shares Tab, Security and Access a user can be selected multiple times.

Recommended Action: Avoid selecting a user more than once.

On the Microsoft Azure platform, a disk device that has been assigned to a storage pool may be listed as Ready to Assign in Disk Devices.

Recommended Action: Take care with SoftNAS on Azure, to assign a disk device to a storage pool only once.

Storage Pools with a mix of encrypted and unencrypted S3 buckets are not recommended.

Issues are noted when deleting mixed encryption S3 pools.

Recommended Action: Do not mix Storage Pools with encrypted and unencrypted S3 buckets. If such pools are deleted, reboot to access StorageCenter UI.

The Disk Devices tab in StorageCenter does not update status for S3 devices when the S3 devices are deleted from the AWS console.

Recommended Action: Don't delete devices from the AWS Console that are in use. Delete S3 devices from StorageCenter Disk Devices before deleting from AWS Console.

In a storage pool with S3 devices, when a hot spare condition occurs from a spare S3 device, StorageCenter UI may be unresponsive.

Recommended Action: Due to the highly durable nature of object storage, using hot spares in an S3-based storage pool is not recommended. Reboot instance if the UI is found unresponsive when using S3 hot spares.

Deleting a target for an iSCSI share with multiple targets may cause all targets to become disconnected from that iSCSI share.

Recommended Action: Reconnect any targets from the iSCSI LUN Targets tab.

Connecting to an iSCSI LUN may cause an errant device to appear in the Disk Devices tab. Device shows up as 0 bytes and needing to be un-mounted.

Recommended Action: Avoid cleaning up or using 0 byte disk devices in the Disk Devices tab.

Storage Pools protected with RAID 6 report Usable Capacity incorrectly by using the raw capacity value. Licensing is impacted.

Recommended Action: RAID 6 usable capacity is determined by subtracting 2 disks' capacity from a Storage Pool's raw capacity. Contact Support to obtain a larger license key.

SoftNAS Cloud® 3.4.0 Release - November 10, 2015

Overview

SoftNAS Cloud® 3.4.0 is a maintenance release containing feature additions, fixes, and improvements.

Upgrading

Upgrading from 3.3.3 or 3.3.4:

No reboot is required.

Upgrading from versions prior to 3.3.3

1-click upgrades are not supported from versions older than 3.3.3. [Follow instructions to migrate.](#)

New in SoftNAS Cloud® 3.4.0

360-degree Encryption™ – Data encryption all the time—at rest and in flight. Data-at-rest is encrypted through open source Linux Unified Key Setup (LUKS). LUKS is accepted as the standard for encryption of stored data. Data-in-flight is encrypted for CIFS and NFS file protocols.

Apple File Protocol Support – Apple File Protocol (AFP) offers file services for Mac OS X. Now Mac users can consolidate time machine backups and search for files with Spotlight when using SoftNAS with AFP for centralized storage.

Dual Factor Authentication – Prevent unauthorized access to SoftNAS management console with two-step authentication for SoftNAS StorageCenter™ through Google Authenticator.

Login Protection from Bots – Human verification through Google reCAPTCHA prevents bots from programmatically gaining access to the SoftNAS management console.

Red Hat AMI on AWS – SoftNAS Cloud for Red Hat Enterprise Linux (RHEL) is now available as a separate RHEL 7 AMI on AWS Marketplace.

Hitachi Data Systems S3 Support – Easily add Hitachi Content Platform (HCP) within StorageCenter to provide file services for Hitachi object storage.

Active Directory Integration Improvements– Trusted Active Directory Domains, user searches and domains with up to 1.35 million objects now supported.

Fixed in SoftNAS Cloud® 3.4.0

Key fixes include:

- Alert system improved to decrease the number of generated emails
- Software upgrade fixed to work with HA
- 1-click software upgrade is restricted to version 3.3.0 and newer
- GUID Partition Tables (GPT) on S3 devices could have been corrupted when upgrading from versions older than 3.3.0.
- Adding 16TB EBS Volumes is now supported from StorageCenter
- IAM improved to be more restrictive
- Samba configuration file preserved across software updates
- Product Registration prompts 7 days after product launch
- NTP configurable for HA
- File permissions synchronize across CIFS shares and NFS exports
- StorageCenter no longer randomly logs out user sessions
- EULA “agree” button fixed to be accessible in FireFox 39.03

Errata for SoftNAS Cloud® 3.4.0

Due to a number of factors, SoftNAS instances may increase resource consumption when moving from POC to Production. Planning for production instances should reflect this by planning for these higher resource requirements. Examples where higher resources are needed include: increased IO load, replacing local storage such as EBS with S3, enabling SnapReplication, scheduling backups.

Recommended Action: Plan scale-out to production by anticipating the need to use larger instances and more resources for the SoftNAS VM.

S3 based Storage Pools continue to grow over time, which can affect S3 bucket usage.

Recommended Action: Contact Support for the patch for Trim/Discard.

SnapReplicate does not replicate SnapClones. The Event Log reports not transferring SnapClones as an error.

Recommended Action: Be aware that SnapClone data is not protected with SnapReplication and HA.

Log files sent by Support Report can fail when too large. Failure is indicated by a pop-up status "Failure: Ajax communication failed".

Recommended Action: Contact Support to transfer log files through FTP.

Users are allowed through StorageCenter UI to remove disk devices from newly created storage pools, even when files are stored in a pool.

Recommended Action: After creating a storage pool, close and reopen the Disk Devices tab before taking any action on devices in the tab.

EBS Volumes may be incorrectly shown as Internal Devices in the Disk Devices tab if created added from the AWS console while other devices are added from StorageCenter.

Recommended Action: Do not add disk devices from StorageCenter and AWS console at the same time.

Errant error message is shown for loading AFP in SnapReplicate event log. The errant message can be viewed in the Events section of Replication Control Panel, "ERROR: AFP Netatalk service failed to reload in remote node...".

Recommended Action: The message is invalid. Ignore.

Refreshing the SnapReplicate tab when connected through RDP will cause the UI frames to scroll to right.

Recommended Action: The issue is cosmetic only. Avoid continual refreshes of the SnapReplicate tab when connected to the UI through RDP.

UI has compatibility issues with FireFox version 41.0.1. A specific example is that the "Next" button on SnapReplicate wizard does not get enabled. **Recommended Action:** Use earlier version of FireFox such as 40.0.3 or another browser such as Internet Explorer, Chrome, Safari.

In General System Settings, the webmin screen lists NFS Exports twice under Networking. NFS v4 and v3 are supported, and are shown here as separate selections.

Recommended Action: Select each NFS Exports option to find the version interested in.

In the CIFS Shares Tab, Security and Access a user can be selected multiple times.

Recommended Action: Avoid selecting a user more than once.

On the Microsoft Azure platform, a disk device that has been assigned to a storage pool may be listed as Ready to Assign in Disk Devices.

Recommended Action: Take care with SoftNAS on Azure, to assign a disk device to a storage pool only once.

Storage Pools with a mix of encrypted and unencrypted S3 buckets are not recommended.

Issues are noted when deleting mixed encryption S3 pools.

Recommended Action: Do not mix Storage Pools with encrypted and unencrypted S3 buckets. If such pools are deleted, reboot to access StorageCenter UI.

The Disk Devices tab in StorageCenter does not update status for S3 devices when the S3 devices are deleted from the AWS console.

Recommended Action: Do not delete devices from the AWS Console that are in use. Delete S3 devices from StorageCenter Disk Devices before deleting from AWS Console.

In a storage pool with S3 devices, when a hot spare condition occurs from a spare S3 device, StorageCenter UI may be unresponsive.

Recommended Action: Due to the highly durable nature of object storage, using hot spares in an S3- based storage pool is not recommended. Reboot instance if the UI is found unresponsive when using S3 hot spares.

Configuring Storage Pools with encrypted S3 devices protected with RAID 5 may require a reboot to access StorageCenter.

Recommended Action: Due the highly durable nature of object storage, using RAID with S3-based storage pool is not recommended. Reboot instance if the UI is found unresponsive when using encrypted S3 with RAID 5.

Deleting a target for an iSCSI share with multiple targets may cause all targets to become disconnected from that iSCSI share.

Recommended Action: Reconnect any targets from the iSCSI LUN Targets tab.

Connecting to an iSCSI LUN may cause an errant device to appear in the Disk Devices tab. Device shows up as 0 bytes and needing to be un-mounted.

Recommended Action: Avoid cleaning up or using 0 byte disk devices in the Disk Devices tab.

An iSCSI LUN exported by SoftNAS to VMware ESXi will not automatically reconnect after the SoftNAS VM is rebooted.

Recommended Action: In StorageCenter, navigate to the tab iSCSI LUN Targets. Select the target and click **Add a new iSCSI**.

Storage Pools protected with RAID 6 report Usable Capacity incorrectly by using the raw capacity value. Licensing is impacted.

Recommended Action: RAID 6 usable capacity is determined by subtracting 2 disks' capacity from a Storage Pool's raw capacity. Contact Support to obtain a larger license key.

SoftNAS Cloud® Features and Benefits

SoftNAS Cloud® is available in the cloud for **Amazon Web Services, Century Link, and Azure** platforms, and as an on-premise solution for **VMware**. Each platform offers the following features and benefits:

- Deduplication & Compression
- Industry-standard file-sharing protocols including iSCSI, NFS and CIFS
- High-performance, multi-tier caching (RAM and SSD)
- Scheduled snapshots via copy-on-write filesystem (**ZFS**)
- Thin provisioning
- Block replication through patent-pending **SnapReplicate** technology
- Data integrity through built-in error detection and correction
- Software and hardware RAID support

Reliable

SoftNAS Cloud® is built on proven, industry-standard platforms like VMware, Linux and **ZFS** for a solid and reliable foundation.

- Rapid Recovery
- Data Integrity & Data Protection
- Error Detection & Correction
- Data is always safe, protected, and available

Robust Features

The commercial-grade feature set previously found only on cumbersome, expensive NAS appliances is now available as a robust software solution regardless of company size and budget.

Private HA with 100% Uptime SLA - highly available virtual IP addressing across AWS availability zones enabling failover of NAS services across zones within a VPC and delivering the only **No Downtime Guarantee SLA** for AWS shared file storage. Azure HA provides the same **No Downtime Guarantee SLA**, provided your two nodes are within an Azure availability set.

Bumpless HA Failovers - NAS services fail over seamlessly across zones, providing uninterrupted CIFS and NFS client access to shared storage

Multi-tenant HA Reliability - detection, filtering and prevention of sporadic HA failovers due to noisy neighbors, zone stresses and sporadic network anomalies occurring infrequently within heavily loaded multi-tenant AWS zones or Azure availability sets.

Secure VPC Networking - secure NAS storage access routing within VPCs with complex routing tables and subnets

High-performance, highly-durable S3 Cloud Disks - RAM write-cache with transactional integrity providing up to hundreds of MB/second throughput with high durability, even in the face of disruptions and instance failures.

High-performance, highly durable Cloud Disks leveraging Azure Blob Storage - On Azure SoftNAS instances, the same RAM write-cache and transactional integrity is provided as for S3 and other Cloud Disk providers. With Azure Blob support, storage is no longer tied to the size of the Azure VM size selected. SoftNAS can leverage up to 16 Petabytes of Azure Blob Storage through multiple blob storage accounts (500 terabytes per storage account).

Hot and Cool Azure Blob Storage Support - Azure blob storage accounts are set as either hot or cool storage upon creation. Storage added via these storage accounts is either hot or cool based on the account used. SoftNAS fully supports and provisions each type, ensuring you get the type of storage you need.

- **Azure Cool Storage** - Object storage that allows economical safe-keeping of less frequently accessed file data.
- **Azure Hot Storage** - Object storage that optimizes frequently accessed stored data to enable continuous IO.

IAM Role-based Security - Use of IAM roles provide least privilege access control and management, without use of access keys for HA setup and S3 cloud disks

Azure RBAC support - Azure Role-Based Access Control (RBAC) enables fine-grained access management for Azure. Using RBAC, you can grant only the amount of access that users need to perform their jobs.

360-degree encryption - supports encryption in flight and at rest to meet security and regulatory requirements

DeltaSync™ – Reduces the Recovery Time Objective (RTO) from days to hours for cluster recovery from a high-availability (HA) failover event.

Lowest Cost

SoftNAS Cloud® is the lowest-cost, most flexible NAS software solution, affordable enough for any small- to medium-sized business, and still powerful enough to scale to enterprise level.

No Training Needed

SoftNAS makes it easy to get started without time-consuming, expensive training courses. Knowledge base and helpdesk resources are available from the day of download.

High Performance

Improving any organization's productivity and streamlining business-critical requirements with:

- Up to 10,000 IOPS on Amazon EC2
- 10,000's IOPS on VMware with SSD caching
- Multiple layers of read and write caching
- High-performance capabilities make applications run at top speeds

Easy to Implement

Zero to NAS in record time.

- Operate with existing and off-the-shelf server hardware with affordable, commodity disk drives
- Re-use existing server hardware
- Quickly download and install **SoftNAS Cloud®** to rapidly create a full-featured NAS.
- Use existing equipment or run a NAS through the cloud with:
 - Amazon EC2
 - Microsoft Azure
 - VMware vSphere

Support

Online Help and Documentation

SoftNAS offers indepth documentation on their website. Simply go to softnas.com, select **Support**, and click [Documentation](#). You can also access [Online Help](#) from softnas.com/helpdesk. From the helpdesk, you can not only create support tickets, but also search an ever growing list of knowledge base articles. Help us help you! [Request new features](#) from the SoftNAS team.

- This option can also be accessed at any time in the top right of the StorageCenter UI.

Register for Premium Support

SoftNAS Cloud® subscribers who register the product will receive access to premium support levels, even during trial periods.

- [Registering SoftNAS Cloud®](#)

SoftNAS Cloud® subscribers have the following support options:

- **Regular Phone Support:** Contact the helpdesk by phone 24/7 or during regular business hours 9 a.m. to 5 p.m. CST, Monday through Friday.
- **Helpdesk Tickets:** Open a help desk ticket for issue tracking and faster support.
- **Email Support:** Email our support team (they will open a help desk ticket).

Support for Free Trial SoftNAS Cloud® Subscribers

Free Trial subscribers have the following support options:

- [SoftNAS Cloud® Knowledge Base](#)
- [Call our Support Line](#)
- [Visit our HelpDesk](#) or [Email Us](#)

Pre-Sales Support Forums

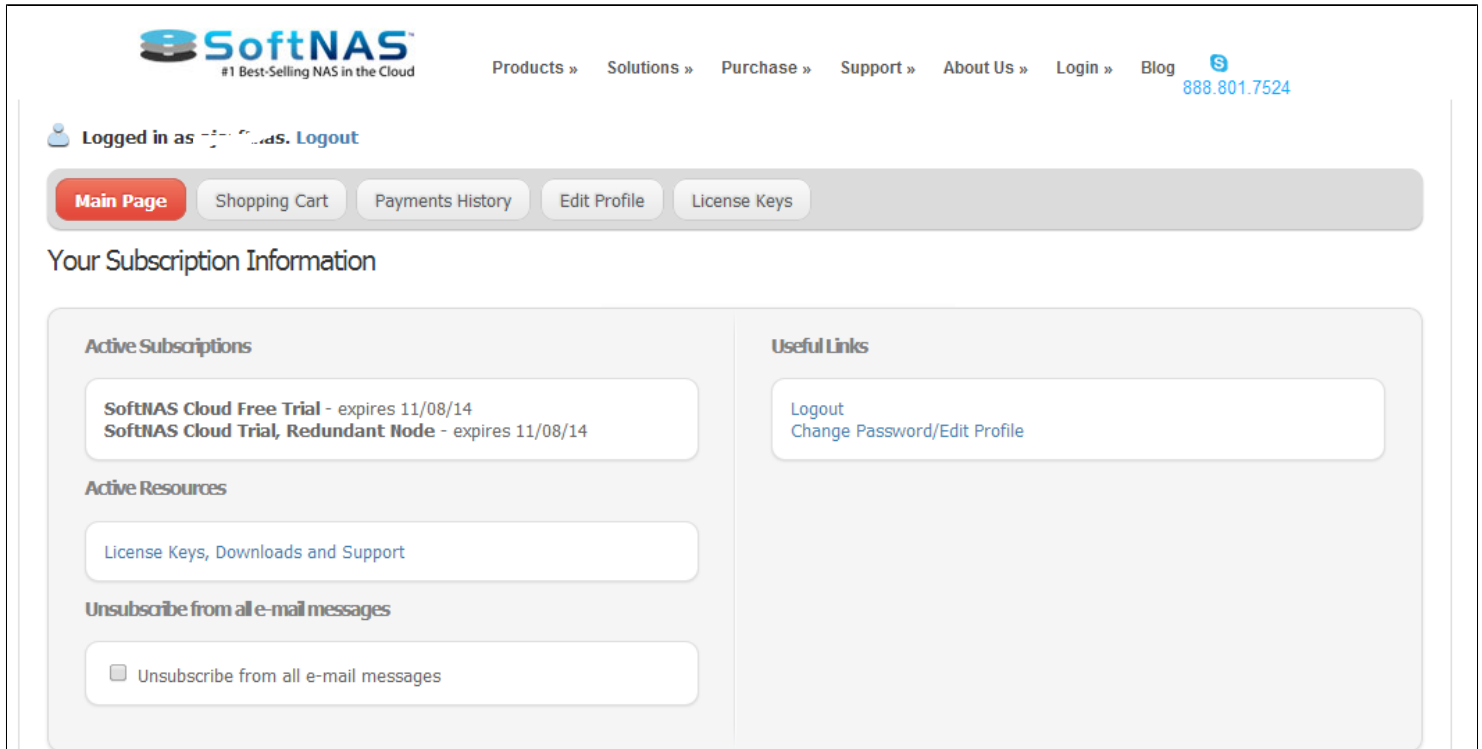
Still researching and deciding? Visit our pre-sales support forums.

- [Pre-Sales Support Forums](#)

Accessing Premium Support Services

1. Log in to [SoftNAS customer account](#).

SoftNAS membership page will be displayed.

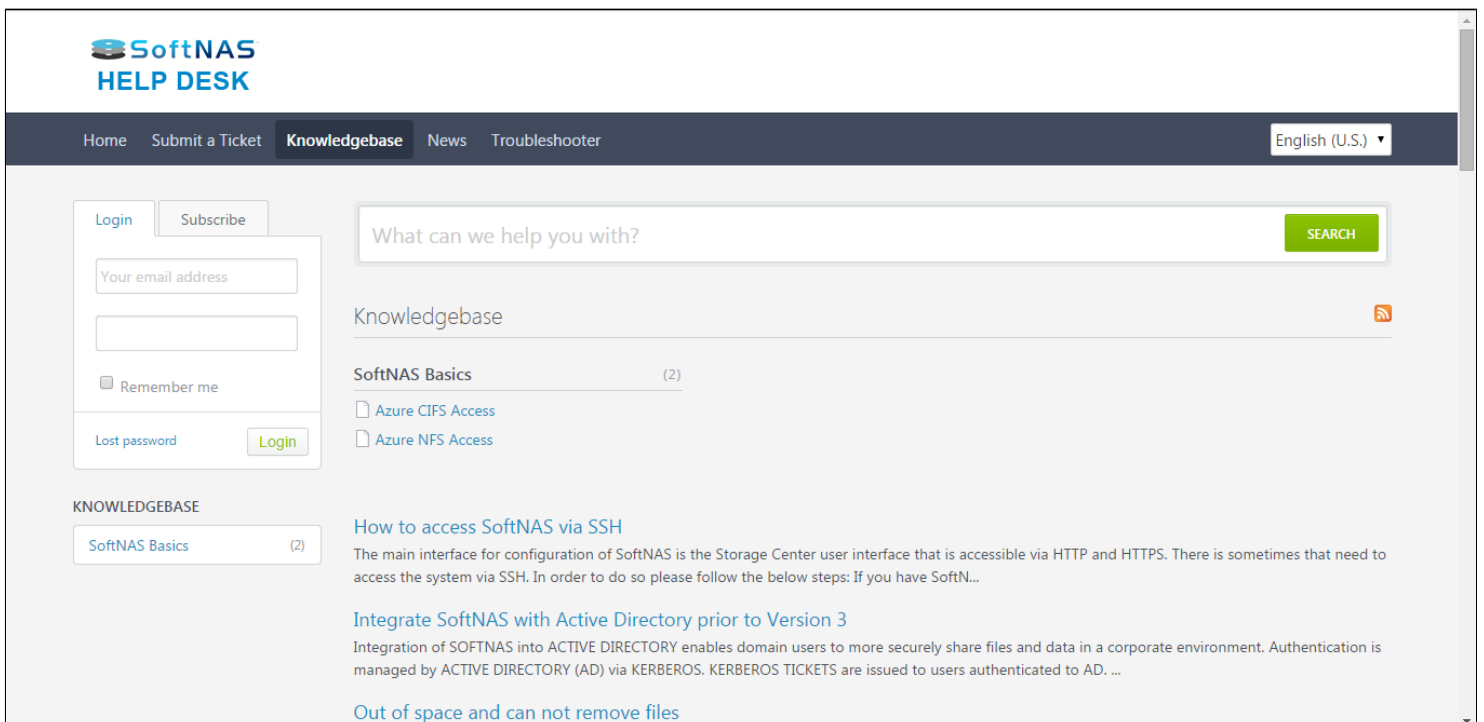


2. Click the **License Keys** tab to access Premium Support services.

Accessing Customer Knowledge Base

All **SoftNAS Cloud®** customers can access the customer knowledge base via the following link.

- [Customer Knowledge Base](#)



Deployment Checklist

0 to SoftNAS Cloud® in 4 Easy Steps:
Plan, Launch, Connect, & Configure.

1. Plan

Review and understand System Requirements for the desired platform.

- [Amazon Web Services EC2](#)
- [Microsoft Azure](#)
- [VMware vSphere](#)

Review and understand NAS Best Practices

- [Performance Considerations](#)
- [RAID Considerations](#)
- [S3 Cloud Disk Best Practices](#)
- [Networking](#)
- [Security](#)

2. Launch

Launch SoftNAS Cloud® on a supported platform

- [Amazon Web Services EC2](#)
- [Microsoft Azure](#)
- [VMware vSphere](#)

3. Connect

Connect to SoftNAS StorageCenter

- [Accessing SoftNAS StorageCenter](#)
- [SoftNAS Cloud® Disk Overview](#)
- [Sharing Volumes over a Network](#)

4. Configure

Configure SoftNAS Cloud® using SoftNAS StorageCenter

- [Configuring SoftNAS StorageCenter](#)
- [Create a Storage Pool](#)
- [iSCSI LUNs and Targets](#)
- [Snapshots in StorageCenter](#)
- [Advanced/Performance Configuration](#)
- [Troubleshooting](#)
- [Setting Up SnapReplicate and SNAP HA™](#)

SoftNAS Cloud Performance Best Practices

The following sections provide a high-level overview of the concepts to understand before getting started with any SoftNAS Cloud® installation and configuration.

Performance Best Practices

The tradeoffs between cost and performance can be significant, so understanding actual, initial performance needs, plus contingency plans to address growth in those needs over time, is important when designing a SoftNAS Cloud® solution.

[Performance Considerations](#)

[RAID Considerations](#)

[Common Performance Use Cases](#)

[S3 Cloud Disk Best Practices](#)

Disk Management & Network Best Practices

SoftNAS Cloud® supports a broad range of data disk formats based on supported platform vendor. For on-premise installations, the following data disk formats are supported:

- Virtual hard disks (VMDK), as well as all VMware-supported datastores including local disks, fiber-channel SAN, iSCSI SAN, and dual path disks.
- SSD, SATA/SAS, HDD disk devices, including Hybrid Storage Pools

For cloud-based offerings, **SoftNAS Cloud®** supports the following disk formats:

- **EBS disks** from Amazon EC2
- [Amazon S3 Disks](#) from Amazon EC2

[Networking Best Practices](#)

[Security Best Practices](#)

Performance Considerations

To get the best performance out of **SoftNAS Cloud®**, in either on-premise or cloud-based solutions, consult and remember these best practices.

Best Practices

As with any storage system, **NAS performance** is a function of a number of many different combined factors:

- Cache memory (first level read cache or ARC)
- 2nd level cache (e.g., L2ARC) speed
- Disk drive speed and the chosen RAID configuration
- Disk controller and protocol

Cache Memory (first level)

Solid state disk (SSD) and PCIe flash cache cards offer high-speed read caching and transaction logging for synchronous writes. However, not all SSDs are created equal and some are better for these tasks than others. In particular, pay close attention to the specifications regarding 4K IOPS.

For read caching (L2ARC), both read and write IOPS matter, as do the sequential throughput specifications of the device. For running a database, VMware VMDK, or other workloads that produce large amounts of random, small (e.g., 4KB) reads and writes, then ensure the SSD and flash cache devices provide high IOPS for 4K reads/writes.

For the write log (ZIL), extremely fast write IOPS is most important (the ZIL is only read after a power failure or other outage event to replay synchronous write transactions that may not have been posted prior to the outage, so write IOPS is most critical for use as a ZIL). **ZFS** always uses a ZIL (unless the variable set "sync=disabled"). By default, the ZIL uses the devices which comprise the storage pool. An "SLOG" device (called a "Write Log" in **SoftNAS Cloud®**) offloads the ZIL from the main pool to a separate log device, which improves performance when the right log device is chosen and configured properly.

2nd Level Read Cache

To further improve read and query performance, configure a Read Cache device for use with **SoftNAS Cloud®**. **SoftNAS Cloud®** leverages the **ZFS** "L2ARC" as its second level cache.

Cloud-based Read Cache

For cloud-based deployments, choose an instance type which includes local solid state disk (SSD) disks. The storage server will make use of as much read cache as it has been provided. Read cache devices can be added and removed at any time with no risk of data loss to an existing storage pool.

For many cloud vendors, there are two choices for SSD read cache:

- 1) Local SSD - this is the fastest read cache available, as the local SSDs are directly attached to each instance and typically provide up to 120,000 IOPS
- 2) Block storage Provisioned IOPS - these volumes can be assigned to SSD, providing a specified level of guaranteed IOPS

On-Premise Read Cache

For on-premise deployments, add one or more SSD devices to the local storage server. Use of a properly-designed read cache is essential to get the IOPS and throughput for database, VDI, vMotion and other workloads comprised primarily of small I/O operations (e.g., lots of small files, VMDKs, database transactions, etc.)

Write Log

The "write log" on **SoftNAS Cloud®** leverages the **ZFS** Intent Log (ZIL). The ZIL is a "transaction log" used to record **synchronous writes** (not asynchronous writes). When **SoftNAS Cloud®** receives synchronous write requests, before returning to the caller, **ZFS** first records the write in memory and then completes the write to the ZIL. By default, the ZIL is located on the same persistent storage associated with the storage pool (e.g., spinning disk media). Once the write is recorded in the ZIL, the synchronous write is completed and the NFS, CIFS or iSCSI request returns to the caller.

To increase performance of synchronous writes, add a separate write log (sometimes referred to as a "SLOG") device, as discussed in the Read Cache section above. A separate write log device enables **ZFS** to quickly store synchronous write data and return to the caller.

Note: This write log is only actually referenced in the event of a power failure or VM / instance crash, to replay the transactions that were not committed prior to the outage event. Writes remain in RAM cache, to satisfy subsequent read requests and to write to stage to permanent storage during normal transaction processing (every 5 seconds by default).

Cloud-based Deployments

Note: Do not use local SSD or ephemeral disks attached directly to an instance for the write log, as these instance local devices are not guaranteed to be available again after reboot. Instead, use volumes with Provisioned IOPS for the Write Log (it's okay to use local SSD devices for Read Cache).

Disk Controller Considerations

There are several ways to get the most performance from these cache devices by following a few disk controller best practices:

Pass-through Controller

In this configuration, the disk controller is passed through to the **SoftNAS Cloud® VM**. This enables the **SoftNAS Cloud® OS** to directly interact with the disk controller. This provides the best possible performance, but requires CPUs and motherboards which support Intel VT-d and disk controllers supported by CentOS operating system.

Note: For servers with the disk controller built into the motherboard, it is now common to install a virtual platform and then boot from USB, freeing up the disk controller for pass-through use.

PCIe Flash Cache Cards

There are flash memory plug-in cards with extremely fast NAND memory available in PCIe form. These make extremely fast memory available at high speeds through the PCIe bus. Be sure to choose a PCIe flash memory card that is supported by the hardware's virtualization vendor.

Raw Device Mapping

Some SSD devices can be mapped directly to the **SoftNAS Cloud® VM** using **Raw Device Mapping (RDM)**. Raw device access allows SCSI commands to flow directly between the **SoftNAS CentOS** operating system and the SSD device for peak cache performance and IOPS, and to reduce context-switching between the **SoftNAS Cloud® VM** running CentOS and the virtualization host.

Disk controller pass-through is preferred to RDM on systems with processors and configurations that support it.

Disk Speed and RAID

Virtual Devices and IOPS

As **SoftNAS Cloud®** is built atop of **ZFS**, IOPS (I/O per second) are mostly a factor of the number of virtual devices (vdevs) in a zpool. They are not a factor of the raw number of disks in the zpool. This is probably the single most important thing to realize and understand, and is commonly not. A vdev is a “virtual device”. A Virtual Device is a single device/partition that act as a source for storage on which a pool can be created. For example, in VMware, each vdev can be a VMDK or raw disk device assigned to the **SoftNAS Cloud® VM**.

A multi-device or multi-partition vdev can be in one of the following shapes:

Stripe (technically, each chunk of a stripe is its own vdev)

- Mirror
- RaidZ
- A dynamic stripe of multiple mirror and/or RaidZ child vdevs

ZFS stripes writes across vdevs (not individual disks). A vdev is typically IOPS bound to the speed of the slowest disk within it. So if with one vdev of 100 disks, a zpool's raw IOPS potential is effectively only a single disk, not 100.

If the environment utilizes a hardware RAID which presents a unified datastore to VMware then the actual striping of writes occurs in the RAID controller card. Just be aware of where striping occurs and the implications on performance (especially for write throughput).

For information about RAID, see section [RAID Considerations](#).

Deduplication

A common misunderstanding is that **ZFS** deduplication is free, which can enable space savings on a **ZFS** filesystems/zvols/zpools. In actuality, **ZFS** deduplication is performance on-the-fly as data is read and written. This can lead to a significant and sometimes unexpectedly high RAM requirement.

Every block of data in a deduplicated filesystem can end up having an entry in a database known as the DDT (DeDupe Table). DDT entries need RAM. It is not uncommon for DDTs to grow to sizes larger than available RAM on zpools that aren't even that large (couple of TBs). If the hits against the DDT aren't being serviced primarily from RAM (or fast SSD configured as L2ARC), performance quickly drops to abysmal levels. Because enabling/disabling deduplication within **ZFS** doesn't actually do anything to the data already committed on disk, it recommended to not enable deduplication without a full understanding of its RAM and caching requirements. It may be difficult to get rid of later, after many terabytes of deduplicated data are already written to disk and suddenly the network needs more RAM and/or cache. Plan cache and RAM needs around how much total deduplicated data is expected.

Note: A general rule of thumb is to provide at least 2 GB of DDT per TB of deduplicated data (actual results will vary based on how much duplication of data is required).

Please note that the DDT tables require RAM beyond whatever is needed for caching of data, so be sure to take this into account (RAM is very affordable these days, so get more than may be needed to be on the safe side).

Extremely Large Destroy Operations - When destroying large filesystems, snapshots and cloned filesystems (e.g., in excess of a terabyte), the data is not immediately deleted - it is scheduled for background deletion processing. The deletion process touches many metadata blocks, and in a heavily deduplicated pool, must also look up and update the DDT to ensure the block reference counts are properly maintained. This results in a significant amount of additional I/O, which can impact the total IOPS available for production workloads.

For best results, schedule large destroy operations for after business hours or on weekends so that deletion processing IOPS will not impact the IOPS available for normal business day operations.

RAID Considerations

SoftNAS Cloud® supports many options for both software and hardware RAID. When planning your deployment it is important to consider the use cases for which you are setting up SoftNAS cloud, best practices for high availability (if applicable) as well as the differences between hardware and software RAID. In the following sections, we will cover these topics, and arm you with the knowledge needed to make the required decisions for your circumstances.

[Software RAID Considerations](#)

[Hardware RAID Considerations](#)

[Amazon EBS RAID Considerations](#)

Software RAID Considerations

SoftNAS Cloud® provides a robust set of software RAID capabilities for non-durable disk drives when there is no hardware protection. Software RAID is best used in scenarios where raw disk devices are attached directly to SoftNAS. Software RAID is **not** recommended for object storage (S3), AWS EBS Volumes, and disks behind hardware RAID controllers.

Software RAID options include RAID 1 and RAID 10 mirrors, RAID 5 (single parity), RAID 6 (dual parity) and even RAID 7 (triple parity) support. It also includes hot spare drive capabilities and the ability to hot-swap spares into operation to replace a failed drive. RAID 10 (striped mirrors) and RAID 6 (dual-parity) are generally recommended for the best balance of read/write I/O performance and fault tolerance. Use RAID 10 for the most performance-sensitive storage pools (e.g., SQL Server, Virtual Desktop Server) and RAID 6 for high-capacity, high-performance applications (e.g., Exchange Server) as it provides the highest write IOPS.

SoftNAS Cloud® is built atop the **ZFS** filesystem. Please take a few moments to become familiar with [ZFS Best Practices](#) for more details on storage pool, RAID and other performance, data integrity and reliability considerations.

The following key points should be considered for RAID Level 10:

- Minimum 4 disks.
- This is also called a “stripe of mirrors”
- Excellent redundancy (as blocks are mirrored)
- Excellent performance (as blocks are striped)
- For higher operating budgets, RAID 10 is the BEST option for any mission critical applications (especially databases).

Best Practices for ZFS RAIDz

RAIDz Level	Allowed # of Disks in Each vdev	
	Minimum	Maximum
RAIDz1*	3	7
RAIDz2	5	10
RAIDz3	7	15

***Note:** Do not use RAIDz1 for disks 1TB or greater in size (use RAIDz2/3 or mirroring instead for better protection).

- Mirrors trump RAIDz every time. Far higher IOPS result from a RAID10 mirror pool than any RAIDz pool, given equal number of drives. This is especially true when using raw disks in situations requiring high write IOPS (typical of VM workloads).
- For 3TB+ size disks, 3-way mirrors begin to become more and more compelling
- Never mix disk sizes (within a few %) or speeds (RPM) within a single vdev
- Never mix disk sizes (within a few %) or speeds (RPM) within a zpool, except for L2ARC & ZIL devices
- Never mix redundancy types for data vdevs in a zpool (use all RAID10 mirrors, RAIDz2, etc. instead of mixing redundancy types)
- Never mix disk counts on data vdevs within a zpool (if the first data vdev is 6 disks, all data vdevs should be 6 disks)
- With multiple JBODs, try to spread each vdev out so that the minimum number of disks are in each JBOD. Given enough JBODs for the chosen redundancy level, it is possible to end up with no SPOF (Single Point of

Failure) in the form of JBOD, and if the JBODs themselves are spread out amongst sufficient HBAs, it becomes possible to even remove HBAs as a SPOF.

- Use RAIDz2/3 over RAIDz1 plus a hot spare, because increased redundancy provides better data protection (and RAIDz3 is like having online hot spares, since it can sustain 2 drive failures).

Hardware RAID Considerations

SoftNAS Cloud® can leverage hardware RAID arrays, where the disk RAID process is managed by the underlying disk controller. Hardware RAID may be available at the disk controller level, which can provide higher performing RAID 5 and RAID 6 configurations, as the better controllers are able to coalesce multiple writes and optimize disk arm write motion. When hardware RAID is used with **SoftNAS Cloud®**, RAID administration takes place outside of **SoftNAS Cloud®**.

When choosing to use hardware RAID, also use software RAID to increase redundancy, performance and recoverability. To store long-term data for more than a few years, it is highly recommended to use the **ZFS** software RAID functionality (even with hardware RAID) for VMDKs. This is because **ZFS** will detect and correct "bit rot" and other errors that creep into storage media over time; otherwise, errors creep in, causing corrupted files over the long haul; e.g., after 4 to 5 years, fewer if using inexpensive disks that are more prone to developing long-term storage accuracy errors.

When choosing a disk controller, if it includes write caching, be sure it also includes a built-in battery backup that will hold onto any cached writes in the event of a power failure. This will increase the system's resiliency to failure.

Storage Configuration Scenario

For the purpose of example, consider a storage solution using twenty 600 GB SAS drives.

One possible configuration is as follows:

- Create two hardware RAID 6 arrays, plus two spares. Each array consists of 8 drives - 6 data + 2 parity.
- Each hardware RAID array becomes a VMware datastore with approximately 3.3 TB of usable storage (two 3.3 TB datastores)

Space Allocation:

For maximum storage capacity and resiliency, create six 1.1 TB VMDKs from the two datastores and attach them to the **SoftNAS Cloud®** VM. This results in six virtual disks of 1.1 TB each becoming available within **SoftNAS Cloud®**.

Inside **SoftNAS Cloud®**, add all six virtual disks to a single, large storage pool using RAID 5 (single parity). The advantage of using both hardware RAID 6 is the arrays can tolerate up to two concurrent drive failures on each array. The software RAID 5 then provides an added layer of parity and recoverability.

Effectively disable software RAID within **SoftNAS Cloud®** by specifying RAID 0 (no redundancy, with striping) and assign all six 1.1 TB virtual disks to a storage pool. Please note that if hardware RAID is used, combined with RAID 0 in **SoftNAS Cloud®**, the built-in **ZFS** filesystem will be unable to recover data, as it will have no parity information to work with. As a result, as with any hardware RAID system, data integrity is reliant upon the hardware level RAID array and its integrity alone.

Alternatively, place the hardware controller into "JBOD mode" and just pass each disk through to **SoftNAS Cloud®** directly as raw storage (no hardware RAID), and use the software RAID within **SoftNAS Cloud®** to handle RAID.

It is important to give careful consideration to which type of RAID configuration will be used to provide the right balance of performance and resilience for applications.

Amazon EBS RAID Considerations

Configure EBS as RAID 0

Each EBS volume attached to an instance is constituted on independent storage hardware within the AWS infrastructure. **SoftNAS Cloud®** storage pools should therefore be configured as RAID 0 to stripe across multiple EBS volumes to gain the highest possible bandwidth and performance. Using any RAID level beyond RAID 0 (RAID levels 1, 10, 5, 6, and 7) merely increases storage costs with little to no benefit to reducing failure rate or improving performance.

EBS SSD and Magnetic Disk Limitations

EBS General Purpose SSD are limited to 10,000 IOPs per volume. EBS Provisioned IOPs are limited to 20,000 IOPs per volume. EBS Magnetic are more severely limited to 40-200 IOPs, which represents the maximum capabilities of today's spinning media. In testing we have seen the EBS SSDs provide more IOPs in shorter durations, but sustained IOPS usage shows these to be bursts that are forced into alignment with disk limitations. By striping across multiple EBS Volumes, of any type, the IOPs can be higher than a single EBS Volume can provide.

AWS EBS Annual Failure Rate (AFR) and Storage Pools

AWS EBS annual failure rate (AFR) is published to be between 0.1% and 0.2%. Aggregating multiple EBS volumes within a **SoftNAS Cloud®** storage pool will magnify the AFR. The AFR is roughly the number of EBS volumes multiplied by AFR rate. Our recommendation is to understand the risk and size of (number of volumes within) storage pools appropriately. Using five EBS volumes within a storage pool (totaling up to 80 TB of capacity) will be an acceptable AFR for most use cases, and many use cases can tolerate an even higher AFR. For high capacity deployments, use multiple SoftNAS storage pools. By setting EBS volumes into separate storage pools, you can achieve high performance and capacity, without adversely affecting AFR.

Common Performance Use Cases

Common Scenarios and Best Practices

For any high-performance on-premise use case, be sure to deploy an adequate amount (e.g., 64 GB or more) of write log (**ZFS** "ZiL") and RAM (plus read cache (**ZFS** "L2ARC") to absorb the high level of 4K block I/O for best results).

For workloads with predominately small (less than 128K) reads and writes, making use of RAM, write log and read cache is critical to achieving maximum throughput, as **ZFS** block I/O occurs in 128K block I/O chunks. Windows also defaults to 4K blocks.

Windows Workloads

One approach that works well for a broad range of applications is to use a combination of SAS and SATA drives - using SSD for read cache/write log (always configure write logs as mirrored pairs in case a drive fails). SATA drives provide very high densities in a relatively small footprint, which is perfect for user mass storage, Windows profiles, Office files, MS Exchange, etc. SQL Server typically demands SAS and/or SSD for best results, due to the high transaction rates involved. Exchange can be relatively heavy on I/O when it's starting up, but since it reads most everything into memory, high-speed caching does little to help run-time performance after initial startup.

Virtual Desktops

Virtual desktops benefit greatly from all the cache memory, level 2 caching and high-speed storage available, because many performance lags quickly become visible as user launch applications, open and save files, etc. Caching also helps alleviate "login storms" and "boot storms" that occur when a large number of simultaneous users attempt to log in first thing in the morning. For these situations, a combination of local caching (on each VDI server), combined with appropriate caching for user profiles and applications can yield excellent results.

S3 Cloud Disk Best Practices

Without proper configuration, a SoftNAS instance leveraging S3-compatible cloud disk extenders can perform poorly. To get the best performance possible for a SoftNAS deployment with S3-compatible cloud disks, keep in mind the following:

Sizing

Sizing a solution involving use of Cloud Disk Extenders is very much the same as for a solution making use of a block-based implementation (VMDK or EBS). There is no change to storage space requirements. However, additional system resources may be required in order to handle the virtualization of the S3 storage required in order to present the S3 Cloud Disk as block storage. Stated another way, the number of buckets that are configured via cloud disk extender influences the amount of additional resources that are required to access the same overall capacity of storage.

CPU

If using cloud disk extenders in your instance/s, it is important to configure your instance with additional processing power (CPU), above and beyond what is required for traditional block-based storage access. Presenting S3 storage as block-based storage requires a number of additional functions to be executed, including, for example, SSL/TLS key exchange and encryption, MD5 block computations, network stack processing, as well as optional encryption options. To avoid performance issues:

- Do not use cloud disk extender on single vCPU instances.
- 2 vCPU instances may be suitable for test scenarios. Two vCPU instances may still prove insufficient if your S3-compatible test/POC environment requires decent performance metrics.
- For a production environment, a minimum of 4 vCPU instances is highly recommended. Many workloads will perform better with additional vCPU.
- For each 75 MB/s of throughput required to perform the same task with block-based storage, an additional two vCPU is highly recommended.
- CPU utilization should be monitored during proof-of-concept and initial production stages to verify that sufficient CPU has been provisioned for the provided workload.
- Monitor email alerts should be monitored and indications of high CPU utilization should be reviewed with respect to the Cloud Disk Extender configuration.
- If operating in a trusted environment, and available as an option for the S3-compatible object storage being used, CPU usage can be reduced by using http rather than https.
- CPU usage can be further reduced by disabling optional encryption options.

Example:

A customer wants to use S3 object storage to save money over EBS. The current workload operates between 100-150MB/s of throughput and is running on an m4.xlarge instance. Evaluating the current workload, we know that it averages a healthy 50% CPU usage. To provide the same 150MB/s of S3 throughput, the general guideline requests 4 additional vCPU over and above the current instance's existing 4 vCPU base. As a result, the CPU recommendation points to an m4.2xlarge instance, in order to provide four additional vCPU.

RAM

As mentioned previously in this document, each instance of the cloud disk extender represents a process that is running inside of the SoftNAS instance for virtualizing the object storage as block storage.

- Cloud Disk Extender should not be used in production on systems with less than 8GB of RAM.
- Memory footprints less than 8GB of RAM may be suitable for test or PoC environments only.
- A general guideline of 512MB of RAM should be provisioned above the normal required memory for a given workload.
- Remember that half of the RAM is utilized for file-system caching. Additional resources are needed for the network file services and the base operating environment (~2GB of RAM).

Network

Cloud Disk Extender utilizes the network interface of an instance in order to access the object storage. Sufficient network bandwidth must be provisioned in order to reach maximum performance profiles using Cloud Disk Extender. When considering the desired available throughput to the object store also consider the amount of network throughput for network file services (NFS, CIFS, iSCSI, AFP) and SnapReplicate/SNAP HATM which, in most configurations and platforms, all come from the same pool of available network bandwidth.

- A somewhat safe calculation can be to determine the available network throughput being used for the instance, and to divide it divided by 3, in order to calculate 1/3 for file services, 1/3 for replication, and 1/3 for object storage I/O.
- When calculating, consider that SnapReplicate only replicates the write bandwidth, not the read bandwidth.
- Be sure to convert properly between bits and bytes when comparing network throughput (usually expressed in bits) to disk throughput (usually expressed in bytes)
- There is inherent overhead in the protocols used on the network (request/response, headers, checksums, control data, etc) such that full network saturation does not yield the full bandwidth as useful throughput. Consider only anticipating 90% of the link-speed as usable throughput.
- Most clouds (and most data centers) do not provide full link-speed bandwidth on a sustained basis as systems are utilizing shared resources. Systems designed to run at full provisioned capacity (of any metric) should be assigned to dedicated hosts rather than shared tenancy.

Example:

A customer uses NFS, SnapReplicate and SNAP HATM, and would like to use object storage. Expected throughput is about 40MB/s with 90% reads. According to calculation, the network throughput for the source node reads as follows:

- 4MB/s writes to NFS (incoming)
- 36MB/s reads to NFS (outgoing)
- 4MB/s writes to SnapReplicate (outgoing)
- 4MB/s writes to Object Storage (outgoing)
- 36MB/s reads to Object Storage (incoming)

Total: 40MB/s incoming 44MB/s outgoing

Calculating the total throughput in bytes, this is 320mbps incoming and 352mbps outgoing.

According to calculation, the network throughput for the target node reads as follows:

- 4MB/s writes from SnapReplicate (incoming)
- 4MB/s writes to Object Storage (outgoing)

Total: 4MB/S incoming and 4MB/S outgoing

In bytes, this works out to 32mbps incoming 32mbps outgoing.

A 100 mbps network connection is certainly not sufficient for this configuration, however, a 1gbps connection should be enough, even considering protocol overhead and avoiding 100% saturation of the network.

Amazon AWS S3 Recommendation: VPC Endpoints

Customers on AWS within a VPC should be using VPC Endpoints for accessing S3 object stores. By using a VPC endpoint, a higher quality service level is provided to S3 object stores within a region, thereby improving the overall reliability and performance when accessing S3 object storage. Additionally, a VPC Endpoint can be used in order to to communicate with resources in other services via private IPs, without exposing instances to the internet.

For guidance on setting up VPC Endpoints via the Amazon AWS console, see [Amazon's help on the topic](#).

Networking

For optimal **SoftNAS Cloud®** performance, adhere to the following Networking considerations and Best Practices:

As with any storage system, NAS performance is a function of a number of many different combined factors:

- Network bandwidth available; e.g., 1 GbE vs. 10 GbE vs. Infiniband
- Network QoS (whether the network is dedicated, shared, local vs. remote, EC2 provisioned IOPS, etc.)
- Network latency (between workload VMs and **SoftNAS Cloud®** VM)
- MTU settings in VM host software and switches
- Network access protocol (NFS, CIFS/SMB, iSCSI, Direct-attached fiber-channel)
- Use of VLANs to separate storage traffic from other network traffic.

Networking Requirements

A minimum of 1 gigabit networking is required and will provide throughput up to 120 MB/sec (line speed of 1 GbE). 10 GbE offers 750+ MB/sec throughput. To reduce the overhead for intensive storage I/O workloads, it is highly recommended to configure the VMware hosts running **SoftNAS Cloud®** and the heavy I/O workloads with "jumbo frames", MTU 9000. It's usually best to allocate a separate **vSwitch** for storage with dual physical NICs with their VMkernels configured for MTU 9000 (be sure to configure the physical switch ports for MTU 9000, as well). If possible, isolating storage onto its own VLAN is also a best practice.

When using dual switches for redundancy (usually a good idea and best practice for HA configurations), be sure to configure the **VMware host vSwitch** for Active-Active operation and test switch port failover prior to placing **SoftNAS Cloud®** into production (as with any other production VMware host).

Choose static IPv4 addresses for **SoftNAS Cloud®**. If the plan is to assign storage to a separate VLAN (usually a good idea), ensure the **vSwitch** and physical switches are properly configured and available for use. For VMware-based storage systems, **SoftNAS Cloud®** is typically deployed on an internal, private network. Access to the Internet from **SoftNAS Cloud®** is required for certain features to work; e.g., Software Updates (which download updates from softnas.com site), NTP time synchronization (which can be used to keep the system clock accurate), etc.

From an administration perspective, allow browser-based access from the internal network only. Optionally, use SSH for remote shell access (optional). To completely isolate access to SoftNAS from both internal and external users, then access will be restricted to the VMware console only (launch a local web browser on the graphical console's desktop). Add as many network interfaces to the **SoftNAS Cloud® VM** as are permitted by the VMware environment.

Prior to installation, allocate a static IP address for **SoftNAS Cloud®** and be prepared to enter the usual network mask, default gateway and DNS details during network configuration. By default, **SoftNAS Cloud®** is configured to initially boot in DHCP mode (but it is recommended to use a fixed, static IP address for production use).

At a minimum, **SoftNAS Cloud®** must have at least one NIC assigned for management and storage. Provide separate NICs for management/administration, storage I/O and replication I/O.

Networking Considerations

A fast NAS response to requests isn't the only governing factor to how well workloads perform. Network design, available bandwidth and latency are also important factors. For example, for high-performance NAS applications, where possible, use of a dedicated VLAN for storage is a must. Configuring all components in the storage path to use MTU 9000 will greatly increase throughput by reducing the effects of round-trip network latency and reducing the interrupt load on the NAS server itself. Interrupts are often overlooked as a source of overhead, because they aren't readily measured, but their effects can be significant, both on the NAS server and workload servers. Configure any NAS requiring the highest level of performance for MTU 9000 along with the switching ports used between the NAS host and workload servers.

A single 1 GbE network segment will, at most, produce up to 120 MB/sec throughput under the most ideal conditions possible. 10 GbE has been observed to deliver up to 1,000 MB/sec of throughput.

The next consideration is protocol - Use NFS, CIFS or iSCSI? The iSCSI protocol often provides the best throughput, and increased resiliency through multi-pathing. Just be aware of the added complexities associated with iSCSI.

For VM-based workloads - it's hard to go wrong with NFS or iSCSI. For user data (e.g., file shares), CIFS is more common because of the need to integrate natively with Windows, domain controllers and **Active Directory** when using a NAS as a file server.

Thick-provisioning VMware datastores provides increased write performance, and should be preferred over thin-provisioning of VMDKs when optimal performance is required.

Regardless of design, verify each implementation by running performance benchmarks to validate the throughput expected before going into production.

Security

IMPORTANT - Note the following to bolster the security of **SoftNAS Cloud®** storage solution. This list is not exhaustive, so apply the most appropriate set of best practices for deploying Linux-based systems locally or on the Internet.

Change Default Passwords

Consider changing the default password that is set for the user **softnas** and for **root** account.

Apply the Latest Software Updates

We identify threats and provide fixes on a regular basis, so be sure to keep up with the latest software updates and maintenance.

Restrict Firewall source IP

Restrict the allowed IP addresses which are allowed access to each port on **SoftNAS Cloud®** - especially HTTPS (port 443). Only allow approved administrators to access the SSH, HTTPS ports by restricting who (which TCP/IP addresses) can access those ports. Restrict NAS ports (e.g., CIFS, NFS, iSCSI, etc.) to only allow EC2 workload instances; e.g., x.x.x.x/24 or a specific range of workload instances.

When publishing storage via NFS, CIFS, iSCSI, or other protocols from **SoftNAS Cloud® via the Internet**, it is also critical to configure encrypted, authenticated access and limit the source ports accordingly. Also, be sure to restrict the range of allowed source IP addresses. If storage services are published only on an internal LAN or WAN, then apply appropriate security measures as for any storage server in this network environment.

NFS and BIND Services:

TCP Port (Service)	Source	Service
111	x.x.x.x/24	portmapper
2010	x.x.x.x/24	rquotad
2011	x.x.x.x/24	nlockmgr
2013	x.x.x.x/24	mountd
2014	x.x.x.x/24	status
2049	x.x.x.x/24	nfs

UDP Port (Service)	Source	Service
111	x.x.x.x/24	portmapper
2010	x.x.x.x/24	rquotad
2011	x.x.x.x/24	nlockmgr
2013	x.x.x.x/24	mountd
2014	x.x.x.x/24	status
2049	x.x.x.x/24	nfs

CIFS/SMB via Samba:

For ease of use, here are the ports to open for two-way CIFS communication with Windows and Linux desktop systems.

Variable	TCP Port #	Service
netbios-ns	137	NETBIOS Name Service
netbios-dgm	138	NETBIOS Datagram Service

netbios-ssn	139	NETBIOS Session Service
microsoft-ds	445	Active Directory

Other ports:

Description	TCP Port #	Note
LDAP	389	Active Directory Mode
NetBIOS	445	Post-Windows 2000 (CIFS)
SWAT	901	Not related to client communication

AFP/Netatalk

Description	TCP Port #	Note
AFP over TCP	548	AppleShare, Personal File Sharing, Apple File Service
Service Location Protocol (SLP)	427	Network Browser

iSCSI:

Description	TCP Port #	Note
iSCSI	3260	Target publishing

ReCaptcha

To prevent brute force password entry into our servers, the SoftNAS login screen uses ReCaptcha. This means that after 5 unsuccessful attempts to log in, Recaptcha will prompt the user to perform an additional action in order to continue attempting new passwords, preventing repeated attempts from eventually guessing the correct login.



Log in to SoftNAS StorageCenter™

Captcha verification

I'm not a robot

reCAPTCHA
Privacy - Terms

Data at Rest Encryption

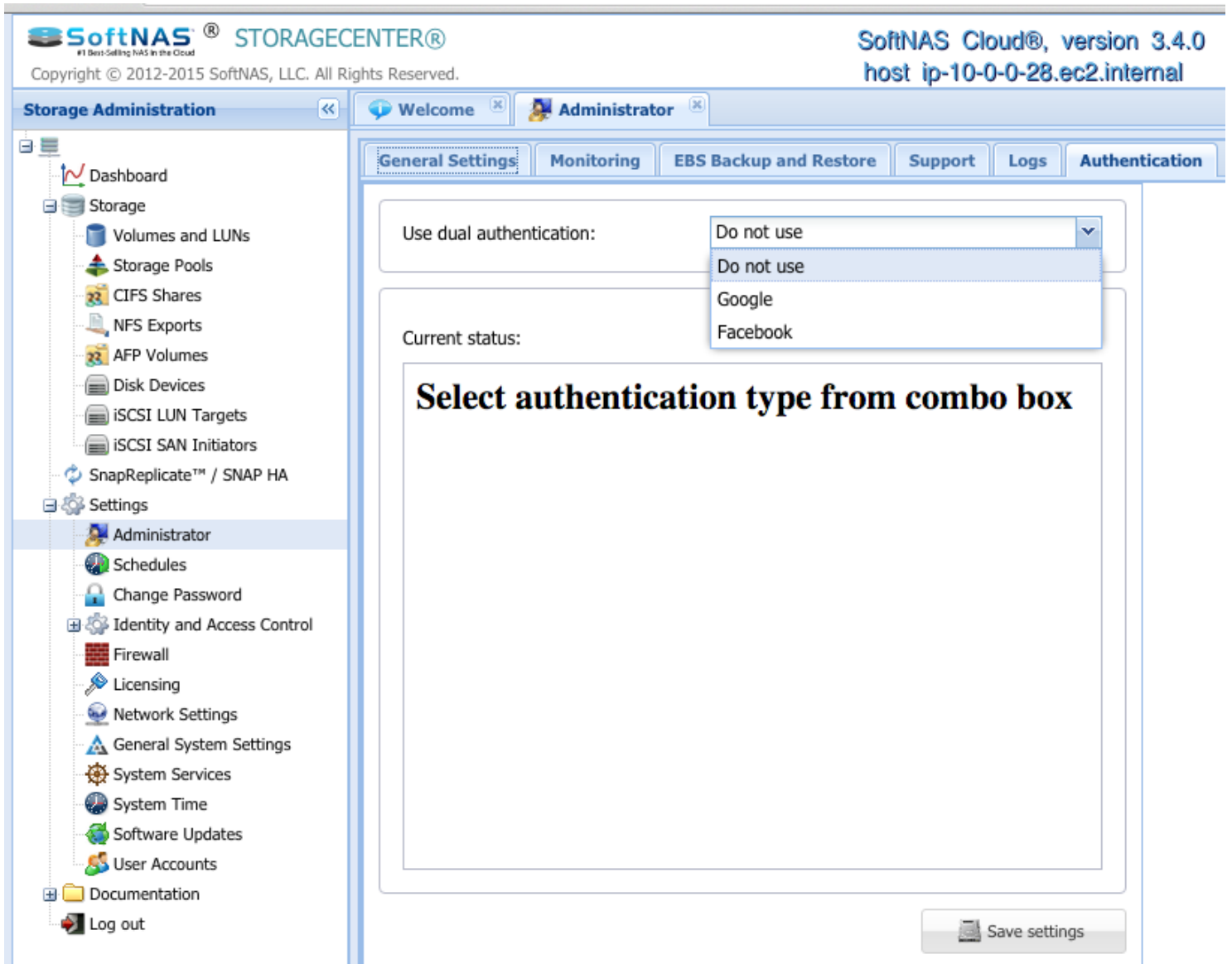
SoftNAS offers encryption for its disks, protecting data at rest. The encryption is FDE (or Full Disk Encryption) and meets AES-256 standards. Encryption is provided at the pool level, using LUKS encryption. To learn more, see [Create a Storage Pool](#).

Enhancement Considerations

The Linux operating system on which **SoftNAS Cloud®** runs includes **iptables** and the ability to configure firewall rules on Linux to provide an additional layer of inbound and out bound security, should that be desired. For those who are serious about fully securing a **SoftNAS Cloud®** environment, there are numerous sources for best practices on security lockdown of Linux-based systems. Since **SoftNAS Cloud®** runs on a standard CentOS 64 Linux-based operating system (the free version of Red Hat Enterprise Linux), the entire spectrum of Linux-based security tools, add-ons and methodologies are available.

Dual Factor Authentication

SoftNAS supports dual factor authentication through Google and/or Facebook login, in order to add another layer of security to your installation. By requiring not only your SoftNAS credentials to manage your instance, but also login to your Google or Facebook account, your SoftNAS instance is twice as secure. This is an optional configuration, allowing you to select the account you wish to secure SoftNAS with (Google or Facebook) or to opt out.



The screenshot displays the SoftNAS StorageCenter web interface. The top header shows the SoftNAS logo and 'STORAGECENTER®' on the left, and 'SoftNAS Cloud®, version 3.4.0' and 'host ip-10-0-0-28.ec2.internal' on the right. Below the header is a navigation bar with tabs for 'General Settings', 'Monitoring', 'EBS Backup and Restore', 'Support', 'Logs', and 'Authentication'. The 'Authentication' tab is active. On the left side, there is a sidebar menu with categories like 'Storage Administration', 'Storage', 'Settings', and 'Documentation'. The main content area shows the 'Use dual authentication:' setting with a dropdown menu currently displaying 'Do not use'. Below this, the 'Current status:' section contains a large text box with the instruction 'Select authentication type from combo box'. A 'Save settings' button is located at the bottom right of the settings area.

Launching SoftNAS Cloud® Platforms

SoftNAS Cloud® is available for various industry platforms, with a focus on local storage management interfaces and requirements. Platform-specific configuration will be explained in dedicated sub-sections of this guide, but most **SoftNAS Cloud®** installations begin the same way.

Note: Regardless of underlying platform, **SoftNAS Cloud®** will require the ability to access the Internet for software updates, activation, etc. For this case, enabling only outbound TCP traffic to the **softnas.com** domain is required.

Setting Up SoftNAS Cloud®

1. Open a web browser and enter the **SoftNAS** website link <https://www.softnas.com/> in the Address bar.

The **SoftNAS** home page will be displayed.

2. For a free trial period, click the **Try Now** option at the bottom of the main **SoftNAS.com** screen.

3. Click through for the desired product registration and download if applicable. Follow the wizards and prompts to register and configure a local SoftNAS platform and GUI. Depending on platform chosen, the next steps may differ slightly; however, the steps are designed to be intuitive with industry best practices.

SoftNAS Cloud®, **SoftNAS StorageCenter™**, **SnapReplicate™**, and **SNAP HA™** are trademarks of **SoftNAS Inc.**. All other trademarks referred to in this guide are owned by their respective companies.

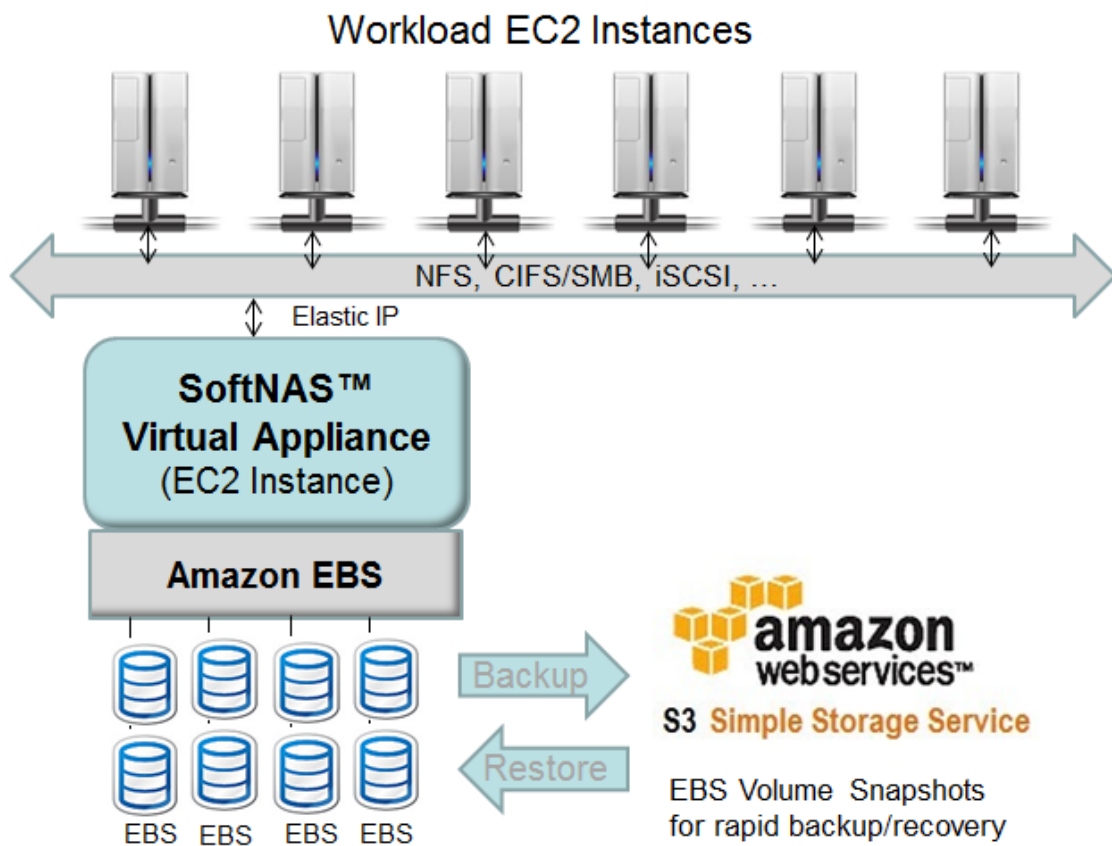
Amazon Web Services (AWS)

Overview

Amazon Web Services provides underlying block-storage devices, namely Elastic Block Storage (EBS), which can be organized into RAID configurations to increase performance and throughput, providing recovery protection from underlying physical disk failures.

SoftNAS Cloud® for AWS Elastic Compute Cloud (EC2) is a virtual cloud storage appliance, providing trusted, commercial-grade NAS capabilities for EC2 cloud business computing workloads. EC2 workloads include web servers, SaaS applications, SQL database servers, Exchange servers, Windows Remote Desktop Servers, Citrix XenApp servers, etc. **SoftNAS Cloud® for EC2** provides the flexible, full-featured storage capabilities for trusted cloud computing applications.

[AWS EC2 System Requirements](#)



SoftNAS Cloud® for EC2 leverages flexible **Elastic IP** addresses, making it fast and easy to fail over across availability zones and regions (i.e., different data centers). It's also straightforward to quickly replicate a **SoftNAS Cloud®** instance from one availability zone to other geographic regions, so that data is always available and performs well for geographically local users and communities.

Because **SoftNAS Cloud® for EC2** uses **Elastic Block Storage (EBS)** and **Amazon S3** object storage for raw data storage, backup and restore operations are fast and easy using **EBS Volume Snapshots**.



The **Amazon EC2** cloud computing environment, which will be referred to simply as **EC2** in this guide, is a robust, powerful virtualization and computing system with many options and capabilities. For our purposes here, we will focus on installing **SoftNAS Cloud®** and configuring it for basic use. Additional options exist for increasing performance and throughput, for database and other, more demanding applications, which will be covered briefly.

In an **Amazon EC2** or other cloud computing environment, **SoftNAS Cloud®** provides the network storage backbone needed for business critical cloud applications.

SoftNAS Cloud® for EC2 leverages EBS (Elastic Block Storage) as its underlying block storage devices. Multiple EBS devices are then organized into RAID configurations, increasing performance and throughput, and providing the ability to recover from underlying physical disk failures that can occur with EBS. **SoftNAS Cloud®** provides the most durable, highest performance NAS solution available for **Amazon EC2**.

Product and Installation Options

SoftNAS Cloud® provides the following applicable products:

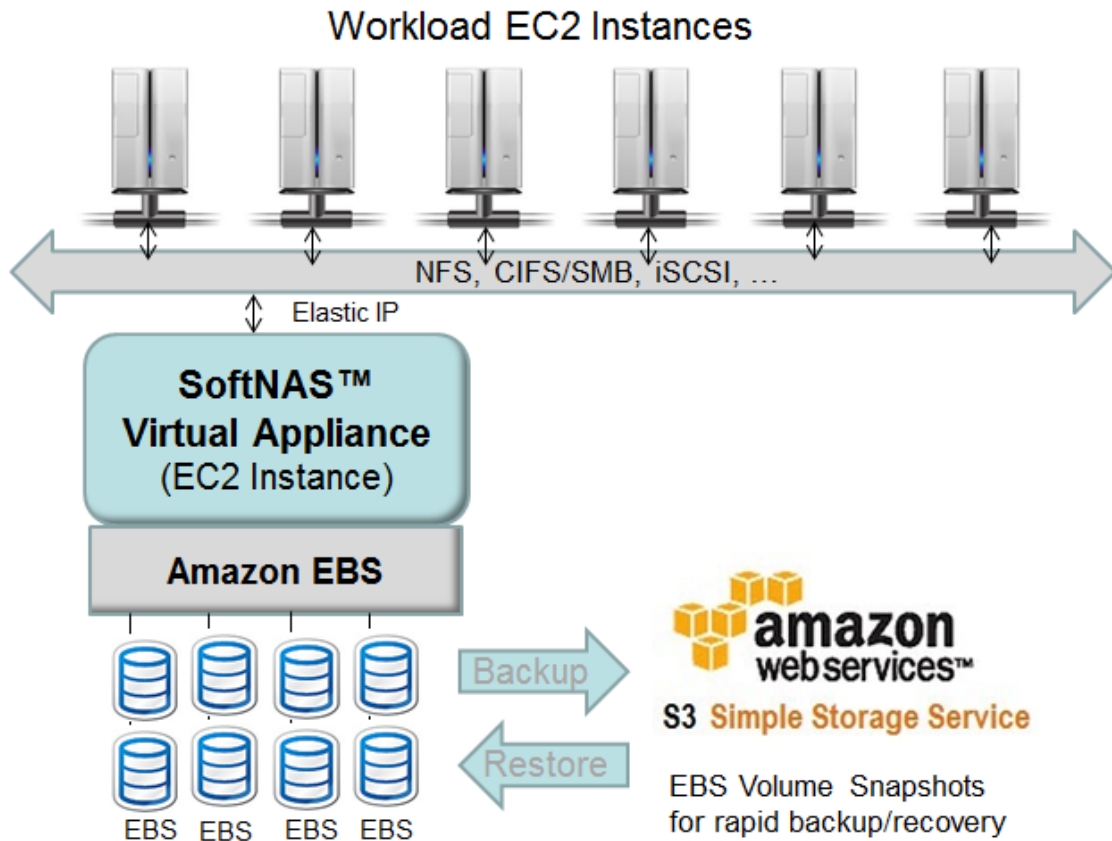
- SoftNAS Cloud® **Express** (1TB of storage)
- SoftNAS Cloud® **Standard** (20TB of storage)
- SoftNAS Cloud® **Enterprise** (up to 16 PB of storage)
- SoftNAS Cloud® **BYOL** (Bring Your Own License)

Product	Storage	Purchase	License
SoftNAS Cloud® Express	1 TB	Subscribe via AWS Marketplace .	Embedded in platform subscription or BYOL available from SoftNAS .
SoftNAS Cloud® Standard	20 TB	Subscribe via AWS Marketplace .	Embedded in platform subscription or BYOL available from SoftNAS .
SoftNAS Cloud® Enterprise	16 PB	Subscribe via AWS Marketplace .	Embedded in platform subscription or BYOL available from SoftNAS .

- SoftNAS SNAP HA™ included with each product.

Amazon EC2 Cloud Disk Overview

SoftNAS Cloud® for EC2 is a virtual cloud storage appliance, providing trusted, commercial-grade NAS capabilities for EC2 cloud business computing workloads. EC2 workloads include web servers, SaaS applications, SQL database servers, Exchange servers, Windows Remote Desktop Servers, Citrix XenApp servers, etc. SoftNAS for EC2 provides the flexible, full-featured storage capabilities for trusted cloud computing applications.



SoftNAS Cloud® for EC2 can leverage flexible Elastic IP addresses or Virtual IP addresses, making it fast and easy to fail over across availability zones and regions (i.e., different data centers). It's also straightforward to quickly replicate a SoftNAS cloud instance from one availability zone to other geographic regions, so that data is always available and performs well for geographically local users and communities.

And because SoftNAS® for EC2 uses Elastic Block Storage (EBS) for raw data storage, backup and restore operations are fast and easy using EBS Volume Snapshots to Amazon's affordable, redundant S3 storage.

The Amazon EC2 cloud computing environment, which will be referred to simply as EC2 hereinafter, is a robust, powerful virtualization and computing system with many options and capabilities. For our purposes here, we will focus on installing SoftNAS® and configuring it for basic use. Additional options exist for increasing performance and throughput, for database and other more demanding applications, which will also be covered briefly.

This section provides concepts that may be helpful for the first-time Amazon EC2 customer along with useful guidelines for making decisions about how to configure SoftNAS® for best results in the EC2 computing environment.

AWS EC2 System Requirements

SoftNAS Cloud® System Requirements

Listed below is a table to assist with the setup decisions during the configuration required to accomplish various tasks and goals.

	Recommended	Configuration Note
Compute		
General Purpose	M4.2xlarge	Standard: a good starting point in regards to memory and CPU resources. This category is suited to handle the processing and caching with minimal requirements for network bandwidth.
High Performance	M4.4xlarge	Medium: good for workloads that are read intensive will benefit from the larger memory-based read cache for this category. The additional CPU will also provide better performance when deduplication, encryption, compression and/or RAID is enabled.
Extreme Performance	M4.10xlarge	High: This category can be used for workloads that require a very high speed network connection due to the amount of data transferred over a network connection. In addition to the very high speed network, this level of instance gives you a lot more storage, CPU and memory capacity.
Memory		
Base RAM	1GB	Required for kernel and system operations.
System RAM	8GB or more for best results	Paired with CPU by instance
Additional RAM	1 GB per 1 TB of deduplicated storage.	Recommended for best performance
	e.g.: 50 TB deduplicated storage = 50 additional GB for deduplication tables.	
Storage		
Boot Disk	30 GB Hard disk for Linux boot and system disk (all EC2 instance types provide enough space to install and use SoftNAS Cloud®)	
Data Disks	Elastic Block Storage (EBS) provides block data storage on Amazon EC2.	
Software RAID	Recommended to configure EBS disks using SoftNAS software RAID for increased performance and data durability.	
Networking		
Up to 120 MB/sec	1 GbE	Small to Large instances provide up to 1GbE connectivity. Use High I/O instances to increase network throughput.
HA Networking	Not supported in Amazon EC2.	
HA Host Failover	Configure multiple redundant SoftNAS Cloud® instances in separate availability zones or different geographic regions.	

Note: Refer to AWS for specific SSD performance metrics.

CRITICAL: Do not use ephemeral disks for write logs. Ephemeral disks are local instance disks providing a much larger second-level read cache than RAM, and are typically more than twice as fast as standard EBS volumes. However, the data stored here is temporary and therefore lost upon each reboot.

SoftNAS Cloud® System Capacities

Listed below is a table representing the capabilities of the **SoftNAS Cloud®** for **Amazon Web Services**.

	SoftNAS Cloud® Capacity	Configuration Note
Editions		
SoftNAS Cloud® Express	1 TB	
SoftNAS Cloud® Standard	20 TB	
SoftNAS Cloud® Enterprise	16 PB	
Memory		
RAM Cache	1 GB to 100 GB	Defaults to 50% total RAM for read cache
SSD Cache	low-speed level 2 cache	Optional
Ephemeral Cache	low-speed level 2 cache	Optional for read cache
Storage		
Maximum Storage	16 PB	Maximum usable storage capacity with SoftNAS Cloud® , contingent on license.
# of Storage Pools	Unlimited	
# of Volumes	Unlimited	
# of Snapshots	Unlimited	
# of Snapshot Clones	Unlimited	
SnapReplicate	Unlimited Pools & Volumes	
SnapReplicate Throttle	56Kb/sec to Unlimited bandwidth	
Active Directory	Kerberos Integration	
Files and Directories	Unlimited	
Network		
Schedules	Unlimited	
NFS Exports:	Linux Default	
iSCSI Targets	Linux Default	
CIFS Shares	Linux Default	
Firewall Ports:	22 (ssh), 443 (https)	Plus NFS, iSCSI, and CIFS as required by network
IP Tables Firewall	Off by default	May be configured, but is not required. Use an alternative method to set Security Groups unless added firewall protection on a SoftNAS Cloud® instance is required.

Configuring AWS Identity and Access Management: Role and User

About IAM

Amazon Web Services (AWS) Identity and Access Management (IAM) is a web service that enables **AWS** customers to manage users and user permissions in **AWS**. The service is targeted at organizations with multiple users or systems that use **AWS** products such as **Amazon EC2**, **Amazon RDS**, and the **AWS Management Console**. With IAM, centrally manage users, security credentials such as access keys, and permissions that control which **AWS** resources users can access.

Without IAM, organizations with multiple users and systems must either create multiple **AWS** accounts, each with its own billing and subscriptions to **AWS** products, or employees must all share the security credentials of a single **AWS** account. Also, without IAM, there is no control over the tasks a particular user or system can do and what **AWS** resources they might use.

IAM addresses this issue by enabling organizations to create multiple users (each user is a person, system, or application) who can use **AWS** products, each with individual security credentials, all controlled by and billed to a single **AWS** account. With IAM, each user is allowed to do only what they need to do as part of the user's job.

There are two methods by which one can set up Identity and Access Management for your SoftNAS Cloud® instance:

- [Creating the IAM Role for SoftNAS Cloud®](#)
- [Specifying the IAM User for SoftNAS Cloud®](#)

We strongly recommend creating the IAM Role prior to setting up your instance, as it is the more secure method. Specifying an IAM User for your SoftNAS Cloud® instance is used when adding IAM functionality to existing instances.

Note: There is no need to create both the IAM Role and an IAM user. It is one or the other.

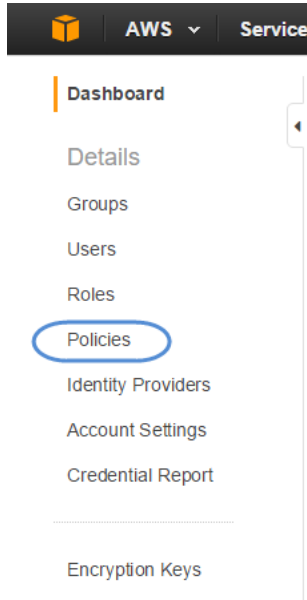
Creating the IAM Role for SoftNAS Cloud®

Creating an IAM Role to govern user access prior to creating your SoftNAS Cloud® instance is recommended best practice, rather than Specifying an IAM User. The IAM Role provides a more secure environment.

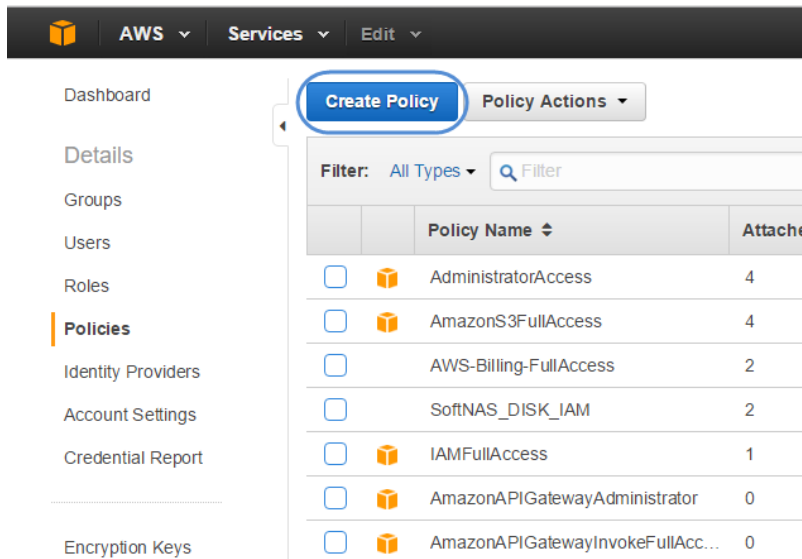
Creating the IAM Role Policy.

SoftNAS recommends the use of a custom policy for IAM role configuration. This custom policy should be created prior to the role itself. Open the Identity and Access Management Console to begin.

1. To create the custom policy, click **Policies** from within the navigation pane.



2. Select **Create Policy**.



3. Select **Create Your Own Policy**.

AWS Services Edit qatester @ softnasdev Global Support

Create Policy

Step 1: Create Policy
Step 2: Set Permissions
Step 3: Review Policy

Create Policy

A policy is a document that formally states one or more permissions. Create a policy by copying an AWS Managed Policy, using the Policy Generator, or typing your own custom policy.

Copy an AWS Managed Policy
Start with an AWS Managed Policy, then customize it to fit your needs. Select

Policy Generator
Use the policy generator to select services and actions from a list. The policy generator uses your selections to create a policy. Select

Create Your Own Policy
Use the policy editor to type or paste in your own policy. Select

4. Provide a **Policy Name**, and copy the policy below into the **Policy Document** box. You can also provide a **Policy Description** in order to help differentiate this policy from others that may be similar. It is always a good idea to validate your policy before creating it. Click **Create Policy**.

Create Policy

Step 1: Create Policy
Step 2: Set Permissions
Step 3: Review Policy

Review Policy

Customize permissions by editing the following policy document. For more information about the access policy language, see [Overview of Policies](#) in the *Using IAM* guide. To test the effects of this policy before applying your changes, use the [IAM Policy Simulator](#).

This policy is valid.

Policy Name
SOFTNAS_IAM_Custom_Policy

Description
Policy for SOFTNAS IAM

Policy Document

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "Stmt1444200186000",
6       "Effect": "Allow",
7       "Action": [
8         "_comment: Required for EBS Add/Delete",
9         "ec2:CreateVolume",
10        "ec2>DeleteVolume",

```

Use autoforamtting for policy editing

Cancel Validate Policy Previous Create Policy

IAM Role Policy

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1444200186000",
      "Effect": "Allow",
      "Action": [
        "ec2:ModifyInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:CreateVolume",
        "ec2>DeleteVolume",
        "ec2:CreateSnapshot",
        "ec2>DeleteSnapshot",
        "ec2:CreateTags",
        "ec2>DeleteTags",
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",

```

```

"ec2:DescribeSnapshots",

"aws-marketplace:MeterUsage",

"ec2:DescribeRouteTables",
"ec2:DescribeAddresses",
"ec2:DescribeTags",
"ec2:DescribeInstances",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:ReplaceRoute",
"ec2:CreateRoute",
"ec2>DeleteRoute",
"ec2:AssociateAddress",
"ec2:DisassociateAddress",

"s3:CreateBucket",
"s3:Delete*",
"s3:Get*",
"s3:List*",
"s3:Put*"
],
"Resource": [
  "*"
]
}
]
}

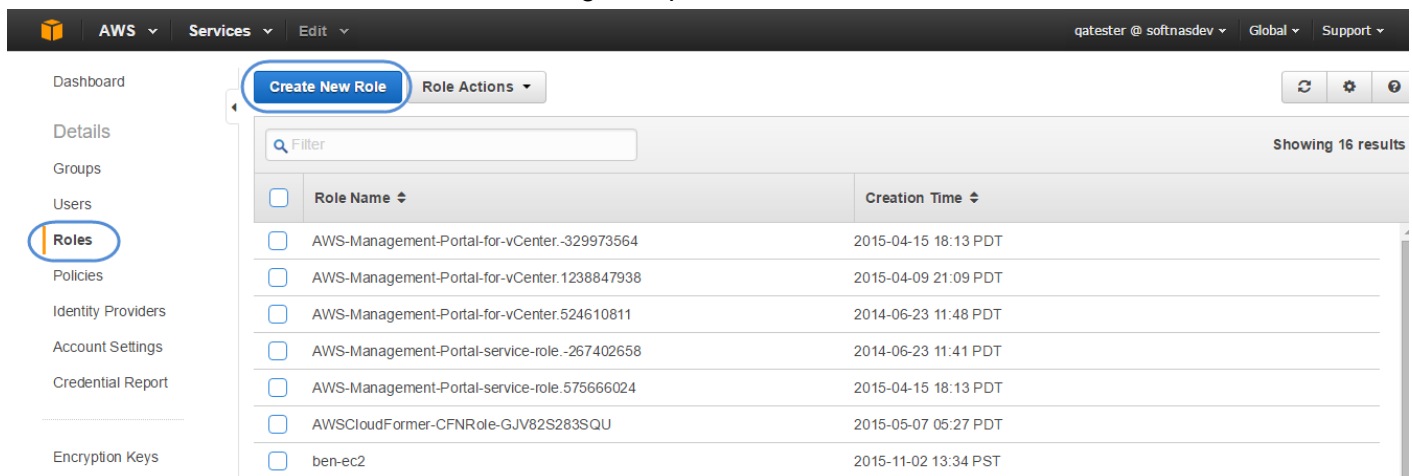
```

Note: S3-BUCKET1 & S3-BUCKETZ are the buckets you create while using Amazon Cloud Disk Extenders. You can learn more about how to create these buckets in [Adding Cloud Disk Extenders](#).

Creating the IAM Role.

Having created the IAM Role policy, you can now create the role and assign the policy.

1. Still within the IAM Console, from the navigation pane, click **Roles**, and then click **Create New Role**.



2. On the **Set Role Name** page, enter the name for the role as **SoftNAS_DISK_IAM** for disk access and click **Next Step**.

AWS ▾ **Services** ▾ **Edit** ▾

Create Role

Step 1: Set Role Name

Step 2: Select Role Type

Step 3: Establish Trust

Step 4: Attach Policy

Step 5: Review

Set Role Name

Enter a role name. You cannot edit the role name after the role is created.

Role Name

Maximum 64 characters. Use alphanumeric and '+=.,@_-' characters

Critical: Use only this role name, and remember that this string is case sensitive.

4. On the **Select Role Type** page, click **Select** next to **Amazon EC2**.

Select Role Type

AWS Service Roles

- Amazon EC2**
Allows EC2 instances to call AWS services on your behalf. **Select**
- AWS Directory Service**
Allows AWS Directory Service to manage access for existing directory users and groups to AWS services. **Select**
- AWS Lambda**
Allows Lambda Function to call AWS services on your behalf. **Select**
- AWS Config**
Allows AWS Config to call AWS services and collect resource configurations on your behalf. **Select**
- AWS SWF**
Allows SWF workflows to invoke Lambda functions on your behalf. **Select**

Role for Cross-Account Access

Role for Identity Provider Access

Cancel **Previous** **Next Step**

5. On the **Attach Policy** page, select the SoftNAS IAM Policy created earlier and click **Next Step**. (If you cannot find the policy in question, change policy type to Customer Managed Policy)

Create Role

Step 1: Set Role Name

Step 2: Select Role Type

Step 3: Establish Trust

Step 4: Attach Policy

Step 5: Review

Attach Policy

Select one or more policies to attach. Each role can have up to 10 policies attached.

Filter: Policy Type ▾ Showing 170 results

	Policy Name	Attached Entities	Creation Time	Edited Time
<input type="checkbox"/>	AdministratorAccess	4	2015-02-06 10:39 PST	2015-02-06 10:39 PST
<input type="checkbox"/>	AmazonS3FullAccess	4	2015-02-06 10:40 PST	2015-02-06 10:40 PST
<input type="checkbox"/>	AWS-Billing-FullAccess	2	2015-07-06 15:53 PDT	2015-07-06 15:53 PDT
<input checked="" type="checkbox"/>	SoftNAS_IAM	2	2015-11-02 23:42 PST	2015-11-02 23:42 PST
<input type="checkbox"/>	AmazonAPIGatewayAdministra...	0	2015-07-09 10:34 PDT	2015-07-09 10:34 PDT
<input type="checkbox"/>	AmazonAPIGatewayInvokeFull...	0	2015-07-09 10:36 PDT	2015-07-09 10:36 PDT
<input type="checkbox"/>	AmazonAppStreamFullAccess	0	2015-02-06 10:40 PST	2015-02-06 10:40 PST
<input type="checkbox"/>	AmazonAppStreamReadOnlyA...	0	2015-02-06 10:40 PST	2015-02-06 10:40 PST
<input type="checkbox"/>	AmazonCognitoDeveloperAuth...	0	2015-03-24 10:22 PDT	2015-03-24 10:22 PDT

Cancel **Previous** **Next Step**

6. Review the policy settings and click **Create Role**.

Specifying the IAM User for SoftNAS Cloud®

Create the **SoftNAS Cloud® AWS IAM** User from the Amazon Web Services Dashboard. Specify the the permissions for the resources that are required by **SoftNAS Cloud®** instances to operate safely and securely in the AWS environment. The permissions are specified by applying a user policy to the **SoftNAS Cloud®** User.

Creating the Policy

To create the policy, follow the steps listed for Creating the IAM Role Policy, listed in short form for your convenience below:

1. Click **Policies** from within the navigation pane.
2. Select **Create Policy**.
3. Select **Create Your Own Policy**.
4. Provide a **Policy Name**, and copy the policy below into the **Policy Document** box. You can also provide a **Policy Description** in order to help differentiate this policy from others that may be similar. It is always a good idea to validate your policy before creating it. Click **Create Policy**.

IAM User Policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1444200186000",
      "Effect": "Allow",
      "Action": [
        "ec2:ModifyInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:CreateVolume",
        "ec2>DeleteVolume",
        "ec2:CreateSnapshot",
        "ec2>DeleteSnapshot",
        "ec2:CreateTags",
        "ec2>DeleteTags",
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",

        "aws-marketplace:MeterUsage",

        "ec2:DescribeRouteTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeTags",
        "ec2:DescribeInstances",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ReplaceRoute",
        "ec2:CreateRoute",
        "ec2>DeleteRoute",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",

        "s3:CreateBucket",
      ]
    }
  ]
}
```

```

    "s3:Delete*",
    "s3:Get*",
    "s3:List*",
    "s3:Put*"
  ],
  "Resource": [
    "*"
  ]
}
]
}
}

```

Note: S3-BUCKET1 & S3-BUCKETZ are the buckets you create while using Amazon Cloud Disk Extenders. You can learn more about how to create these buckets in [Adding Cloud Disk Extenders](#).

Linking the Policy

To link the policy with the **SoftNAS Cloud®** User:

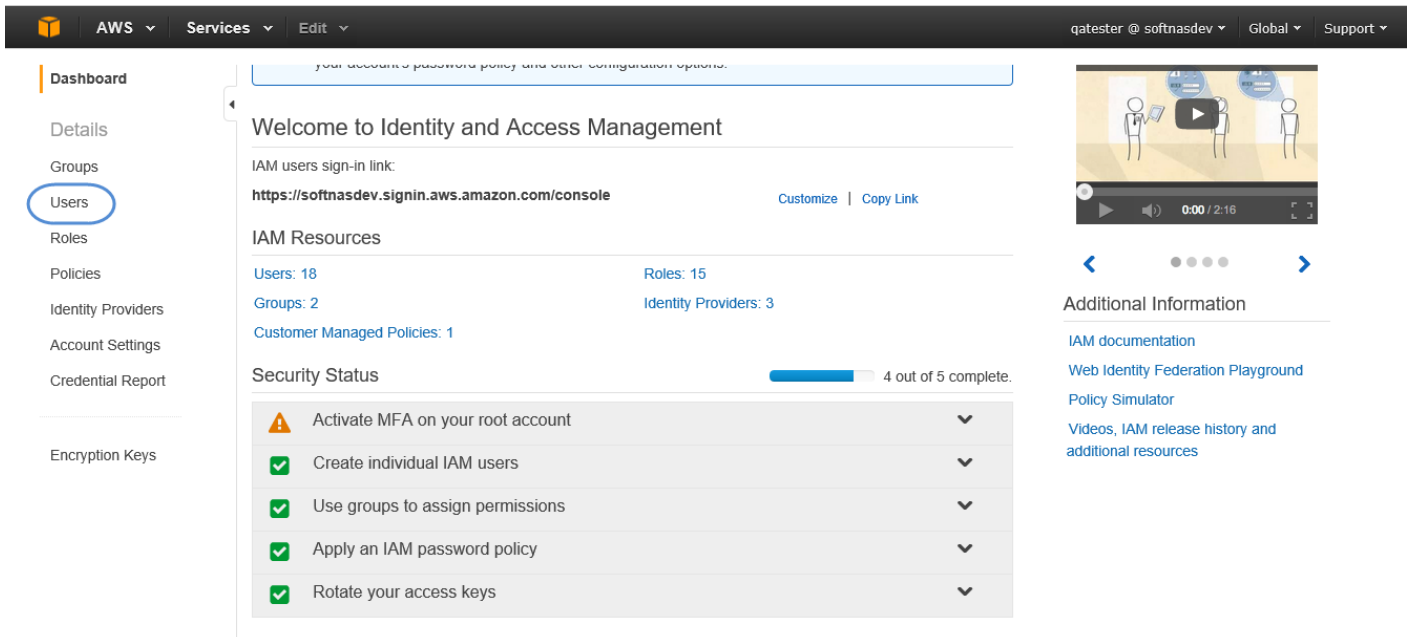
1. Login to the Amazon Web Services Dashboard.
2. Click on Identity & Access Management (IAM).

Amazon Web Services

<p>Compute</p> <ul style="list-style-type: none"> EC2 Virtual Servers in the Cloud EC2 Container Service Run and Manage Docker Containers Elastic Beanstalk Run and Manage Web Apps Lambda Run Code in Response to Events <p>Storage & Content Delivery</p> <ul style="list-style-type: none"> S3 Scalable Storage in the Cloud CloudFront Global Content Delivery Network Elastic File System PREVIEW Fully Managed File System for EC2 Glacier Archive Storage in the Cloud Import/Export Snowball Large Scale Data Transport Storage Gateway Integrates On-Premises IT Environments with Cloud Storage <p>Database</p> <ul style="list-style-type: none"> RDS Managed Relational Database Service DynamoDB Predictable and Scalable NoSQL Data Store ElastiCache In-Memory Cache Redshift Managed Petabyte-Scale Data Warehouse Service 	<p>Developer Tools</p> <ul style="list-style-type: none"> CodeCommit Store Code in Private Git Repositories CodeDeploy Automate Code Deployments CodePipeline Release Software using Continuous Delivery <p>Management Tools</p> <ul style="list-style-type: none"> CloudWatch Monitor Resources and Applications CloudFormation Create and Manage Resources with Templates CloudTrail Track User Activity and API Usage Config Track Resource Inventory and Changes OpsWorks Automate Operations with Chef Service Catalog Create and Use Standardized Products Trusted Advisor Optimize Performance and Security <p>Security & Identity</p> <ul style="list-style-type: none"> Identity & Access Management Manage User Access and Encryption Keys Directory Service Host and Manage Active Directory Inspector PREVIEW Analyze Application Security WAF Filter Malicious Web Traffic 	<p>Internet of Things</p> <ul style="list-style-type: none"> AWS IoT BETA Connect Devices to the cloud <p>Mobile Services</p> <ul style="list-style-type: none"> Mobile Hub BETA Build, Test, and Monitor Mobile apps Cognito User Identity and App Data Synchronization Device Farm Test Android, Fire OS, and iOS apps on real devices in the Cloud Mobile Analytics Collect, View and Export App Analytics SNS Push Notification Service <p>Application Services</p> <ul style="list-style-type: none"> API Gateway Build, Deploy and Manage APIs AppStream Low Latency Application Streaming CloudSearch Managed Search Service Elastic Transcoder Easy-to-use Scalable Media Transcoding SES Email Sending Service SQS Message Queue Service SWF Workflow Service for Coordinating Application Components <p>Enterprise Applications</p>
--	--	--

This will bring up the IAM Secure AWS Access Control Dashboard.

3. From the Dashboard, click on **Users**.



4. Click **Create New Users**.

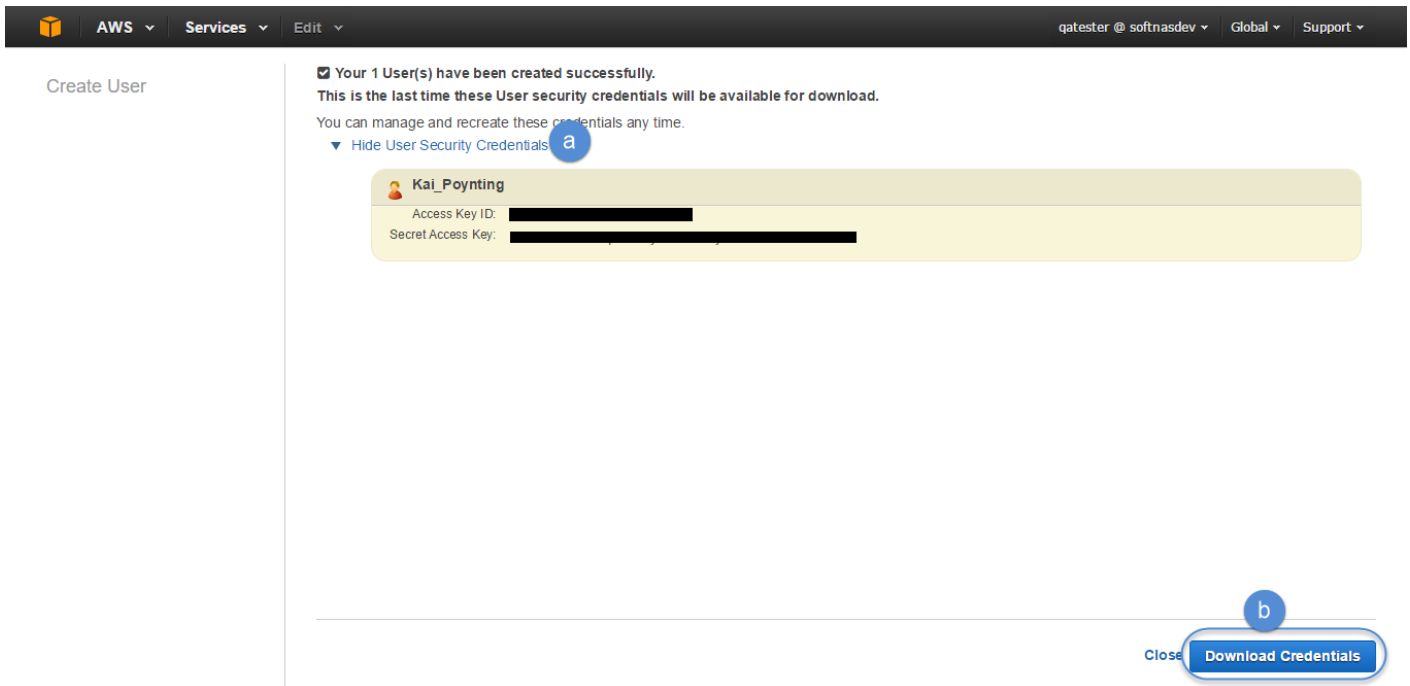
5. Enter a name for the User (e.g. **SoftNAS_User**). Check the box stating **Generate an access key for each User**.

6. Click **Create User**.

Record the Access Key ID and Secret Access Key at this time. These will be required later when setting up HA for **SoftNAS Cloud®** instances.

a) To view your credentials, click Show User Security Credentials.

b) To quickly record your credentials, click Download Credentials. Your credentials will be saved to your local machine as a CSV file.



7. Navigate to the list of Users and select the newly created **SoftNAS Cloud®** User.

8. Click on Permissions to bring up the User Policies section.

<input checked="" type="checkbox"/>	Kai_Poynting	0		N/A	1 active
<input type="checkbox"/>	lino	1	✓	2015-10-26 05:35 PDT	1 active

Select the User

IAM > Users > Kai_Poynting

Summary

Click on Permissions

Groups **Permissions** Security Credentials

9. Click **Attach Policy**. Then select the **Custom Policy** you created above. It will appear as an attached policy under permissions.

IAM > Users > Kai_Poynting

Summary

User ARN: arn:aws:iam::892064206063:user/Kai_Poynting
Has Password: No
Groups (for this user): 0
Path: /
Creation Time: 2015-10-31 09:59 PDT

Groups **Permissions** Security Credentials

Managed Policies

The following managed policies are attached to this user. You can attach up to 10 managed policies.

Attach Policy

Policy Name	Actions
SoftNAS_IAM	Show Policy Detach Policy Simulate Policy

Inline Policies

Regions and Availability Zones for Amazon Machine Images

Availability Zones & Regions

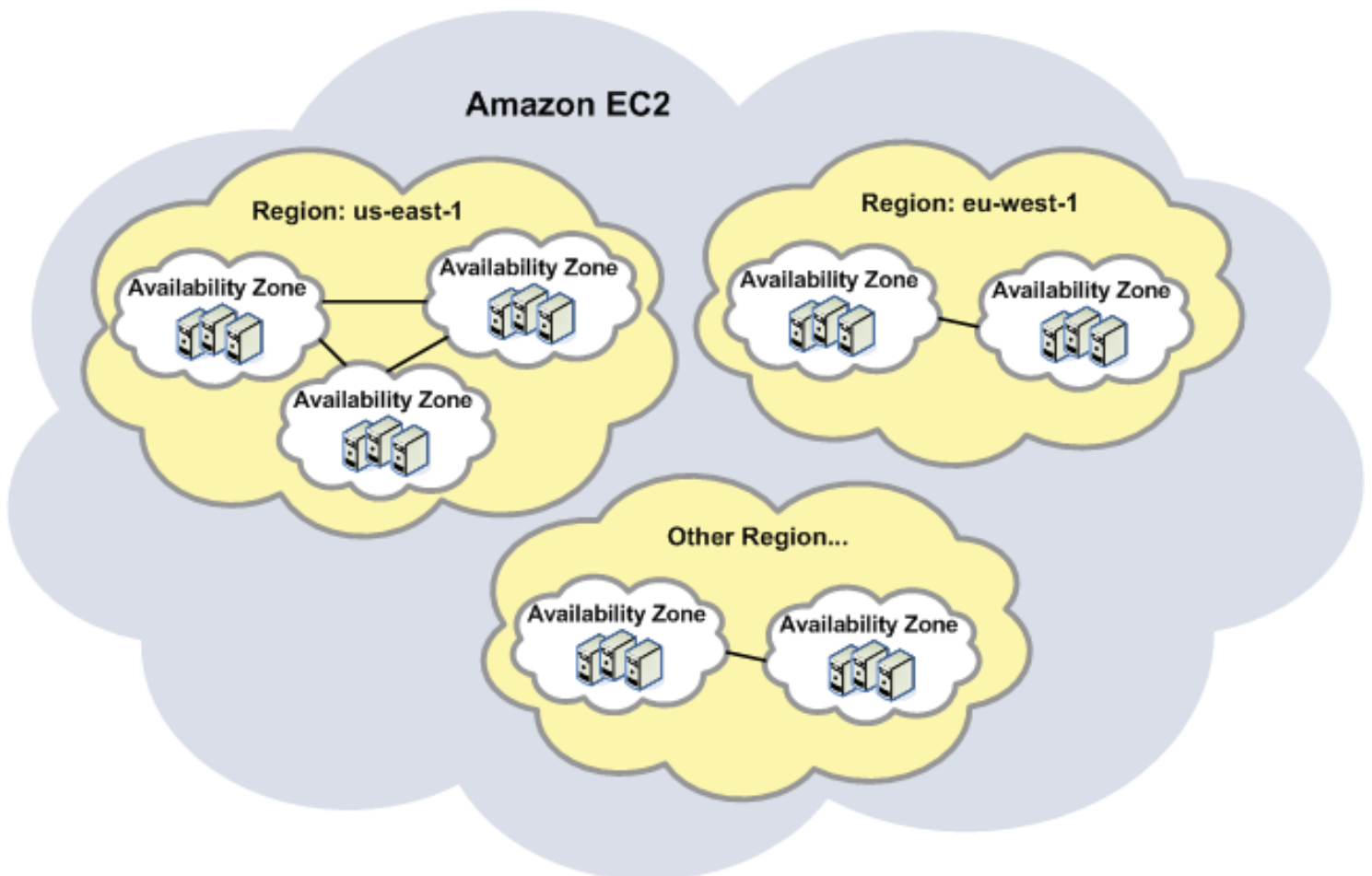
Amazon EC2 provides the ability to place instances in multiple locations. **Amazon EC2** locations are composed of **Availability Zones** and **Regions**.

- **Regions** are dispersed and located in separate geographic areas (US, EU, etc.).
- **Availability Zones** are distinct locations within a Region that are engineered to be isolated from failures in other Availability Zones and provide inexpensive, low latency network connectivity to other Availability Zones in the same Region.

Benefits of launching instances in separate Regions include:

- physical proximity of the application to specific customers, improving data transfer speeds
- may meet legal or other business requirements
- With the appropriate settings, it protects the application/s from the failure of a single location.

The following graphic shows a representation of **Amazon EC2**. Each Region is completely independent. Each Availability Zone is isolated, but connected through low-latency links.



There may be some minor cost differences depending on the availability zone chosen.

Another factor to be used in choosing an availability zone is geographic proximity to where applications and users will be located. It's typically a good idea to minimize the network latency between the web server / applications and users, which is likely a deciding factor for which region to use.

Before beginning the configuration of **SoftNAS** on **Amazon EC2**, select the nearest location/region for **Amazon Machine Image** of **SoftNAS** on the **SoftNAS** site.

Note : **SoftNAS Cloud®** is already installed as **Amazon Machine Image (AMI)**, which means there's nothing to download. Simply choose an AMI and subsequent **AWS** region.

Pricing Details

For region

- US East (N. Virginia)
- US West (Oregon)
- US West (N. California)
- EU (Ireland)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- South America (Sao Paulo)

charges will still apply, unless you use this product on a Micro instance, use less than 750 hours per month and qualify for [AWS Free Usage Tier](#). Free Trials will automatically convert to a paid subscription upon expiration. Note that Free Trials are only applicable for hourly subscriptions, but you can opt to purchase an annual subscription at any time.

Hourly Fees

Total hourly fees will vary by instance type and EC2 region.

Software Pricing: **Hourly** **Annual**

Take note of the region chosen. All AMIs created with this account will be launched in that region.

Elastic and Virtual IP Addresses

When planning your AWS instance, it is important to keep high availability in mind prior to creating your instance. The decision to create a highly available storage solution using SoftNAS must be made early in order to allow you to prepare your build accordingly. One decision that needs to be made early is whether to use Instance, Elastic or Virtual IPs. Beyond choosing the type of IP address you wish, there are many configuration steps required to prepare for a high availability configuration. For complete coverage of high availability through SoftNAS, go to our [SoftNAS High-Availability Guide](#).

Amazon EC2 provides three types of IP addresses:

- 1) **Instance IP address:** each instance is assigned a dynamic IP address, assigned by DHCP. These are on the internal, private network, assigned by DHCP. They will be different each time a SoftNAS instance is booted.
- 2) **Elastic IP address:** these are static IP addresses, and is recommended for use with SoftNAS, if not using **Virtual IPs**. These IP addresses are public-facing, static IP addresses which are "associated" with a particular instance. While associated with an instance, these IP addresses are always the same, so there is a predictable way to address each SoftNAS instance in the environment. Elastic IP addresses are termed "elastic" as they can be dynamically reassigned (moved) from once instance to another.
- 3) **Virtual IP addresses:** SoftNAS now supports the set up of highly available VPCs with private subnets using virtual IPs. Elastic IP setup is still supported for legacy purposes. However, Virtual IP setup, more secure because it does not require a public facing IP, is our recommended best practice. If setting up SoftNAS SNAP HA™ with virtual IPs, there is no need to create Elastic IPs at all. The IPs assigned statically or via DHCP at instance creation time can be retained.

Virtual IPs and High Availability

Setup and maintenance of Virtual IP addresses are covered in the [SoftNAS High-Availability Guide](#). Virtual IP addresses are relatively simple to set up, requiring only that each VPC instance must have an IP in the same CIDR block. A third IP outside this CIDR block will be selected during the HA wizard setup. This will be the IP address you will use to access the highly available share, whichever instance is currently the primary.

There are multiple ways to configure secure administrative access to the **SoftNAS SNAP HA™** storage controllers:

- 1) VPN - this is the most secure stand-alone solution, and a recommended minimum best practice for limiting access to the private IPs of each **SoftNAS Cloud®** controller. In this case, use DNS to assign a common name to each controller (e.g., "nas01.localdomain.com", "nas02.localdomain.com"), making routing to each **SoftNAS Cloud®** controller convenient for administrators.
- 2) Admin Desktop - an even more secure approach is to combine VPN access with an Administrator's desktop, (sometimes referred to as a jumpbox) typically running Windows and accessed via RDP. This secure admin desktop adds another layer of authentication, namely Active Directory (or local account) authentication.

Elastic IPs, HA and Dynamic DNS

Elastic IPs were long the go-to method, providing the flexibility to create a high-availability (HA) configuration. With the ability to configure Virtual IPs, more secure because it offers no public IP access point, Elastic IPs are no longer the recommended configuration, but are supported for legacy purposes as they are still widely used.

For more information on the SoftNAS High Availability technology via SNAP HA™ or SnapReplicate, consult the [SoftNAS High-Availability Guide](#).

As a quick example, consider two SoftNAS instances with replication between them configured as an Active-Passive HA pair in different availability zones in the same region (or across regions, as applicable to local needs). Let's call these SoftNAS instances "A" and "B", where "A" is currently the active, primary NAS.

Assign three elastic IP addresses - one for A, one for B, and one "floating" elastic IP used for failover. Applications and DNS for **SoftNAS Cloud®** would reference the third elastic IP, as shown below.

Elastic IP	Assigned To
IP 1	SoftNAS Instance A
IP 2	SoftNAS Instance B
IP 3	DNS - points to instance A initially

In this configuration, IP 1 and IP 2 are used to administer and perform replication between SoftNAS instances. DNS points to "A", which is the active SoftNAS instance. In this configuration, replication is configured to flow from "A" to "B", so that "B" is effectively a mirror of "A", always ready for a failover.

In the event of a zone failure, physical disk failure or scheduled downtime / maintenance, IP 3 can be reassigned to "B", which becomes the active instance. When "A" is restored, replication can be reconfigured to flow from "B" to "A".

Note: It can take up to 30 seconds to complete an elastic IP reassignment to a different instance.

Alternatively, use IP 1 and IP 2 (without IP 3) and use dynamic DNS with a short TTL (time to live) and perform failover by simply reassigning the IP 1 or IP 2 via dynamic DNS.

There are many different ways to configure HA and IP addresses - the above represents just a few ways, provided to illustrate the flexibility provided by elastic IP addressing and/or dynamic DNS.

For more information:

- [Allocating New Elastic IP Address](#)
- [Associating and Disassociating an Address](#)

Releasing the Address

It is best practice to release the addresses that are no longer being used.

To do so:

1. On the **Elastic IP** addresses page, select the address to be released.

Note: Release the Elastic IP address that is **not associated with an instance**.

2. Click **Release Address**.

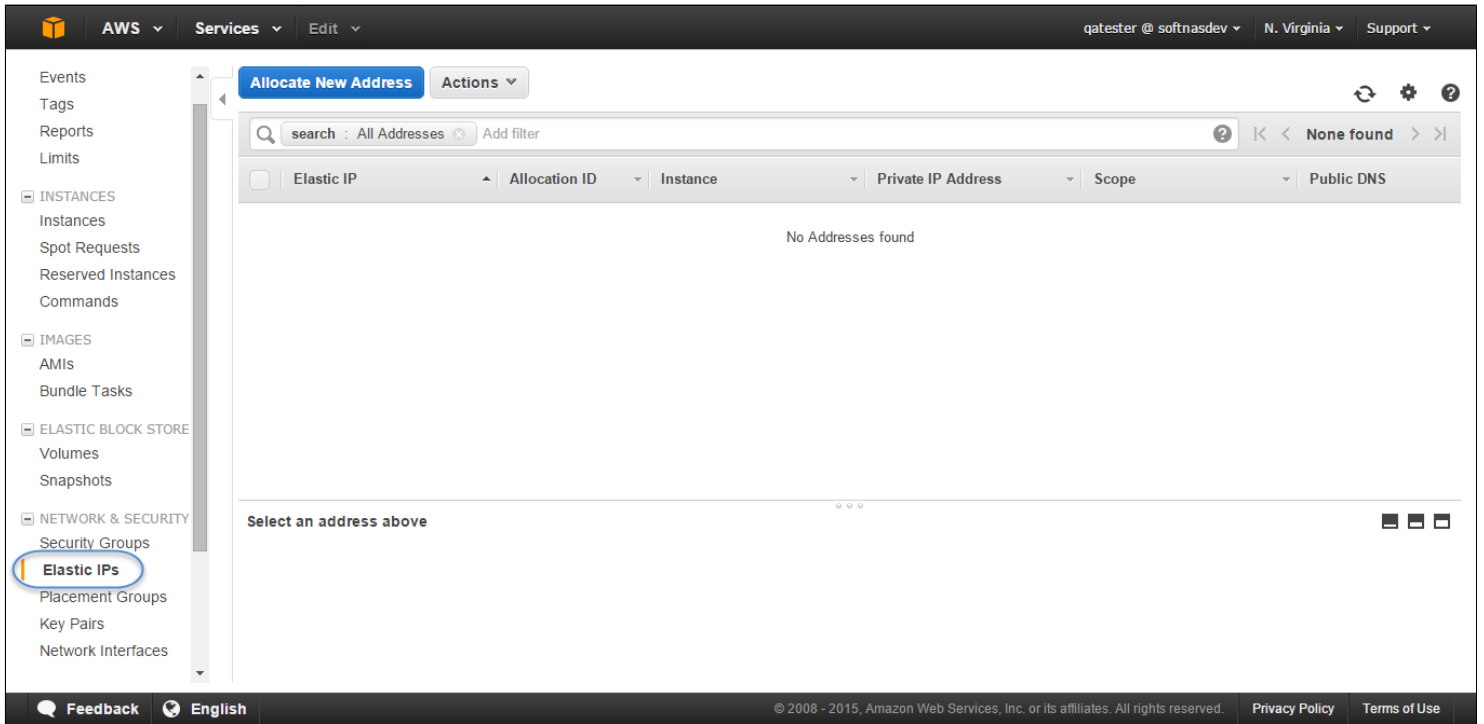
The **Release Address** message box asking to confirm the releasing of the address will be displayed.

The selected IP address will be released.

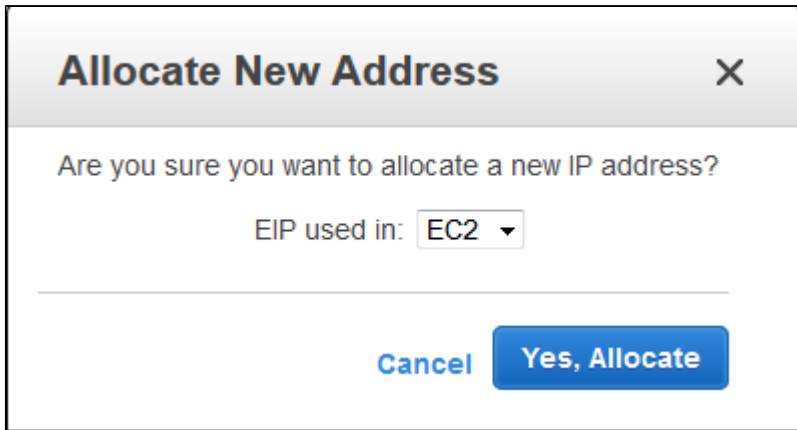
Allocating New Elastic IP Addresses

Allocate an Elastic IP

1. From the EC2 Dashboard, click on **Elastic IPs**.



2. Click on **Allocate New Address**.




3. Confirm the allocation of the new address to the EIP.

4. Click **Yes, Allocate**.

The allocated elastic IP and its IPv4 address will be displayed. Keep a record of this information.

Allocate New Address ✕

 **New address request succeeded**
Elastic IP: 54.214.1.3. [View Elastic IP](#)

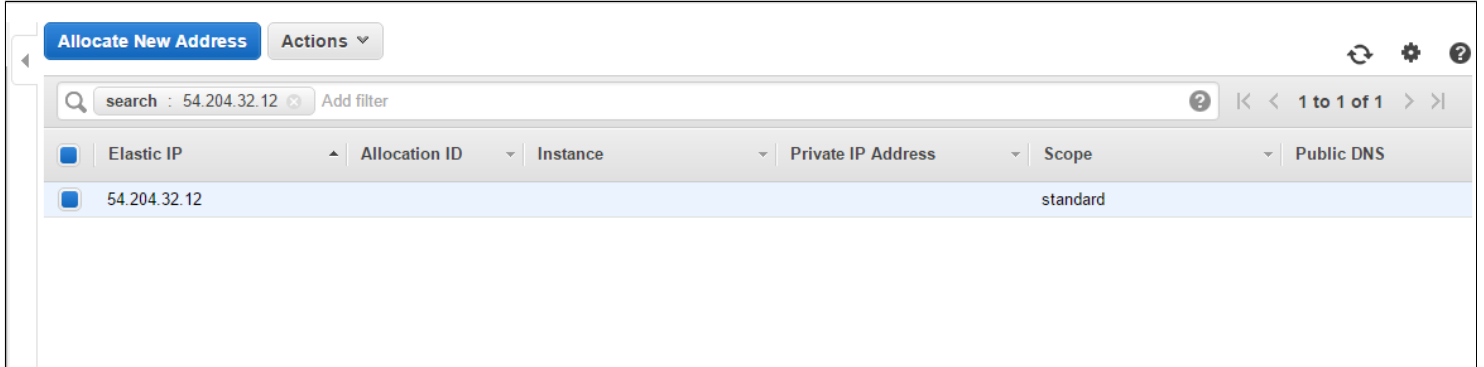
Close

Associating and Disassociating an Address

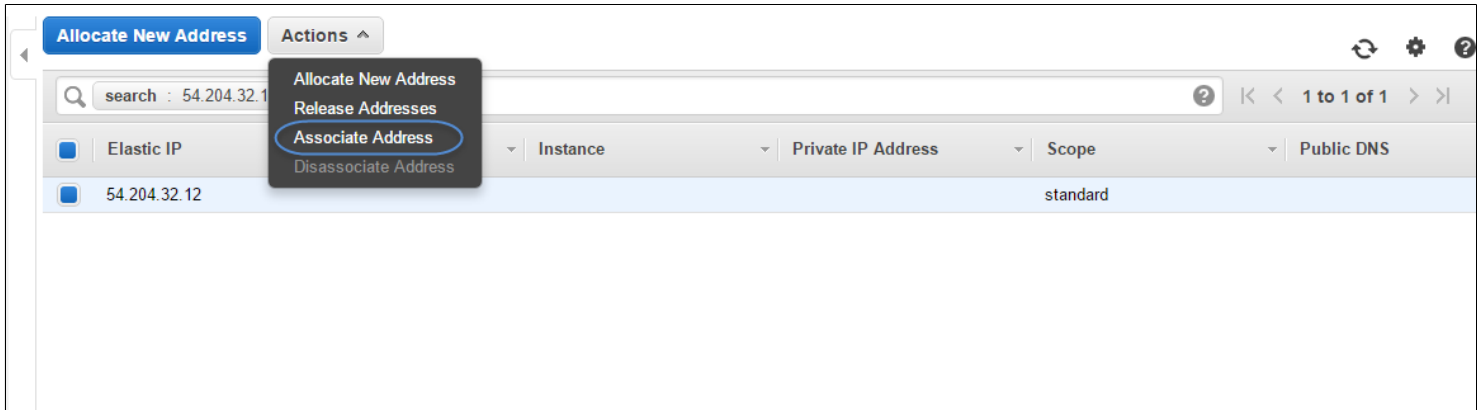
Associate or dissociate an elastic IP address with an instance.

Associating an Address

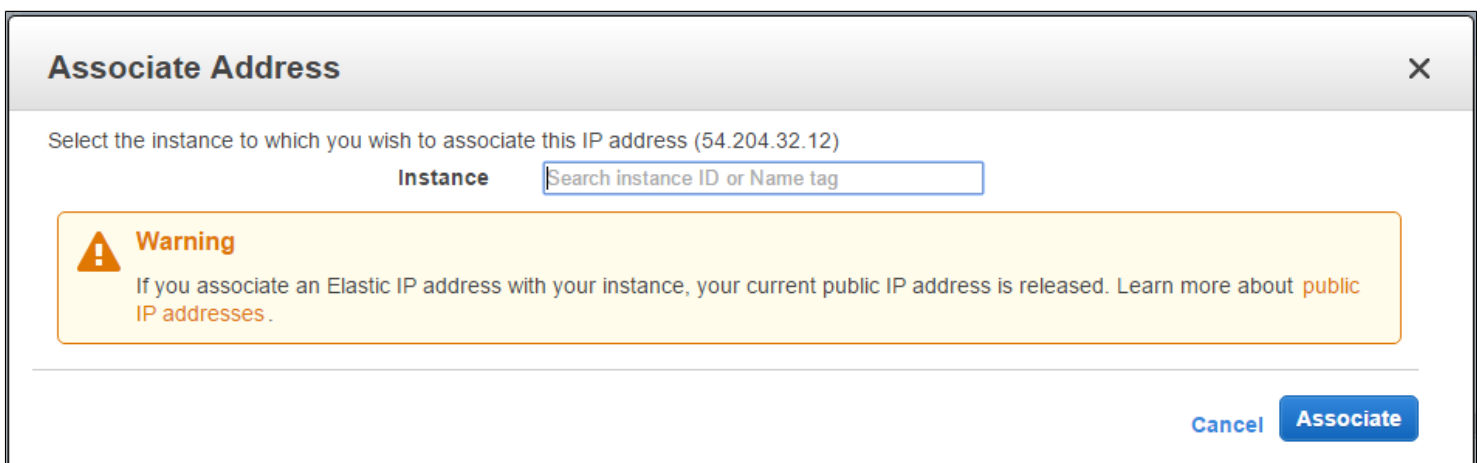
1. On the **Elastic IP** addresses page, select the address to be associated with an instance.



2. Under Actions, click **Associate Address**.



The **Associate Address** dialog will be displayed.



3. Select the instance to be associated from the Instance drop down list.

4. Click **Associate**.

The elastic IP address is now associated with **SoftNAS Cloud®**.

Disassociate Address

Similarly, it is possible to dissociate an address from the associated instance.

1. Select the elastic IP address to be dissociated from the instance.
2. Click **Dissociate Address**.

The Dissociate Address message box asking for confirmation of the dissociation of address with the specific instance will be displayed.

3. Click **Yes, Disassociate**.

The selected address will be dissociated from the instance.

Amazon EC2 Setup and Performance Considerations

Network Planning Considerations

Take into account best practices for **AWS EC2** combined with **SoftNAS Cloud®** [optimization configurations](#) before getting started with **SoftNAS Cloud® for Amazon EC2**.

Note: For extremely heavy workloads, increase cache memory with **High Memory Instances** and / or **EBS-Optimized** and **Bursting IOPS** to provide better control over available IOPS. Consult the [AWS Instances](#) section for more detailed recommendations and explanations on this topic.

2nd Level Read Cache

To further improve read and query performance, configure a Read Cache device for use with **SoftNAS Cloud®**. **SoftNAS Cloud®** leverages the **ZFS L2ARC** as its second-level cache.

AWS EC2 Read Cache

During instance creation, choose an instance type that includes local solid state disk (SSD) disks. The storage server will make use of as much read cache as is provided to it. Read cache devices can be added and removed at any time with no risk of data loss to an existing storage pool. There are two choices for SSD read cache on EC2:

1. **Local SSD** - the fastest read cache available, as the local SSDs are directly attached to each EC2 instance and provide up to 120,000 IOPS.
2. **EBS Provisioned IOPS** - these EBS volumes can be assigned to SSD, providing a specified level of guaranteed IOPS.

Create and Configure an Instance in AWS

Amazon Web Services provides virtual cloud platform and computing resources for developers and IT professionals. **SoftNAS Cloud®** provides a powerful shared-storage interface into this robust resource through unified connections of CIFS, NFS, iSCSI, giving the virtually unlimited capacity, remote replication, and high availability needed for the expected workload.

1. Complete the [Launching SoftNAS Cloud® Platforms](#) initial registration procedure, beginning from www.softnas.com and choose **SoftNAS Cloud® for AWS**.
2. Continue through the registration wizard.
3. A **SoftNAS Cloud®** for Amazon Marketplace pricing page will ultimately appear. Choose to **Launch with 1-Click** or change preferred settings in the **Manual Launch** page and Launch from **EC2 Console**.

Note: Review all pricing structure and usage fees in each section before confirming or launching an instance. Some settings will impact usage and subscription fees, even during a trial period. Amazon defines **instance** as "a copy of an Amazon Machine Image running as a virtual server in the **AWS cloud**." This guide will use the **AWS** terminology in this section for UI consistency.

Manual Launch Procedure

To maximize customization, **Manual Launch** is the recommended choice for initial setup. Below are the basic steps to follow.

1. Launch Instance

- Once an AWS account has been created, log on to [Amazon EC2](#) and navigate to **EC2 Dashboard**.
- Create Instance from the **Launch Instance** item that appears on the Dashboard as well as the Instances page.

 Launch Instance

Note: The active region is visible in the Amazon Header menu next to the access email address. This can be changed to create servers in different regions, but keep in mind budgeted subscription costs and data usage fees. Also consider permissions for different user levels at this stage.

2. Choose a SoftNAS Cloud® Amazon Machine Image (AMI)

From the menu on the left, click **AWS Marketplace** and search for **SoftNAS**.

Note: **SoftNAS Cloud®** supports two different virtualization types, either paravirtual (**PV**) or hardware virtual machine (**HVM**, required for **Enhanced Network Support**, recommended) on General Use or Enterprise Level. [Choose the instance type](#) that supports predicted network requirements.

- 1. Choose AMI
- 2. Choose Instance Type
- 3. Configure Instance
- 4. Add Storage
- 5. Tag Instance
- 6. Configure Security Group
- 7. Review

Step 1: Choose an Amazon Machine Image (AMI)

[Cancel and Exit](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Quick Start

My AMIs

AWS Marketplace

Community AMIs

Categories

All Categories

Software Infrastructure (4)

Business Software (4)

Operating System

Clear Filter

All Linux/Unix

CentOS (4)

<< 1 to 4 of 4 Products >>

SoftNAS Cloud - High-Performance Cloud NAS (PV/20TB)

★★★★★ (6) | SoftNAS Cloud 3.1 | Sold by SoftNAS

Free Trial

Starting from **\$0.18/hr** or from **\$1,451/yr** (up to 68% savings) for software + AWS usage fees

Linux/Unix, CentOS 6.5 | 64-bit Amazon Machine Image (AMI) | Updated: 10/2/14

SoftNAS is the leading cloud NAS for Amazon EC2. Supports standard mounts including NFS, CIFS and iSCSI through the simple SoftNAS StorageCenter GUI with multiple EBS, SSD ...

[More info](#)

Select

SoftNAS Cloud - High-Performance Cloud NAS (HVM/SRV-IO/20TB)

★★★★★ (0) | SoftNAS Cloud 3.0 [Previous versions](#) | Sold by SoftNAS

Free Trial

Starting from **\$0.45/hr** or from **\$3,627/yr** (8% savings) for software + AWS usage fees

Linux/Unix, CentOS 6.5 | 64-bit Amazon Machine Image (AMI) | Updated: 8/17/14

SoftNAS is the leading cloud NAS for Amazon EC2. Supports standard mounts including NFS, CIFS and iSCSI through the simple SoftNAS StorageCenter GUI with multiple EBS, SSD ...

[More info](#)

Select

Note: Prices and version levels may have changed. Select the version that most accurately fits the needs of deployment. Click **Next**.

3. Choose an Instance Type

- Tick the Instance that best fits the expected environment. Then click **Next: Configure Instance Details**.

- 1. Choose AMI
- 2. Choose Instance Type
- 3. Configure Instance
- 4. Add Storage
- 5. Tag Instance
- 6. Configure Security Group
- 7. Review

Step 2: Choose an Instance Type

Filter by:

All instances

Current generation

[Show/Hide Columns](#)

Currently selected: m1.small (1 ECUs, 1 vCPUs, Intel Xeon Family, 1.7 GiB memory, 1 x 160 GiB Storage Capacity)

	Family	Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
<input type="checkbox"/>	Micro instances <small>Free tier eligible</small>	t1.micro	up to 2	1	0.613	EBS only	-	Very Low
<input type="checkbox"/>	General purpose	m3.medium	3	1	3.75	1 x 4 (SSD)	-	Moderate
<input type="checkbox"/>	General purpose	m3.large	6.5	2	7.5	1 x 32 (SSD)	-	Moderate
<input type="checkbox"/>	General purpose	m3.xlarge	13	4	15	2 x 40 (SSD)	Yes	Moderate
<input type="checkbox"/>	General purpose	m3.2xlarge	26	8	30	2 x 80 (SSD)	Yes	High
<input checked="" type="checkbox"/>	General purpose	m1.small	1	1	1.7	1 x 160	-	Low
<input type="checkbox"/>	Compute optimized	c3.large	7	2	3.75	2 x 16 (SSD)	-	Moderate

Cancel

Previous

Review and Launch

Next: Configure Instance Details

Note: At any point past this screen, skip to **Review and Launch** to accept the default settings for the rest of the option screens.

Copyright ©2017 SoftNAS, Inc.

General Instance Types and Setup Recommendations

Consider the recommendations in section [AWS Instances](#) for a clearer network design.

Note: Micro instances may be adequate for some development and QA testing purposes, but consider the limitations on memory, CPU and network that are imposed on micro instances. These limitations have a significant impact on **SoftNAS Cloud®**'s performance and throughput.

View Instance Details

View the complete details of an instance that is successfully launched.

1. Click **Instances** in the left panel.

All the instances in the region will be displayed.

2. Select the instance for whose details are to be viewed.

The details of that instance will be displayed at the bottom of the screen in different tabs.

Instance: **i-af588d87** Public DNS: -

Description

Status Checks

Monitoring

Tags

Instance ID i-af588d87	Public DNS -
Instance state running	Public IP -
Instance type m1.small	Elastic IP -
Private DNS ip-10-135-42-108.ap-southeast-1.compute.internal	Availability zone ap-southeast-1a
Private IPs 10.135.42.108	Security groups launch-wizard-1 . view rules
Secondary private IPs -	Scheduled events No scheduled events
VPC ID -	AMI ID SoftNAS 2.1.3 PV (ami-347a2966)
Subnet ID -	Platform -
Network interfaces -	IAM role -
Source/dest. check False	Key pair name JinchengSoftNAS2
EBS-optimized False	Owner 892064206063
	Launch time April 24, 2014 7:13:15 PM UTC-4 (less than

3. The **Description** tab shows all the basic and general information of the instance.

4. The **Status Checks** tab displays the information on system status checks and instance status checks. **Status Check Alarms** are created from here.

Status Checks & Alarms

5. The **Monitoring** tab displays all the **CloudWatch** alarm and metrics in graph format.

6. The **Tags** tab will show all the tags that are associated with the instance. Add, edit or remove tags in this area.

Provide Instance Details

Setting	Recommended	Notes
Number of Instances	1	
Network	EC2	See VPC Notes below
Availability Zone	No preference	Choose a preset zone
IAM	None	
Shutdown Behavior	Stop	
Enable Termination Protection	Checked	Prevent Instances from being accidentally deleted
Monitoring	As preferred	See CloudWatch notes below

Consider the following elements when configuring an Instance:

Element	Setup Recommendations
Memory	• 4GB or more for best results.
	• 1GB RAM needed for kernel and system ops
	• Anything >1GB is available for use as cache memory
	• Add 1GB RAM per TB of deduplicated data.
CPU	• Minimum of 2 required for normal operation.
	• Add CPUs if CPU usage is observed at >60%.
Network	• Elastic Block Storage disks run across the network in a SAN configuration.
	• High-performance needs can be met with the extra-charge option Provisioned IOPS .

VPC Notes: For optimal efficiency, launch an instance into an **Amazon VPC (Virtual Private Cloud)** environment instead of the default **Launch Into** option to EC2. VPCs can be useful if all computing will be done in the EC2 environment, or to interconnect an existing network via a VPN gateway to the VPC environment; e.g., setting up an IPsec tunnel between an existing data center and the VPC. To operate **SoftNAS Cloud®** within the private subnet of a VPC, create an outbound NAT route that enables the **SoftNAS Cloud®** instance to access the Internet to perform software updates, activation, etc. In this case, only outbound TCP traffic to the softnas.com domain is required to be enabled; i.e., inbound access to ports 22 and 443 for administration can be restricted to VPC subnet access only.

Note: Use a VPC to use **SoftNAS Cloud®** in high availability mode (**SNAP HA™**). For more information, see the document [SoftNAS High Availability Guide](#).

CloudWatch provides a detailed monitoring of the **SoftNAS Cloud®** instance. The Free Tier includes basic monitoring metrics at 5-minute intervals, 10 monitoring metrics, 10 alarms and 1 million API requests at no additional charge. Check the box in the **Monitoring** field to enable **CloudWatch**, which is recommended.

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot Instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances	<input type="text" value="1"/>
Purchasing option	<input type="checkbox"/> Request Spot Instances
Network	<input type="text" value="Launch into EC2-Classic"/> Ⓢ Create new VPC
Availability Zone	<input type="text" value="No preference"/>
IAM role	<input type="text" value="None"/>
Shutdown behavior	<input type="text" value="Stop"/>
Enable termination protection	<input type="checkbox"/> Protect against accidental termination
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring <small>Additional charges apply.</small>

▶ Advanced Details

Cancel Previous Review and Launch Next: Add Storage

Advanced Details may also be set up in this step.

▼ Advanced Details

User data ⓘ As text As file Input is already base64 encoded

(Optional)

Cancel Previous Review and Launch Next: Add Storage

Click **Next: Add Storage**.

Add Storage

Attach additional EBS volumes and instance store volumes, or edit the settings of the root volume.

Note: Instance store volumes may not be attached after launching an instance; however, EBS volumes may be attached after the instance is launched. Keep this in mind during initial network planning.

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Type ⓘ	Device ⓘ	Snapshot ⓘ	Size (GiB) ⓘ	Volume Type ⓘ	IOPS ⓘ	Delete on Termination ⓘ	Encrypted ⓘ
Root	/dev/sda1	snap-2e229192	<input type="text" value="30"/>	General Purpose (SSD) ▼	90 / 3000	<input checked="" type="checkbox"/>	Not Encrypted
Instance Store 0 ▼	/dev/sdb ▼	N/A	N/A	N/A	N/A	N/A	Not Encrypted ✕

Add New Volume

Configure Root and Instance Store

Create and configure additional volumes for **SoftNAS Cloud®** use. A default installation includes one **SoftNAS Cloud®** 30GB root device and a configurable first volume as an Instance Store.

Recommended Initial Configuration Settings:

Type ⓘ	Device ⓘ	Snapshot ⓘ	Size (GiB) ⓘ	Volume Type ⓘ	IOPS ⓘ	Delete on Termination ⓘ	Encrypted ⓘ
Root	/dev/sda1	snap-276e1a89	30	General Purpose (SSD)	90 / 3000	<input type="checkbox"/>	Not Encrypted
Instance Store 0	/dev/sdb	N/A	N/A	N/A	N/A	N/A	Not Encrypted ✕

[Add New Volume](#)

See also: [Managing Volumes](#)

Add More Storage

1. In the above menu, click **Add New Volume**.
2. Alternatively, go to **Elastic Block Storage** in the menu, and click **Volumes**.

Create Volume ✕

Type ⓘ General Purpose (SSD) ▼

Size (GiB) ⓘ 100 (Min: 1GiB, Max: 1024GiB)

IOPS ⓘ 300 / 3000 (3000 IOPS bursts and baseline of 3 IOPS per GB)

Availability Zone ⓘ us-east-1a ▼

Snapshot ID ⓘ Search (case-insensitive)

Encryption ⓘ Encrypt this volume

Cancel
Create

3. Enter the configuration settings best suited for an environment based on best practices and the relevant interface above.

Note: Key Pairs and Instance Tags secure data and verify ownership. Properly set up, these layers of validation protect EC2 Instances from accidental or unauthorized users.

Instance Tags

The EC2 environment takes advantage of keyword tag benefits by proactively setting a connection between an account and access to the current instance.

Step 5: Tag Instance

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn more](#) about tagging your Amazon EC2 resources.

Key (127 characters maximum)	Value (255 characters maximum)
<input type="text" value="Name"/>	<input type="text"/>

(Up to 10 tags maximum)

Note the following basic tag restrictions:

- The **aws:** prefix is reserved for AWS use, and tags with this prefix do not count against tags per resource limit.
- Maximum Tags: 10 tags per resource
- Maximum Key String: 127 Unicode characters (case-sensitive)
- Maximum Value String: 255 Unicode characters (case-sensitive)

Creating or Selecting a Security Group

Next, network settings and services can be determined in advance by setting up a Security Group.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance **6. Configure Security Group** 7. Review

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: Create a **new** security group

Select an **existing** security group

Security group name:

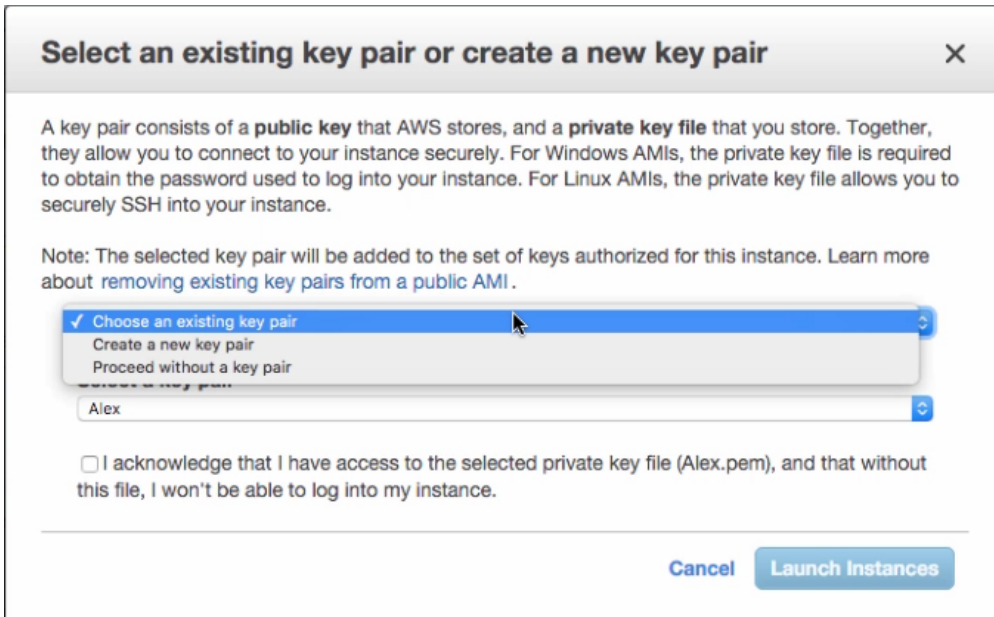
Description:

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ
HTTPS ▾	TCP	443	Custom IP ▾ 172.16.151.0/32 ✕
Custom UDP Rule ▾	UDP	88	Custom IP ▾ 172.16.151.0/32 ✕
Custom TCP Rule ▾	TCP	88	Custom IP ▾ 172.16.151.0/32 ✕
SSH ▾	TCP	22	Custom IP ▾ 172.16.151.0/32 ✕

1. If creating a new security group for your instance, select the **Create a new security group** radio button.
2. To create a custom configuration, simply click **Add Rule**, and select the desired protocol, the desired port, and for improved security, place a limit on the accepted source IP.
3. To select an existing security group configuration, click the **Select an existing security group** radio button, and select the desired option from the dropdown that appears.

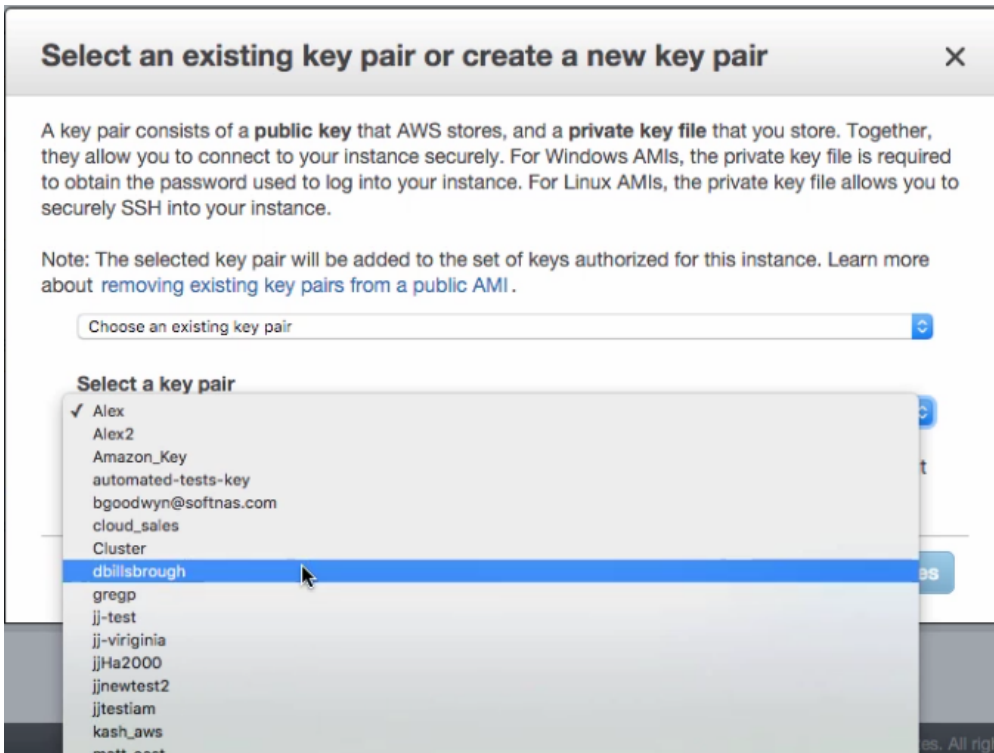
Creating a Key Pair

A Key Pair is a pair of security credentials associated with this Instance; the **Public Key** and the **Private Key**. The **Create Key Pair** section of the wizard will be displayed. In this step, create a public/private key pair used with SSH to access and administer the **SoftNAS Cloud®** instance in the cloud.

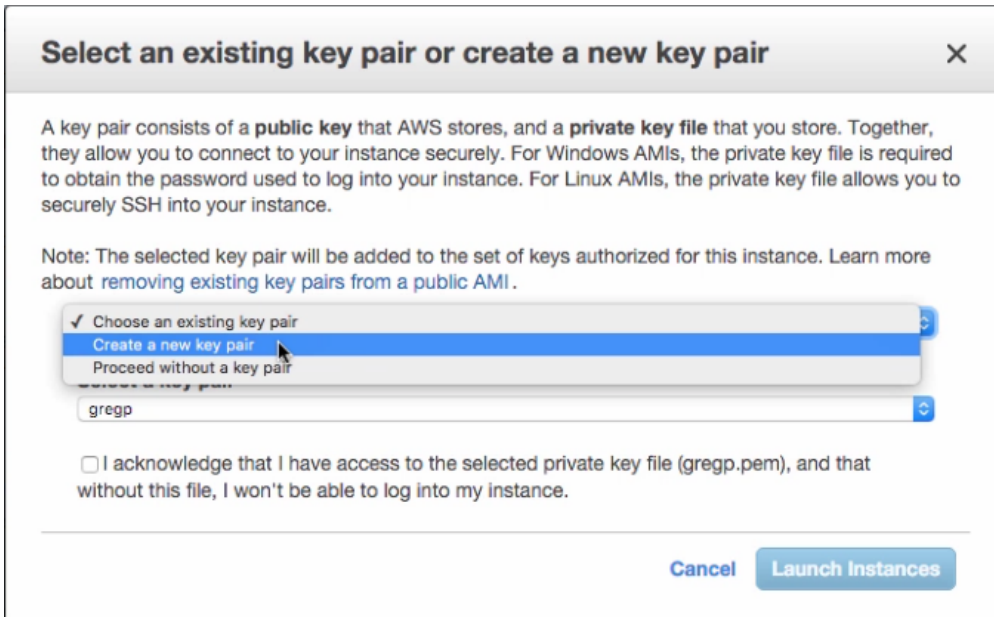


The **Key Pair** helps to securely connect to an instance when it is launched. Either choose from existing key pairs that have been created in the current region or create a new key pair. In the above example, the option **Choose from existing Key Pairs** is selected.

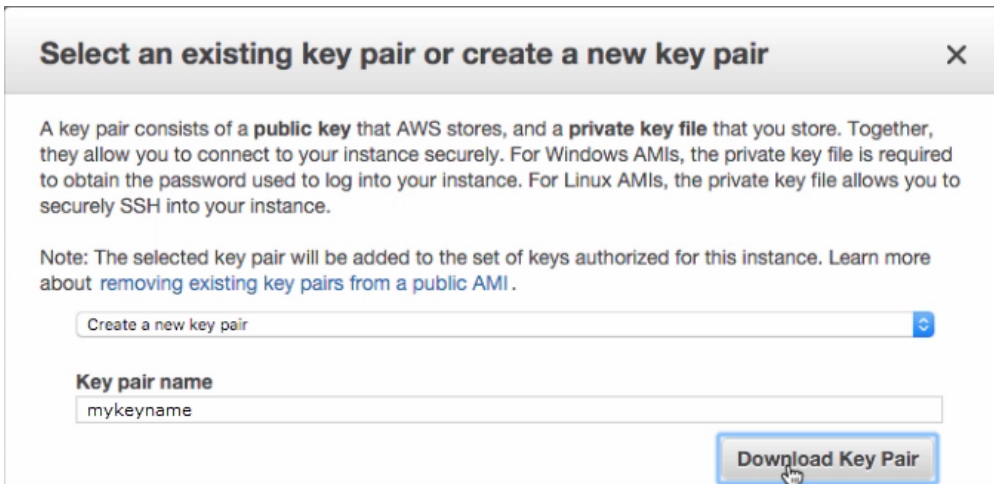
If choosing from existing key pairs, simply select from the available options under



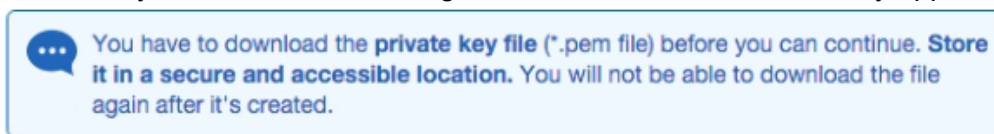
If creating a key pair, simply select said option from the top dropdown.



Upon clicking **Create a new key pair**, the following dialog appears:



Name this key pair something that will help identify it later. Download the .pem file created, in order to gain access to your VM. As the warning below states, this will be the only opportunity to do so.



Note: Do not select the **Proceed without a Key Pair** option. If an instance is launched without a key pair, it will be inaccessible. This option is used only when creating an AMI, and/or when connecting to the instance is not critical.

Click on **Launch Instances**.

Add Disks

[Adding Amazon S3 Cloud Disks](#)

[Adding Amazon EBS Disks](#)

AWS Instances

Description

Amazon EC2 provides computing **instances**, which are virtual machines running on the XenSource hypervisor. Each instance is a unique copy of a virtual machine image. We will use EC2 terminology **instance** to refer to these VMs.

There are over 200 possible combinations of the EC2 instance type. When choosing an instance type for production deployment, give careful consideration to the overall storage demand and best practices for performance.

The top two things to consider are IOPS and Throughput. SoftNAS Cloud® specific configurations to consider are the use of Deduplication and / or Compression.

Instance Types Matrix

To maximize IOPS and Throughput, create instances that support Enhanced Networking and EBS Optimization. Listed below are the instance types that best meet these settings, based on settings pulled from [Amazon Web Services](#).

The following instance types* also include the following optimization benefits:

- Intel® AES-NI
- Intel® AVX
- Intel® Turbo
- EBS Optimization
- Enhanced Networking
- Intel Xeon E physical processors

Instance Type	vCPU	Memory (GiB)	Storage (GB) SSD	Networking Performance	Clock Speed (GHz)
c3.xlarge	4	7.5	2x40	Moderate	2.8
c3.2xlarge	8	15	2x80	High	2.8
c3.4xlarge	16	30	2x160	High	2.8
r3.xlarge	4	30.5	1x80	Moderate	2.5
r3.2xlarge	8	61	1x160	High	2.5
r3.4xlarge	16	122	1x320	High	2.5
i2.xlarge	4	30.5	1x800	Moderate	2.5
i2.2xlarge	8	61	2x800	High	2.5
i2.4xlarge	16	122	4x800	High	2.5

*-Settings may have changed slightly since the publication of this guide.

SoftNAS performance and throughput is governed by:

- **Available Memory:** **SoftNAS** uses approximately 1 GB of RAM for the kernel and system operation. Memory beyond 1 GB is available for use as cache memory, which greatly improves overall system performance and response time - more memory = better performance, to a point. If application workloads involve a high number of small, random I/O requests, then cache memory will provide the best performance increase by reducing random disk I/O to a minimum. If running a SQL database application, cache memory will greatly improve query performance by keeping tables in memory. At a minimum, 2 GB of RAM will yield around 1 GB for cache. For best results, start with 4 GB or more RAM. With deduplication, add 1 GB of RAM per terabyte of deduplicated data (to keep deduplication look-up tables in RAM)

- **CPU:** **SoftNAS** needs a minimum of 2 CPUs for normal operation. To maintain peak performance when using the Compression feature, add CPUs (e.g., 4 CPU) if CPU usage is observed at 60% or greater on average.
- **Network** - In EC2, **SoftNAS** uses Elastic Block Storage (EBS), which are disks running across the network in a SAN (storage area network) configuration. This means all disk I/O travels across a shared network connecting the EC2 computing instance with the SAN. This makes network I/O an important factor in **SoftNAS Cloud®** environment performance.
- **Multiple Performance & Scale Options:** EC2 offers **Fixed Performance** Instances (e.g. m3, c3, and r3) as well as **Burstable Performance** Instances (e.g. t2) for occasional heavy use over baseline. EC2 also offers many instance sizes and configurations. Consider all potential networking requirements when choosing instance type. Purchasing models include **On-Demand**, **Reserved**, and **Spot Instances**.

AWS EC2 Best Practices

To get the best performance out of **SoftNAS Cloud®** in an AWS environment, consult the following best practices:

[Regions for Amazon Machine Images](#)

[AWS Instances](#)

[Elastic IPs](#)

General Instance Type Recommendations

Here are some general recommendations for getting started with EC2 and SoftNAS.

- **Standard:** A good starting point in regards to memory and CPU resources. This category is suited to handle the processing and caching with minimal requirements for network bandwidth.
- **Medium:** Good for workloads that are read intensive, and will benefit from the larger memory-based read cache for this category. The additional CPU will also provide better performance when deduplication, encryption, compression and/or RAID is enabled.
- **High:** This category can be used for workloads that require a very high speed network connection due to the amount of data transferred over a network connection. In addition to the very high speed network, this level of instance gives you a lot more storage, CPU and memory capacity.

For extremely heavy workloads, increase cache memory with "High-Memory Instances" and/or use EBS-Optimized and Provisioned IOPS to provide better control over available IOPS.

Note: Micro instances may be adequate for some development and QA testing purposes, and to keep costs low; however, be aware of the significant memory, CPU and network limits imposed on micro instances, which will certainly limit performance and throughput of SoftNAS.

Accessing SoftNAS Cloud® for EC2

In order to log in to **SoftNAS Cloud®** for an EC2-based network, go to the Instances page and select the instance to connect to. To create a new instance, consult the [Create and Configure An Instance in AWS](#) section of this guide.

The bottom half of the screen will show various details about this instance. Note the IP address and the Instance ID. Both of these items will be required for initial login.

Description	Status Checks	Monitoring	Tags
Instance ID	i-04dcc6ea		
Instance state	running		
Instance type	m3.medium		
Private DNS	ip-70-0-0-130.ec2.internal		
Private IPs	70.0.0.130		
Public DNS	ec2-54-164-14-220.compute-1.amazonaws.com		
Public IP	54.164.14.220		
Elastic IP	54.164.14.220		
Availability zone	us-east-1c		
Security groups	default, automated-tests . view rules		

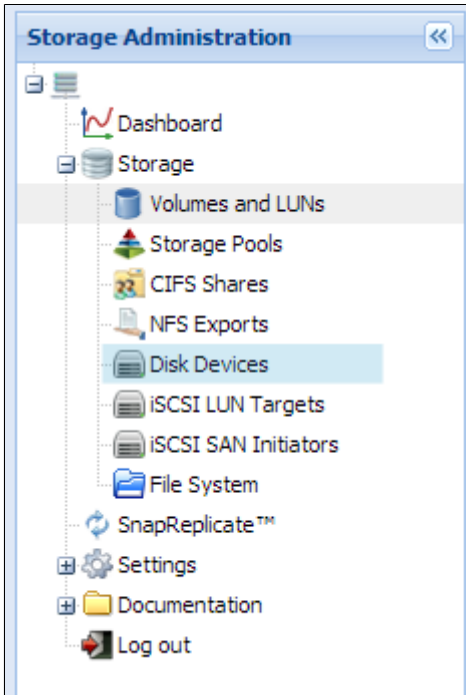
1. In a web browser, enter the Public IP or Elastic IP address (they should be the same as per [Elastic IP Address](#)) in the format `https://[instanceip]`
2. Enter **softnas** as the user ID. (Root logins are defaulted as disabled for security reasons - use `sudo su` to become root on Amazon EC2 systems.)
3. The default **password** is the string in the **Instance ID** field. Copy/paste the entire field for convenience and foolproof data entry.
4. Consult the [SoftNAS Cloud® Configuration](#) section to continue with storage management settings.

Adding Amazon EBS Disks

Before adding EBS disks, and creating your storage pools and volumes, there are many considerations specific to creating volumes and pools for EBS disks. Review the AWS EBS considerations found in [Amazon EBS RAID Considerations](#).

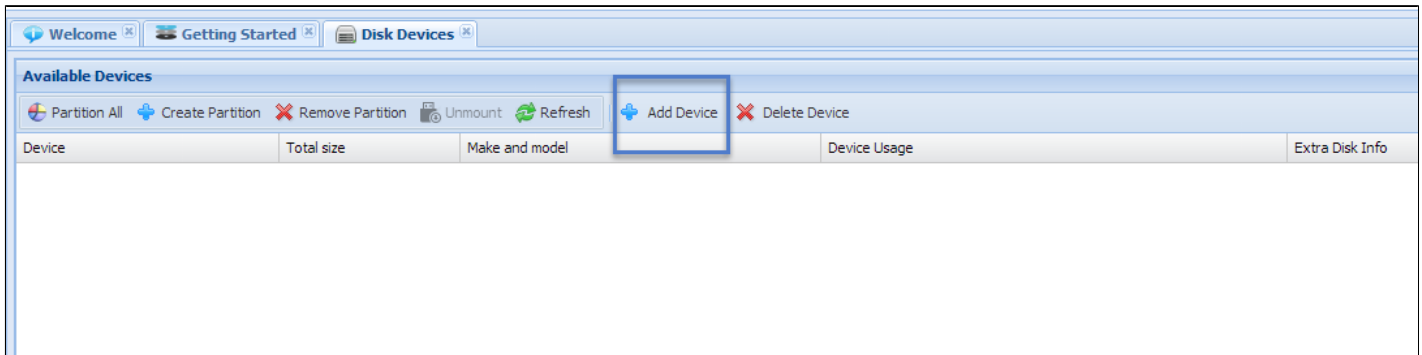
How to Add Amazon EBS Disks

1. In **SoftNAS StorageCenter**, choose **Disk Devices** from the main menu.



The Disk Devices panel appears.

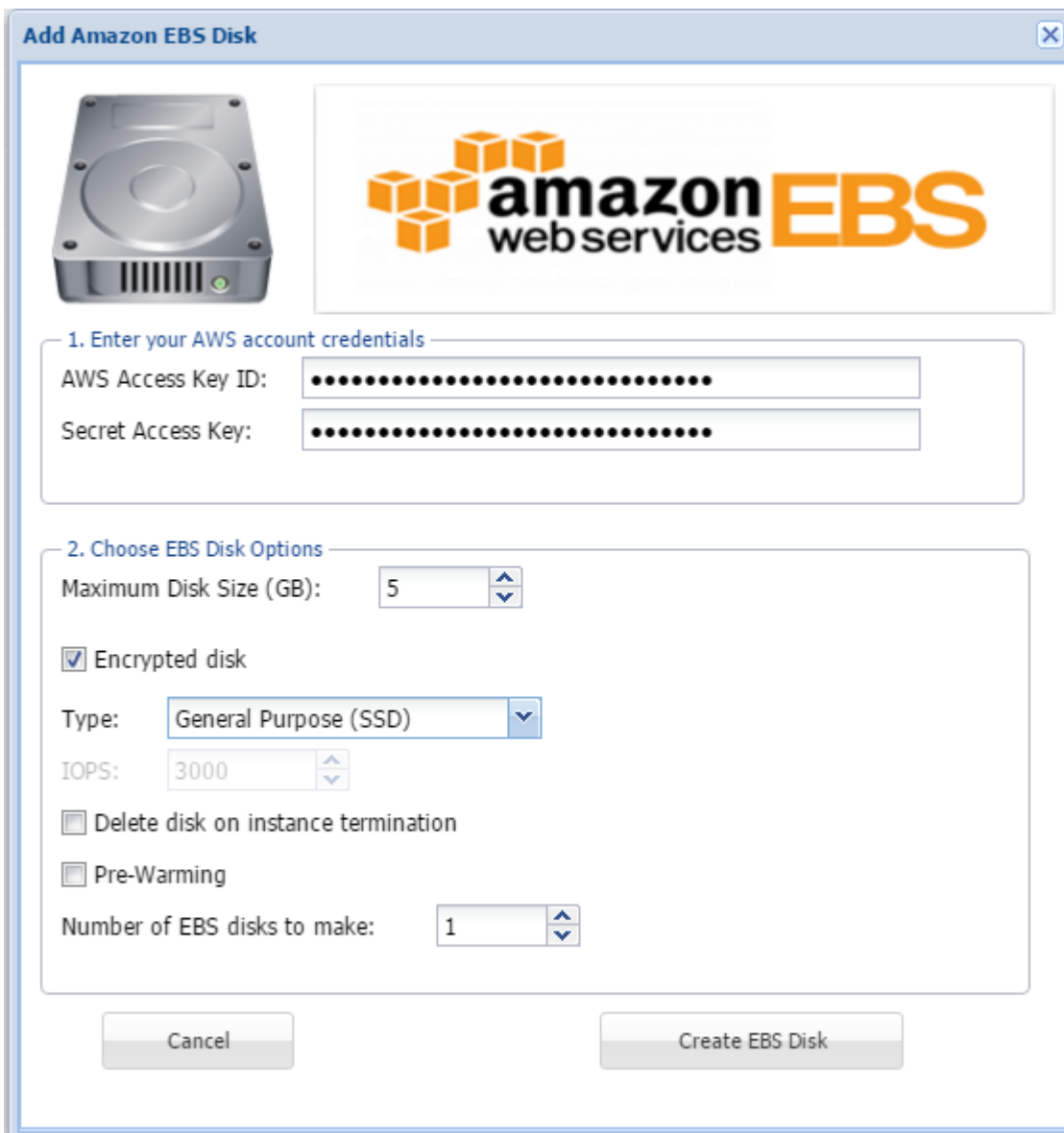
2. From Disk Devices, click on **Add Device**.



3. From Add Device screen, select **Amazon EBS Disk**.



Complete the **Amazon EBS Disk** form as described in the table below.



Add Amazon Disk Reference Table

Parameter	Description
<p>AWS account credentials</p>	<p>Enter the AWS account credentials used to access Amazon Web Services.</p> <p>Note: If AWS account credentials are unavailable (grayed out), an Amazon IAM Role was specified at SoftNAS Cloud® instance creation. Creating a SoftNAS Cloud® IAM user from the Amazon Web Services Dashboard is the recommended approach for a more secure connection to AWS.</p> <p>Creating the SoftNAS Cloud® S3/EBS IAM Role for AWS</p>
<p>EBS Disk Options</p>	<p>Maximum Disk Size: Must be between 1-1024 GB.</p> <p>Encrypted Disk: Check this option and provide a Disk Password to encrypt the contents of the EBS disk to ensure its contents cannot be accessed, except via this EBS Disk.</p> <p>Type: General Purpose SSD: General Purpose (SSD) volumes offer cost-effective storage that is ideal for a broad range of workloads. These volumes deliver single-digit millisecond latencies, the ability to burst to 3,000 IOPS for extended periods of time, and a base performance of 3 IOPS/GiB. General Purpose (SSD) volumes can range in size from 1 GiB to 1 TiB.</p> <p>Provisioned IOPS (SSD): Provisioned IOPS (SSD) volumes are designed to meet the needs of I/O-intensive workloads, particularly database workloads, that are sensitive to storage performance and consistency in random access I/O throughput. Specify an IOPS rate (using the dropdown provided when the option is selected) when the volume is created, and Amazon EBS delivers within 10 percent of the provisioned IOPS performance 99.9 percent of the time over a given year.</p> <p>Standard: Magnetic volumes provide the lowest cost per gigabyte of all Amazon EBS volume types. Magnetic volumes are backed by magnetic drives and are ideal for workloads performing sequential reads, workloads where data is accessed infrequently, and scenarios where the lowest storage cost is important. These volumes deliver approximately 100 IOPS on average, with burst capability of up to hundreds of IOPS, and they can range in size from 1 GiB to 1 TiB. Magnetic volumes can be striped together in a RAID configuration for larger size and greater performance.</p>

5. Click on Create **SSD Disk**.

The EBS Disk is created and automatically partitioned and ready for use.

Disk Devices				
Partition All + Create Partition ✖ Remove Partition 🔄 Refresh + Add Device ✖ Delete Device				
Available Devices				
Device	Total size	Make and model	Device Usage	Extra Disk Info
/dev/s3-19	500.0GB	SoftNAS, Amazon Cloud Disk (file)	Available to assign	S3 bucket: asydneyone-54061-s3disk-19, in 'U.S. Standard' region
/dev/s3-20	500.0GB	SoftNAS, Amazon Cloud Disk (file)	Available to assign	S3 bucket: adisk-25893-s3disk-20, in 'sydney' region
/dev/s3-21	500.0GB	SoftNAS, Amazon Cloud Disk (file)	Available to assign	S3 bucket: adisk-50963-s3disk-21, in 'ireland' region
/dev/s3-22	500.0GB	SoftNAS, Amazon Cloud Disk (file)	Available to assign	S3 bucket: adisk-70213-s3disk-22, in 'tokyo' region

The next step is to create a Storage Pool which uses the EBS disk.

Note: Ensure sufficient licensed capacity in **SoftNAS Cloud®** to accommodate the amount of storage capacity that will be added.

Next Steps

[Create Storage Pool](#)

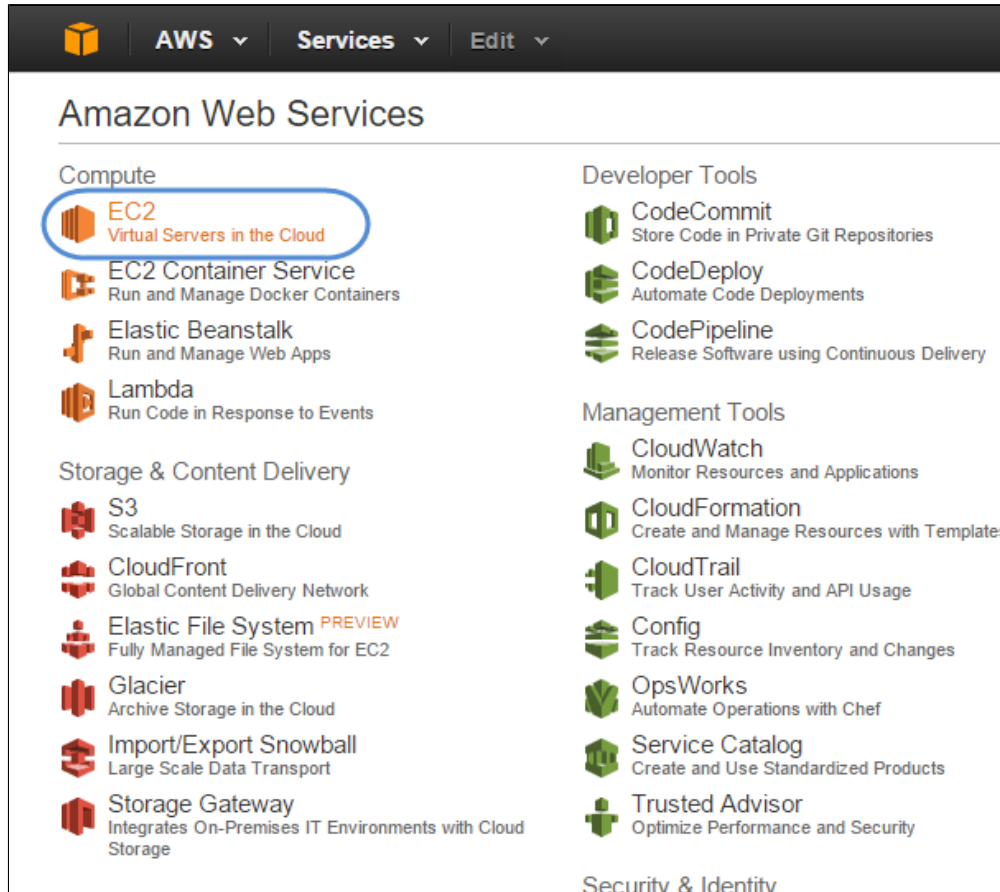
[Add & Manage Volumes](#)

[Share Volumes over a Network](#)

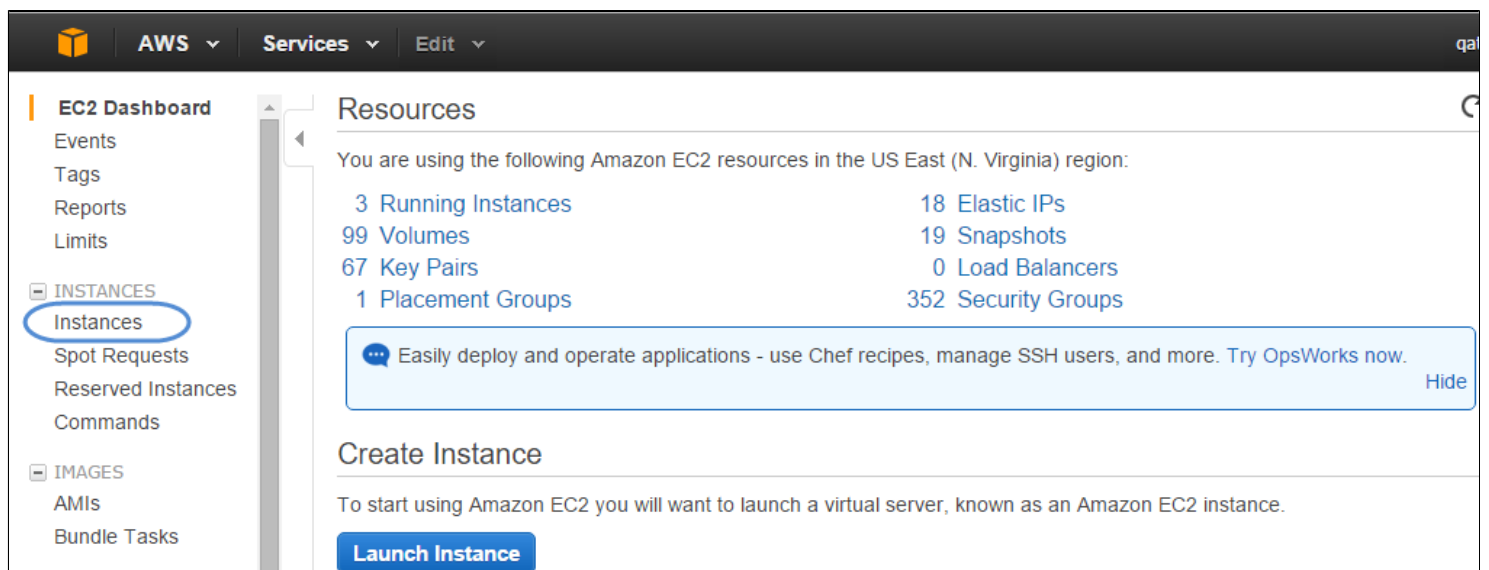
Managing EC2 instances in AWS

While configuration is largely handled within the SoftNAS UI, EC2 instances can also be managed from within the EC2 Dashboard, in AWS.

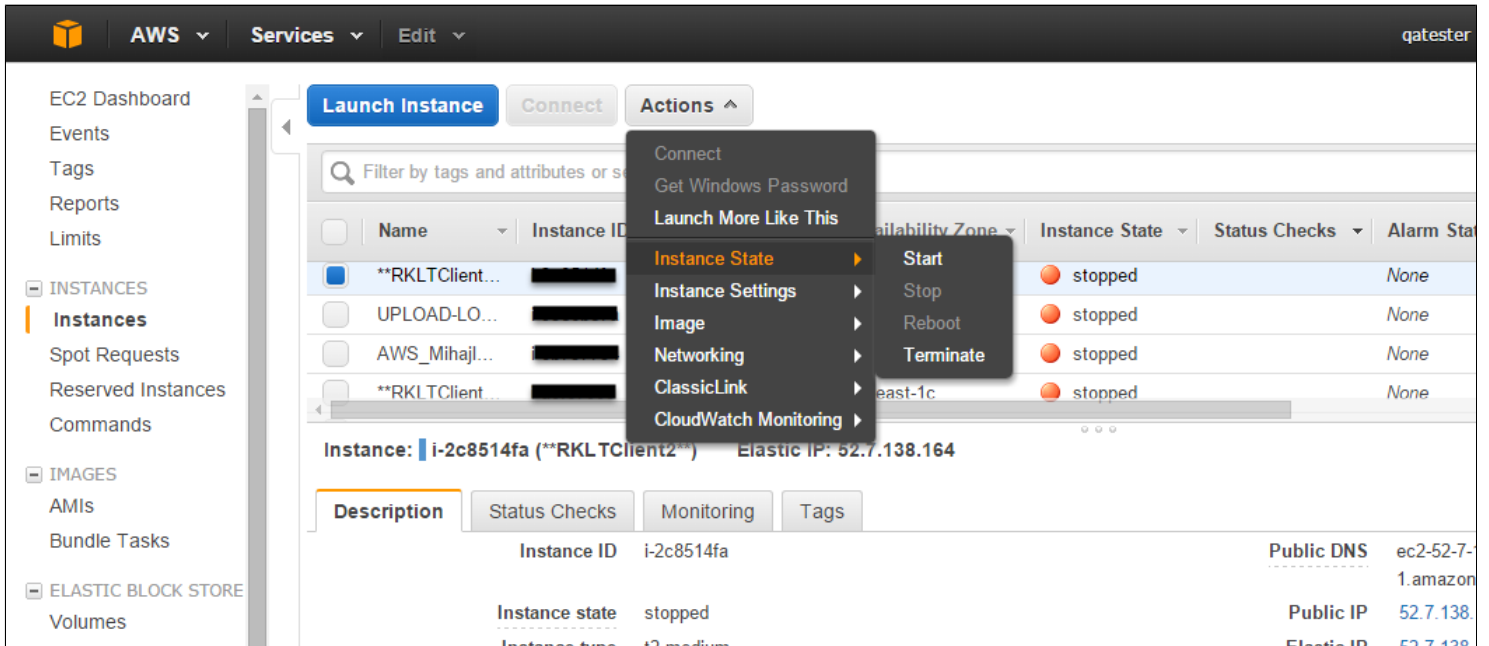
1. Log into your account in the AWS console via your [browser](#).
2. Once logged into the console, select **EC2** from the available options.



3. You can review a summary of account resources from the EC2 Dashboard. Click **Instances** to manage your individual instances.



4. You can stop and start individual instances, launch new instances, and many other management tasks by navigating the EC2 console. Select the Instance you would like to manage, click **Actions**, and select the desired option.



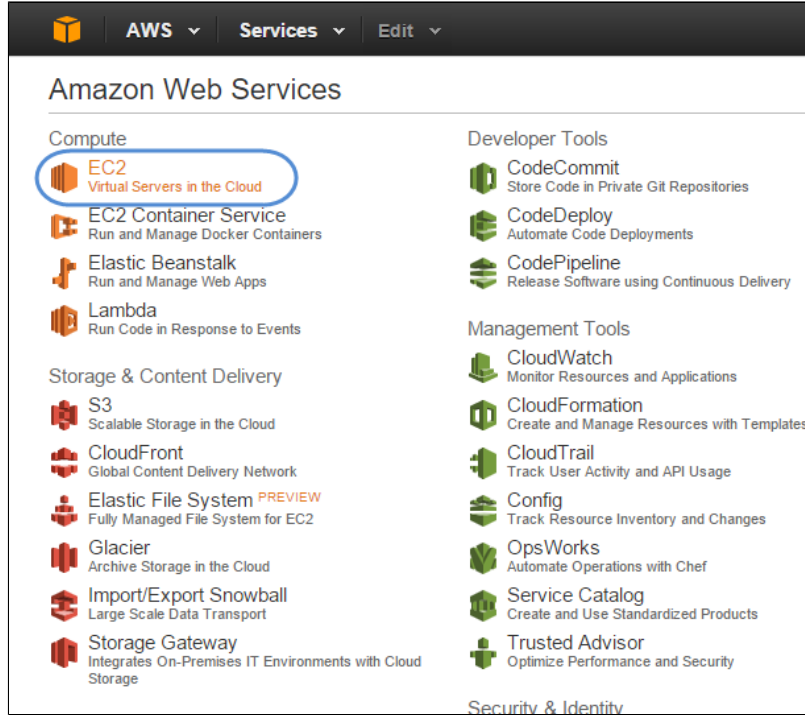
For more in depth information on individual features or tasks within the EC2 console, review Amazon Web Services very thorough [documentation](#).

Creating an EC2 Volume

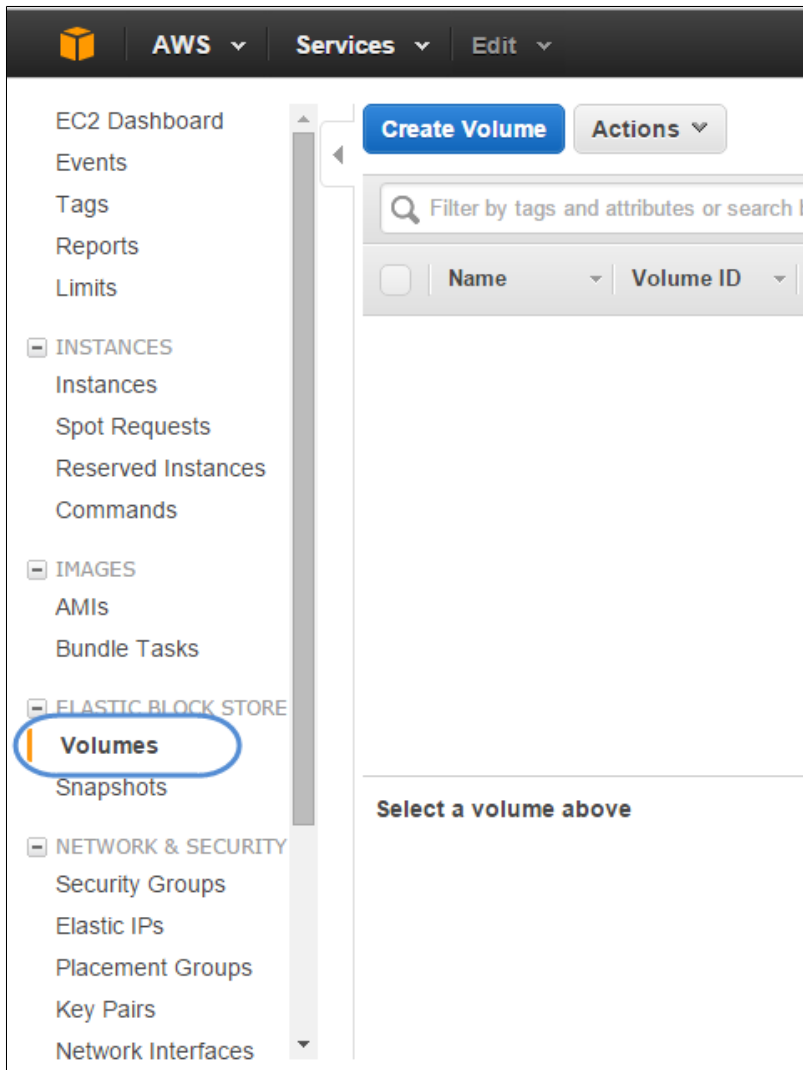
EBS volumes can be created from within the EC2 console, in order to manage storage for your SoftNAS volumes.

To create a volume:

1. Log into AWS and select EC2.

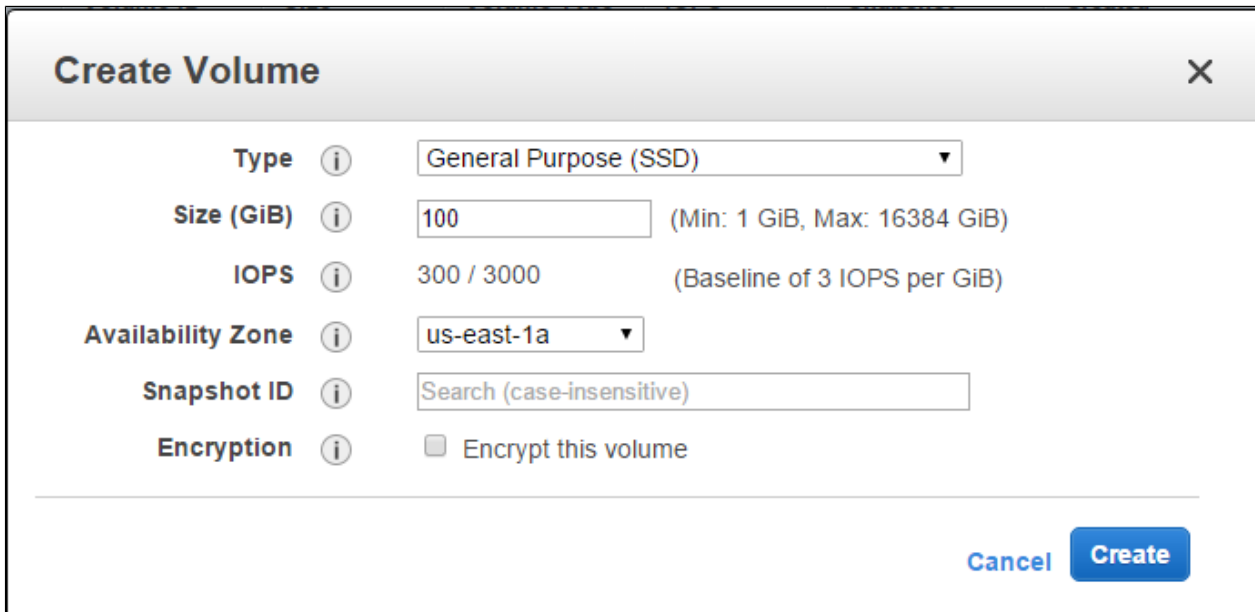


2. Navigate to **EC2 Dashboard** -> **Volumes**.



3. Click on **Create Volume**.

The Create Volume dialog will be displayed.



Create Volume Dialog Settings:

1. Select the desired type from the **Volume Type** drop down.

- **General Purpose (SSD):** Default IOPS (no guaranteed IOPS level in shared environment - less predictable, less consistent performance)
- **Provisioned IOPS:** assign a specific level of IOPS by entering the number of I/O per second you want assured for the EBS data volumes (see Choosing an Instance Type)
- **Magnetic:** IOPS limited to constraints of magnetic disks.

2. Enter the size of the volume in the **Size** text entry box.

3. View the IOPS based on the **Volume Type** selected under IOPS. If Provisioned IOPS is selected, this value can be manually set.

4. Select the desired zone from the **Availability Zone** drop-down. This helps you to attach the volume to your instance.

5. If creating the volume from a Snapshot, select the required snapshot from the Snapshot drop down list.

6. If the volume is to be encrypted, check the "**Encrypt this volume**" box.

7. Click the **Create** button.

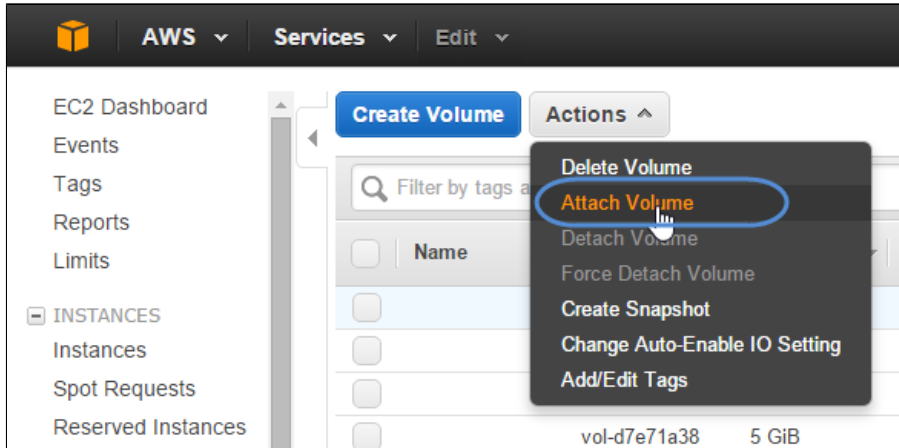
The new standard volume is created.

Managing Volumes

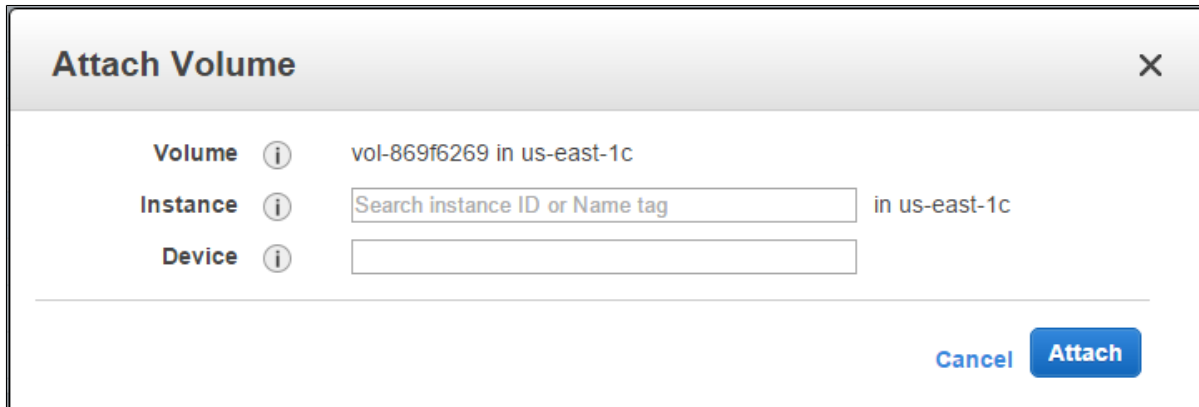
Once volumes are created, attach or detach volumes to an instance.

Attach a Volume

1. To do so, on the **Volumes** page, select the volume to be attached to an instance.
2. From the **Actions** drop down list, select **Attach Volume**.



The **Attach Volume** dialog will be displayed.



3. Select the instance to be attached from the **Instance** drop down list.

Enter a device name for the EBS volume; e.g., `/dev/sdf1`, `/dev/sdp15`. Refer to [EBS Volumes and Device Mapping](#) for more information on how best to allocate EBS volume device names.

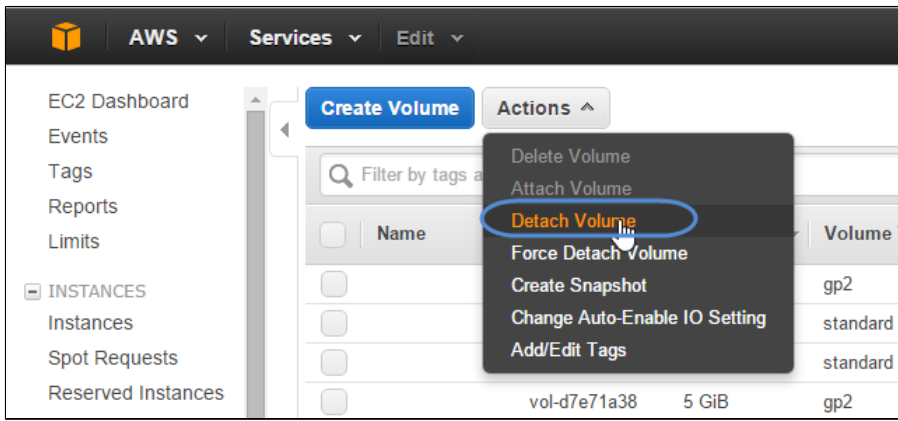
4. Click **Yes, Attach**.

The volume is now attached to a **SoftNAS Cloud® instance**.

Detach a Volume

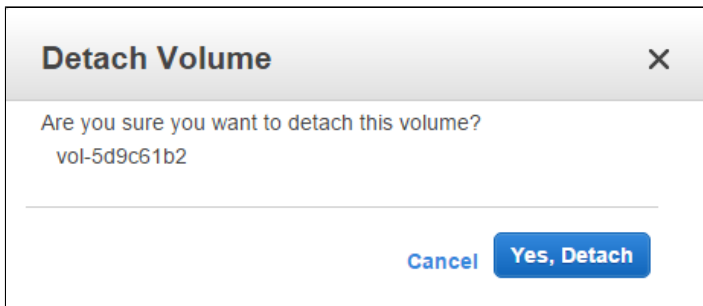
Detach a volume from the attached instance.

1. Select the volume to be detached from the instance.
2. From the **Actions** drop down list, click **Detach Volume**.



WARNING - BE CAREFUL. Do not detach volumes from an active **SoftNAS Cloud®** instance unless the volume will be moving to a new instance, in which case, re-attach the EBS volumes and **Import** to regain access to data.

The **Detach Volume** message box asking to confirm the dissociation of address with the specific instance will be displayed.

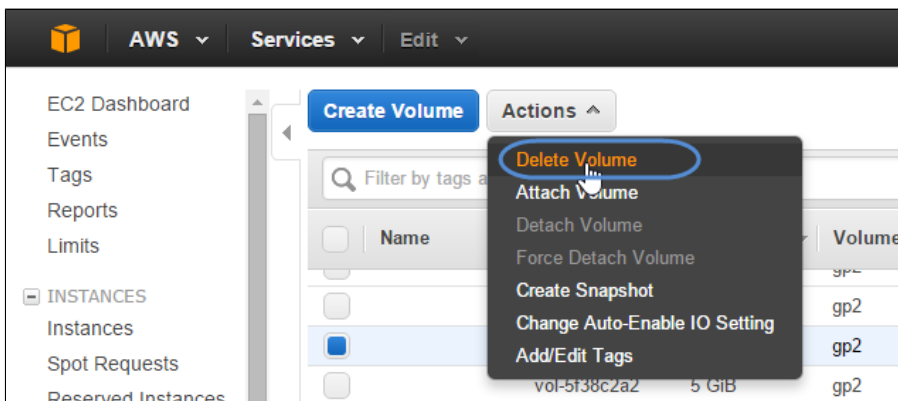


3. Click **Yes, Detach**. The selected volume will be detached from the instance.

Delete a Volume

Note: Permanent data loss can occur when EBS volumes are deleted.

1. To delete a volume, select it from the **Volumes** page on EC2 dashboard.



2. On the **Actions** drop down list, select the **Delete Volume** option and confirm by clicking **Yes, Delete**. The selected volumes will be deleted.

EBS Volumes and Device Mapping

EBS volumes are used to provide raw storage disk devices to **SoftNAS Cloud®** by attaching to the **SoftNAS Cloud®** instance using the **AWS console**. The recommended naming convention depends on the virtualization type of device. See the table below for the **AWS-recommended device mapping method**.

EBS to Linux Device Mapping Table

Type of Virtualization	Available String Blocks	Reserved for Root	Instance Store Volumes	Recommended for EBS Volumes
Paravirtual	/dev/sd[a-z] /dev/sd[a-z][1-15] /dev/hd[a-z] /dev/hd[a-z][1-15]	/dev/sda1	/dev/sd[b-e]	/dev/sd[f-p] /dev/sd[f-p][1-6]
HVM	/dev/sd[a-z] /dev/xvd[b-c][a-z]	Differs by AMI /dev/sda1 or /dev/xvda	/dev/sd[b-e] /dev/sd[b-y] (hs1.8xlarge)	/dev/sd[f-p]

Note: Approval by **AWS Support** may be required to go beyond the initial 20 TB limit account default.

About EBS Volume Naming

EBS volumes are used to provide raw storage disk devices to SoftNAS. EBS volumes are attached to the SoftNAS instance using the AWS console. The number of disks that can be attached is based on the type of virtualization used - HVM or PV.

HVM

The key restriction of using HVM virtualization is the limit of 11 attachable EBS volumes to your SoftNAS instance. This limit is based on the volume naming convention used by HVM instances. For HVM, AWS supports EBS volume naming of /dev/sd[f-p]. This means that as each EBS volume is attached, it is assign a device name of "/dev/sdf", then "/dev/sdg", and so on. Once the recommended name range of "f" through "p" are used, no additional EBS volumes should be attached.

/dev/sd[f-p][1-15]

Even though a-z may appear to work, use of those device names is not supported, and AWS might be using a-g and q-z range at some stage for something else, so for now, it's a good idea to stick with the device names from [f-p] when attaching EBS volumes via AWS console to an HVM instance.

PV

The primary benefit to using PV AMIs to deploy SoftNAS is the ability to attach a much higher count of EBS volumes. This is based on the volume naming convention used by PV virtualization. While HVM only supports limited alpha characters for volume naming, PV supports the ability to add numeric values at the end of the volume name. For PV, AWS supports EBS volume naming of /dev/sd[f-p][1-6]. This means that up to 66 EBS volumes can be attached to a PV instance with a total raw EBS capacity of over 1 petabyte (11*6*16TB = 1.056PB).

For example: USE: /dev/sdf1, /dev/sdf2, /dev/sdf3 ... /dev/sdp5, /dev/sdp6

Note: While it is possible to add 66 EBS volumes as stated above, AWS guidance states that support for configurations above 40 EBS volumes is on a best effort basis.

In the past, PV virtualization performance was much better than that of HVM. With improvements in today's hardware (IOMMU & SR-IOV), this is no longer the case. AWS has releasing their latest generations of c4 and m4 instances with HVM AMI exclusive support. The c3 and m3 instance families do provide both PV and HVM support, but AWS recommends using HVM AMIs across the board for best performance.

Note: If using a PV instance of SoftNAS, **DO NOT USE** the `/dev/sdf` or `/dev/sdp` base device names, or you will limit the number of EBS volumes that can be attached to a maximum of 11 disks. [F - P] should always be followed by a number, or you will restrict your instance's EBS add-on volumes.

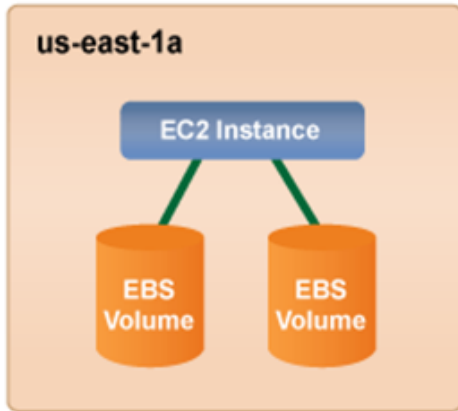
This means you can assign 66 extra disks to an instance for a maximum of 154 TB of storage space.

Note: Approval from AWS Support may be required to go beyond the initial 20 TB limit that is the default for your account.

EBS Mount SoftNAS Linux Mapping	
<code>/dev/sda1</code>	<code>/dev/xvde1</code> (Root Disk - 30 GB, do not use or partition)
<code>/dev/sdf1 ... 15</code>	<code>/dev/xvdj1 ... xvdj15</code>
<code>/dev/sdg1 ... sdg15</code>	<code>/dev/xvdk1 ... xvdk15</code>
<code>/dev/sdh1 ... 15</code>	<code>/dev/xvd11 ... 15</code>
<code>/dev/sdi1 ... 15 /</code>	<code>dev/xvdm1 ... 15</code>
<code>/dev/sdj1 ... 15</code>	<code>/dev/xvdm1 ... 15</code>
<code>/dev/sdk1 ... 15</code>	<code>/dev/xvdo1 ... 15</code>
<code>/dev/sdl1 ... 15</code>	<code>/dev/xvdp1 ... 15</code>
<code>/dev/sdm1 ... 15</code>	<code>/dev/xvdq1 ... 15</code>
<code>/dev/sdn1 ... 15</code>	<code>/dev/xvdr1 ... 15</code>
<code>/dev/sdo1 ... 15</code>	<code>/dev/xvds1 ... 15</code>
<code>/dev/sdp1 ... 15</code>	<code>/dev/xvdt1 ... 15</code>

About Amazon EBS Disks

Amazon Elastic Block Store (Amazon EBS) provides persistent, block-level storage volumes for use with **Amazon EC2** instances in the **AWS Cloud**. Each **Amazon EBS** volume is automatically replicated within its Availability Zone to protect from component failure, offering high availability and durability. **Amazon EBS** and **SoftNAS Cloud®** provide access to store and retrieve any amount of data, at any time, from anywhere on the web. It gives anyone access to the same highly scalable, reliable, secure, fast, inexpensive infrastructure that Amazon uses to run its own global network of web sites. The service aims to maximize benefits of scale and to pass those benefits on to customers.



Attach Multiple Volumes to the same EC2 Instance.

EBS Volumes

- 1TB -16TB
- \$0.10/GB per month
- Attach an EBS Volume(s) to any EC2 instance in the same Availability Zone
- Create an EBS Snapshot of an EBS Volume at any point in time
- Create an EBS Volume(s) from any EBS Snapshot

As an example: For 1 TB of usable storage with RAID Redundancy for increased performance and data redundancy, one potential configuration could be:

- Two 1 TB EBS volumes, configured as RAID 1 mirrors
- Five 250 GB EBS volumes, configured as RAID 5 (four data, single parity)
- Seven 250 GB EBS volumes, configured as RAID 6 with a spare (four data, dual parity, one spare)

S3 Cloud Disks for Cloud Storage

Use S3 Cloud Disks to manage up to 4 petabytes of Amazon S3 cloud storage per device. For more information on Cloud Disks, refer to the [SoftNAS Cloud® Disk Overview](#) section of this guide.

Instance Tags and Key Pairs secure data and verify ownership. Properly set up, these layers of validation protect EC2 Instances from accidental or unauthorized users.

Status Checks & Alarms

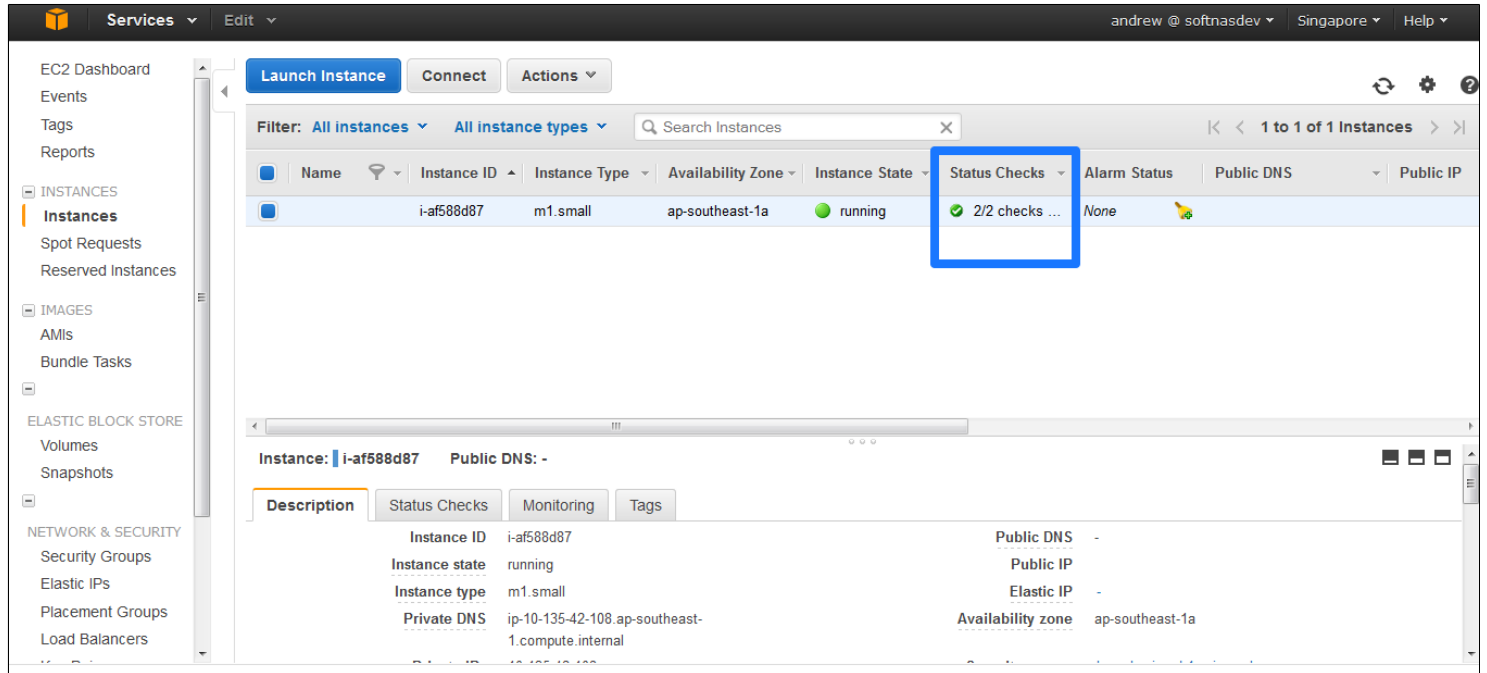
Status Checking

In order to know that instance is successfully launched, check its status.

1. Click **Instances** in the left panel.

All the instances related to the specific region will be displayed.

2. When **SoftNAS Cloud®** is fully booted and is ready for initial configuration and use, the **Status Checks** column will show a green checkmark with the message that 2/2 checks passed:



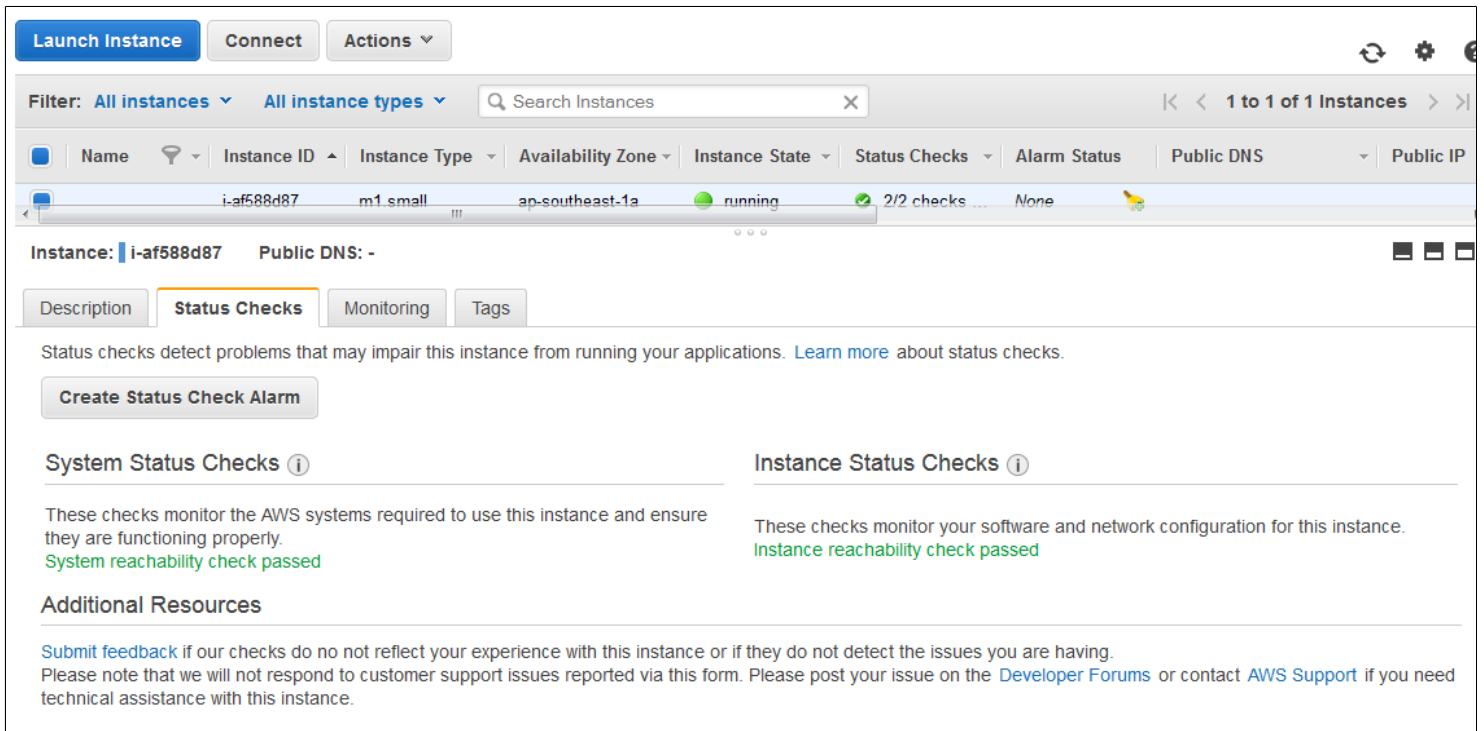
At this point, **SoftNAS Cloud®** instance is operational.

Status Check Monitoring

Set **CloudWatch** alarms in order to be notified automatically whenever the metric data reaches a pre-defined level.

Create a status check alarm

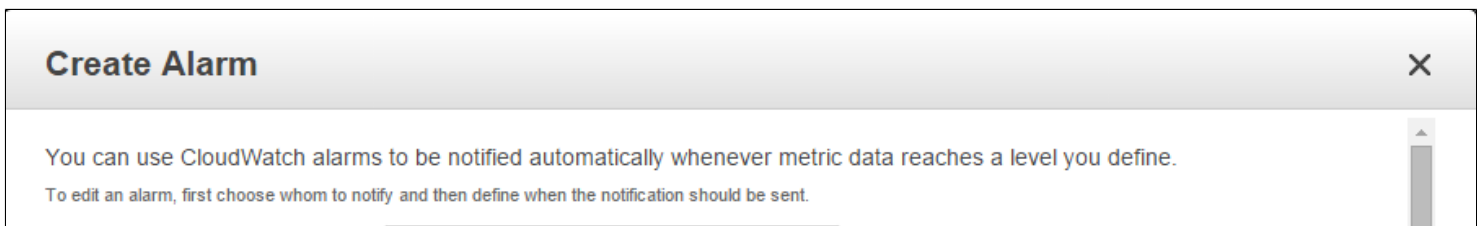
1. On the **EC2 Dashboard**, click the Instances option in the left panel.
2. Select the instance to which to add **CloudWatch** alarm.
3. Navigate to the **Status Checks** tab.



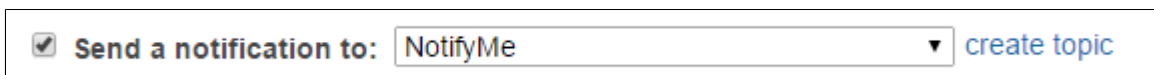
The **Status Checks** tab displays the information on the system status checks and instance status checks.

Status Check Alarm

Click **Create Status Check Alarm**. This will prompt the **Create Alarm** dialog.



1. Check the box behind the **Send a Notification to** field.



2. Click **Create Topic** to specify email addresses for all contacts involved. If only the admin needs to be notified, keep the default choice NotifyMe.



3. Check the box behind the **Take the Action** field to initiate the action to be taken in case of the metric reaching a certain level. Also check the box for the type of the action to be initiated as **Stop** or **Terminate** this instance.

4. Select the condition for defining the required metric from the **Whenever** drop down list and then from the description drop down list.

5. The **Is** field is static at the setting **Failing**.

6. Continue the condition for the number of executions for a period.

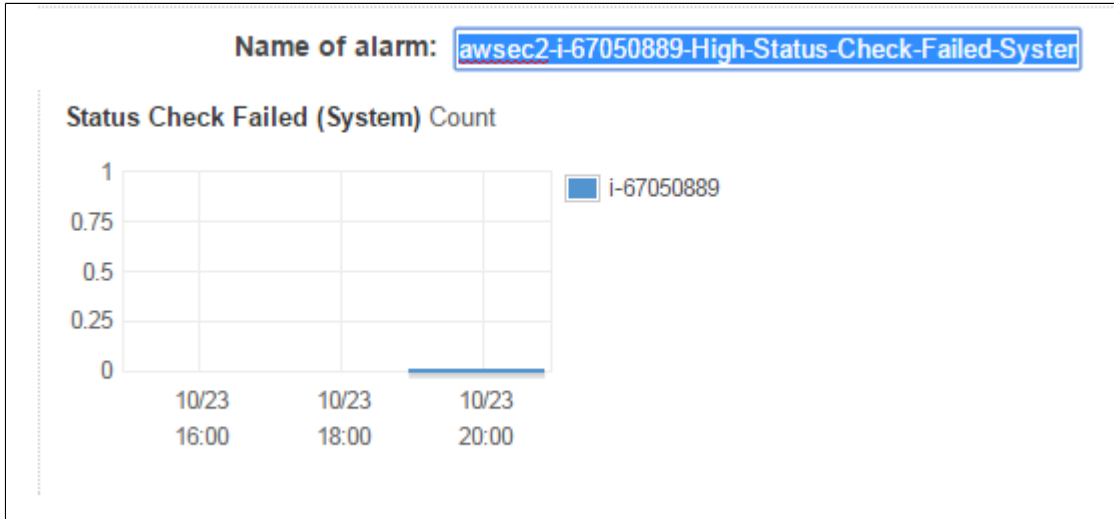
Take the action: Stop Terminate this instance.

Whenever: Status Check Failed (Any) ▼

Is: Status Check Failed (Any)
Status Check Failed (Instance)
Status Check Failed (System)

For at least: consecutive period(s) of ▼

7. Change the **Name of alarm** if desired.



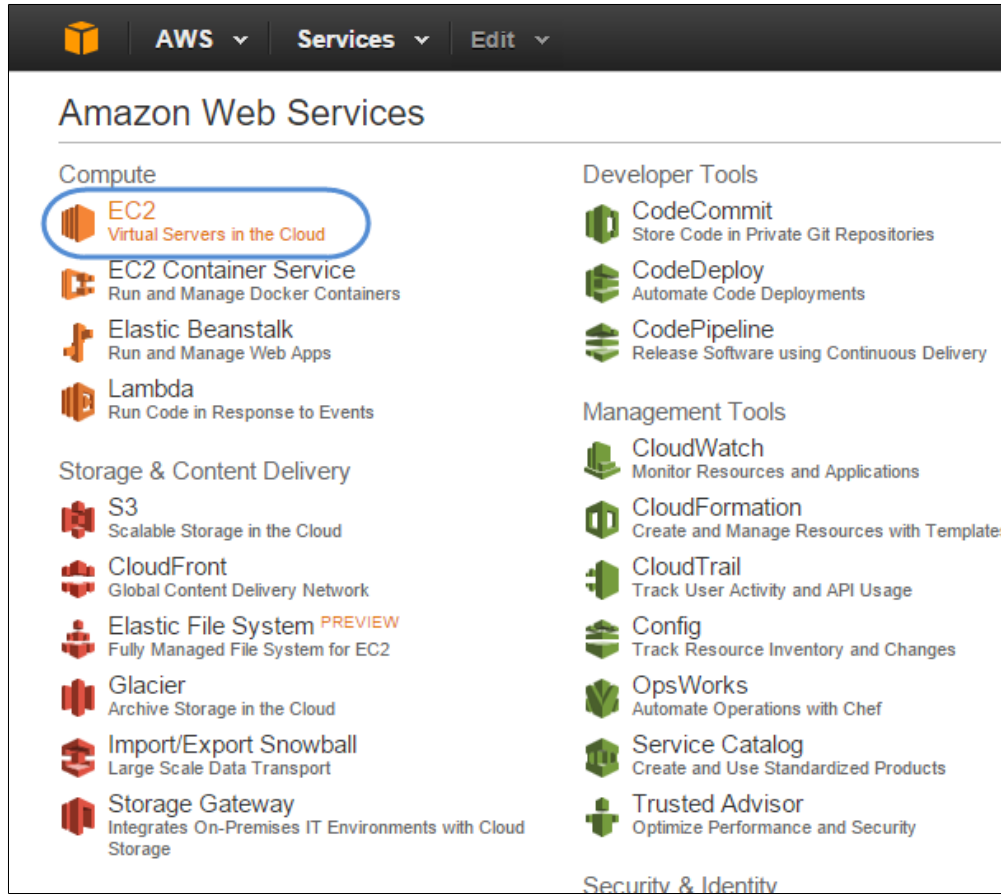
8. **Create Alarm.**

The new **CloudWatch alarm** will be initiated.

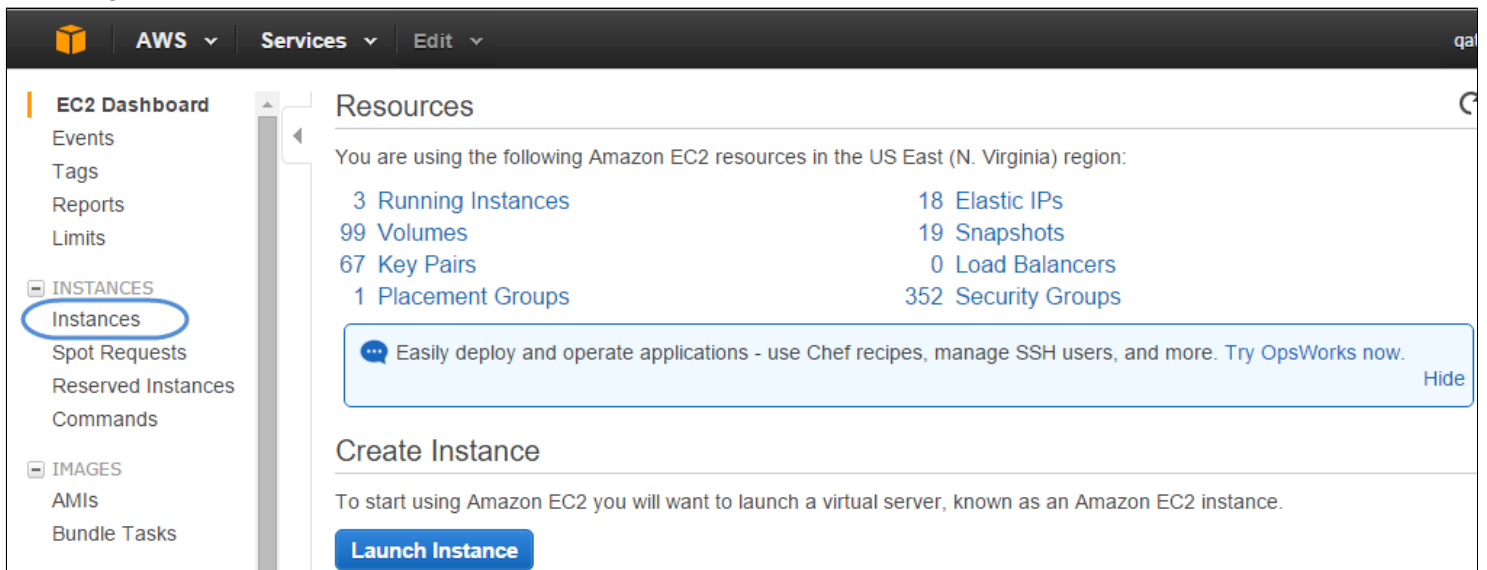
Connecting to an Instance via SSH from the EC2 Console

Connecting to an EC2 instance directly via SSH is rarely necessary, however, the instructions below provide the required information should the need arise.

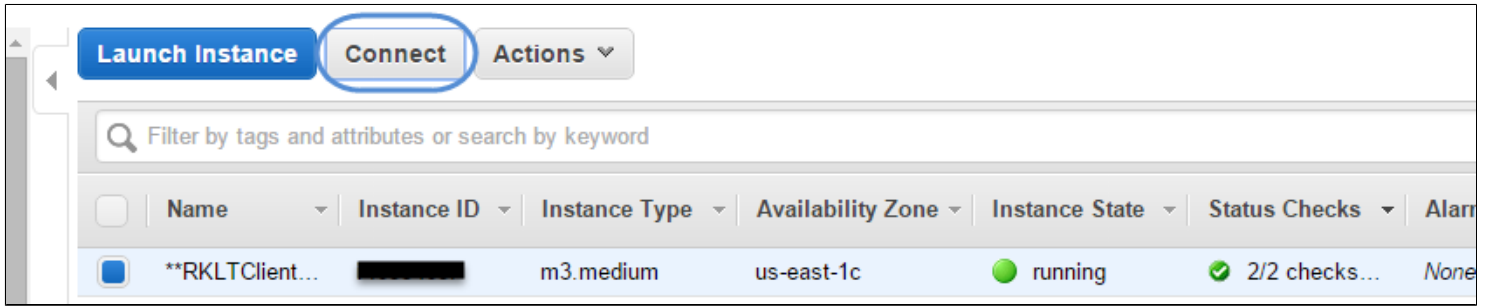
1. Log on to Amazon, and select the **EC2 Dashboard**.



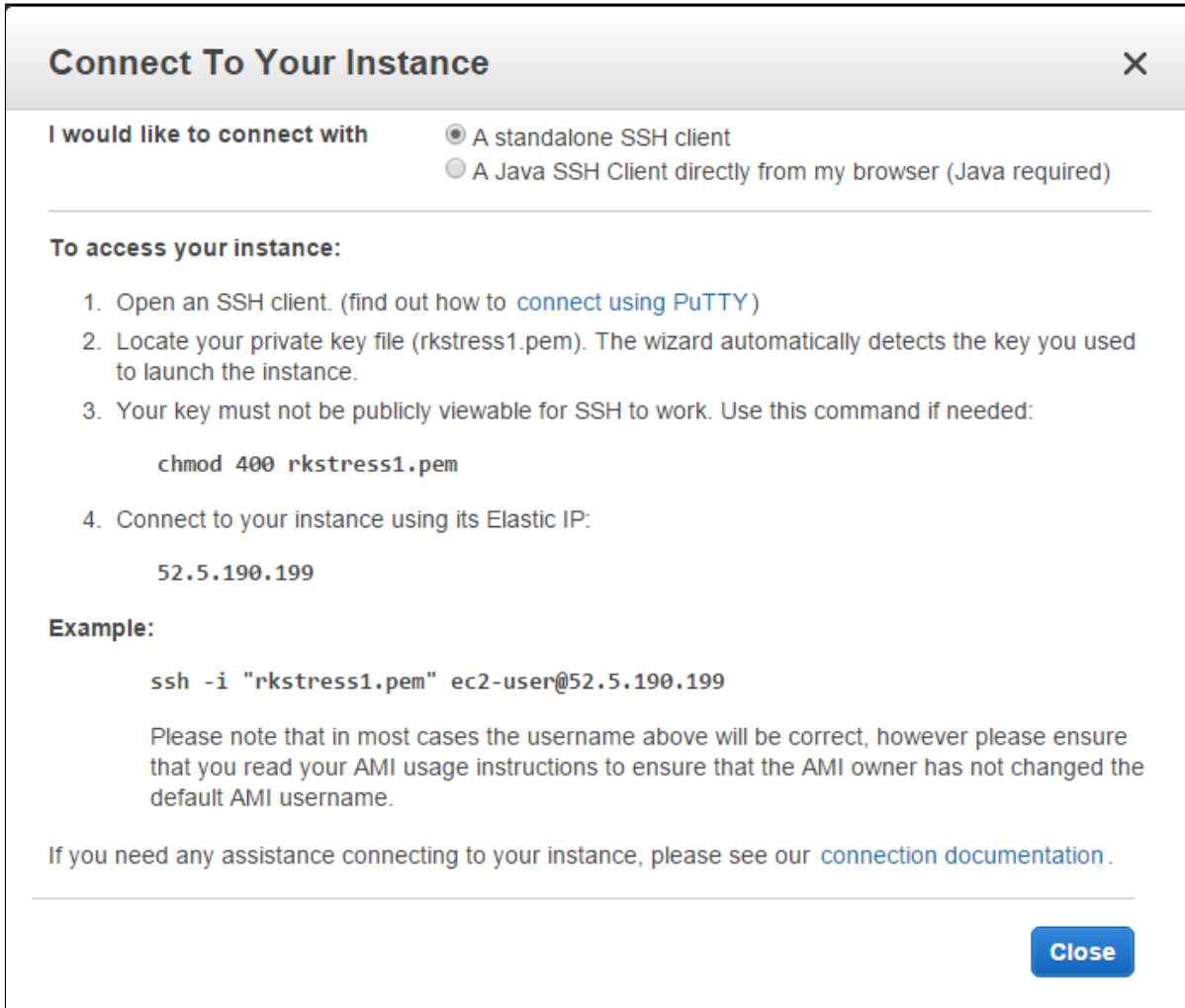
2. Navigate to EC2 Dashboard -> Instances.



3. Select the instance that you wish to connect. Click **Connect**.



The **Connect to an Instance** dialog will be displayed.



Note: You can connect from your web browser using either the Java SSH Client or as the standalone SSH client. Choose an SSH client and use the following login credentials and your private key (created earlier in the installation process and saved in your secret location).

For Browser based Java SSH Client Connection

1. Select the connection type as **A Java SSH Client running directly from my browser(Java Required)**.
2. Enter the user name in the **User Name** text entry box.
3. Enter the private key path in the **Private Key Path** text entry box.
4. To store the key location, check the box in the **Save Key Location** field.

9. Click the **Launch** button.

Note: You can use a user name of "ec2-user". The password-only logins via SSH are disabled for added security in the cloud. You will only need the ec2-user name and password should it be required for any reason while working at the command line in Linux. Be sure to change the default "root" login ID to "ec2-user" when logging into the SoftNAS on EC2 instance.

For Standalone SSH Client Connection

Note: To use a standalone SSH client, first download and install the SSH client. Then click on **A standalone SSH client** in the above dialog for more detailed instructions.

Some of the Windows SSH clients are given below and for more information on installing them, click the below links.

Bitwise Tunnelier: This is a powerful SSH client with integrated SSH and SFTP for file transfers and other features. This is recommended for power SSH users.

Putty: The ubiquitous Putty client is always a good choice for SSH users.

SoftNAS Cloud® Configuration

Regardless of platform, the **SoftNAS StorageCenter** UI remains visually consistent throughout the **SoftNAS Cloud®** experience. Some of the more common tasks can be done through the **SoftNAS StorageCenter** UI.

This section can be accessed once any preferred platform mentioned in this guide has been configured up to this point. Refer to the appropriate section of this guide to ensure all steps have been followed.

Application Type	Platform
Cloud-based	Amazon Web Services
Cloud-based	Microsoft Azure
On-Premise	VMware vSphere

SoftNAS Cloud®™, **SoftNAS StorageCenter™**, **SnapReplicate™**, and **SNAP HA™** are trademarks of **SoftNAS Inc.**. All other trademarks referred to in this guide are owned by their respective companies.

Accessing SoftNAS StorageCenter

Navigating to StorageCenter

Follow the instructions to set up and configure **SoftNAS StorageCenter** for the chosen environment. Each configuration will supply an IP address that is used to access the StorageCenter UI.

- For Amazon Web Services EC2, see [Accessing SoftNAS Cloud® for EC2](#).
- For VMware vSphere, use the IP address configured as per the instructions in [Configuring the Network Using SoftNAS Console](#).
- For Azure, you will use an IP address assigned during instance creation, or modified in **Network Interfaces**. To view or manage the IP address used to connect to your SoftNAS Cloud on Azure instance, see [Microsoft Azure: Managing Network Settings](#).

Generally, a privacy error warning due to a self-signed SSH certificate will pop up. Bypass this for now, and update this certificate at the earliest convenience.

Logging In

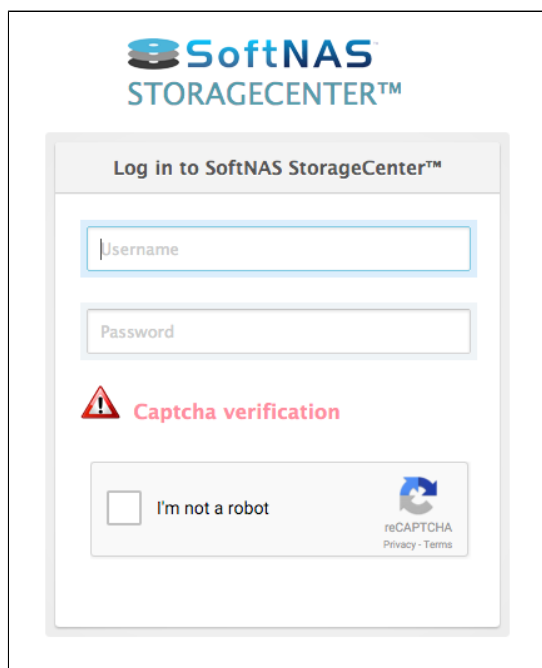
Upon the first access of **StorageCenter** administration interface, a prompt will require login with administrator credentials, as shown below. The default username is **softnas**, and the default passwords for each platform are listed below.

Changing Default Passwords

SoftNAS Cloud® Platform	Default Password
Amazon Web Services EC2	[Instance Name]
Microsoft Azure	[Set via SSH]
VMware vSphere*	Pass4W0rd

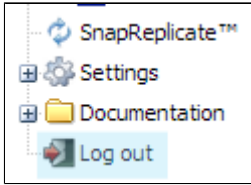
* Note the **zero** in Pass4W0rd.

To prevent brute force entry, after 5 unsuccessful attempts to log in, Recaptcha will prompt the user to perform an additional action in order to continue attempting new passwords.



Logging Out

To log out, click on the Log Out icon in the main menu.

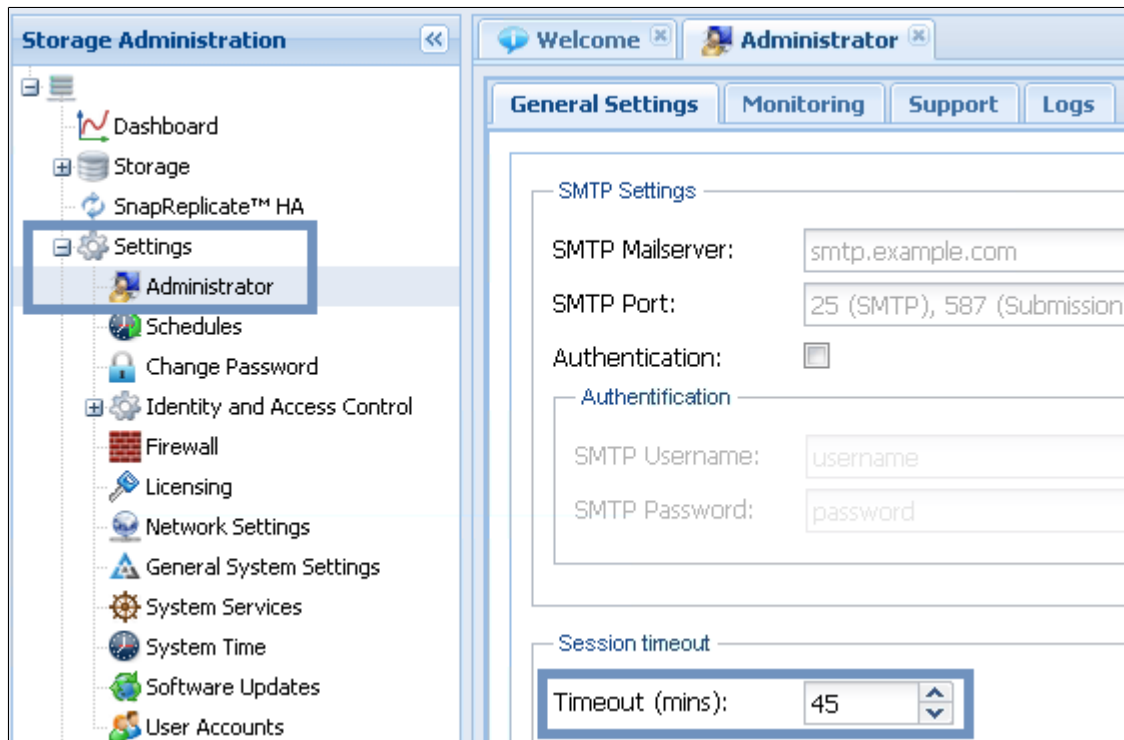


Session Timeout and Auto Logoff

After a default 15 minutes of inactivity, **StorageCenter** will automatically log out of idle sessions. After a session timeout, the web browser will provide a hyperlink with which to log back in.

Click on the link to return to the login screen and continue with the **StorageCenter** login process.

The **StorageCenter** Timeout setting can be changed on the **General Settings** tab in the Administrative section under Settings.



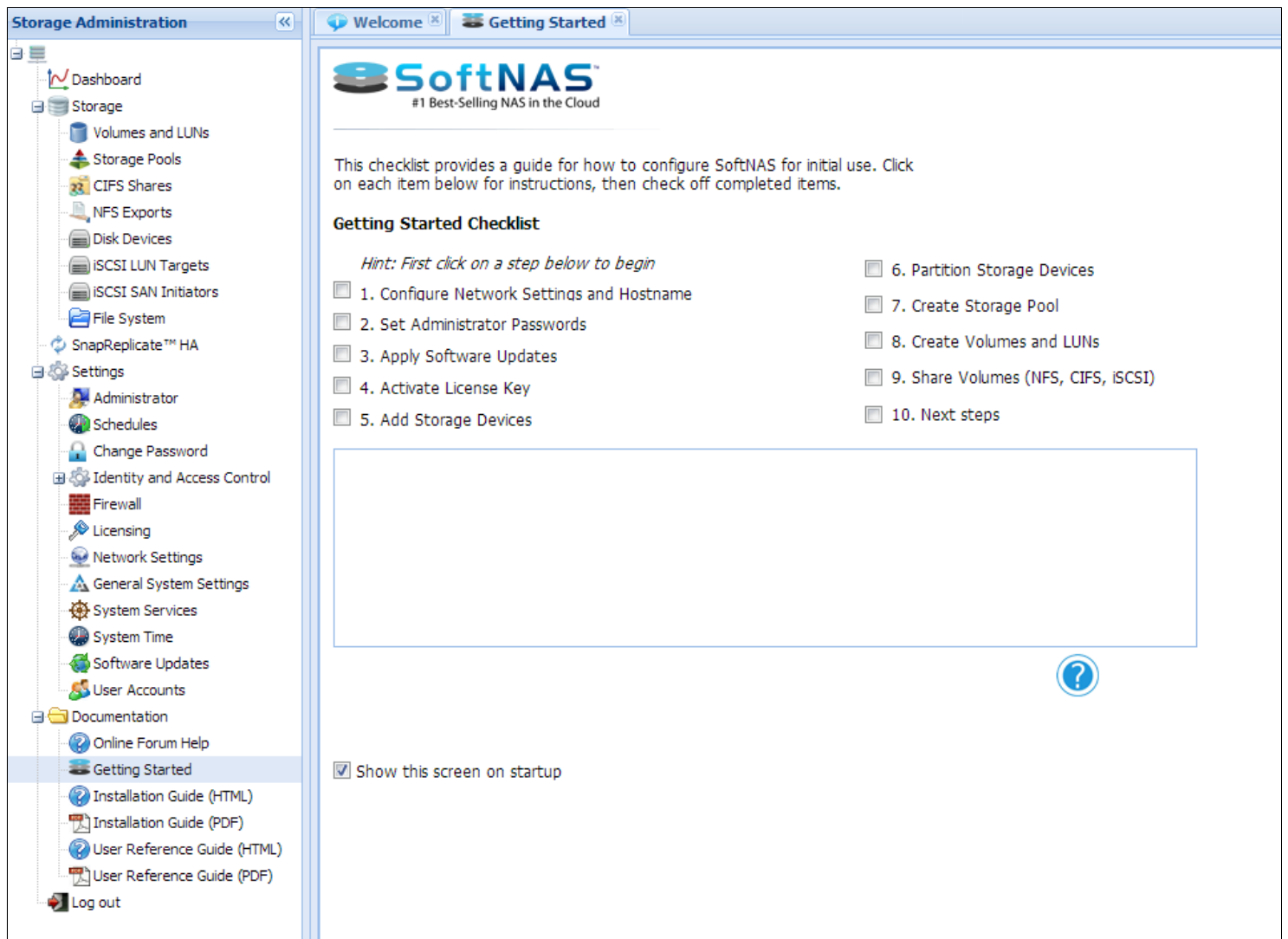
Getting Started Checklist

When **SoftNAS StorageCenter** is first started, the **Getting Started Checklist** will be displayed. This helper provides a set of step-by-step, on-screen instructions designed to make initial configuration, setup and use of **SoftNAS Cloud®** faster and easier for first-time users.

Access this option from the **SoftNAS Cloud® Documentation** section. Simply follow the steps given below.

1. Log on to **SoftNAS StorageCenter**. Be sure to enter your password correctly, as 5 unsuccessful attempts will prompt ReCaptcha to protect your account.
2. In the **Left Navigation Pane**, select the **Getting Started** option under the **Documentation** section.

The **Getting Started** panel will be displayed.




The screenshot shows the 'Storage Administration' interface with the 'Getting Started' checklist active. The left navigation pane includes sections like Storage, Settings, and Documentation. The main content area displays the 'Getting Started Checklist' with 10 numbered steps, each with a checkbox. A hint suggests clicking on a step to begin. A large empty box is provided for instructions, and a help icon is visible at the bottom right. A checkbox at the bottom allows the user to 'Show this screen on startup'.

The **Getting Started Checklist** has various introductory steps for initial configuration needs.

3. Click the step to be configured.

Note: It is best to follow the same order of steps as mentioned in the checklist.

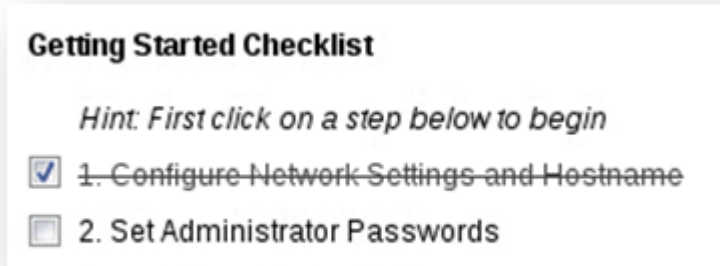
4. Refer and follow the instructions specified in the **Instruction Box** for completing the selected step.

5. Click **Help**  for more information and detailed instructions on how to configure the item in the selected step.

6. Click **Configure Now** to launch the configuration settings window for the step.

7. When the configuration task for the selected step is completed, click the checkbox in front of that step.

The step will be marked off the list to show that it is completed.



8. Repeat the above procedure for all tasks of each configuration step.

9. When all the initial configuration steps are completed, un-check the box in the **Show this screen on startup** field below the configuration area. This setting may also be accessed via **SoftNAS StorageCenter > Administrator > Other Settings > Show/Hide**

10. Set the Notification/Administrator Email. To set your administrator email, follow the instructions found in [Changing Monitoring Notification Frequency](#).

IMPORTANT: An administrator email must be set in order to monitor the health of SoftNAS instances/virtual machines. Critical alerts will be sent to this email address, such as:

- Disk Full
- Resource Overload
- other significant errors and issues

11. Remember to click **Save settings** to commit revisions.

12. Close the **Getting Started** panel.

Changing Default Passwords

Default Passwords:

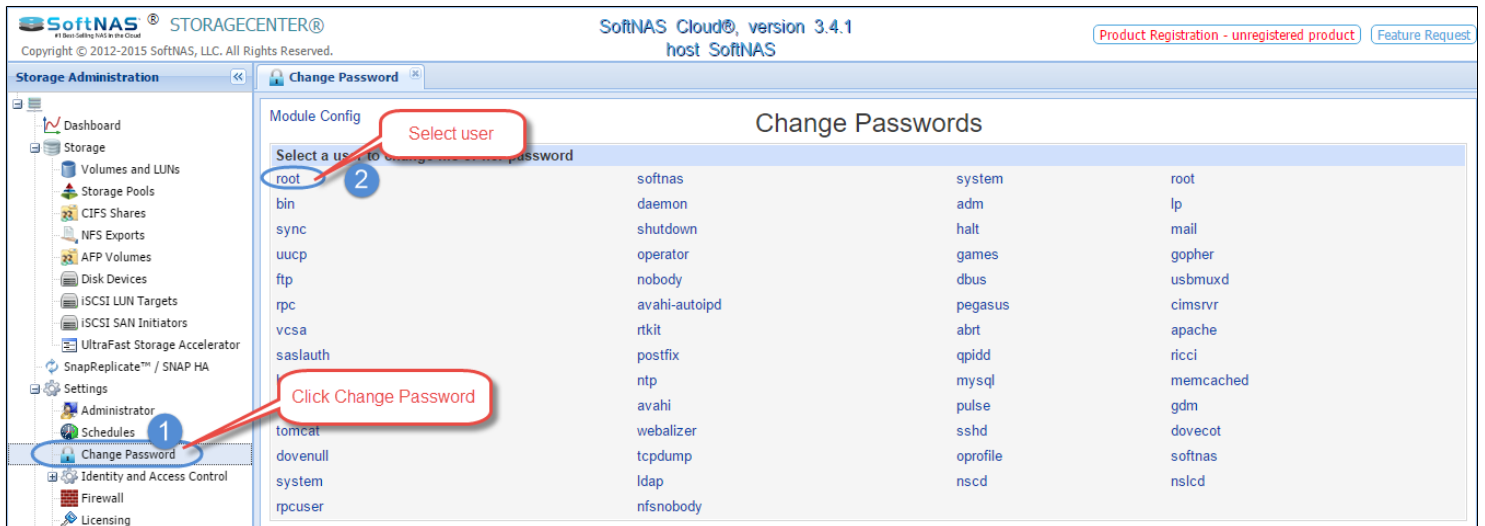
To see the default passwords shipped with **SoftNAS Cloud®**, consult the **Default Passwords Table** in the [Accessing SoftNAS StorageCenter](#) section of this guide.

Security best practices encourage changing these passwords to unique, secure passwords in order to increase the security of important data managed by **SoftNAS Cloud®**.

To change the login password:

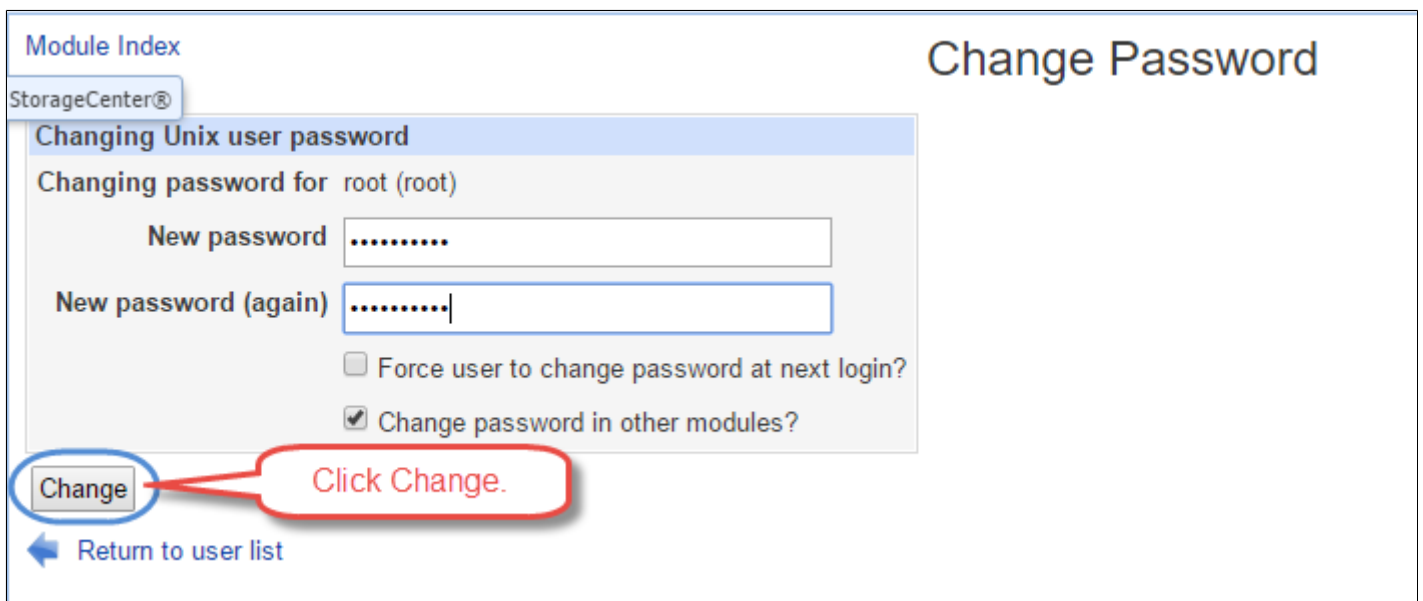
1. Log on to **SoftNAS StorageCenter**.
2. In the **Storage Administration Pane** (on the left), select the **Change Password** option under **Settings**.

The **Change Password** panel will be displayed.



3. Select the user whose password is to be changed.

The **Changing Unix User Password** section will be displayed.



4. Enter the new password in the **New Password** text entry box.

5. Confirm the password by re-entering it in the **New Password (Again)** text entry box.
6. Check "**Force User to change password at next login?**" to force the user to change the password when he logs on to the system next time. This allows an admin to provide a user a temporary password if he/she has login issues.
7. Check "**Change password in other modules?**" to enforce the change of password in other modules also.
8. Click **Change**.

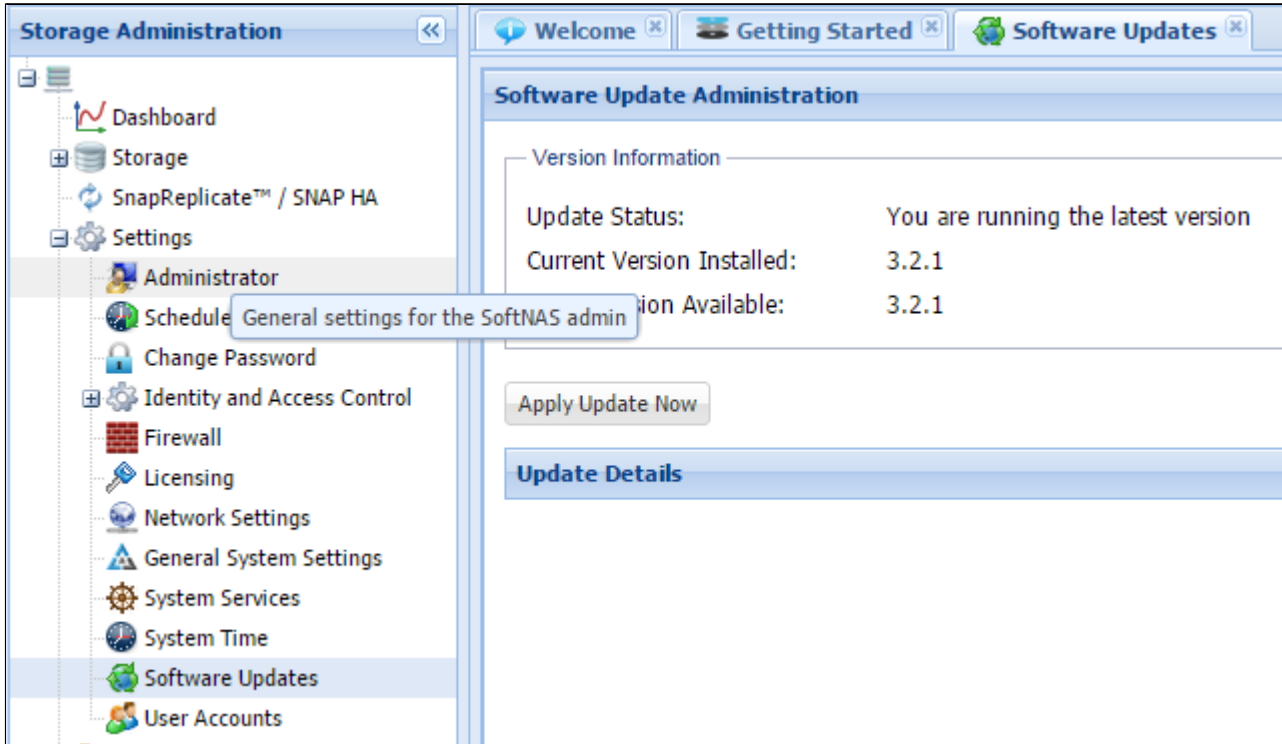
The password of the selected user will now be changed and he/she can now log on to the system with the new password.

Updating to the Latest Version

After installing **SoftNAS Cloud®**, it is recommended to perform a software update to ensure the latest version.

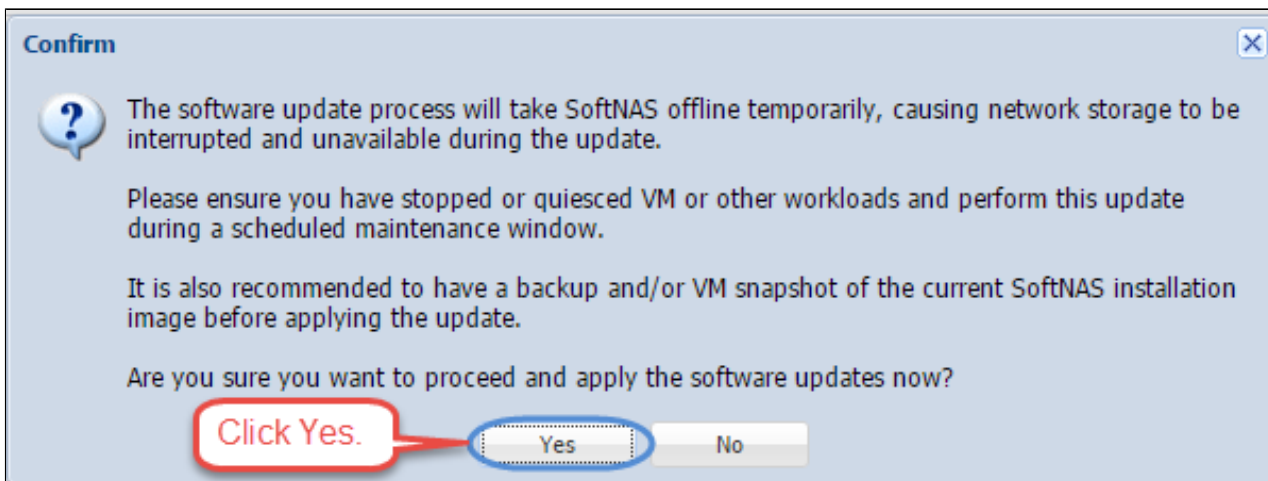
1. Log on to **SoftNAS StorageCenter**.
2. Click the **Software Updates** option under the **Settings** section in the **Left Navigation Pane**.

The **Software Updates** panel will be displayed.



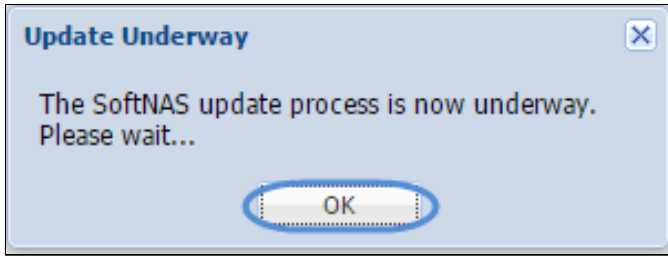
3. If the existing version is not the latest version, click **Apply Update Now**.

The **Confirm** message box recommends backing up and creating a VM Snapshot of the current **SoftNAS Cloud®** installation image.



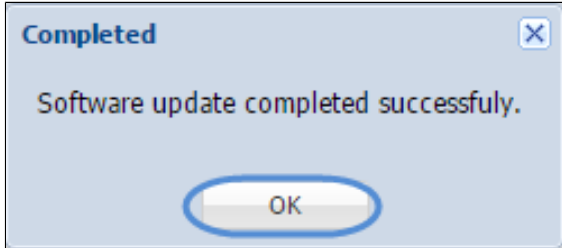
4. Confirm that all prerequisite steps have been satisfied. Click **Yes**.

The **Update Underway** message box describing the progress of the update process will be displayed.



5. Click **OK**.

The **Completed** message box reporting the successful completion of the update process will be displayed.



6. Click **OK**.

The software update will be performed. Upon clicking **OK**, your browser will automatically refresh, and reload the application.

Your update is complete.

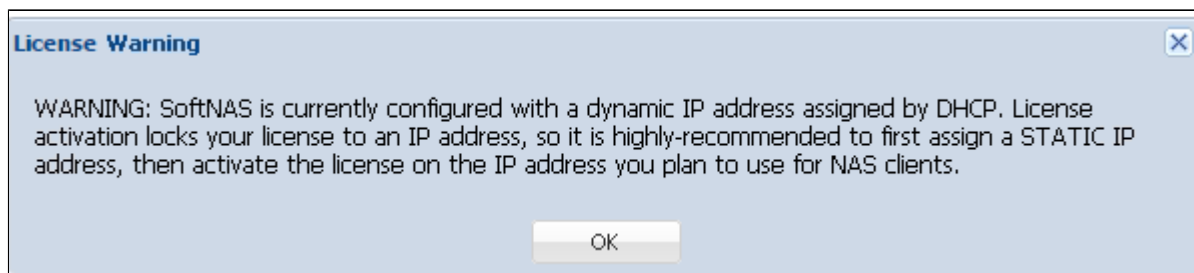
Activating SoftNAS Cloud® License

SoftNAS Cloud® for VMware vSphere requires a license purchased from softnas.com. SoftNAS Cloud® for Amazon Web Services and Microsoft Azure are licensed through subscription plans and do not require further activation.

SoftNAS Cloud® is available as a **SoftNAS Cloud® Free Trial** with the potential for up to 20 TB of storage. To gain access to additional storage capacity and features and personalize a **SoftNAS Cloud®** product after installation, be sure to activate **SoftNAS Cloud®** using the license key found in the administrator's customer control panel. Available versions include **SoftNAS Cloud® Express**, and **SoftNAS Cloud® Standard**.

To activate a **SoftNAS Cloud®** product :

1. Collect the credentials via reference email received after signing up with **SoftNAS**. Alternatively, log in to the **SoftNAS Customer Portal** and find a pre-assigned license key there.
2. Log in to **SoftNAS StorageCenter**.
3. From the **Getting Started Helper** tab, click step 4: **Activate License Key** and click **Configure Now**. Alternatively, simply click on the Licensing category in the Storage Administration Menu.



A License Warning will pop up, encouraging a Static IP for the network. This may be completed as is convenient.

4. Refer to the email received after initial login and download with the **License Key** and **License Owner** credentials. Enter these values into the appropriate fields.

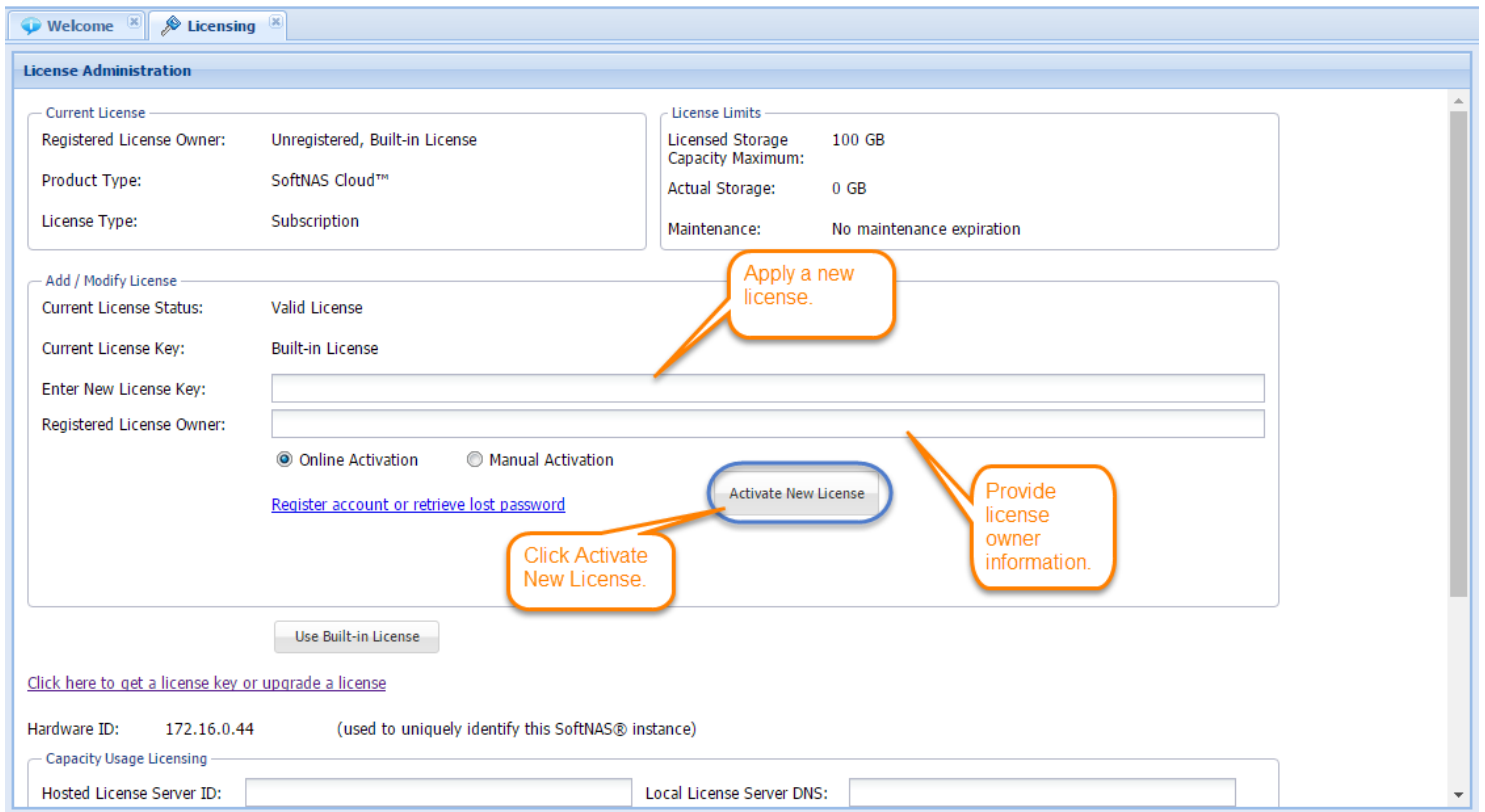
Note: Copy/Pasting the string from one medium to another is the best way to avoid data entry errors.

Before Activation

- **Internet Explorer Extended Security Configuration (ESC) must be disabled** before activating if applicable. ESC interferes with normal Javascript operation and is not supported. If ESC is enabled, activation will not operate correctly, so be sure to verify it is disabled.

- To move a **SoftNAS Cloud®** license to a different machine, please contact our support team. We will help with deactivating an old license and activating it on a new machine.

If using **SnapReplicate** between two **SoftNAS Cloud®** nodes, then a unique license key must be purchased for each node. In the **Storage Administration** pane, expand **Settings** to find **Licensing**.



5. Click **Activate New License**.

The license is activated.

Note: The license activation associates a **SoftNAS Cloud®** license to the IP address (**VMware vSphere**) or EC2 instance (**Amazon EC2**).

This IP address (or EC2 instance ID) is fixed and will not change during normal production operation.

Manual Activation

In cases where **SoftNAS Cloud®** does not have outbound Internet access (for security or other reasons), the license must be activated manually.

Note: For manual activation, please contact **SoftNAS Support** and we will provide a unique **Activation Code** that can be entered to manually activate **SoftNAS Cloud®**.

Automatic Recurring Subscription Updates

Once per month or year, depending on **SoftNAS Cloud®** subscription period, **SoftNAS Cloud®** will automatically contact the **SoftNAS Cloud®** license activation server to verify the renewal of a subscription. If it was renewed successfully, the new license key will be automatically downloaded and activated.

Note: Please ensure that **SoftNAS Cloud®** has outbound Internet access for auto renewal to take place.

License Grace Period

In the event **SoftNAS Cloud®** is running in a production environment and its license expires, it will enter the grace period. During this grace period, all functions continue to be available, and each login to access the **StorageCenter UI** will prompt a license expiration warning notice reminder (e.g., **SoftNAS Cloud®** not connected to Internet, credit card on file failed or expired, etc.). An email notification will have already been sent to the administrator about renewal at this point.

Note: The grace period defaults to one week (7 days) for all monthly and annual licenses for **SoftNAS Cloud®**, providing ample time to resolve any license renewal issues. If there is a billing error, once that is corrected, the system will automatically download and install the renewed license key. In environments operating **SoftNAS Cloud®** without an Internet connection, it is recommended to use the annual subscription method, so it is only necessary to enter a license key once a year (or license **SoftNAS Cloud®** for multiple years if preferred).

SoftNAS Cloud® S3 Disk Overview

About SoftNAS Cloud® S3 Disks

SoftNAS Cloud® Disks are storage devices created from local storage devices or **Amazon S3 Cloud Disks**.

Amazon S3 Cloud Disks

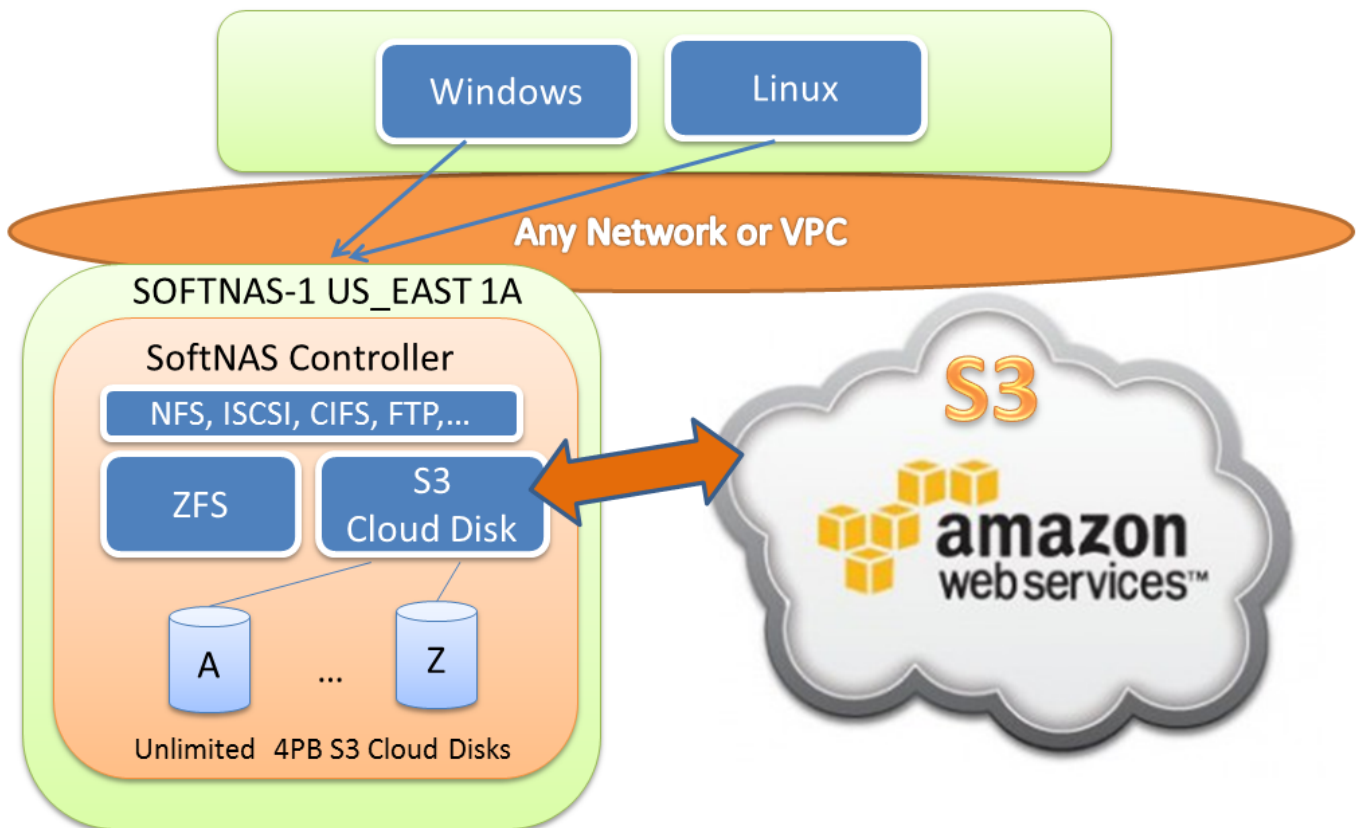
Amazon S3 is storage for the Internet, specifically designed to make web-scale computing easier. **Amazon S3** and **SoftNAS S3 Cloud Disks** provide access to store and retrieve any amount of data, at any time, from anywhere on the web. It gives anyone access to the same highly scalable, reliable, secure, fast, inexpensive infrastructure that Amazon uses to run its own global network of web sites. The service aims to maximize benefits of scale and to pass those benefits on to customers.

As shown below, **SoftNAS S3 Cloud Disks** are block devices created from **Amazon S3 storage**.

[Adding Cloud Disk Extenders](#)

SoftNAS S3 Cloud Disks™

Secure, unlimited cloud data from anywhere



Access from anywhere...
AWS, VMware, Windows Hyper-V



Each S3 Cloud Disk device can store up to 4 petabytes (PB) of data. An unlimited number of S3 Cloud Disks are supported. Each S3 Cloud Disk is thin-provisioned, so storage space is only consumed when data is actually written to the device and actually used.

S3 Cloud Disks are attached to **SoftNAS Cloud®** Storage Pools and provide unlimited cloud storage. Each cloud disk is encrypted and authenticated to provide added security.

S3 Cloud Disks can be created and accessed on-premise from **VMware ESXi** systems, as well as within the Amazon EC2 cloud environment.

Cloud disks benefit from **SoftNAS Cloud®** features, including RAM caching, SSD caching, compression, deduplication, scheduled snapshots and read/write clones. This means the best balance of performance and NAS features combined with the off-site data storage redundancy of S3.

Amazon S3 storage subscription costs are industry-competitive, and the EC2 offerings integrate smoothly with SoftNAS Cloud® solutions. Consult [Amazon S3](#) product information for latest details and pricing.

S3 Cloud Disks can also be copied for long-term archive storage into AWS Glacier (functionality that is built into the AWS console).

It is strongly recommended that users review [S3 Cloud Disk Best Practices](#) prior to creating their instances.

Next Steps

[Creating Storage Pools](#)

[Configuring Volumes](#)

[Sharing Volumes over a Network](#)

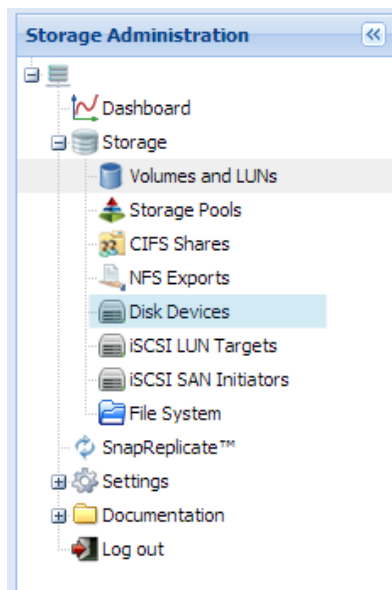
Adding Cloud Disk Extenders

Amazon S3 is storage for the Internet, specifically designed to make web-scale computing easier. **Amazon S3** and **SoftNAS S3 Cloud Disks** provide access to store and retrieve any amount of data, at any time, from anywhere on the web. Other vendors also provide S3 based storage solutions, including Cloudian, Dunkel, Century Link, and many others. SoftNAS supports integration of these cloud disk extenders, and other vendors based on the same technology. Guidance on adding S3 based cloud disks to SoftNAS is provided below, including best effort support for vendors not yet added to our wizard.

Note: For Amazon AWS S3 Users *only*, SoftNAS recommends the use of VPC Endpoints. For more information on VPC Endpoints, see [S3 Cloud Disk Best Practices](#).

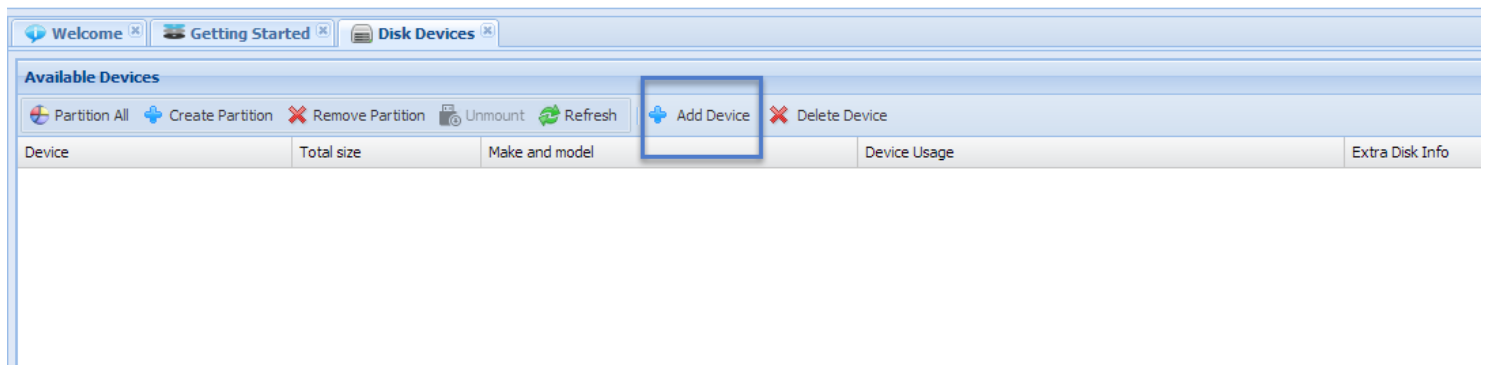
How to Add SoftNAS S3 Cloud Disks

1. Launch **SoftNAS StorageCenter** and choose **Disk Devices** from the main menu



The **Disk Devices** panel appears.

2. From **Disk Devices**, choose **Add Device**



3. From **Add Device** screen, choose the desired S3 provider you wish to connect to from the dropdown, and click **Next** to continue.



Amazon S3 Cloud Extender Disk Settings

The following section illustrates how to connect to your Amazon S3 Cloud Extender Disk. The settings presented, however, (RAM, Bucket Basename, block cache file, etc.) apply equally to the other cloud disk extenders available for selection.

If adding your S3 Cloud Disk through Amazon, the following wizard pop-up will appear, allowing you to connect by entering credentials, associating a region and a bucket, as well as configuring disk size and encryption.



Note: The settings below apply equally to all cloud disk extenders listed in the sections following. If using another cloud disk extender, please follow the guidance provided by said vendor.

RAM

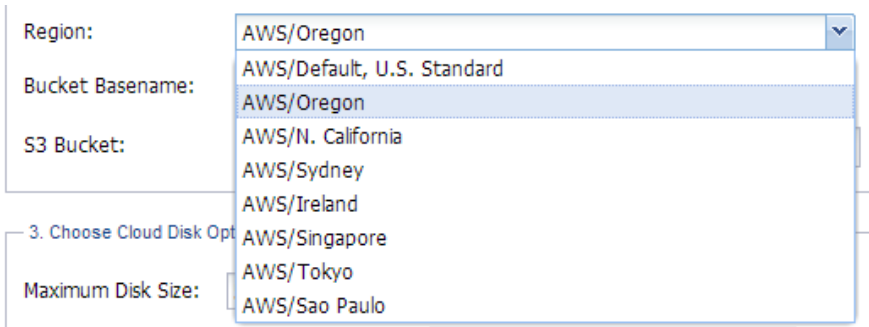
At least 1 GB of RAM is required to support S3 disks.

Bucket Basename

This name is used to automatically generate unique S3 bucket names to host the S3 Cloud Disk. Enter any unique bucket name comprised of all lower-case letters or an automatically generated name.

Region

Use the pull-down menu to choose a regional data center where the S3 Cloud Disk and its corresponding S3 bucket will be created and maintained.



The screenshot shows a configuration form with the following fields and options:

- Region:** A dropdown menu with "AWS/Oregon" selected.
- Bucket Basename:** "AWS/Default, U.S. Standard"
- S3 Bucket:** A dropdown menu with "AWS/Oregon" selected.
- 3. Choose Cloud Disk Opt** (Section Header)
- Maximum Disk Size:** A dropdown menu with "AWS/Tokyo" selected.

The dropdown menu for Region is open, showing the following options: AWS/Oregon, AWS/Default, U.S. Standard, AWS/Oregon, AWS/N. California, AWS/Sydney, AWS/Ireland, AWS/Singapore, AWS/Tokyo, and AWS/Sao Paulo.

For more information on this topic, consult:

[Amazon Regions and Availability Zones](#)

Next, choose cloud disk options:

Maximum Disk Size

This value can be between 1 GB and 4095 TB (4 petabytes). This is the maximum cloud disk size for the device. As cloud disks are thin provisioned, there are no Amazon S3 storage costs until data is actually stored in a **SoftNAS Cloud®** storage pool and volume.

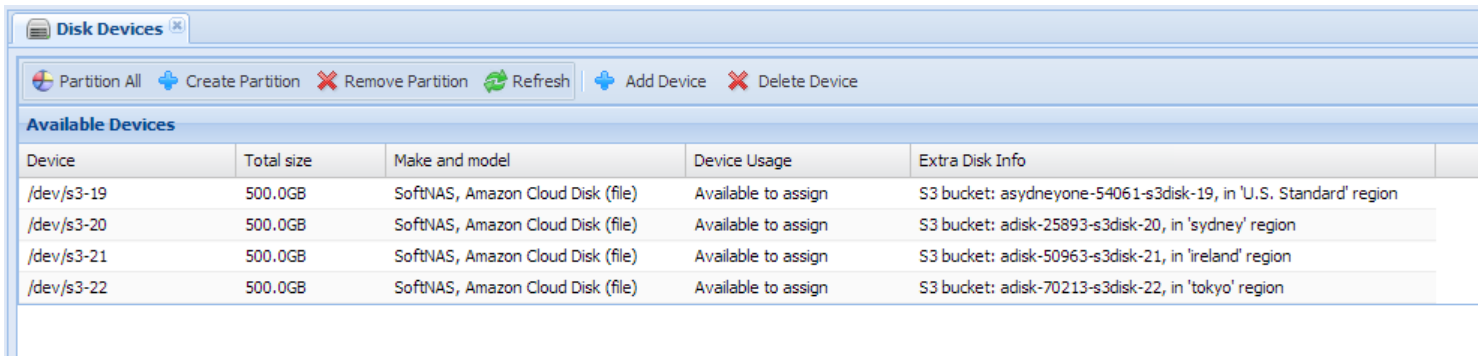
When choosing a Maximum Disk Size, please keep in mind that a **SoftNAS Cloud®** license will be required for the maximum amount of storage planned for use. VMs will consume approximately 30GB of disk space.

Encrypted disk

Check this option and provide a **Disk Password** to encrypt the contents of the S3 cloud disk. This will ensure its contents cannot be accessed, except via this S3 Cloud Disk.

Press **Create S3 Cloud Disk**.

The S3 Cloud Disk is created, automatically partitioned, and ready for use.



Device	Total size	Make and model	Device Usage	Extra Disk Info
/dev/s3-19	500.0GB	SoftNAS, Amazon Cloud Disk (file)	Available to assign	S3 bucket: asydneyone-54061-s3disk-19, in 'U.S. Standard' region
/dev/s3-20	500.0GB	SoftNAS, Amazon Cloud Disk (file)	Available to assign	S3 bucket: adisk-25893-s3disk-20, in 'sydney' region
/dev/s3-21	500.0GB	SoftNAS, Amazon Cloud Disk (file)	Available to assign	S3 bucket: adisk-50963-s3disk-21, in 'ireland' region
/dev/s3-22	500.0GB	SoftNAS, Amazon Cloud Disk (file)	Available to assign	S3 bucket: adisk-70213-s3disk-22, in 'tokyo' region

Note: The Extra Disk Info column shows the S3 bucket name and region where the bucket is located.

The next step is to [Create a Storage Pool](#) which uses the already-partitioned S3 cloud disk.

Adding Clouidian Cloud Storage Disk Extenders

As with Amazon S3 disks, it is a simple matter of going into **Disk Devices**, and selecting **Add Device** to start the process.

In the **Add Device** popup, simply select **Clouidian Cloud Storage** from the dropdown.

Click **Next**.

The **Clouidian Disk Extender Wizard** will open. The settings are very similar to Amazon S3, enter the access key ID and access key, select your endpoint (Clouidian equivalent to Region), Bucket, etc, based on the above Amazon S3 guidance.



Click **Create Cloud Disk** once settings have been configured.

Adding Century Link Object Storage Disk Extenders

As with Amazon S3 disks, it is a simple matter of going into **Disk Devices**, and selecting **Add Device** to start the process.

In the **Add Device** popup, simply select **Century Link Object Storage** from the dropdown.

Click **Next**.

The **Century Link Disk Extender Wizard** will open. The settings are very similar to Amazon S3, enter the access key ID and access key, select your endpoint (Century Link equivalent to Region), Bucket, etc, based on the above Amazon S3 guidance.



Add Century Link Cloud Disk Extender

1. Enter your account credentials

Access Key ID:

Secret Access Key:

2. Select a bucket (or create a new bucket) for this disk to use as cloud storage

Endpoint:

Bucket Basename: Enter base name to automatically generate bucket names

Bucket:

3. Choose Cloud Disk Options

Maximum Disk Size: (thin-provisioned)

Encrypted disk

Disk Password:

Retype Password:

Click **Create Cloud Disk** once settings have been configured.

Adding NetApp StorageGRID Object Storage Disk Extenders

As with Amazon S3 disks, it is a simple matter of going into **Disk Devices**, and selecting **Add Device** to start the process.

In the **Add Device** popup, simply select **NetApp StorageGRID Object Storage** from the dropdown.

Click **Next**.

The **NetAPP StorageGRID Disk Extender Wizard** will open. The settings are very similar to Amazon S3, enter the access key ID and access key, select your endpoint (NetAPP equivalent to Region), Bucket, etc, based on the above Amazon S3 guidance.

Add NetApp Cloud Disk Extender

NetApp®

1. Enter your account credentials

Access Key ID:

Secret Access Key:

2. Select a bucket (or create a new bucket) for this disk to use as cloud storage

Endpoint:

Bucket Basename: Enter base name to automatically generate bucket names

Bucket:

3. Choose Cloud Disk Options

Maximum Disk Size: (thin-provisioned)

Encrypted disk

Disk Password:

Retype Password:

Click **Create Cloud Disk** once settings have been configured.

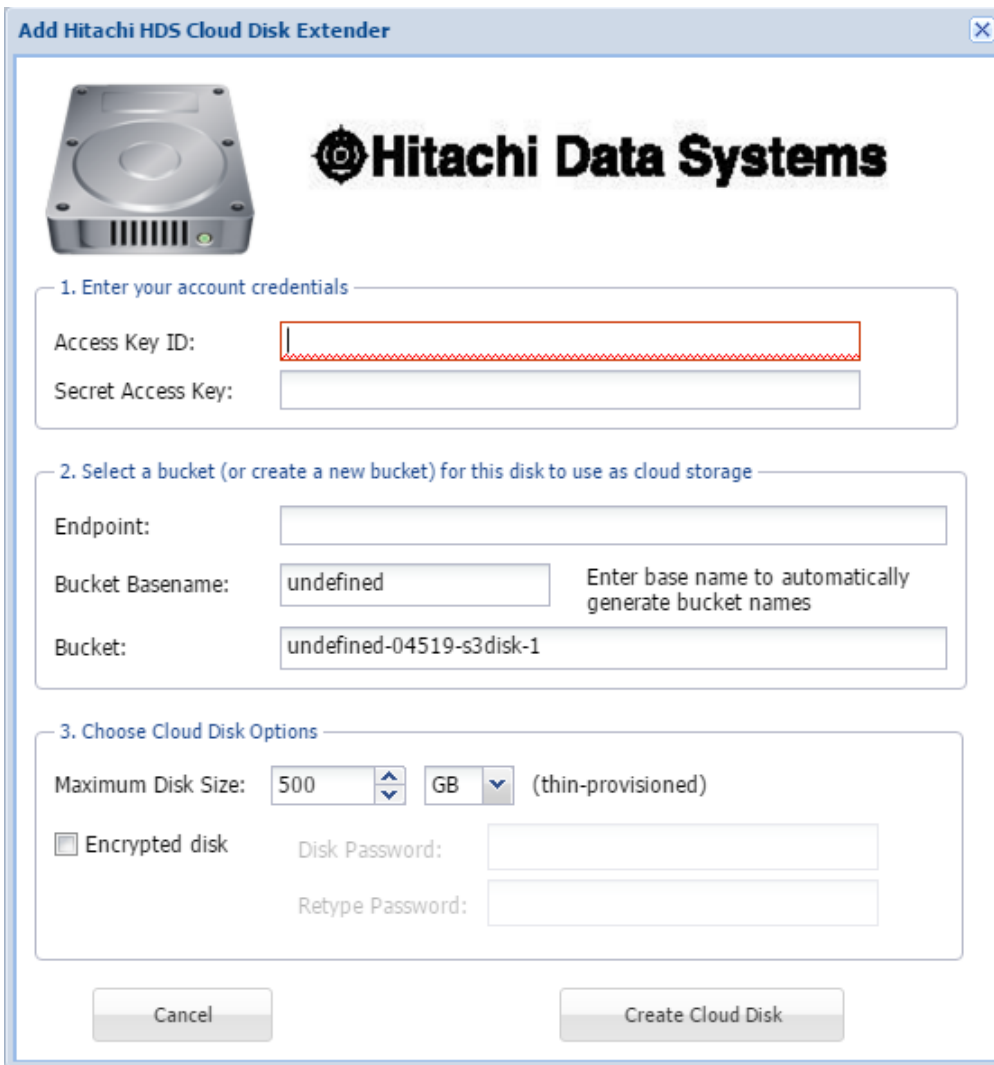
Adding Hitachi HDS Disk Extenders

As with Amazon S3 disks, it is a simple matter of going into **Disk Devices**, and selecting **Add Device** to start the process.

In the **Add Device** popup, simply select **Hitachi HDS** from the dropdown.

Click **Next**.

The **Hitachi HDS Disk Extender Wizard** will open. The settings are very similar to Amazon S3, enter the access key ID and access key, select your endpoint (Cloudian equivalent to Region), Bucket, etc, based on the above Amazon S3 guidance.



Add Hitachi HDS Cloud Disk Extender

Hitachi Data Systems

1. Enter your account credentials

Access Key ID:

Secret Access Key:

2. Select a bucket (or create a new bucket) for this disk to use as cloud storage

Endpoint:

Bucket Basename: Enter base name to automatically generate bucket names

Bucket:

3. Choose Cloud Disk Options

Maximum Disk Size: (thin-provisioned)

Encrypted disk

Disk Password:

Retype Password:

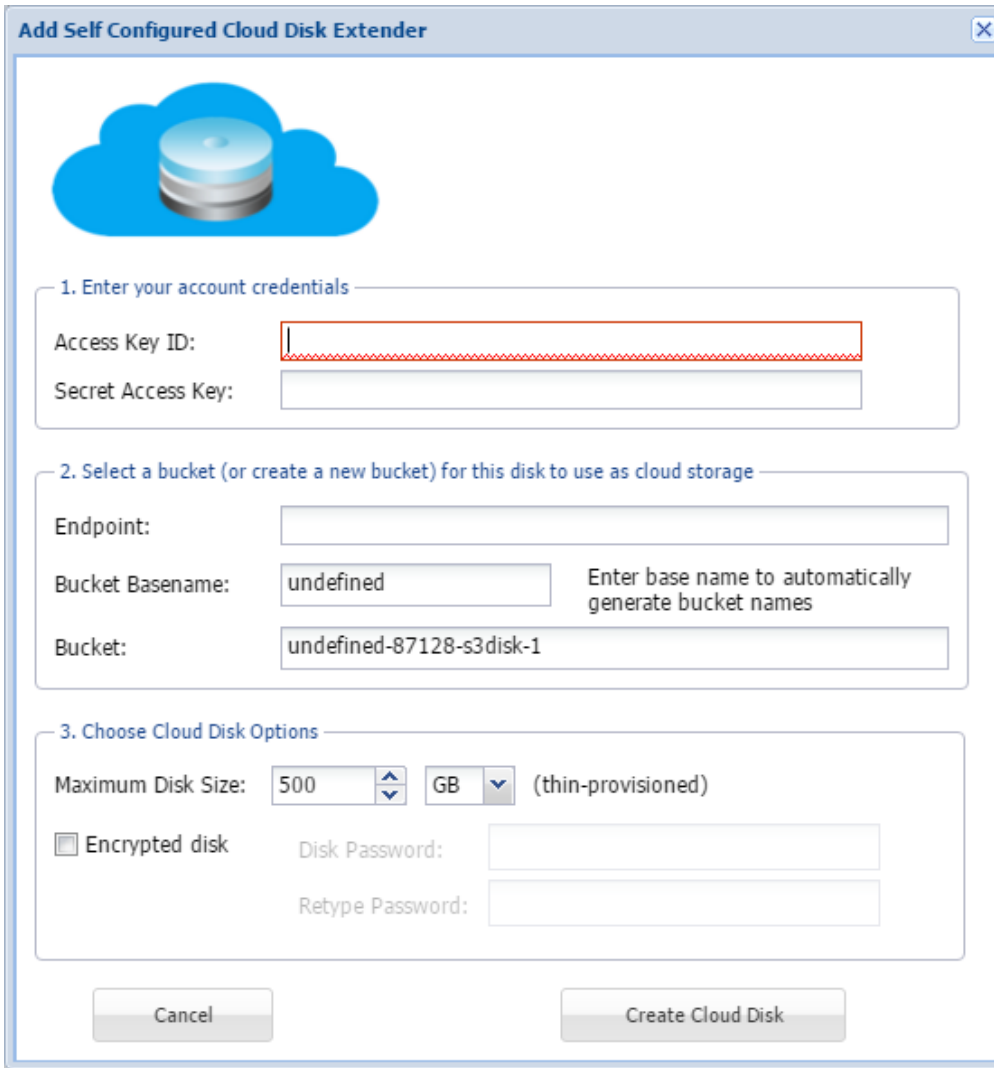
Click **Create Cloud Disk** once settings have been configured.

Adding Self-Configured Disk Extenders

There are numerous S3 compatible cloud storage vendors, each with similar functionality. To allow adding of disks from any vendors we have not yet added to our wizard, you can use the self-configured disk extender to connect to their storage. As with the other options, simply select **Self Configured**.

Click **Next**.

The **Self-Configured Cloud Disk Extender Wizard** will open. This wizard should work for any vendor with S3 compatible storage. As with Amazon S3, you need to add the Access Key ID and Access Key. Select the Endpoint according to the guidance found on the vendor site. The same with the remaining settings. S3 compatible storage typically use a fairly standard list of settings.



The dialog box is titled "Add Self Configured Cloud Disk Extender" and features a blue cloud icon with a disk inside. It is divided into three sections:

- 1. Enter your account credentials**: Contains two text input fields labeled "Access Key ID" and "Secret Access Key".
- 2. Select a bucket (or create a new bucket) for this disk to use as cloud storage**: Contains three text input fields: "Endpoint", "Bucket Basename" (with a value of "undefined" and a note "Enter base name to automatically generate bucket names"), and "Bucket" (with a value of "undefined-87128-s3disk-1").
- 3. Choose Cloud Disk Options**: Contains a "Maximum Disk Size" field with a value of "500", a unit dropdown menu set to "GB", and the text "(thin-provisioned)". Below this is a checkbox for "Encrypted disk" which is unchecked, followed by "Disk Password" and "Retype Password" text input fields.

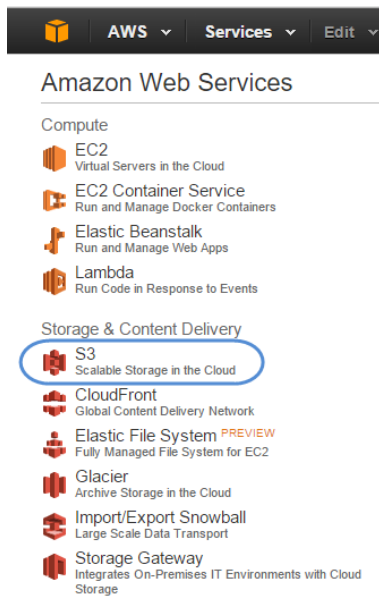
At the bottom of the dialog are two buttons: "Cancel" on the left and "Create Cloud Disk" on the right.

Once you have configured the disk, simply click **Create Cloud Disk**, and your disk should be added.

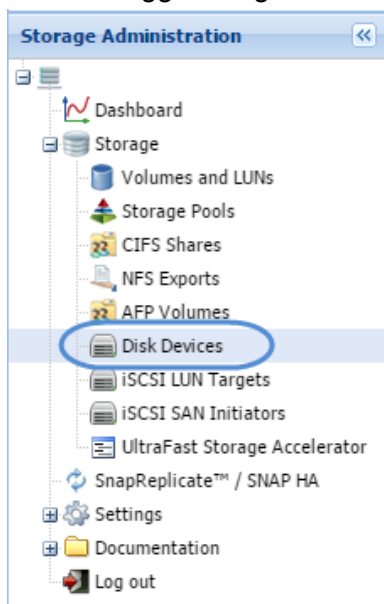
Importing S3 Disks

Amazon S3 buckets have long been leveraged by SoftNAS to provide affordable and easy to manage storage. These buckets of data are resilient, and can survive the failure of a hosting service, such as SoftNAS. Should your existing instance be compromised, SoftNAS makes it easy to recover your S3 bucket by allowing you to retrieve it by importing it to a new instance. This solution limits downtime, and allows you to recover mission critical data quickly and easily.

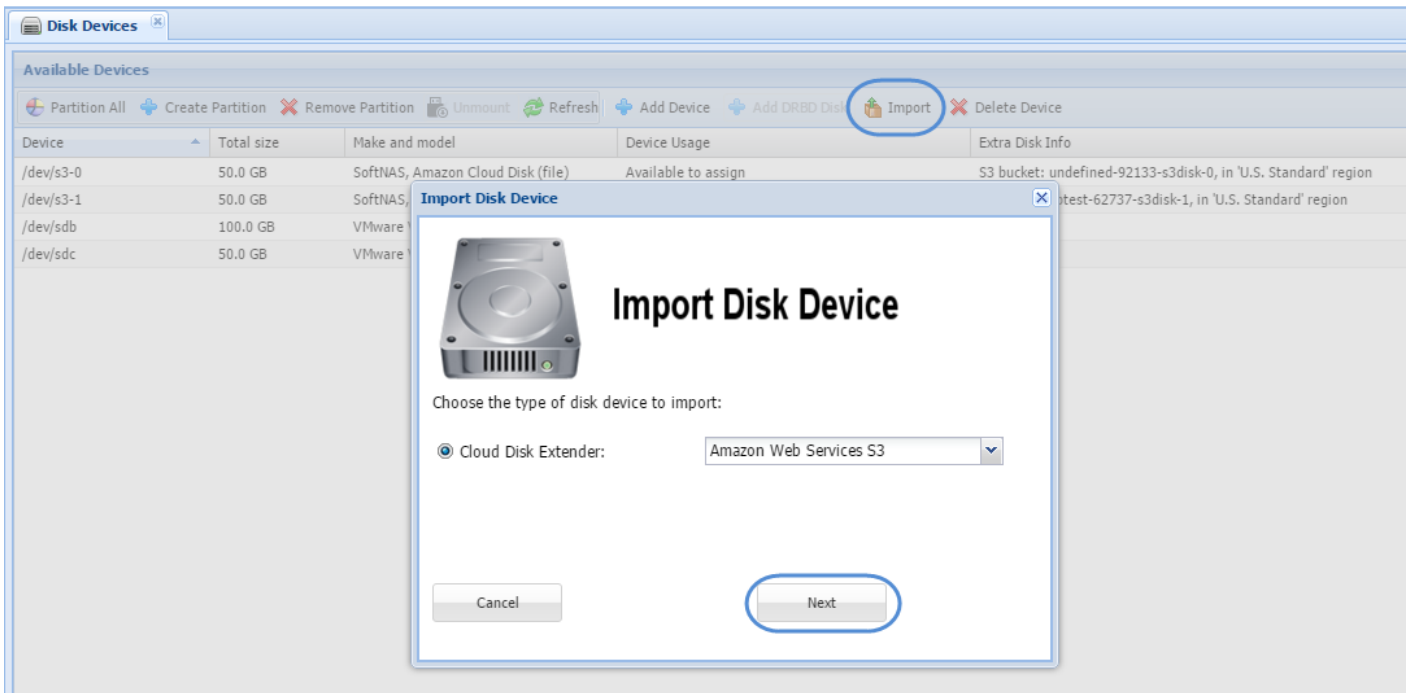
1. To access SoftNAS' import S3 functionality, first create a new SoftNAS VM to serve as host to the imported data.
2. Record the name, bucket information etc, from your previous SoftNAS (or other) instance. If your previous instance cannot be opened, this can be retrieved from the AWS console, under S3.



3. Login to the SoftNAS instance, using the default credentials (unless you have already changed them).
4. Once logged in, go to the **Storage Administration** pane and select **Disk Devices**.



5. Once in **Disk Devices**, select **Import Disk**. Click **Next** on opening frame of the **Import Disk Device** wizard.



6. Here you can retrieve your S3 bucket by providing the required information.
 - a. AWS Access and Secret key
 - b. Device Name - once AWS credentials have been entered, the device names available to that account will be listed. Select the desired device.
 - c. Bucket Name
 - d. Region
 - e. NFS/CIFS if applicable.



7. Click **Import** when done.

Storage Pools Overview

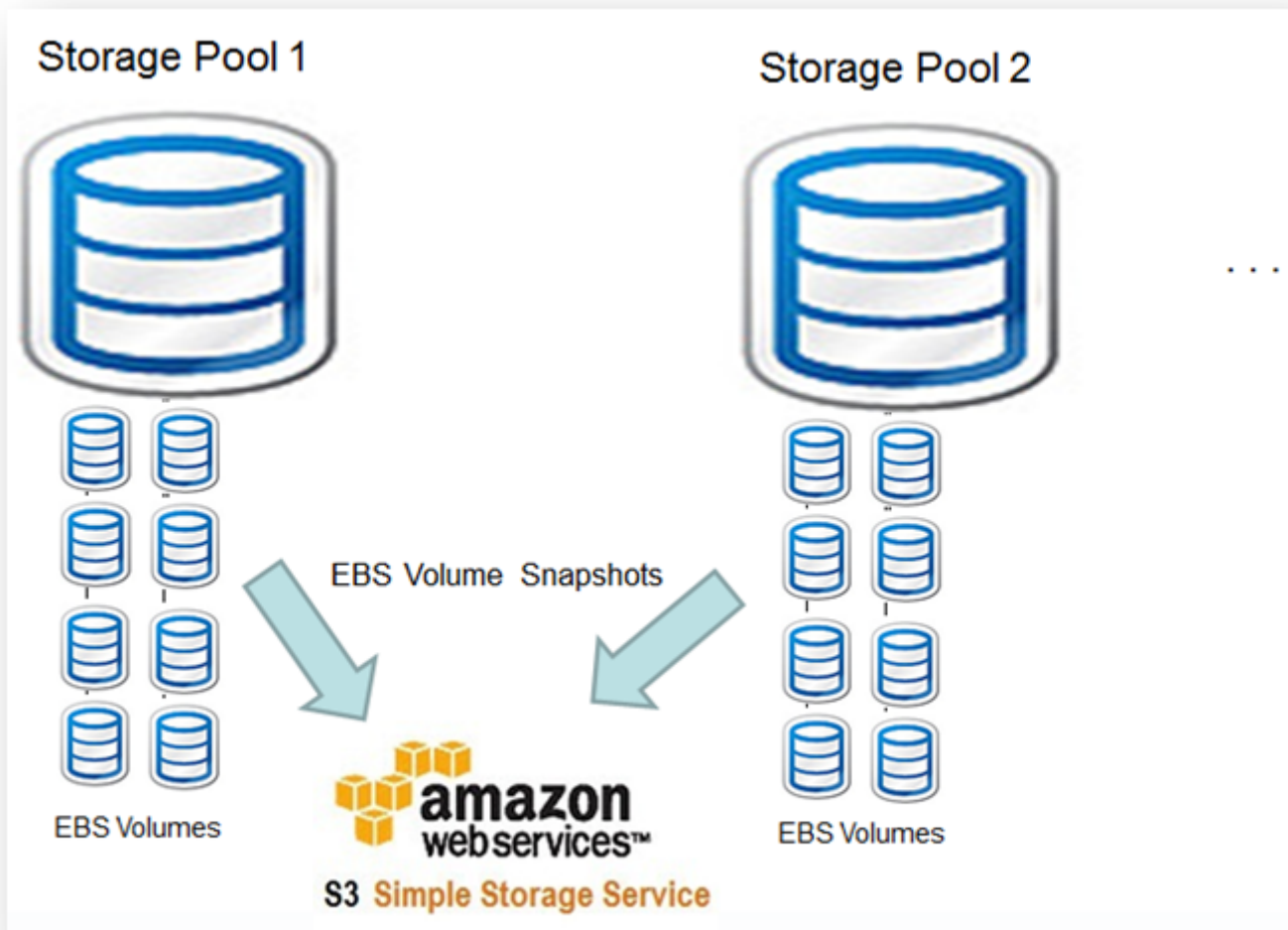
In case of **Amazon EC2**, EBS Volumes may be added as data disks to the **SoftNAS Cloud®** instance and in case of **VMware vSphere**, data disks may be added to the **SoftNAS Cloud® VM**. All applicable disks have been partitioned by this point, so it is time to set up a storage pool.

Storage pools are used to aggregate disk storage into a large **pool** of storage that can be conveniently allocated and shared by **volumes**.

Storage Pools for Amazon EC2-Based SoftNAS Cloud® Instance

In the following example, there are two **storage pools** designed for **Amazon EC2** based **SoftNAS Cloud®** instance. The **Storage Pool 1** is a high-performance pool with SAS disks arranged in a RAID configuration. The **Storage Pool 2** is a high-capacity pool with SATA disks arranged in a RAID configuration. Design any kind of **storage pool** or RAID configuration to best fit the local environment. But these two are the most recommended type of **storage pools**.

The **EBS volumes** can be conveniently backed up to **Amazon S3** redundant storage using **EBS Volume Snapshot** functionality, which is built into **Amazon Web Services**.

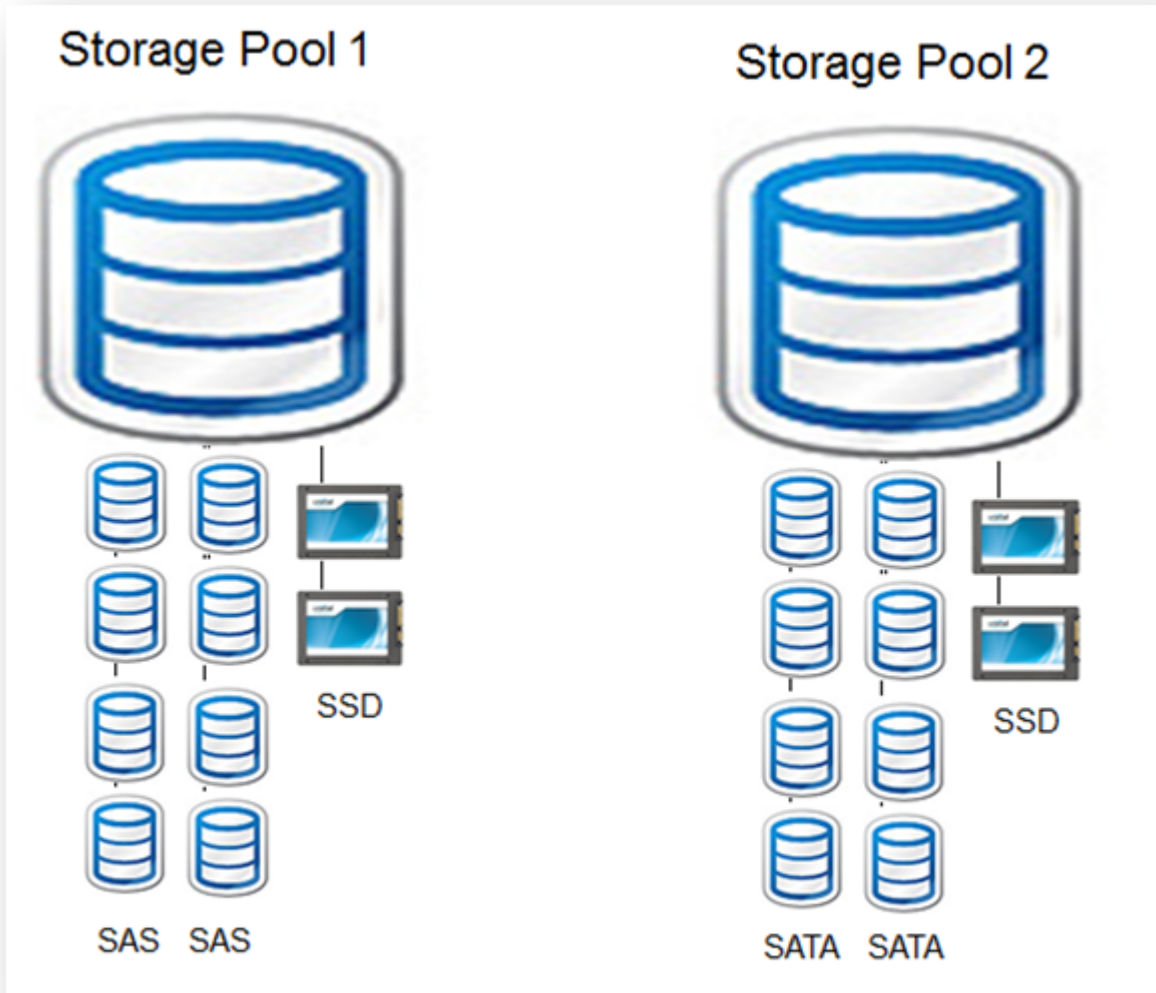


Storage Pools for VMware vSphere Based SoftNAS Cloud® VM

In the following example, there are two **storage pools** designed for **VMware vSphere** based **SoftNAS Cloud®** VM. The **Storage Pool 1** is a high-performance pool with SAS disks arranged in a RAID configuration. It is supplemented with two SSD devices - one for read cache and other for write log SSD. The **Storage Pool 2** is a high-capacity pool with SATA disks arranged in a RAID configuration. It is also supplemented with two SSDs.

Design any kind of **storage pool** or RAID configuration desired, but these two are the most recommended type of **storage pools**.

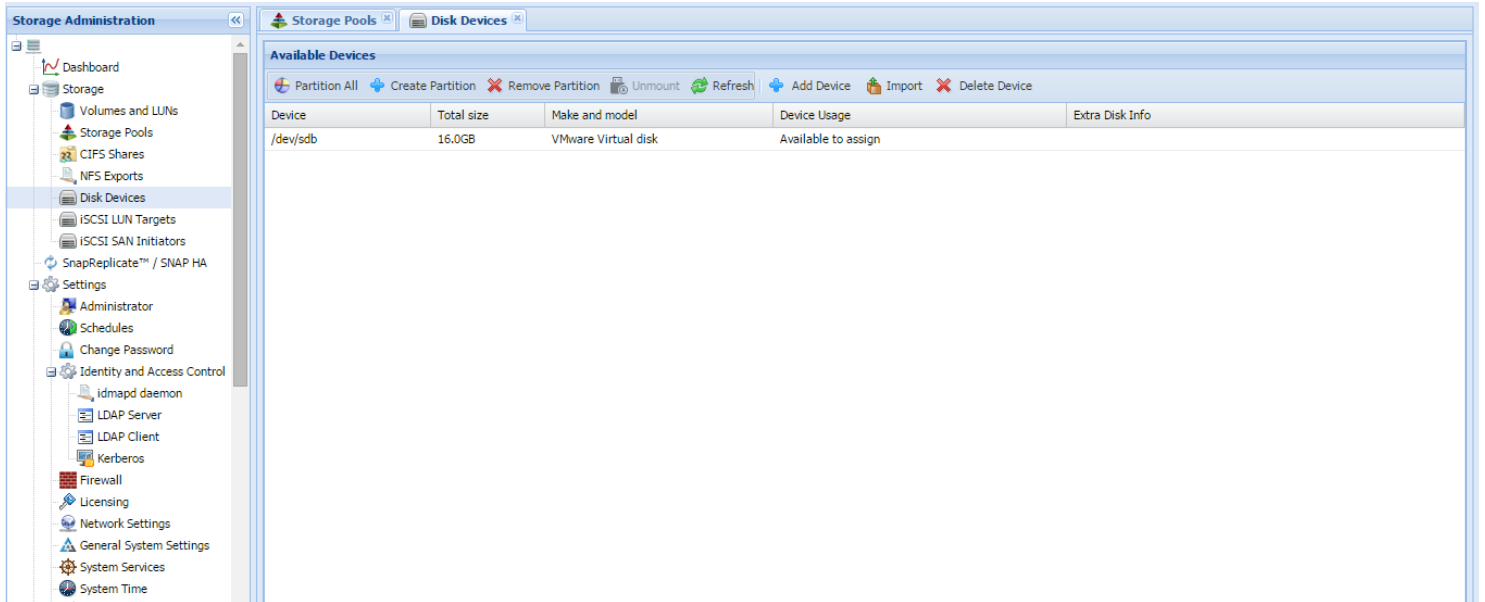
The SSDs are optional, but they provide an enormous boost in read/write performance and have the ability to absorb spikes in I/O (each SSD can handle 20K to 40K IOPS).



Partitioning Disks

1. Log on to **SoftNAS StorageCenter**.
2. In the **Left Navigation Pane**, select the **Disk Devices** option under the **Storage** section.

The **Disk Devices** panel will be displayed.



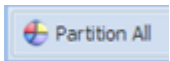
Disk devices must be partitioned prior to use. The available devices are listed in the **Available Devices** grid, as shown above.

Device Usage - indicates the current status of the device, which can be:

- **Device needs partition** - the initial state for a new device that has no partition
- **Available to assign** - the device is partitioned and ready for use in a storage pool
- **Used in pool <poolname>** - the device is in use by the indicated storage pool name

Use the buttons on the toolbar to partition the devices for initial use.

Use **Partition All** to partition all disk devices.



Select each disk device, then use **Create Partition** to partition a device individually.

Remove Partition can be used to remove an existing partition that is no longer needed.

Create a Storage Pool

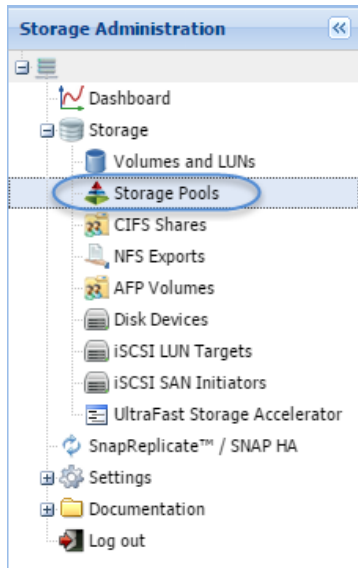
Before implementing the instructions in this section, ensure several EBS volumes have already been created for a [AWS SoftNAS Cloud®](#) instance OR several VHDs for **VMware vSphere** based **SoftNAS Cloud® VM**.

These EBS volumes or VHDs provide the underlying storage for **SoftNAS Cloud®** storage pools. Whenever a volume or VHD is added, it begins as a **raw disk** which means that the disk has no partitions.

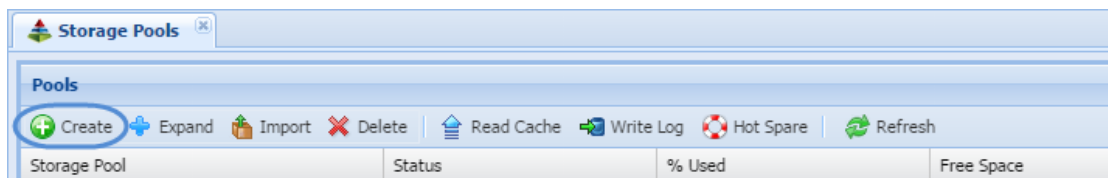
Note: Before disk devices can be assigned to a **storage pool**, [the disks must be partitioned](#).

Create a Storage Pool

1. Click the **Storage Pools** option under the **Storage** section in the **Storage Administration Panel** (on the left).

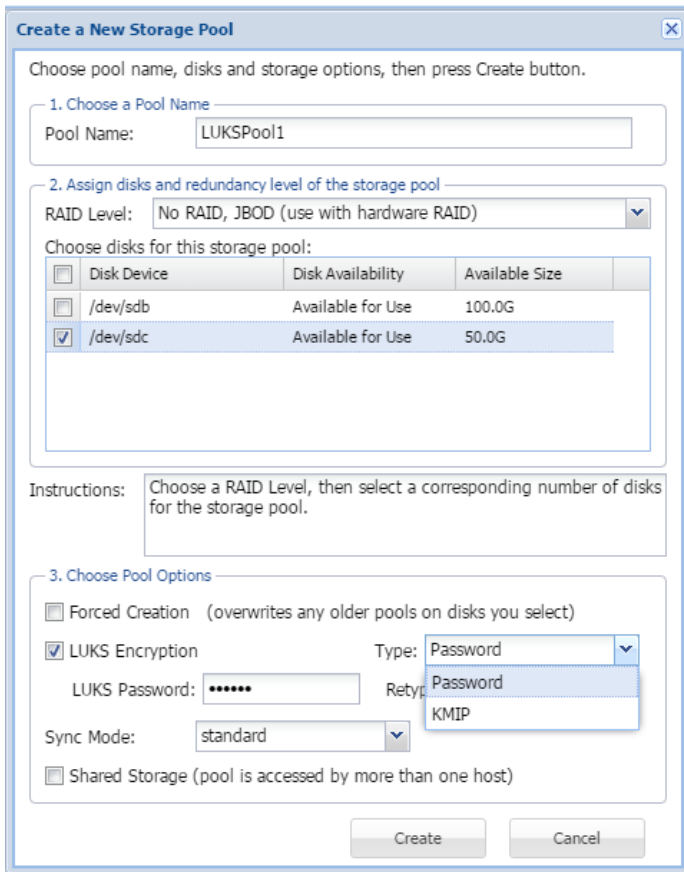


2. The **Storage Pools** panel will be displayed with the list of all the existing storage pools that are already allocated. To create a new storage pool, click **Create**.



The **Create New Storage Pool** dialog will be displayed.

3. Enter the name for the storage pool to be created in the **Pool Name** text entry box.



Choose pool name, disks and storage options, then press Create button.

1. Choose a Pool Name
Pool Name: LUKSPool1

2. Assign disks and redundancy level of the storage pool
RAID Level: No RAID, JBOD (use with hardware RAID)

Choose disks for this storage pool:

<input type="checkbox"/>	Disk Device	Disk Availability	Available Size
<input type="checkbox"/>	/dev/sdb	Available for Use	100.0G
<input checked="" type="checkbox"/>	/dev/sdc	Available for Use	50.0G

Instructions: Choose a RAID Level, then select a corresponding number of disks for the storage pool.

3. Choose Pool Options
 Forced Creation (overwrites any older pools on disks you select)
 LUKS Encryption Type: Password
LUKS Password: ***** Retype: Password
Sync Mode: standard
 Shared Storage (pool is accessed by more than one host)

Create Cancel

Some example storage pool naming schemes might include:

- **Generic naming:** naspool1, naspool2, ...
- **Disk-type naming:** SAS1, SAS2, SATA1, SATA2
- **Use-case naming:** OS1, OS2, Exchange1, SQLData1, UserData1, Geology, Accounting, IT, R&D, QA, Corp01, etc.

3. Select the redundancy level from the **RAID Level** drop down list.

Note: If using hardware RAID at the disk controller level and have a single data disk presented to **SoftNAS Cloud®** for a storage pool, then software RAID may not be required; in such case, select No RAID/JBOD, as the RAID is implemented at a lower level and have no need for software RAID.

4. Select the disks to be allocated to this storage pool.

Note: Each of the devices show the **Disk Availability** status as **Available for Use**. This implies that these disks are already partitioned. New disk devices must be **partitioned** before use.

5. In the **Choose Pool Options** step, check the box in the **Forced Creation** field to overwrite any older pools on the disks selected.

Note: If any of the disk devices chosen have been used as a part of another storage pool in the past (e.g., one that was deleted), use the **Forced Creation** option to overwrite the previous data in order to use the disk in a different pool (a precaution to prevent accidental data loss).

6. Decide whether you wish to add LUKS Encryption (optional).

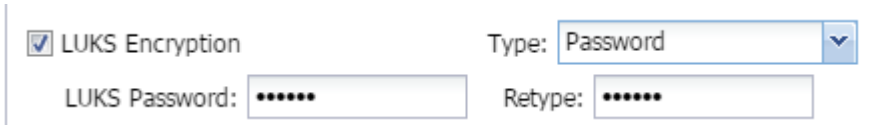
Adding LUKS Encryption

LUKS (Linux Unified Key Setup) encryption is an encryption platform created by Clemens Fruhwirth in 2004 and developed for Linux, but which offers a platform-independent standard on-disk format for use in various tools.

This ensures interoperability and compatibility between different programs, and ensures password management between these programs in a secure and documented manner.

LUKS encryption allows you to add a layer of security to your SoftNAS volumes and pools, and if implemented along with Data-In-Flight encryption via SMB3 for CIFS, or by tunneling through SSH for NFS, can protect your data both at rest and in-flight.

- a. To add LUKS encryption check the box.
- b. In the **Type** dropdown, select Password.
- c. Provide a password and confirm.



The screenshot shows a configuration form for LUKS encryption. It includes a checked checkbox for 'LUKS Encryption', a 'Type' dropdown menu set to 'Password', and two password input fields labeled 'LUKS Password:' and 'Retype:' with masked characters (dots).

7. Choose the required Sync Mode:

- **standard:**

This is the default option. Synchronous file system transactions (fsync, O_DSYNC, O_SYNC, etc) are written out (to the intent log) and then secondly all devices written are flushed to ensure the data is stable (not cached by device controllers).

- **always:**

For the ultra-cautious, every file system transaction is written and flushed to stable storage by a system call return. This obviously has a big performance penalty.

- **disabled:**

Synchronous requests are disabled. File system transactions only commit to stable storage on the next DMU transaction group commit which can be many seconds. This option gives the highest performance. However, it is very dangerous as **ZFS** is ignoring the synchronous transaction demands of applications such as databases or NFS. Setting sync=disabled on the currently active root or /var file system may result in out-of-spec behavior, application data loss and increased vulnerability to replay attacks. This option does ***NOT*** affect **ZFS** on-disk consistency. Administrators should only use this when these risks are understood.

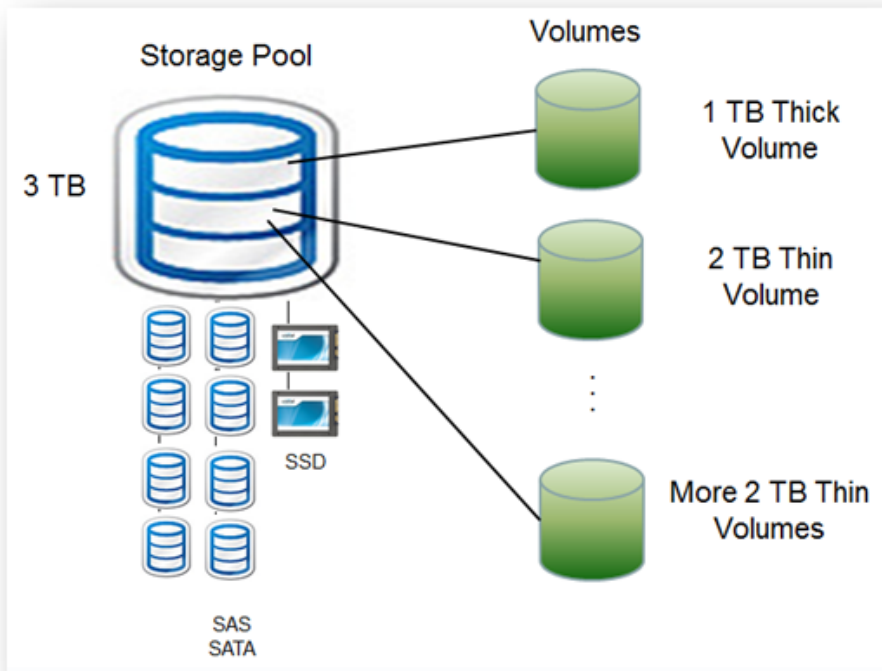
8. If the pool is to be shared (accessed by more than one person at a time), check the box for **Shared**.

9. Click **Create** at the end.

The new storage pool is created and is ready for use.

Sharing Volumes over a Network

Volumes provide a way to allocate storage available in a storage pool and share it over the network.



In the above example, the **Storage Pool** with 3 TB of disk space is allocated from several SAS, SATA and/or SSD devices. There are 3 volumes and like VMDK, a volume can be either **thick-provisioned** or **thin-provisioned**. The thick-provisioned volumes cause storage space to be reserved from the storage pool, reducing the amount of storage available for use by other volumes. The thin-provisioned volumes consume actual storage pool space when the data is written to the volume.

So, there is a thick-provisioned volume which reserves 1 TB of the available 3 TB storage pool and there are also 2 thin-provisioned volumes up to 2 TB of thin-provisioned storage space available to each of them.

Note: As each thin-provisioned volume grows with actual data written to the volume, the available storage pool space for all thin-provisioned volumes shrinks to the remaining unused storage pool space. Volumes allocate and organize storage, and are published for sharing on the network using either **CIFS (Common Internet File System)** or **NFS (Network File System)**.

Configure filesystem volumes for sharing as **CIFS Share** or **NFS Share** so that storage is available for use by the applications, servers and clients on the network.

Configure block device volumes as **LUNs** (block data storage devices), for use with **iSCSI targets**.

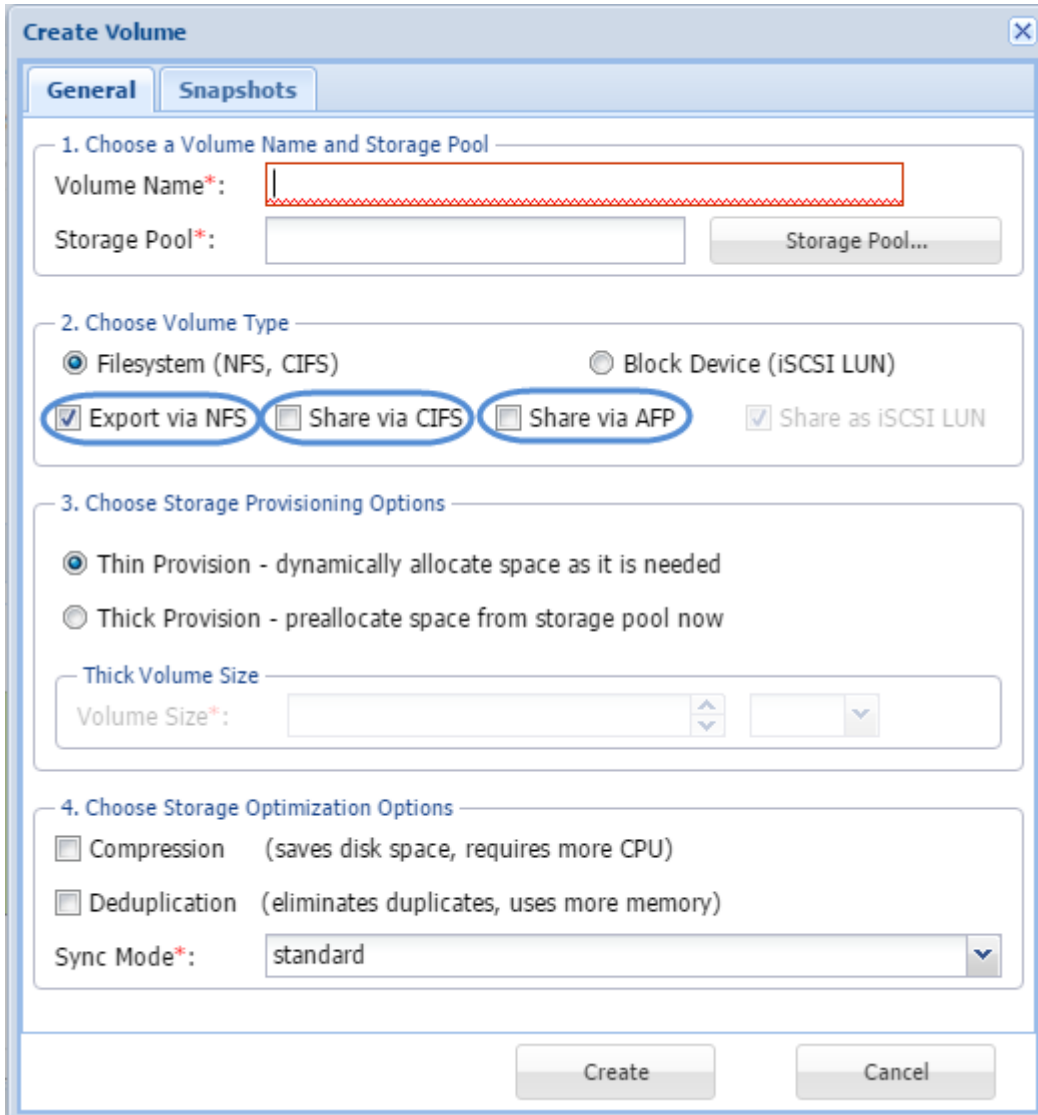
- [Creating CIFS Share](#)
- [Creating NFS Share](#)
- [Creating an AFP \(Apple Filing Protocol\) Share](#)
- [Creating an iSCSI Target and LUN](#)

Create & Configure Volumes

Create the Volume

1. Click **Create** in the toolbar.

The **Create Volume** dialog will be displayed.



Create Volume

General | **Snapshots**

1. Choose a Volume Name and Storage Pool

Volume Name*:

Storage Pool*:

2. Choose Volume Type

Filesystem (NFS, CIFS) Block Device (iSCSI LUN)

Export via NFS Share via CIFS Share via AFP Share as iSCSI LUN

3. Choose Storage Provisioning Options

Thin Provision - dynamically allocate space as it is needed

Thick Provision - preallocate space from storage pool now

Thick Volume Size

Volume Size*:

4. Choose Storage Optimization Options

Compression (saves disk space, requires more CPU)

Deduplication (eliminates duplicates, uses more memory)

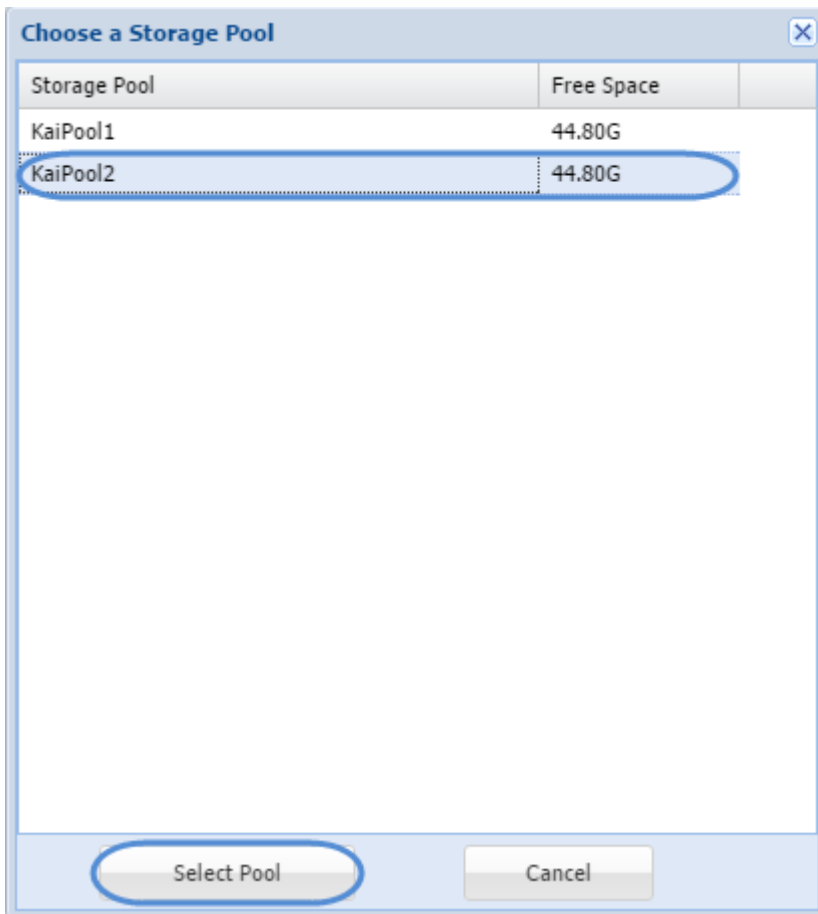
Sync Mode*:

Note: Take a moment to learn more about the **SoftNAS** advantage with our leading-edge [Creating CIFS](#) and [Creating NFS Share](#) solution sections. AFP file sharing is also possible, and is covered in [Creating an AFP Share](#).

2. Enter the name of the volume in the **Volume Name** text entry box.

3. To select the storage pool where the storage space for the volume has to be reserved, click **Storage Pool**.

The **Choose a Storage Pool** dialog will be displayed.



Select the required storage pool from the list of available storage pools. Click **Select Pool**.

Back in the **Create Volume** dialog, the name of the selected storage pool will be displayed in the **Storage Pool** field.

4. Select the type of the volume from the **Volume Type** section. The available volume types are **File System (NFS, CIFS, AFP)** and **Block Device (iSCSI LUN)**.

Note: To share the volume via iSCSI, choose **Block Device** instead of accepting the default **File System** volume type.

5. **One-click Sharing - SoftNAS Cloud®** supports **one-click sharing** during Volume creation. Choose the appropriate sharing option checkboxes to Export to NFS, Share via CIFS and/or Apple Filing Protocol, as appropriate. Verify the type of one-click sharing selected. The available options are **Export via NFS** and **Share via CIFS** for **File System** volume type and **Share as iSCSI LUN** for **Block Device** volume type.

6. Select the type of the storage provisioning option. The available options include **Thin Provision - Dynamically allocate space as it is needed** and **Thick Provision - Preallocate space from storage pool now**.

Thin Provision and Thick Provision

Thin-provisioning allows a volume to acquire storage from its Storage Pool on an as-needed basis, as new data is written to the volume. Thin-provisioning enables many volumes to share a storage pool without an upper limit being placed on the volume itself (the only upper limit to the volume's size is available space in the pool). Thick-provisioned volumes reduce the amount of space available in the Storage Pool by reserving this space for use by a specific volume. When a thick-provisioned volume reaches its maximum volume size, no more data can be written and a volume full error will be returned for writes to a full volume. Thick-provisioned volumes can be re-sized at any time to add space (or return space to the storage by by reducing the volume size).

Volume Size:

1. Select the type of the storage provisioning option as **Thick Provision** in the previous step, then specify the size of the volume in the **Volume Size** field and select the size unit.

Once a Storage Pool has been selected for a thick-provisioned volume, the amount of available space to allocate is displayed below the **Volume Size** field, as shown in the example below.

The **Volume Size** value can be any valid numeric value; e.g., 10, 12.5, 100.0, 1.25

2. The **Size Units** selector is used to choose the units for the **Volume Size**. Select the required size unit from the drop down list. The available units include MB – Megabytes, GB - Gigabytes (default) and TB – Terabytes.

Storage Optimization

1. Select the required option for storage optimization in the **Storage Optimization Options** section. The available options are **Compression** and **Deduplication**. The **Compression** type saves disk space, but requires more of CPU space. The **Deduplication** type eliminates duplicates, but consumes more memory space.

The **Compression** type saves disk space, at the expense of additional CPU overheads for each read and write request (to decode and encode the data). Depending on how compressible the data is, it is common to see data compression rates up to 50% or more.

Note: When compressing a significant amount of data, be sure to observe the amount of actual CPU consumed during a typical day, and if necessary, add more CPU capacity to the **SoftNAS Cloud®** VM as required to ensure compression is fast and efficient. If data is not highly compressible, then disabling compression provides a better performance tradeoff.

- The **Deduplication** type eliminates duplicates, but consumes more memory space. For certain types of data (e.g., Windows virtual machine images, which are highly redundant in virtual desktop applications), deduplication can save up to 80% on storage requirements by eliminating duplicate data. Each time a duplicate data block is to be written, a pointer to the existing duplicate block is created instead, along with increasing the duplicate block reference count. To make these operations as fast as possible, a table of deduplicated blocks is maintained. A hash table of deduplicated blocks is kept in memory to make lookups very fast. When a duplicate block is read, it is usually in cache memory and is simply returned with no disk I/O required.

Note: It is recommended to avoid using deduplication unless the data is highly-duplicative, because of the memory impact of deduplication. It is estimated that for every terabyte of deduplicated data managed, one gigabyte of memory is required for the deduplication lookup tables. These tables compete with cache memory, which can reduce the overall performance of **SoftNAS Cloud®**.

Snapshots

[Snapshots in StorageCenter](#)

iSCSI LUNs

[iSCSI LUNS and targets](#)

Creating a CIFS Share

Note: The easiest and recommended method for creating CIFS Shares is through Volume and LUN Create. It is also possible to create a CIFS Share through the CIFS Share option under Storage Administration. However, if using this method, exercise caution. Improper configuration can result in the inability to control the volume, and an inability to create snapshots.

The **Common Internet File System (CIFS)** is the standard way that computer users share files across corporate intranets and the Internet. It provides users with seamless file and print interoperability between VMs and Windows-based clients. **CIFS** allows multiple clients to access and update the same file while preventing conflicts by providing file sharing and file locking.

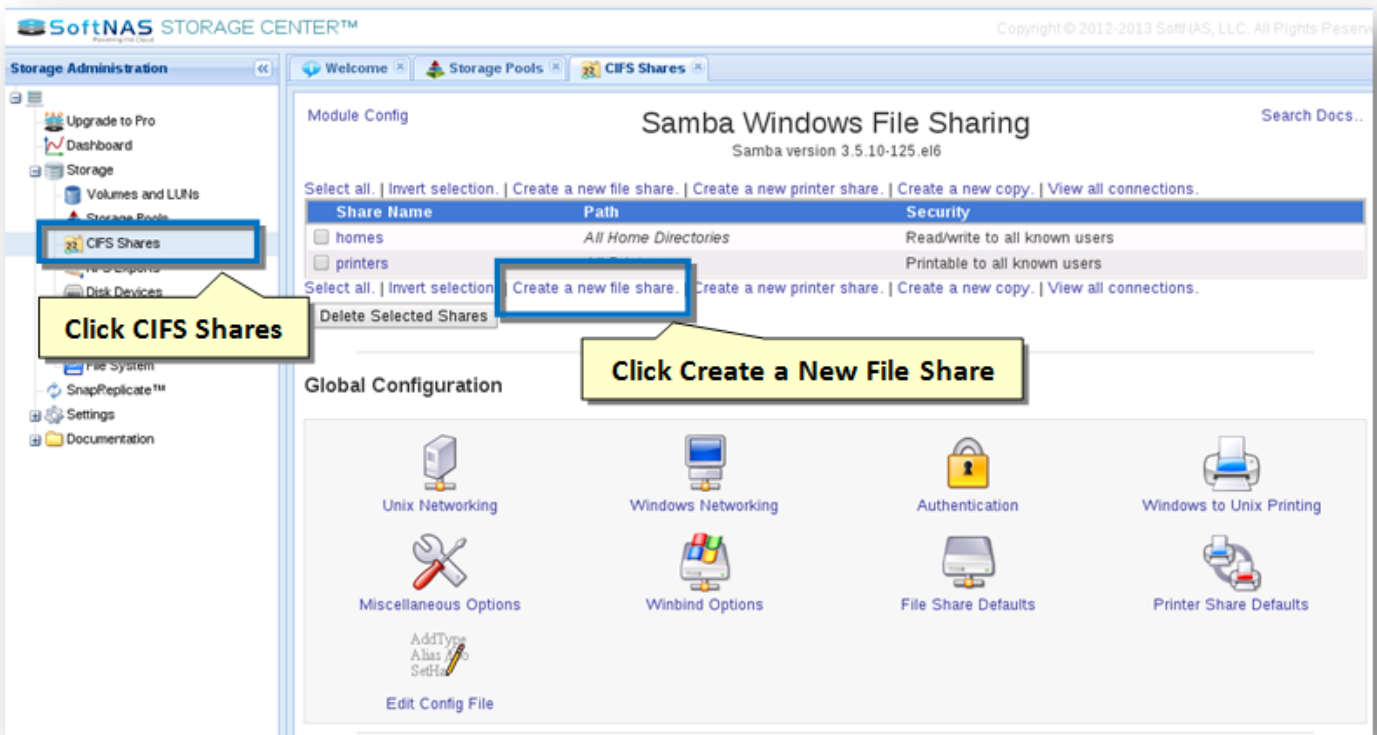
SoftNAS Cloud® uses **Samba Windows File Sharing** for secure, stable, and fast file sharing and print services. **Samba** integrates Linux/Unix Servers and Desktops into Active Directory environments using the winbind daemon.

Allocating storage and network permissions for multiple organizations and dispersed users in branch offices or on a corporate network can be complicated. It is common practice to organize users into groups to provide specific permissions when accessing data. For this reason, the settings of Shares, Users and Groups are closely related in the **CIFS Shares** section of SoftNAS' Storage Administration.

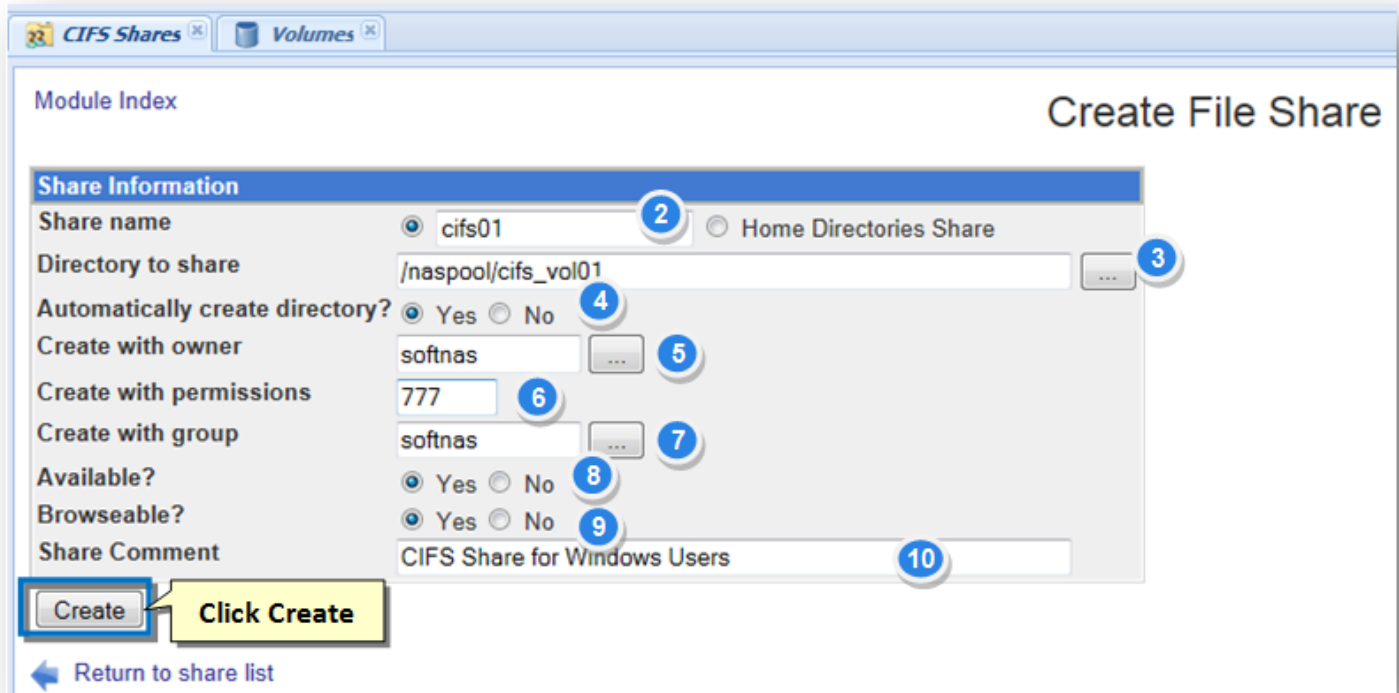
If networking, users, and groups have already been configured for your deployment, the only requirement to make your CIFS Share available is to create one and assign the appropriate permissions. Otherwise Windows Networking and Authentication will need to be configured. In order to assist you, the steps to configure Windows Networking and Authentication are included after "**Creating a New CIFS Share**".

Creating a New CIFS Share

1. On the **CIFS Shares** panel, click the **Create a New File Share** link.



The **Create File Share** section of the panel will be displayed.



2. For most use cases, select the first radio button. Enter a unique alphanumeric name for the share (such as 'documents1') in the **Share Name** text entry box. This name will appear as the network mount point.

Note: If you enter the name of a Unix user, his automatic home directory share will be overridden.

3. The **Directory to share** is the path to the **Volume** that was created in '**Volumes and LUNs**'. Click **Browse** to select the **Volume** from the filesystem for sharing. Click **OK** once the desired volume is selected.

Note: Make sure you select the volume and not just the pool, to be associated with the CIFS Share being created. Failure to do this will cause the ability to manage the volume under SoftNAS' **Volume and LUNs** to be lost. This also means Snapshots will be disabled for the volume.

4. Set the **Automatically Create Directory** field option to **Yes**.

5. The **Create with Owner** field determines which Linux user will be assigned to the shared folder. This will also be the username required to use the CIFS Share on the Windows client.

6. Enter the permission mask in the **Create with Permissions** text entry box. The permissions can be set for the owner, group, and all other users. The leftmost digit is used for the owner, with the center digit specifying the group, and the rightmost is for all other users. Each permission has a predetermined value:

- Read = 4
- Write = 2
- Execute = 1

Adding the permission values together establishes the specific permission level for the owner of the file/directory, group of users, and all other users. For example: 777 is read/write/execute for the owner, group and all users.

7. The **Create with Group** field determines which Linux group will be assigned to the shared folder.

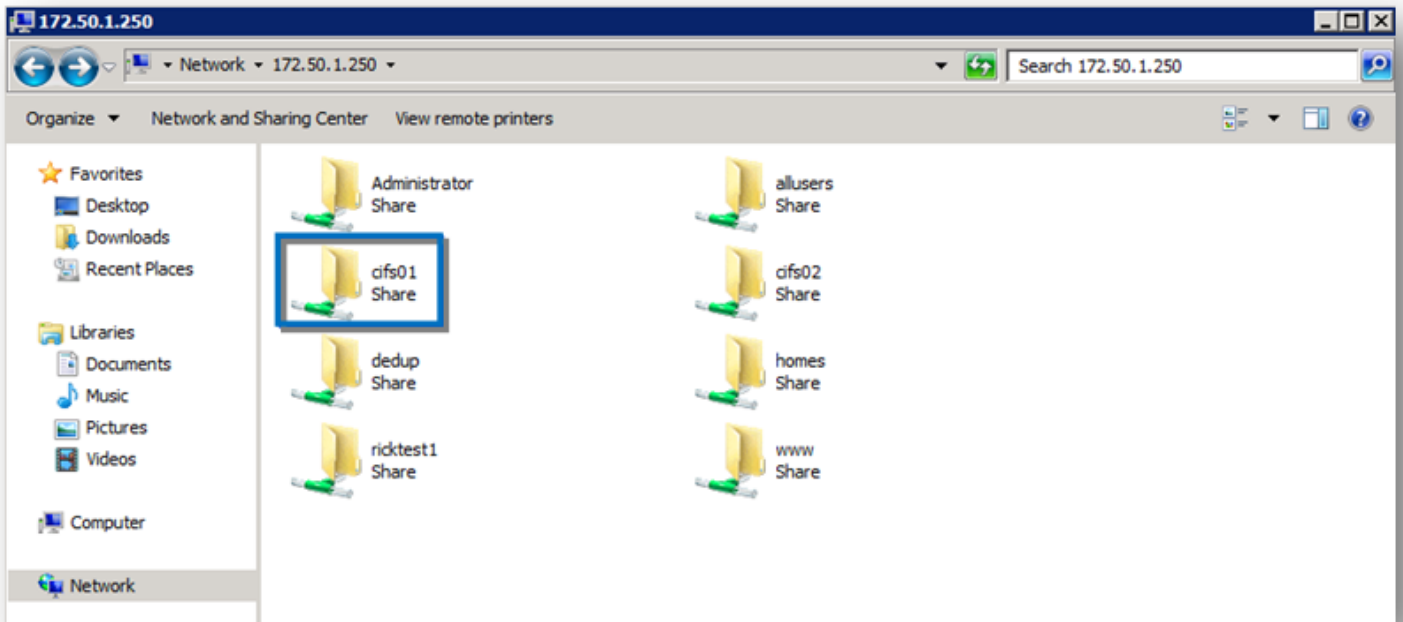
8. To make the share available on the network, check the **Yes** option in the **Available** field. Setting this field to **NO** is useful if you want to temporarily take it offline until all the options have been configured. You will need to change the option to **Yes** to make the share available to the Windows client.

9. To make the share browseable on the network, check the **Yes** option in the **Browseable** field. Setting this option to **NO** will hide the share from the list of shares when this Node is browsed. However, it can still be directly accessed using a \\servername\sharename path.
10. Enter a comment (if applicable) that will display to users who browse the share, in the Share Comment text entry box. Adding a short description is helpful to quickly identify the purpose/use of the share, for example "Personnel documents".
11. Click **Create**.

The new file share will be created and published for access by Windows servers and clients.

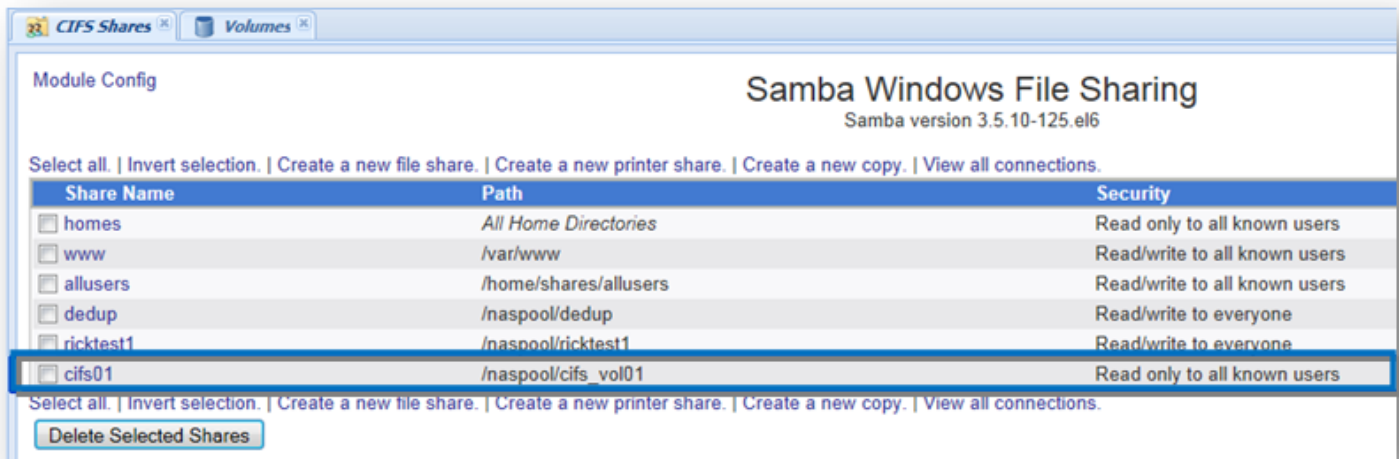
Verifying Access to the CIFS Share

1. To verify access to the CIFS share, navigate to **Windows System > Windows Explorer**.
2. Enter the UNC path of the **SoftNAS Cloud®** server (or the DNS hostname if one has been assigned to **SoftNAS Cloud®**).
3. Click on the **Share** icon and verify access permissions are set correctly from the Windows perspective.
4. Create a folder or text file and then right-click on the file/folder to verify that the **Security** permissions are as expected.



The CIFS share that was created is now available and ready for use.

Note: If you use the File Share Defaults to set defaults for all shares, there is no need to configure settings for each share unless specific CIFS Shares require unique access permissions.



Configuring Windows Networking Settings

1. Log on to **SoftNAS StorageCenter**.
2. In the **Left Navigation Pane**, select the **CIFS** option under the **Storage** section.

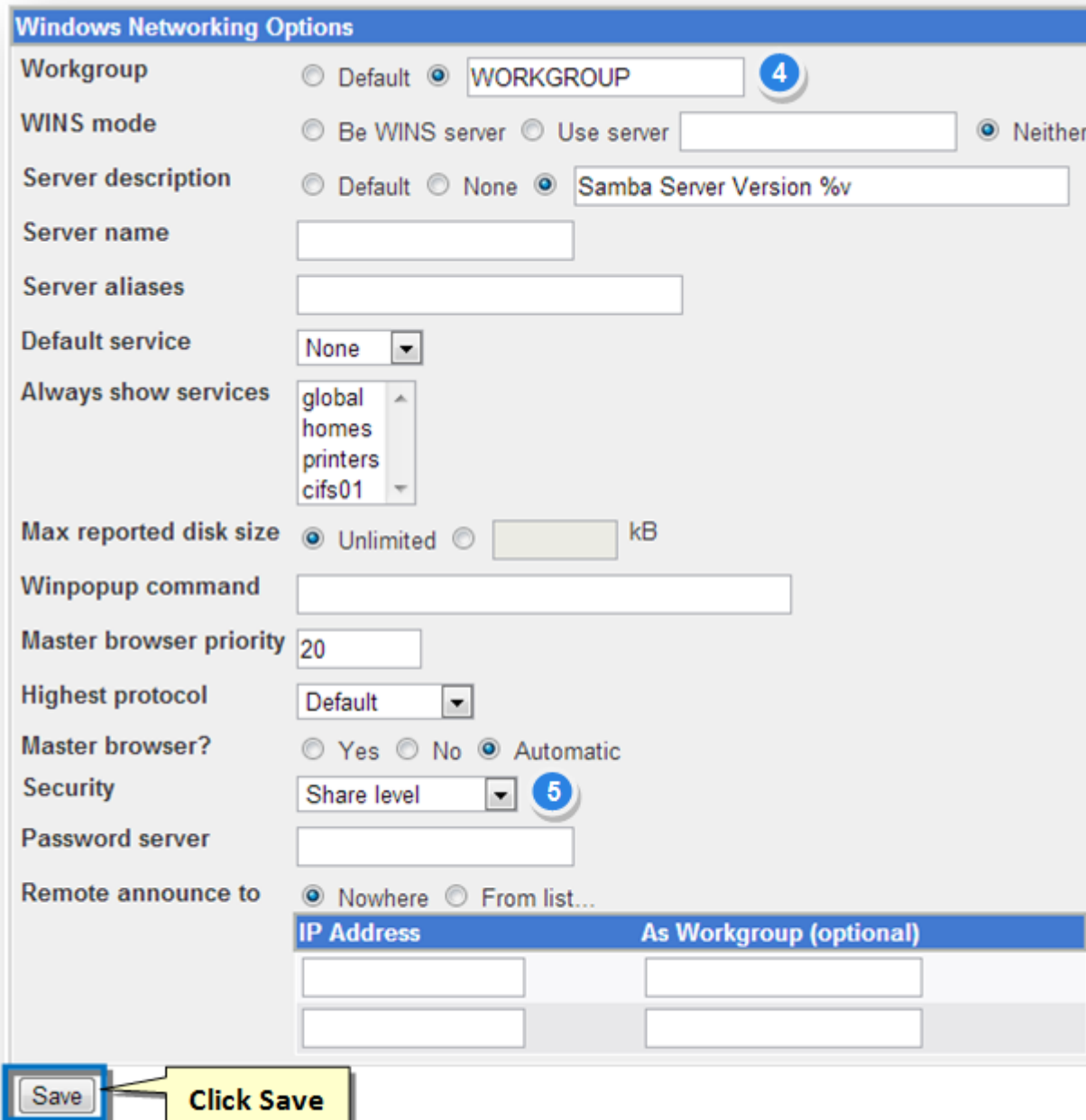
The **CIFS Shares** panel will be displayed. From here, configure and manage **CIFS** sharing.



3. Click the **Windows Networking** icon in the **Global Configuration** section.

Note: Any configuration settings applied under the Global Configuration section applies to all the CIFS Shares managed by this server.

The **Windows Networking Options** dialog will be displayed.



4. Set the name of the workgroup in the **Workgroup** field. This setting should be appropriate to the planned environment. It should match a Windows workgroup or domain environment. To set a workgroup for your server, select the second radio button in the Workgroup field and enter a short name into the text box next to it. If your network already has a few SMB servers that are members of a workgroup, this server should be made a member as well.

5. Select the appropriate security option for this particular environment from the **Security** drop down list. The available options include **Default, Share Level, User Level, Password Server, Domain** and **Active Directory**.

- Default or User level is the recommended level using the pre-existing passwords on this server.
- Password Server directs Samba to contact another SMB server to validate passwords instead of checking its own user list. If this is selected, you will need to provide the address to the authenticating server in the Password Server box.
- Share level security is rarely used anymore with modern clients
- Domain and Active Directory security is too broad a topic for this guide. For more information on Domains and AD, see [Microsoft's Technet](#).

Note: Configuring other settings in the **Windows Networking Options** dialog is optional.

6. Click **Save**.

Other options on this form:

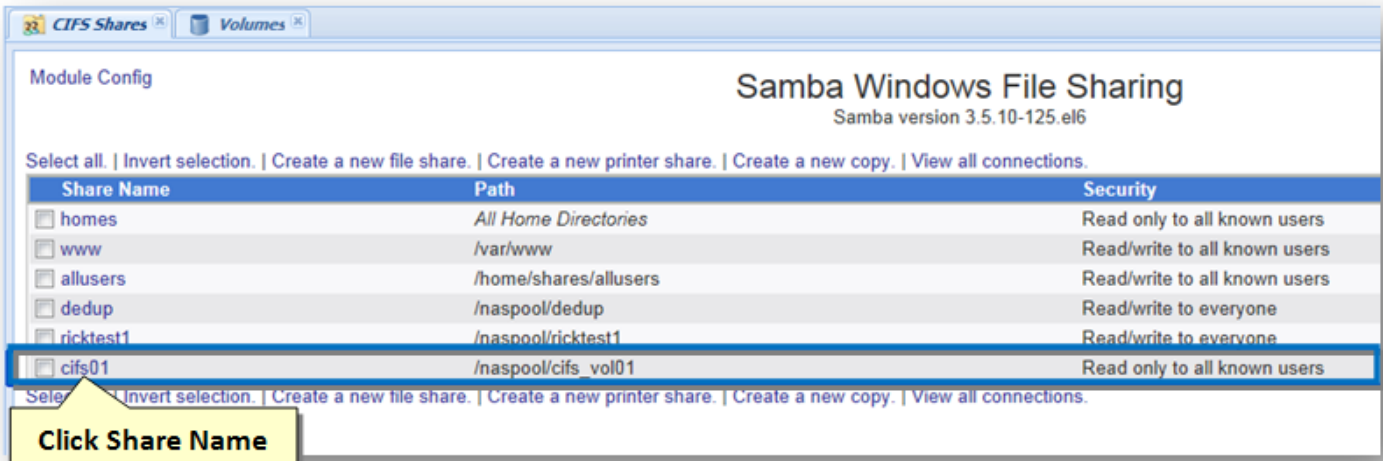
- If your network already has a WINS protocol server, select Use server in the WINS mode field and enter its IP address. If not, you should choose Be WINS server so that Windows clients can use your system to lookup IP addresses for SMB server names. More recent versions of Windows (and Linux clients) do not need to use WINS, as they can look up server names in the DNS - assuming your network has a DNS server that has entries for all your hosts.
- To set a description for your system, fill in the Server description field with something like Corporate file server.
- Normally, Samba will use the first part of your system's DNS name as the SMB server name. To change this, enter something else in the Server name field. Clients will be able to refer to this server by whatever name you specify.
- To define alternate names that clients can use to refer to your server, fill in the Server aliases field with a space-separated list of names.
- If you want your system to be the master browser for a network (the server that maintains lists of other SMB servers and clients on the network, as seen in Window's network neighborhood), change the Master browser? field to Yes. If you are running multiple Samba servers on the same subnet, this option should be set for only one. If there are other Windows or Samba servers on the network that want to be master browsers, the one with the highest operating system level will win the 'election' that decides who gets the job. You can increase your system's change of winning by increasing the Master browser priority field - the default of 20 will win against Windows 95 systems, but you would need to enter 65 to beat Windows NT servers.
- Normally, an SMB server broadcasts information about itself to other servers on the network so that it can be included in browse lists. However, if your network spans multiple subnets then broadcasts from one system may not reach others. To get around this problem, the Remote announce to table can be used to specify the addresses of browser master servers to which this server's IP address and workgroup should be sent. To configure remote announcements on this page, first select the From list option above the table. Then in the IP address field of each row enter the hostname or IP address of a server to announce to, and in the As workgroup field the name of the workgroup that your server should appear under. If the second field is left empty, the servers real workgroup (set in step 2) will be used. To enter more than two remote servers you will need to save and re-open this page so that more empty rows appear in the table.

Now this environment is ready for CIFS sharing.

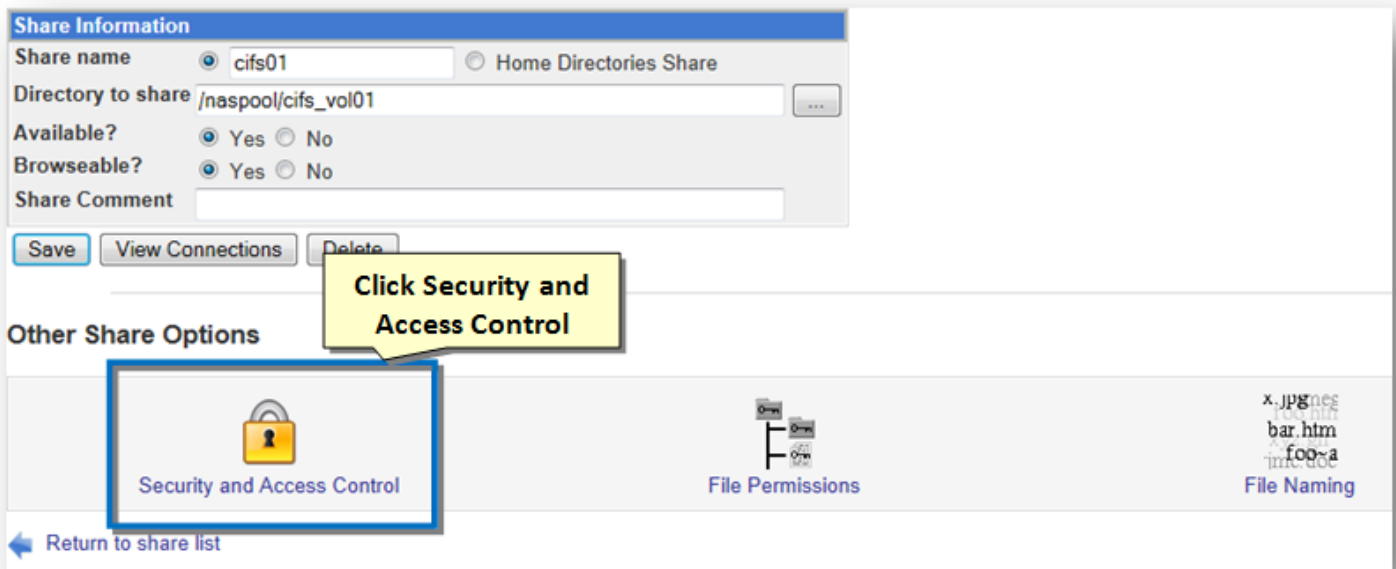
Managing Security and Access Control in CIFS Share

Once a CIFS Share has been created, you can edit various security-related options that control who has access to it and which hosts they can connect from. This can be useful if some shares contain files that only certain people should have access to, or if your Samba server is for use by clients only on your internal network. Normally this is applied "Globally" to address of the CIFS Shares managed by this server but can be set for individual CIFS Shares. To manage individual CIFS Shares, "click" on the appropriate Share Name.

1. On the **CIFS Shares** panel, click the name of the CIFS share link.



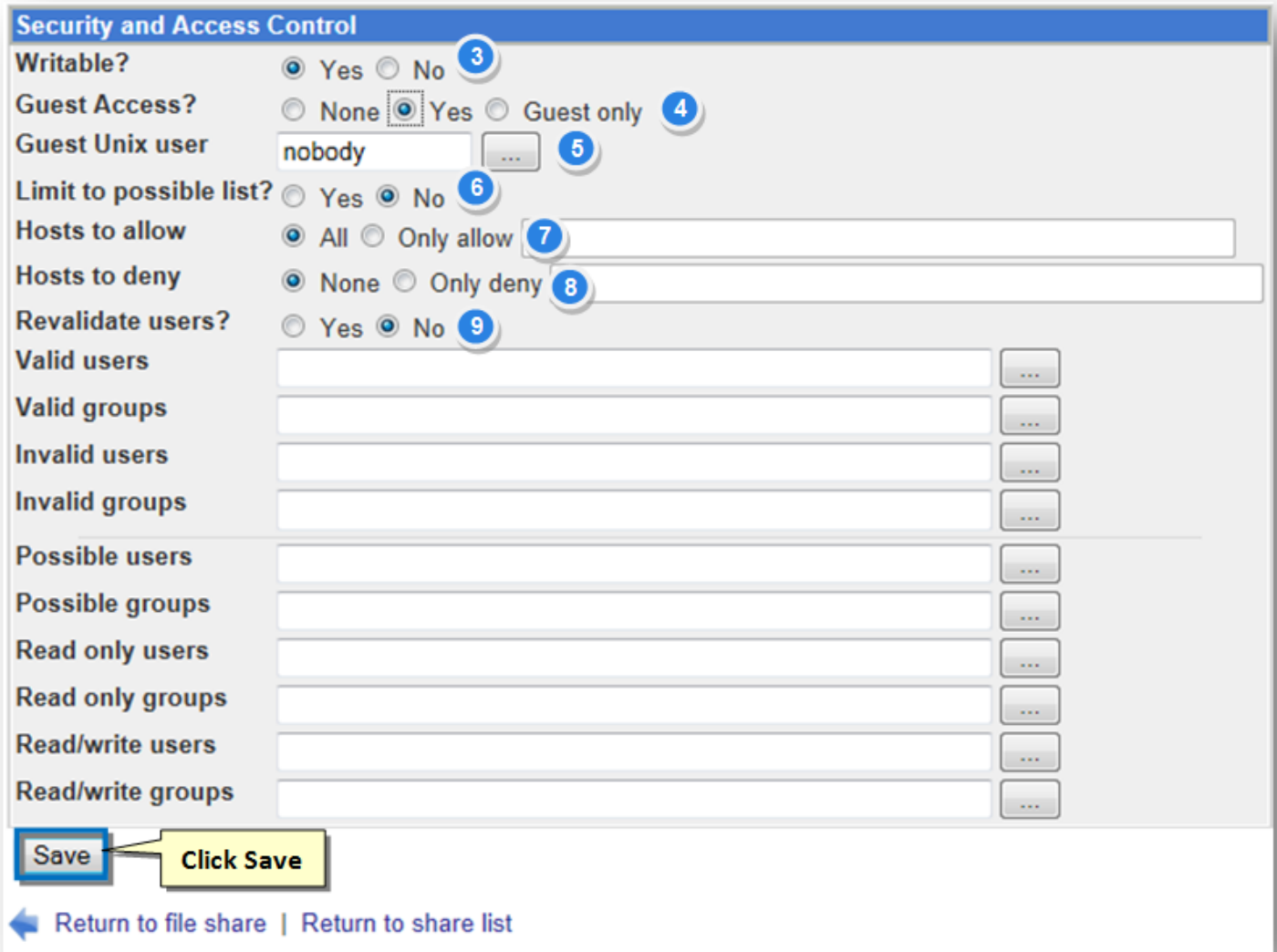
The **Edit File Share** dialog will be displayed. Changing the Security and Access Control settings here will apply only to the specific CIFS Share selected.



2. To configure and manage security and access control, click the **Security and Access Control** icon.

The **Security and Access Control** dialog will be displayed. Choose the settings that best match the particular needs and use case for this share.

The settings shown below allow full read/write access by all users.



3. Set the **Writable** field to **Yes** so that writing is allowed in the files that are shared.
4. Set the **Guest Access** field to **Yes** in order to allow guest Unix users read and write access to the files. Set the **Guest Unix User** to **Nobody** so that guest Unix users are not allowed to access file sharing.
6. Set the **Limit to Possible List** to **No** in order to allow unlimited sharing.
7. Set the **Hosts to Allow** to **Yes** in order to allow all hosts access file sharing. You can enter a list of hostnames and IP addresses into the adjacent text box. Partial IPs like 192.168.1. or network addresses like 192.168.1.0/255.255.255.0 can be used to allow an entire network. If your system is an NIS client, you can enter a netgroup name preceded by an @_ (such as @_servers) to allow all of the group's members. If **All** is selected, all hosts will be granted access, unless you fill in the next field. No matter what you enter, connections from the local host (127.0.0.1) are always allowed unless it is specifically listed in the ***Hosts to deny*** field.
8. If hosts are specified for **Hosts to deny**, this setting will block specific hosts from accessing this CIFS Share. To use this option, fill in the **Hosts to deny** field with a similar list of hostnames, IP addresses, networks or netgroups. If both fields are filled in, **Hosts to allow** takes precedence. If **None** is selected, all hosts will be permitted. Typical configurations will use only one of these two options (either **Hosts to allow**, or **Hosts to deny**). SoftNAS recommends setting **Hosts to deny** to **None**.
9. Set **Revalidate Users?** to **No**
10. Click **Save**.

Additional Options available:

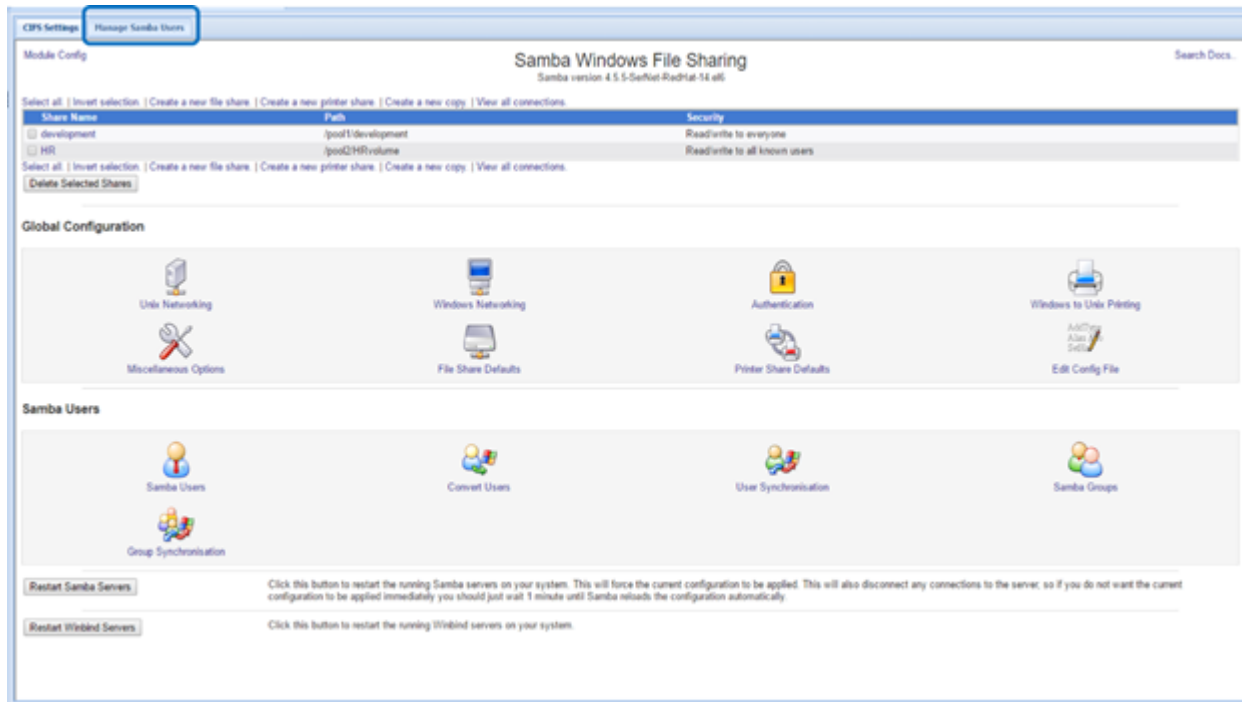
- To allow only certain users to access this share, fill in the Valid users field with a space separated list of usernames. You can also fill in the Valid groups field with a list of groups whose primary and secondary members will be granted access. Only if both lists are empty will all users be allowed.
- Alternately, to deny specific users and members of groups, fill in the Invalid users and Invalid groups fields. If a user appears in both the valid and invalid lists then they will be denied access.
- To restrict some users to read-only access for this share, enter a list of usernames into the Read only users field. You can also enter a list of Unix groups in the Read only groups to restrict their primary members. Everyone else will have full read/write access, assuming that the share is actually writeable and that the Read/write fields have not been filled in.
- To give only certain users permission to write to the share and restrict everyone else to read only access, enter a list of usernames into the Read/write users field. As usual, the Read/write groups field can be used to enter a list of groups whose primary members will be allowed to write as well. Naturally, normal Unix file permissions that may be prevent writing to files or directories still apply to all users. If a user appears in both the Read only and Read/write lists, he will be allowed to write. The fields in this and the previous step have no effect on printer shares. Instead, all allowed users will be able to print.

The share security permission settings are now configured.

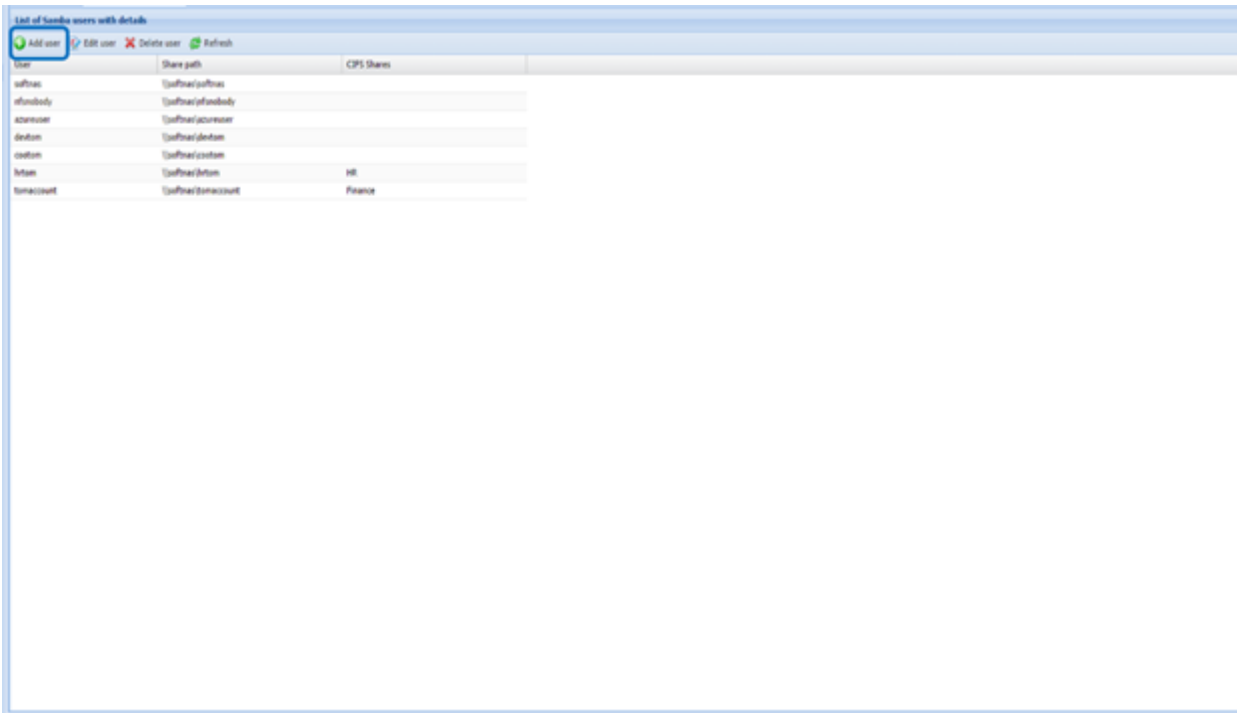
Access for a specific user to a CIFS Share

Samba allows you to specify a one to one relationship between a user and CIFS Share through “**Manage Samba Users**”.

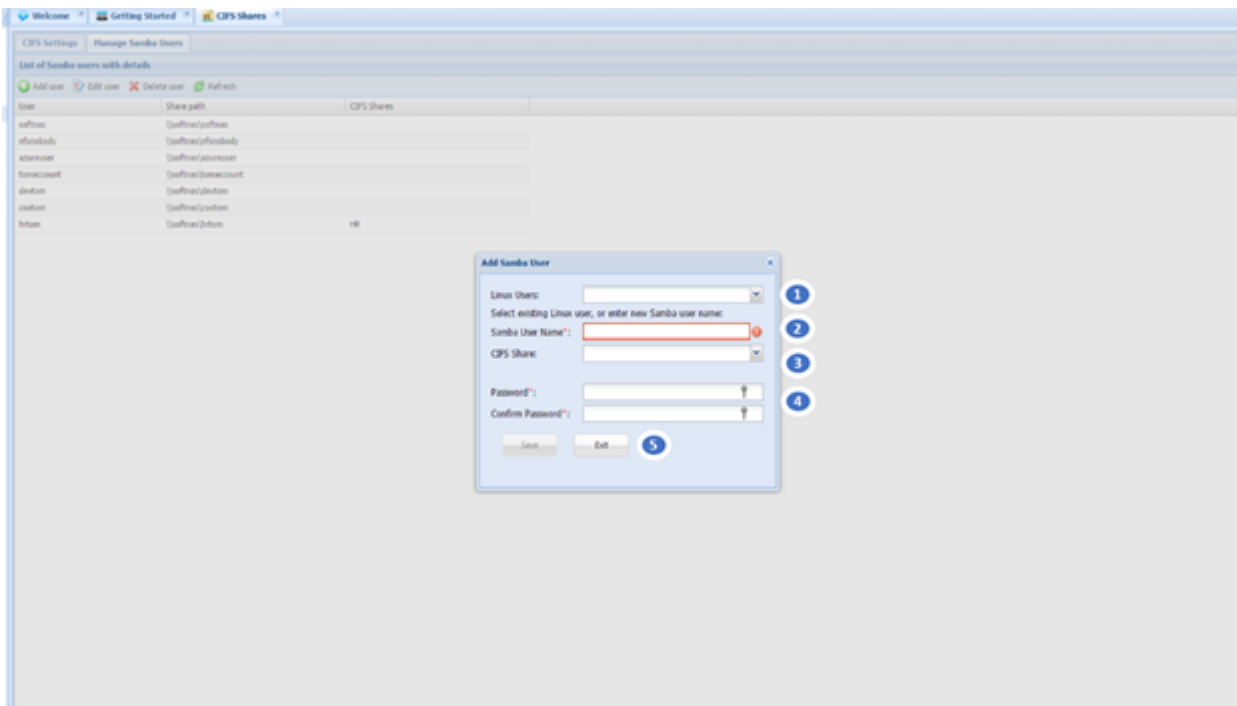
Select Manage Samba Users in order to manage or add new Samba users for this SoftNAS Cloud Server.



To add a user, select **Add User** and a panel will open to allow you to provide the necessary information.



Note: If the user is already listed in the User list, you will need to first delete the user before you can add the specific relationship of the user to a CIFS Share. Edit user only allows for the setting of the password for the user.



In order to associate and configure a specific user to a specific CIFS Share, you will need to perform the following steps:

1. This is an optional field. Enter the Linux user name if the user already exists on the SoftNAS Cloud Server. This is the name of the user on the SoftNAS Cloud Server. You can search for the user by selecting the “down arrow” next to the field.
2. If the Linux user name was provided, Samba will automatically set the Samba User Name to the same. Otherwise you can enter in a different name to be used.
3. Use the “down arrow” to select a CIFS Share already created.

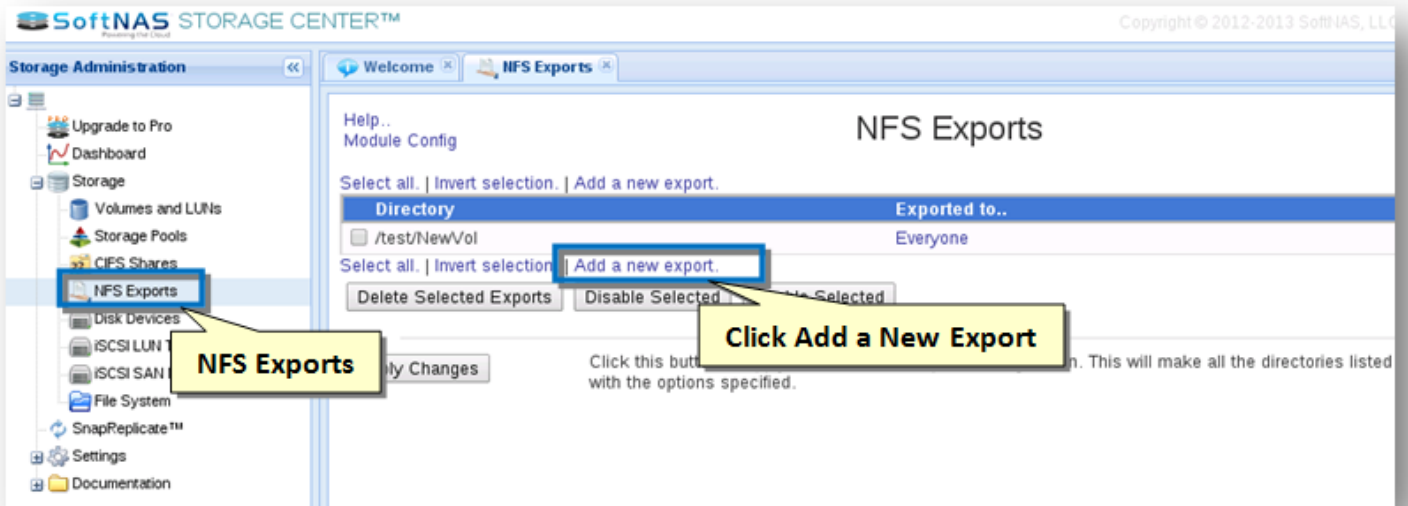
4. Set up the Samba User's password and confirm it.
5. Select **Save** to apply the information to the newly added user.

Creating NFS Share

Before creating an NFS Export, [create a volume to share](#). When creating a volume, there is an option to create a **default NFS share**. Use the functions on this page to add new or modify existing NFS export shares.

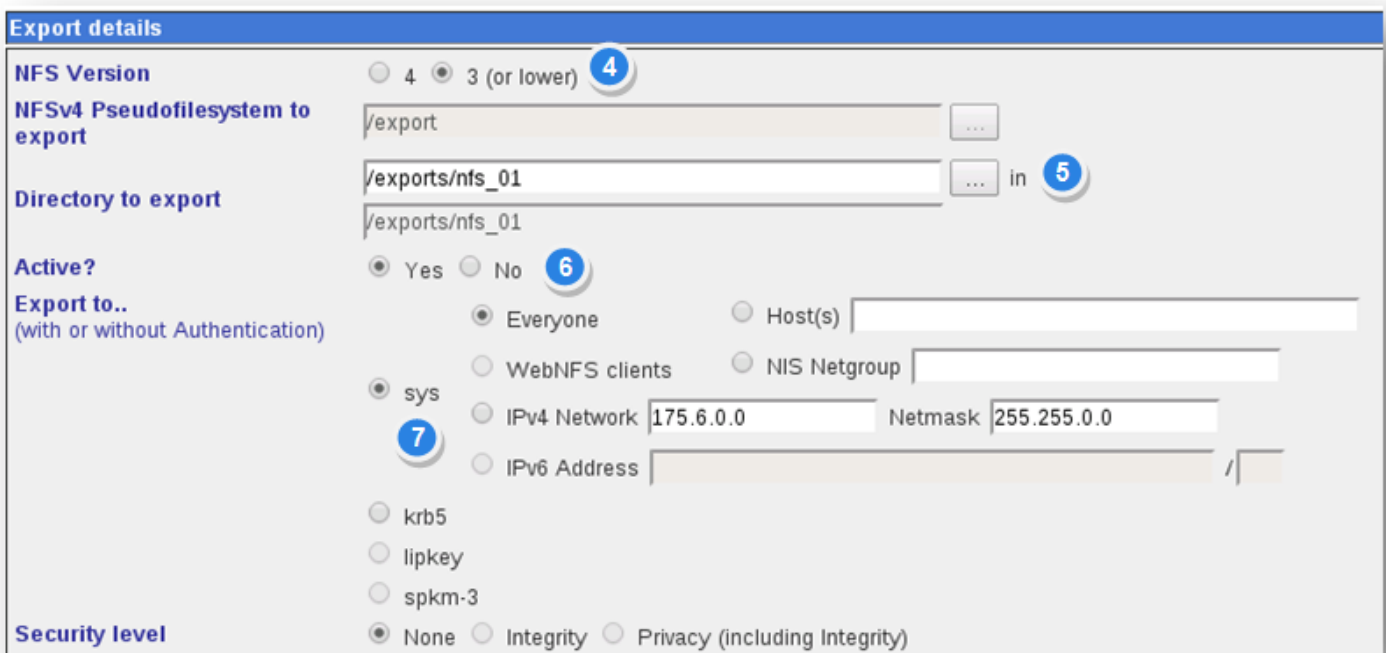
1. Log on to **SoftNAS StorageCenter**.
2. In the **Left Navigation Pane**, select the **NFS Exports** option under the **Storage** section.

The **NFS Shares** panel will be displayed. From here, configure and manage NFS sharing.




3. Click the **Add a New Export** link.

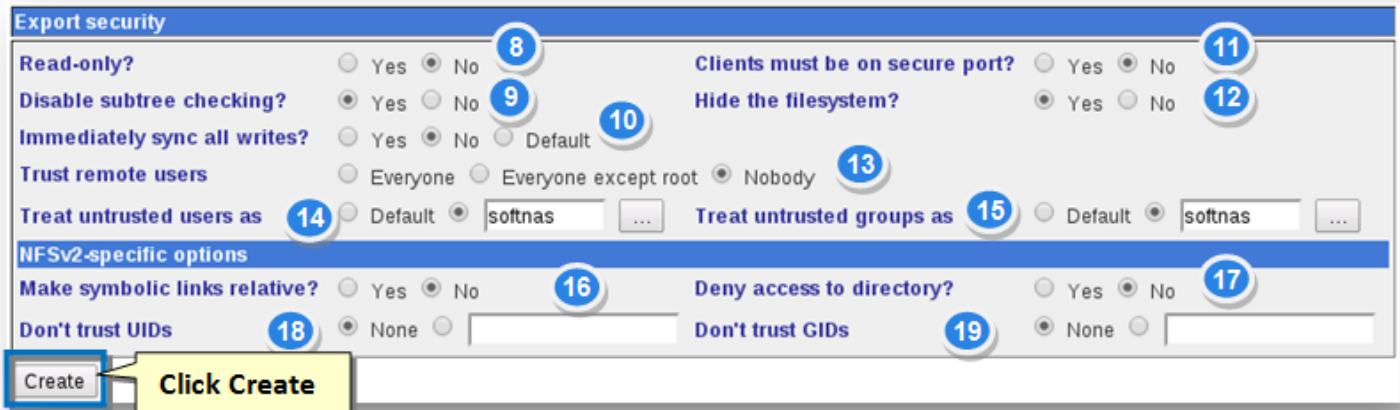
The **Create Export** section of the panel will be displayed.



4. In the **Export Details** section, specify the NFS version in the **NFS Version** field.

Note: This example has NFS version 3, but other settings such as NFS version 4 may also work better in some environments. Choose the most appropriate settings for this particular environment, security and operational needs.

5. In the **Directory to Export** field, click the  button to select the directory to export.
6. Set the **Active** field to **Yes**.
7. In the **Export to** field, specify the system **IPV4 Network** and **Netmask** addresses in the respective text entry boxes.



8. In the **Export Security** section, specify the **Read-only** field as **No**.
9. Set the **Disable Subtree Checking** field to **Yes**.
10. Set the **Immediately Sync All Writes** field to **Yes**.

Note: For best performance throughput, choose **No** for **Immediately Sync All Writes** field. This option allows NFS to cache the write and return to the caller immediately (up to 10 times better throughput has been observed by not immediately syncing writes, so **No** setting makes a big difference in performance sensitive applications). If **No** is chosen for this option, writes will be cached in memory longer (NFS "async" option), which increases the potential for loss of data should there be a loss of power or other unexpected system failure, so take this into consideration, as well as performance. Only consider setting this option to **No** if there is a proper UPS in place. Note that cached data not yet written to disk could be lost if this option is set to **No** (which in turns sets NFS export to "async").

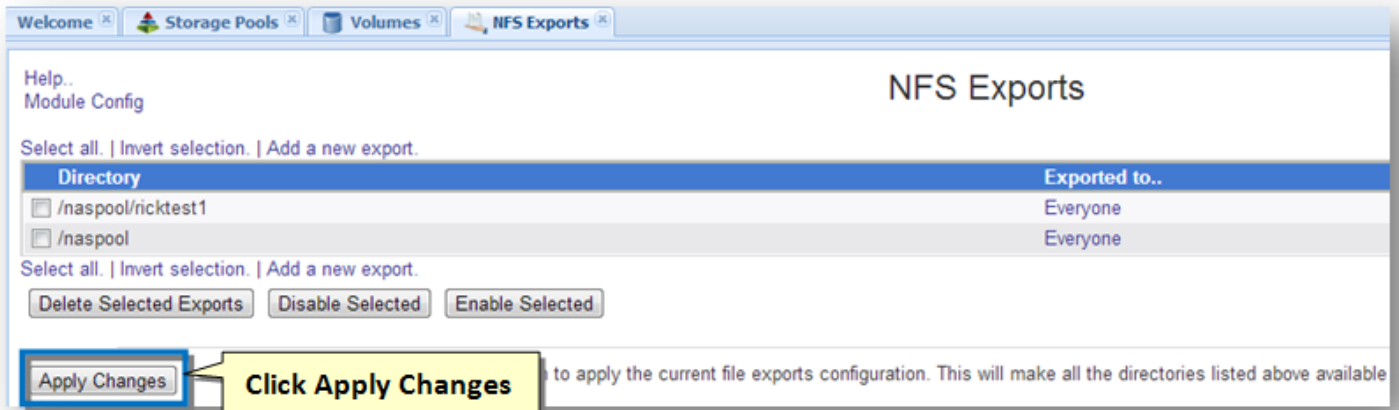
11. Set the **Clients Must be On Secure Port** to **No**.
12. Set the **Hide the filesystem** field to **Yes**.
13. Set the **Trust Remote Users** field to **Nobody**.

Note: To mount this NFS share from **VMware vSphere**, select **Nobody** as the **Trust Remote Users** choice. **VMware vSphere** hosts do not authenticate by default, so it's also best to restrict the IP address range appropriately to limit which NFS clients can connect to the NFS export.

14. Specify the untrusted users in the **Treat Untrusted Users** as **softnas**.
15. Specify the untrusted groups in the **Treat Untrusted Groups** as **softnas**.
16. Set the **Make Symbolic Links Relative** field to **No**.

17. Set the **Deny Access to Directory** field to **No**.
18. Set the **Don't Trust UIDs** field to **None**.
19. Set the **Don't Trust GIDs** field to **None**.
20. Click **Create**.

The **NFS Exports** panel will be displayed.



21. Click **Apply Changes**.

The NFS export settings will be activated.

Mounting the NFS Share from VMware vSphere

Now that an NFS Share is available, mount and use the NFS-shared volume as a **VMware vSphere datastore**.

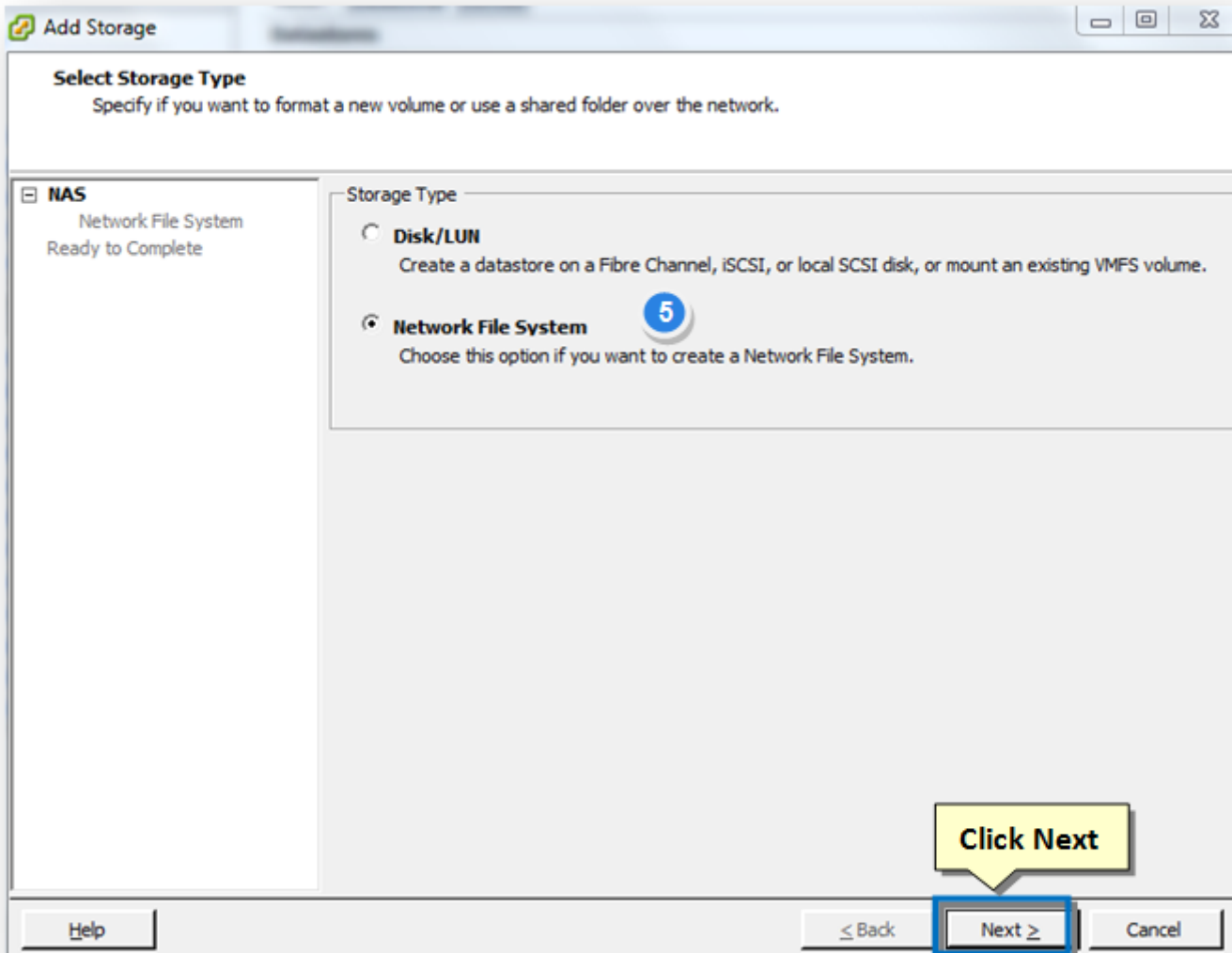
To mount NFS as a datastore, simply follow the steps given below.

1. Log into **vCenter** (or **VMware vSphere** if managing VM hosts directly)
2. For each **VMware vSphere** host that needs shared access to the NFS-shared datastore, select the **Configuration** tab in **VMware vSphere** client.
3. Select the **Storage** option from left-side menu.

The datastore list will be displayed.

4. Select the **Add Storage** option from upper-right menu.

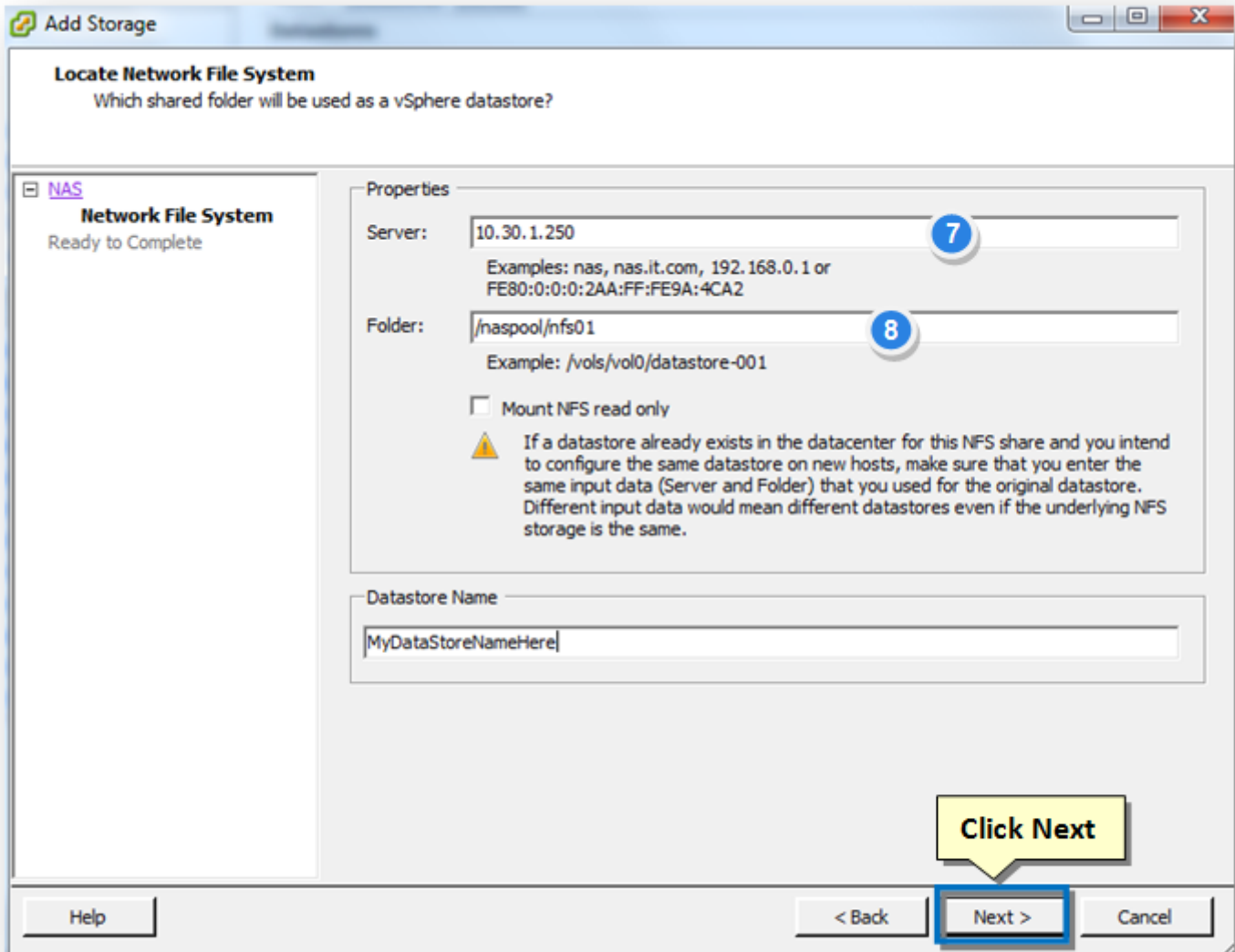
The **Add Storage** wizard will be displayed.



5. Select the **Network File System** option in the **Storage Type** section.

6. Click **Next** to continue.

The **Locate Network File System** section of the wizard will be displayed.



7. In the **Properties** section, enter the IP address of the **SoftNAS Cloud®** in the **Server** text entry box.

Note: If the **SoftNAS Cloud®** IP has been added to **DNS**, use the **SoftNAS Cloud®** DNS name itself.

8. Enter the path of the folder for NFS export in the **Folder** text entry box.

9. Enter the name of the datastore in the **Datastore Name** text entry box.

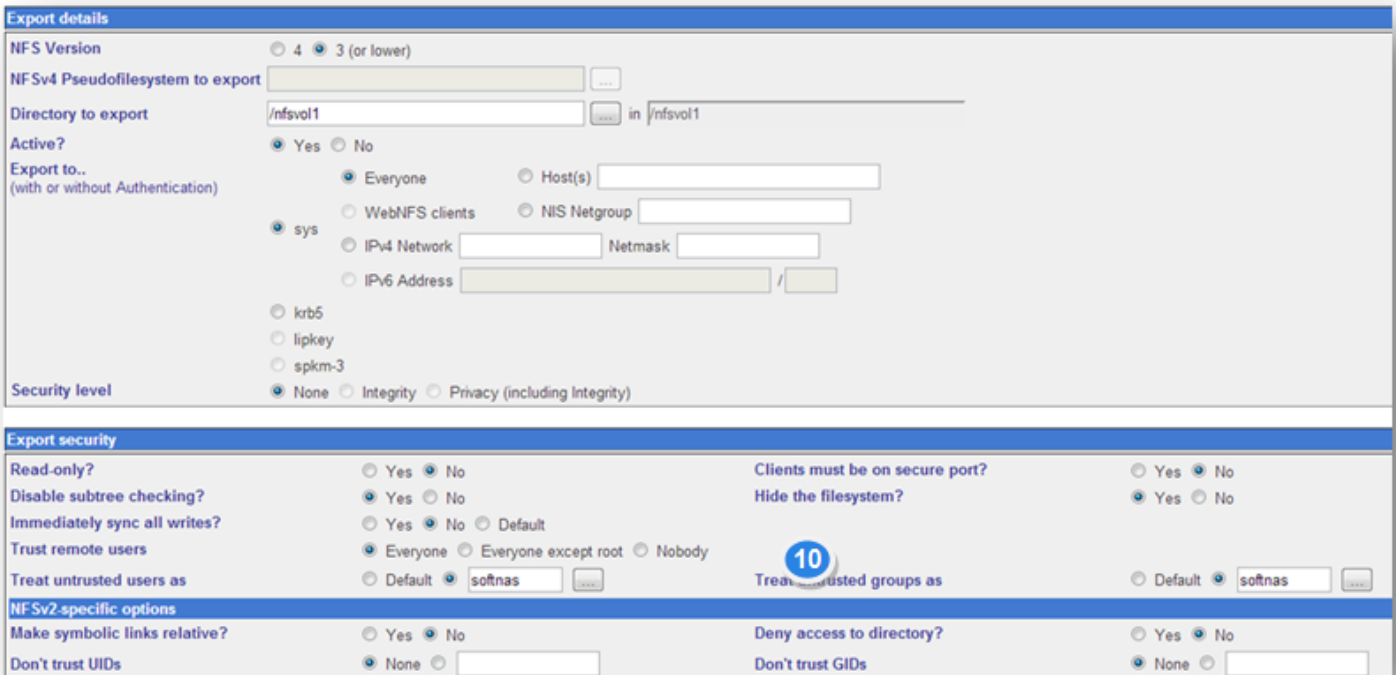
Note: Repeat the above process for each **VMware vSphere** host that needs to access the datastore. In an HA configuration, Make sure that all **VMware vSphere** hosts have this NFS datastore configured.

10. Click **Next**.

Note: The most common issue at this point is an **Access Denied** error when trying to mount the NFS export. This typically denotes that the **Nobody** option under **Trust remove users** was not chosen, or another security configuration setting may have a problem. Go back to the NFS export configuration panel, click on the **NFS export** and resolve the security issue. The settings shown above are known to work correctly with **VMware vSphere** (there may be other security settings preferred depending on environment.)

Mounting from Windows NFS Clients

The following settings work well for Windows-based NFS clients:



The screenshot shows the 'Export details' and 'Export security' sections of the configuration interface. In the 'Export details' section, 'NFS Version' is set to 3 (or lower), 'Directory to export' is /nfsvol1, and 'Active?' is checked. Under 'Export to..', 'sys' is selected. In the 'Export security' section, 'Read-only?' is set to No, 'Disable subtree checking?' is checked, and 'Trust remote users' is set to 'softnas'. A blue circle with the number '10' is overlaid on the 'Trust remote users' dropdown.

Note: Although the above example shows certain settings, such as NFS version 3, other settings such as NFS version 4 may work better in some environments. Choose the most appropriate settings for local particular environment, security and operational needs.

NFS and Firewall Settings

Using NFS may involve opening additional ports in any firewalls that sit between **SoftNAS Cloud® VMs** and workload VMs, which will otherwise block traffic (esp. if traversing to an external IP in cloud-based situations).

Here are the ports required for NFS client mounts, according to the settings located in `/etc/sysconfig/nfs`:

TCP Port (Service)	Source	Service
111	x.x.x.x/24	portmapper
2010	x.x.x.x/24	rquotad
2011	x.x.x.x/24	nlockmgr
2013	x.x.x.x/24	mountd
2014	x.x.x.x/24	status
2049	x.x.x.x/24	nfs

UDP Port (Service)	Source	Service
111	x.x.x.x/24	portmapper
2010	x.x.x.x/24	rquotad
2011	x.x.x.x/24	nlockmgr
2013	x.x.x.x/24	mountd

2014	x.x.x.x/24	status
2049	x.x.x.x/24	nfs

The above ports were determined by logging into **SoftNAS Cloud®** and running an **rpcinfo -p** command, which displays the ports being used for RPC.

Be sure to should lock the address range down to only the subnet where allowed EC2 instances reside (or the particular IP range that's appropriate).

NFS Client Mount from Linux

To mount the NFS volume from Linux, Unix or Mac OS, use the mount command as the **root** user:

```
# mount -o rsize=32768,wsiz=32768,noatime,intr <ip-address>:<export-path>
<mnt-point>
```

Where **<ip-address>** is the IP address (or DNS name) of the **SoftNAS Cloud®** server, **<export-path>** is the path chosen when exporting the filesystem via NFS and **<mnt-point>** is the mount point in the local filesystem.

For example:

```
# mkdir /myvol
# mount 172.16.1.100:/naspool1/myvol01 /myvol
```

The above command creates a new directory to be used as the mount point, then mounts a storage pool **naspool1** with volume **myvol01** at export path **/naspool1/myvol01** to **/myvol**, on the **SoftNAS Cloud®** server at 172.16.1.100.

For better performance, use this command variation, which sets the read/write size to 32K and disables setting last access time and intr options:

```
# mount -o rsize=32768,wsiz=32768,noatime,intr 172.16.150.100:/export/vol01 /
mnt/vol01
```

To unmount the filesystem, use the **umount /poolname/volname** command.

NFS v4 and Authentication Considerations

NFS v4 provides for separation of filesystem metadata and file data I/O, improving performance and throughput. It is also possible to configure NFS v4 to operate in conjunction with Kerberos and LDAP for user authentication. Use of an authentication server allows each user who mounts and accesses NFS exports to have their unique user ID (uid) and group ID (gid) maintained on the NFS server. [More details on configuring NFS v4 and use of NFS in conjunction with kerberos and LDAP.](#)

Common NFS Issues

The most common issue encountered when mounting and using an NFS volume are **Access Denied** and **read-only** types of problems.

Access Denied - This typically happens when trying to mount an NFS export that has been restricted by IP address range, user ID or other permission restrictions. Try opening up the NFS export for access by any IP address and **Everyone**; i.e., loosen the security up during initial testing, then lock it back down one step at a time.

Read-Only Access - When this happens, it is possible to mount the filesystem, but not possible to write to the mounted filesystem. This is a security permissions issue. Try opening up the permissions on the NFS export to **Everyone** as a starting point, then with a working NFS mount, choose to lock the security down incrementally.

Creating an AFP (Apple Filing Protocol) Share

SoftNAS allows you to create shares via the Apple Filing Protocol (AFP). Support of AFP allows Mac users to quickly and easily integrate with SoftNAS storage. Much like a CIFS share, AFP allows multiple clients to access and update the same file while preventing conflicts by providing file sharing and file locking.

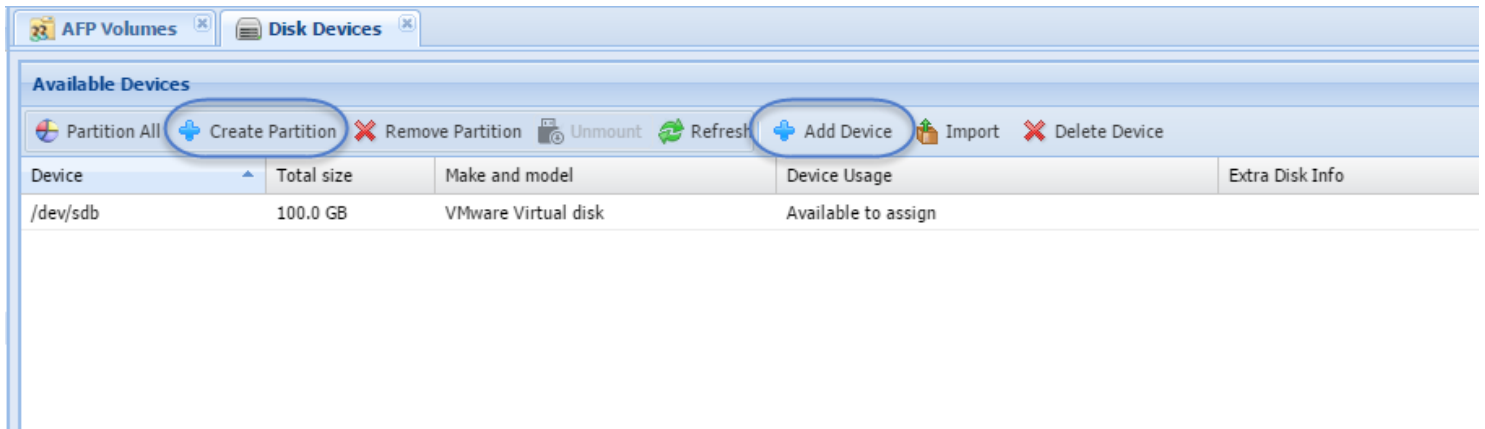
SoftNAS Cloud® uses Netatalk AFP server for secure, stable, and fast file sharing and print services. Using Netatalk's AFP 3.3 compliant file-server leads to significantly higher transmission speeds compared with Macs accessing a server via SaMBa/NFS, while providing clients with the best possible user experience (full support for Macintosh metadata, flawlessly supporting mixed environments of classic Mac OS and OS X clients).

Note: Before creating a new file share, configure the default **Netatalk** network environment settings.

Adding an AFP Volume through Volumes and LUNS

The following guide assumes you are creating a new AFP share on a new volume and pool. If you have already created a pool, skip to volume creation below. An AFP volume can be created on a storage pool that also has CIFS volumes, NFS volumes, and iSCSI LUNs.

In order to create a new AFP volume, you first need an available disk, partitioned and ready. Open **Disk Devices**, and partition an available disk, by selecting **Create Partition**. If none is available, create a disk via any one of the available disk extenders via **Add Device** (and then partition via **Create Partition**). Once partitioned, the device should read "**Available to assign**" under **Device Usage**.



Next, go to **Storage Pools**, and create a pool using the available disk, or disks. If performing a RAID configuration, you will need more than one disk. Select **Create** to create a new pool. If you already have an existing storage pool you wish to add your volume to, skip this step, and select the desired pool when creating your volume.

In the **Create** wizard:

1. Provide a new pool name.
2. Select the RAID level appropriate for your environment from the dropdown.
3. Select the disk or disks required for your RAID selection.
4. Click **Create**.

Create a New Storage Pool

Choose pool name, disks and storage options, then press Create button.

1. Choose a Pool Name
 Pool Name:

2. Assign disks and redundancy level of the storage pool
 RAID Level:

Choose disks for this storage pool:

<input checked="" type="checkbox"/>	Disk Device	Disk Availability	Available Size
<input checked="" type="checkbox"/>	/dev/sdb	Available for Use	100.0G

Instructions: Choose a RAID Level, then select a corresponding number of disks for the storage pool.

3. Choose Pool Options

Forced Creation (overwrites any older pools on disks you select)

LUKS Encryption Type:

LUKS Password: Retype:

Sync Mode:

Shared Storage (pool is accessed by more than one host)

Once you have created a storage pool, select **Volumes and LUNS** from the **Storage Administration Panel** on the left, then click **Create**.

Storage Administration

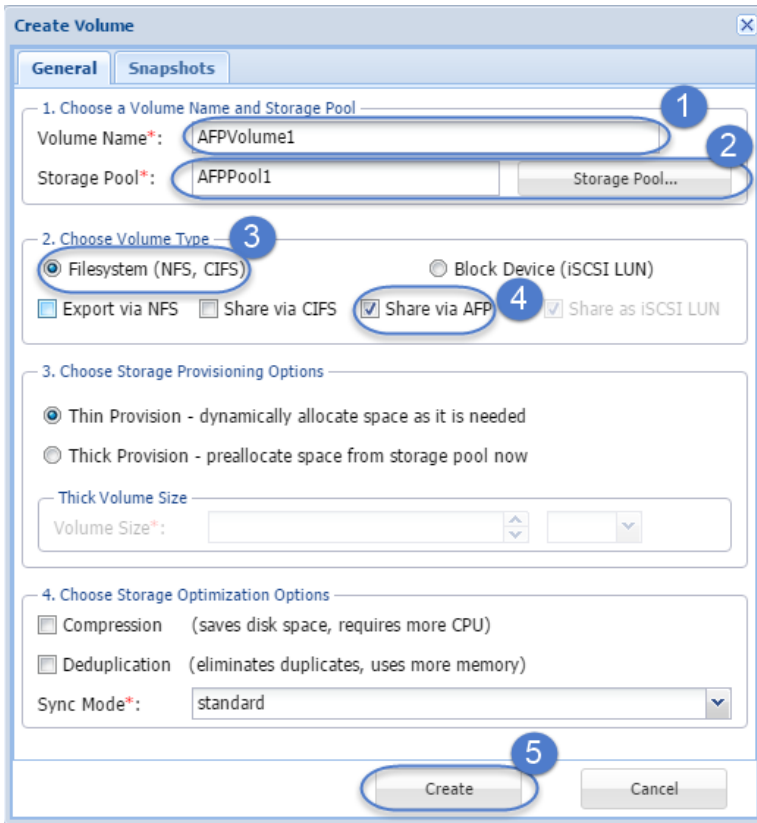
Storage Pools | **Volumes and LUNS**

Volumes

Volume Name	Storage Pool	Status	% Used	Total Used Space	Used by Snapshots	Used by Dataset
Page 0 of 0						

In the **Create Volume** popup:

1. Provide a **Volume Name**.
2. Type in the pool name, or click **Storage Pool** to search for the desired pool.
3. For an AFP volume, select the **Filesystem (NFS, CIFS)** radio button.
4. Check the box for **'Share via AFP'**.
5. Click **Create**.



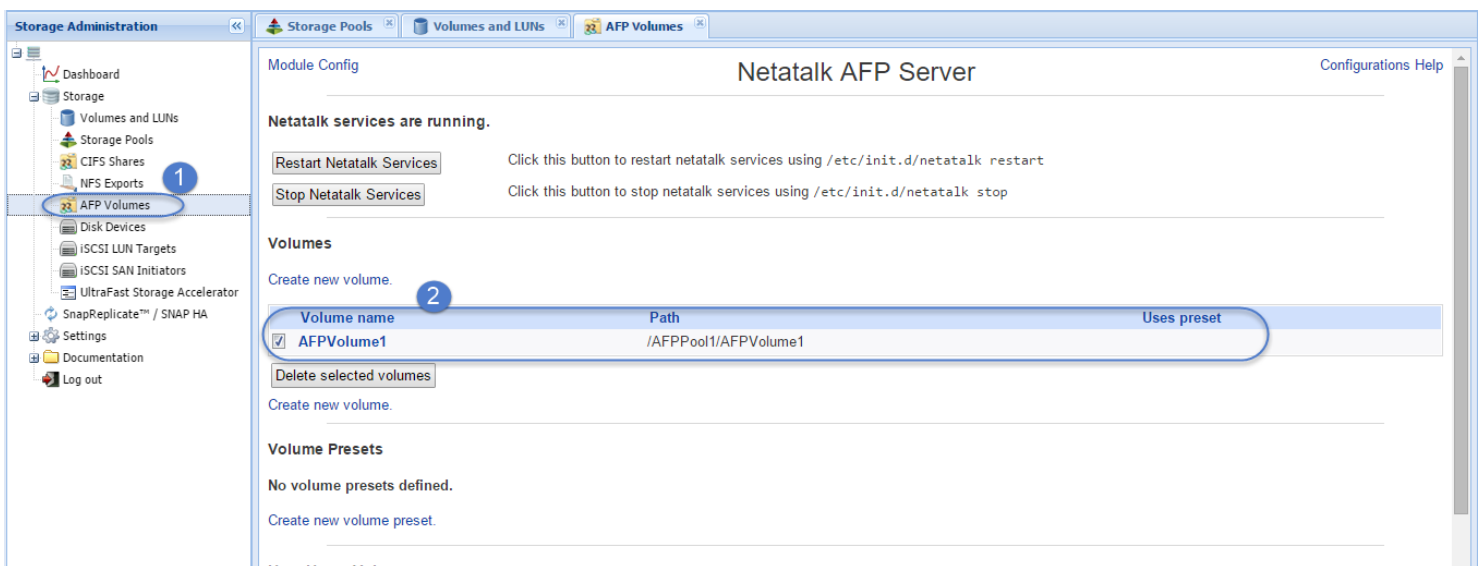
Note: It is possible to have a filesystem configured with any combination of NFS, CIFS, or AFP enabled. However, in this case we are selecting only AFP. By default, **Export via NFS** will be checked. Uncheck it, unless you intend to use both protocols.

Your AFP volume is created. Go to **AFP Volumes** to finish configuring.

Configuring Apple File Network Sharing

1. In the **Left Navigation Pane**, select the **AFP Volumes** option under the **Storage** section.

The **Netatalk AFP Server** panel will be displayed. AFP Volumes created following the steps above will appear here. From here, configure and manage **AFP** sharing.



2. If you have a volume created, check the box to select it, then scroll down. Click **Server Options** to edit your settings.

The **Edit Global Settings** panel will appear.

In this panel, you can configure the global connection settings for your share. This section allows you to provide server settings, specify alternate AFP ports, set up authentication, set alternative location for log files, and more.

Module Config

Edit Global Settings

Configurations Help

Settings

Server name leave empty to use the host name of machine

AFP listen system's first IP address (netatalk default)

AFP port 548 (netatalk default)

User settable password disabled enabled

Login message

Authentication Standard UAM Cleartext UAM Guest UAM Kerberos UAM

Additional non-standard UAM modules Standard UAM=uams_dhx.so uamsdhx2.so (netatalk default)

Kerberos	Keytab	Service name	Realm	FQDN
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Log file ... leave empty to log through syslog daemon

Log level default:note (netatalk default)

Volume preset for all volumes

Database path ... /var/netatalk/CNID/ (netatalk default)

[Return to index page](#)

Once your global settings are configured, return to the Netatalk AFP Server by clicking **Return to index page**.

Note: If creating an AFP share from an AWS or other cloud storage, be sure to add port 548 for AFP traffic.

3. If you had not created an AFP Volume already, you could have selected **Create new volume** in order to create/configure your AFP Volume. You can also select **Create new Volume Preset** in order to set standard settings for your volume. However, best practice is to create volumes from the **Volumes and LUNs** tab.

The screenshot shows the Netatalk AFP Server configuration page. On the left, under the 'Volumes' section, there is a 'Create new volume.' link and a table with one entry: 'AFPVolume1' with path '/AFPpool1/AFPVolume1'. Below this is a 'Create new volume.' button. Further down, there is a 'Create new volume preset.' button. On the right, two modal windows are shown: 'Create new Volume' and 'Create new Volume Preset'. Both windows have identical settings: Volume preset (no preset), Name (empty), Path (empty), Extended attributes (auto), Read Only (no), Search DB (no), Unix Privileges (yes), File permissions (empty), Directory permissions (empty), umask (empty), Time machine support (no), Password (empty), Valid users/groups (Users, Groups), and Invalid users/groups (Users, Groups). Blue arrows point from the 'Create new volume.' and 'Create new volume preset.' buttons to their respective modal windows.

As we have created a volume, click the Volume Name to enter the **Edit Volume** screen.

The screenshot shows the 'Edit Volume' screen for 'AFPVolume1'. The 'Volumes' section contains a table with the following data:

Volume name	Path	Uses preset
<input type="checkbox"/> AFPVolume1	/AFPpool1/AFPVolume1	

Below the table is a 'Delete selected volumes' button. The 'Volume Presets' section shows 'No volume presets defined.'

Settings from Volume creation will carry over. However, you can change any settings required from here.

Module Config Configurations Help

Edit Volume

Settings

Volume preset no preset 1

Name AFPVolume1 2

Path /AFPpool1/AFPVolume1 3

Extended attributes auto (netatalk default) 4

Read Only no (netatalk default) 5

Search DB no (netatalk default) 6

Unix Privileges yes (netatalk default) 7

The following is only relevant if Unix Privileges are set to 'yes'. Enter values in octal format (e.g. 0777).

File permissions 0777

Directory permissions 0777

umask 0777

Time machine support yes 8

Password

Valid users/groups

Users 9

Groups

Invalid users/groups

Users

Groups

Read only users/groups

Users

Groups

Read write users/groups

Users

Groups

Hosts allow 0.0.0.0/0

1. Presets:

A preset is a set of parameters for a new AFP volume that you do not have to configure. Rather than re-entering each setting, you can select a preset to populate all the required/desired fields. Presets are created via the Create New Volume Presets option under Netatalk AFP Server. If no presets are available, enter the data manually.

2. Name:

The name of the fileshare to be created.

3. Path:

The path used to connect to the new share.

4. Extended Attributes:

Extended attributes on OS X allow applications to store additional metadata alongside data files. Here you can determine whether this additional metadata should be stored.

5. Read Only:

Govern whether files within the share are editable or read-only.

6. Search DB:

If enabled, **Search DB** can speed up searches via CatSearch significantly in special cases: It then uses a separate database (db) that's normally used by netatalk to remember the correlation between a file and the "CNID". It can use that db to look up items by name, making this lookup much much faster than performing a directory tree walk to match the names.

7. Unix Privileges:

Enables Unix Privileges for AFP permissions.

8. Time Machine/Time Machine Password:

Mac OS X 10.5 (Leopard) added support for **Time Machine** backups over AFP. Two new functions ensure that backups are written to spinning disk, not just in the server's cache. Different host operating systems honor this cache flushing differently. SoftNAS and Netatalk offer Time Machine support, allowing backup and recovery of your files. To enable this for the volume in question, switch **Time Machine Support** to "yes", and provide a password.

9. Users and Groups:

Configure users and groups who will have access to the data and applications stored within the file share.

Note: The Edit Volumes screen contains the same options as **Create New Volume**, if you elected to skip the volume creation process above. An AFP Volume can be created from within AFP Volumes as well. Again, best practice is to create volumes from the **Volumes and LUNs** tab.

iSCSI LUNs and Targets

Overview

Sharing block devices via **iSCSI** is a common way to make network-attached storage available. An **iSCSI LUN** is a logical unit of storage. In **SoftNAS Cloud®**, the basic storage **LUN** is a volume that is accessed as a **block device**. The block device volumes have a mount point in the **Linux /dev/zvol** filesystem because they are disk block devices.

For example, a storage pool **naspool1** with volume name **lun01** would be named **/dev/zvol/naspool1/lun01** as its mount point. These device references are links to Linux block devices used to access the volume's raw data blocks via **iSCSI**.

iSCSI targets are used by **iSCSI initiators** to establish a network connection. The target serves up the **LUNs**, which are collections of disk blocks accessed via the **iSCSI** protocol over the network. A target can offer one or more **LUNs** to the **iSCSI** clients, who initiate a connection with the **iSCSI** server.

For example, **VMware vSphere** or **Windows** connects to the **iSCSI** server and retrieves a list of available targets. Then, for each target, the list of its published **LUNs** are available for use.

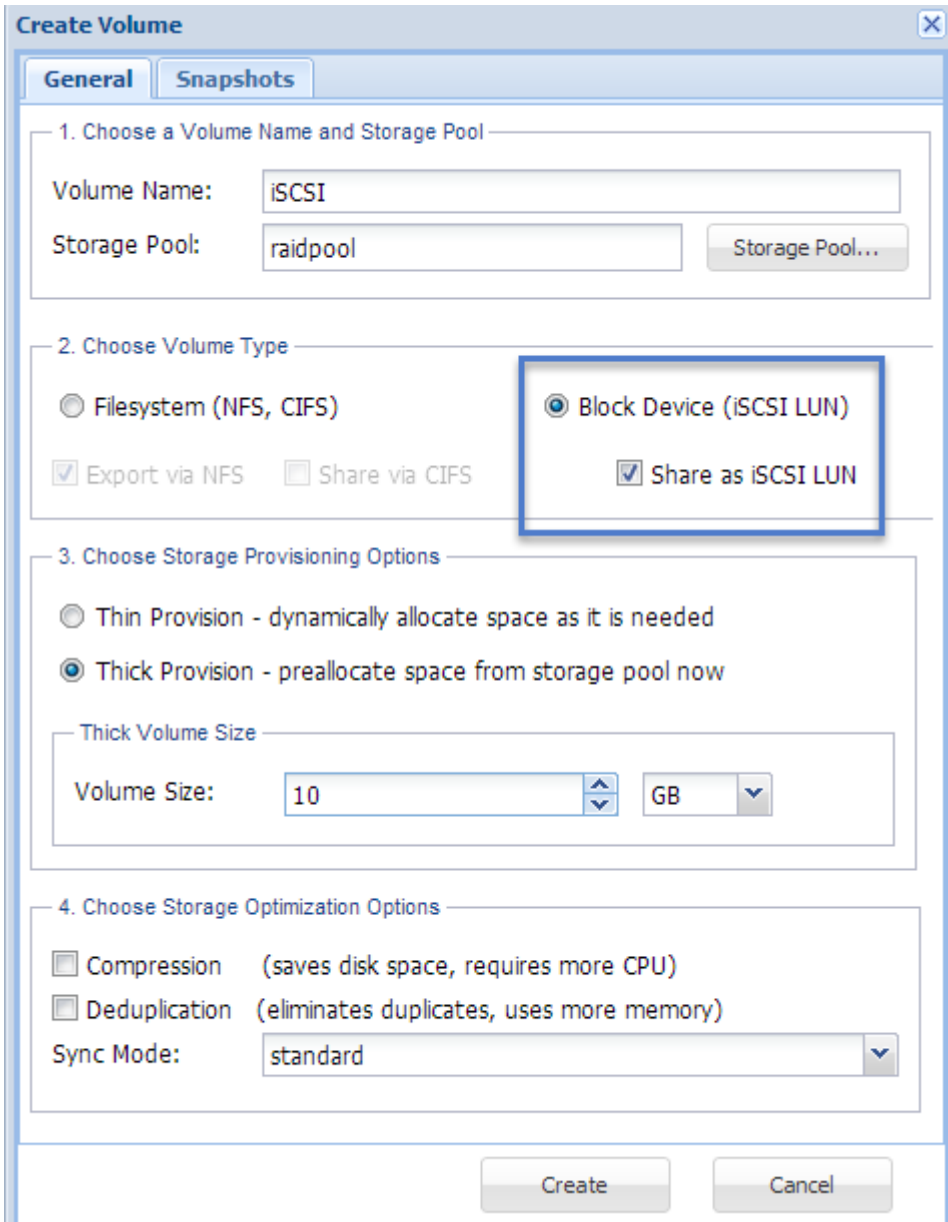
Creating a Volume and Sharing as iSCSI Target

To share a volume as an **iSCSI target**:

1. Create a new volume and choose the **Block Device** option as shown below as by default. The new volume will be shared as an iSCSI LUN upon creation. The block device volume is automatically added to the default iSCSI target.

Note: The mountpoint for block device volumes is named **LUN_lun1** (in the example below). Block device volume mount points always use the prefix **LUN_** followed by the user-assigned volume name, to distinguish LUNs from regular filesystem volumes. Block devices are comprised of a sparsely-allocated file named **lundata.dat**. So for a pool name **naspool** and block device volume named **lun1**, the full mount point path is **/naspool1/LUN_lun1/lundata.dat**. These LUN names are automatically maintained by **SoftNAS Cloud®** and shown in the iSCSI Targets configuration panel, as well as the Volumes list.

For more information on creating a volume, refer to the **Configuring Volumes** section.



Create Volume

General | Snapshots

1. Choose a Volume Name and Storage Pool

Volume Name:

Storage Pool:

2. Choose Volume Type

Filesystem (NFS, CIFS) **Block Device (iSCSI LUN)**

Export via NFS Share via CIFS **Share as iSCSI LUN**

3. Choose Storage Provisioning Options

Thin Provision - dynamically allocate space as it is needed

Thick Provision - preallocate space from storage pool now

Thick Volume Size

Volume Size:

4. Choose Storage Optimization Options

Compression (saves disk space, requires more CPU)

Deduplication (eliminates duplicates, uses more memory)

Sync Mode:

Note the default is **Thick Provision**, which reserves space for the LUN at time of creation. Alternatively, choose **Thin Provision**, which will create a "sparse" LUN that only consumes space as it is actually used.

Configuring and Sharing Storage using iSCSI

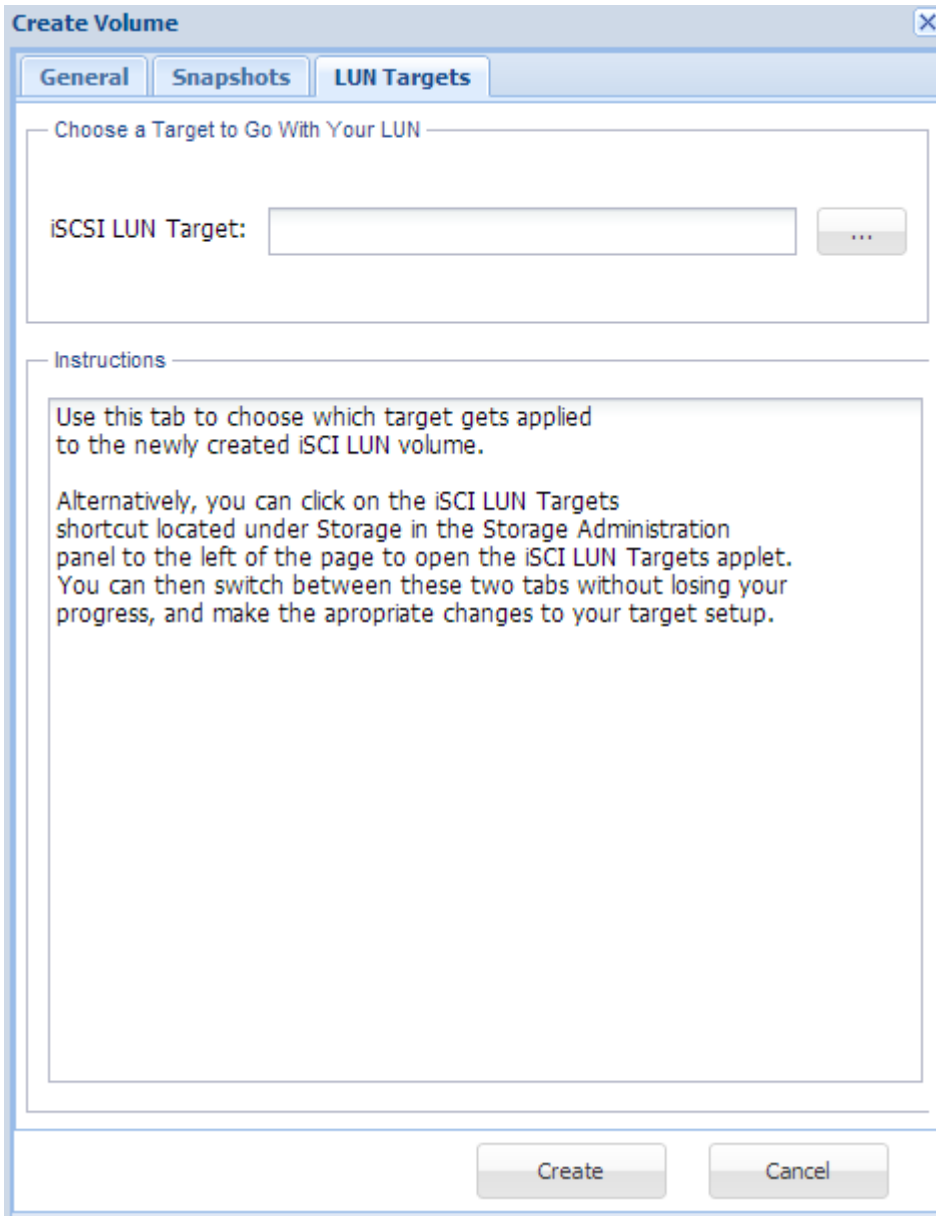
iSCSI LUN volumes can be shared by applying LUN Targets to the storage.

This can be done directly at time of Volume creation, when selecting **Block device (iSCSI LUN)**. It can also be done after the fact, via the **iSCSI LUN Targets** applet.

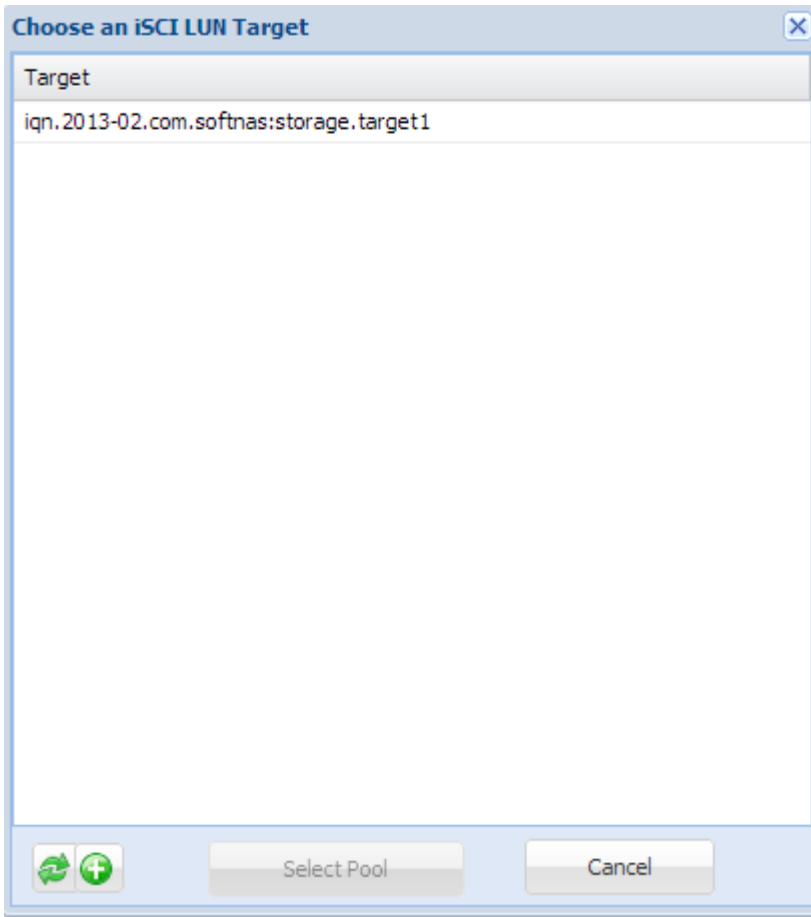
Applying The Target at Volume Creation Time

1. From **Volumes and LUNS**, click on **Create**.
2. Follow the standard instructions for creating a new Volume, and select **Block Device (iSCSI LUN)**.

The LUN Targets tab is displayed.



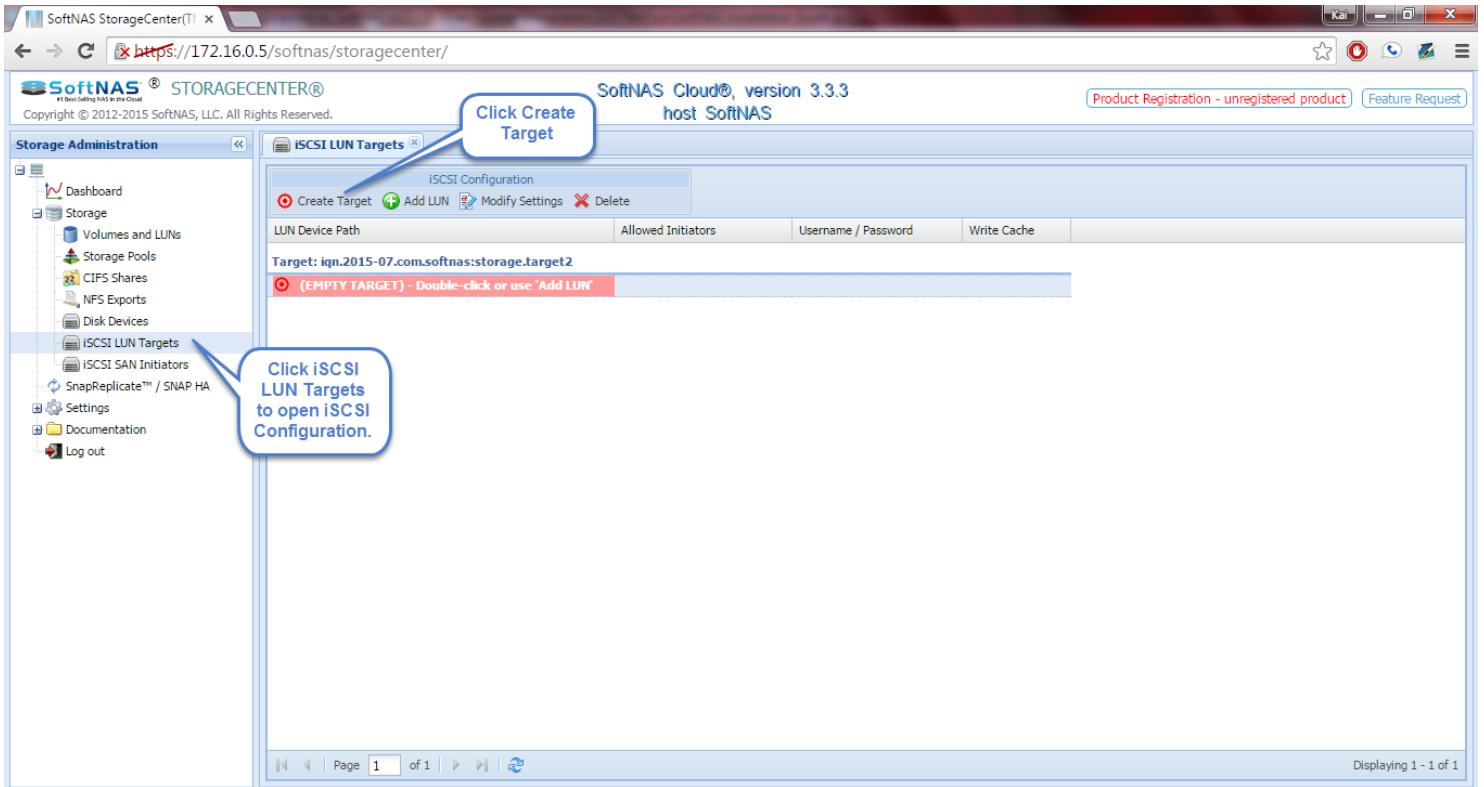
3. Select the appropriate **LUN Target** from the dropdown.



Applying The Target Using the Applet

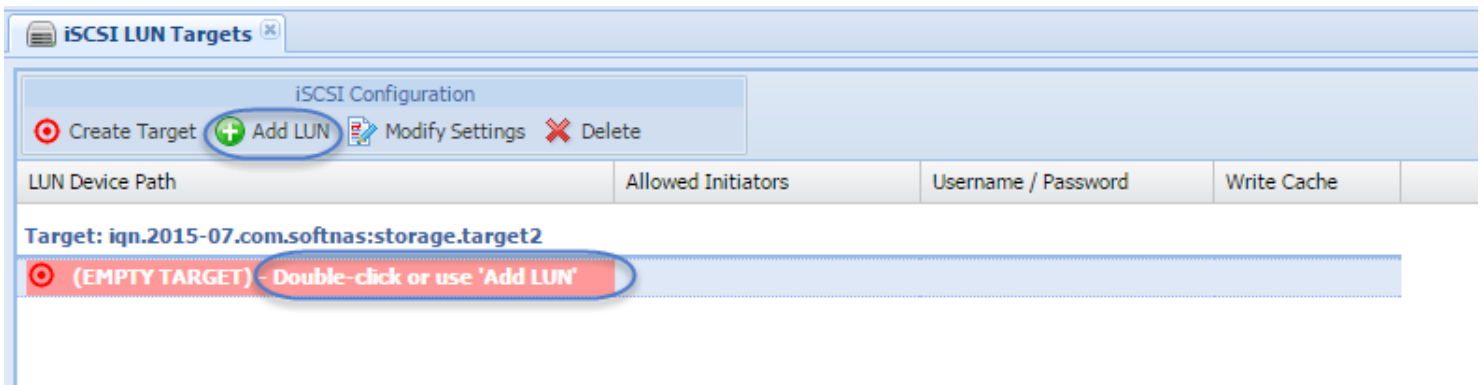
1. Log on to **SoftNAS StorageCenter**.
2. In the **Left Navigation Pane**, select the **iSCSI LUN Targets** option under the **Storage** section.

The **iSCSI LUN Targets** panel will be displayed. From here, configure and share storage using iSCSI.



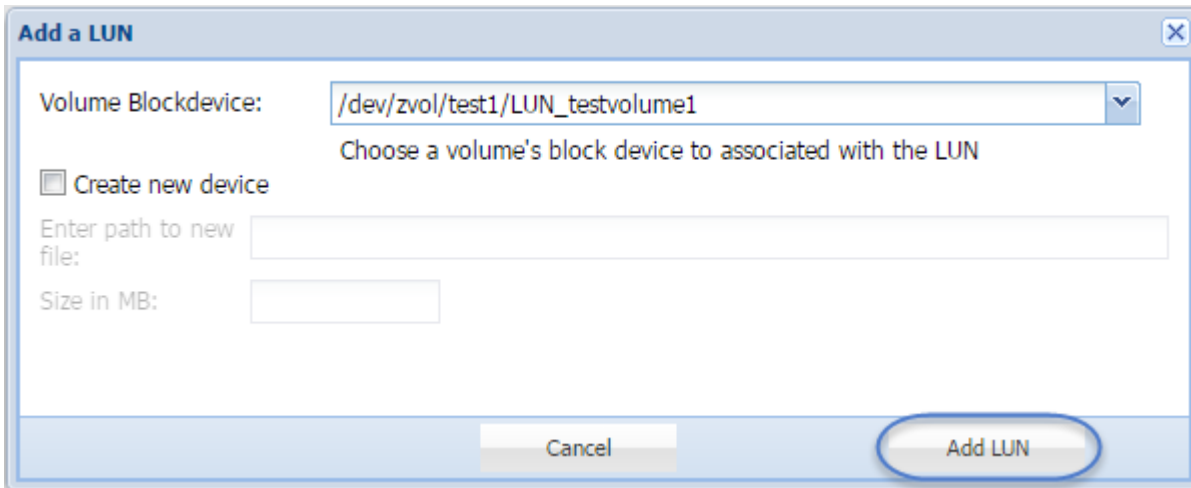
3. By default, an empty iSCSI target will be presented for you. However, if you need more than one, click **Create Target**.

Once the target is created, either double-click the empty target, or click **Add LUN**.

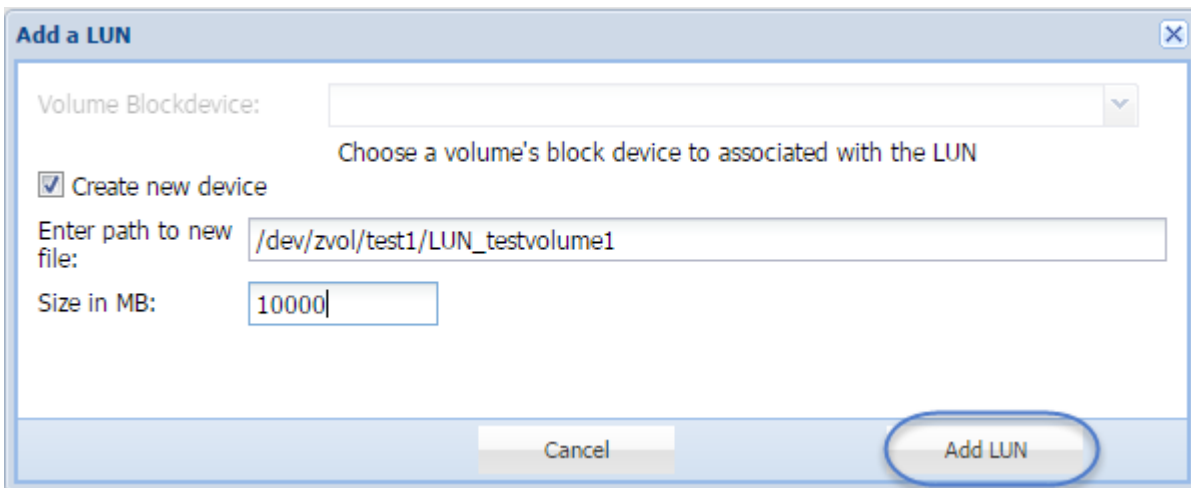


The **iSCSI Add A LUN** dialog box will be displayed.

4. Either select the volume's block device from the dropdown (which will show available volumes)...



...or check the box for Create a New Device, and enter the path, and the desired size to associate with the LUN.



5. Click **Add LUN** to link the block device to the iSCSI Target as a LUN.

The LUN is created and added to the target.

You may have to refresh the screen for the targets to present themselves.

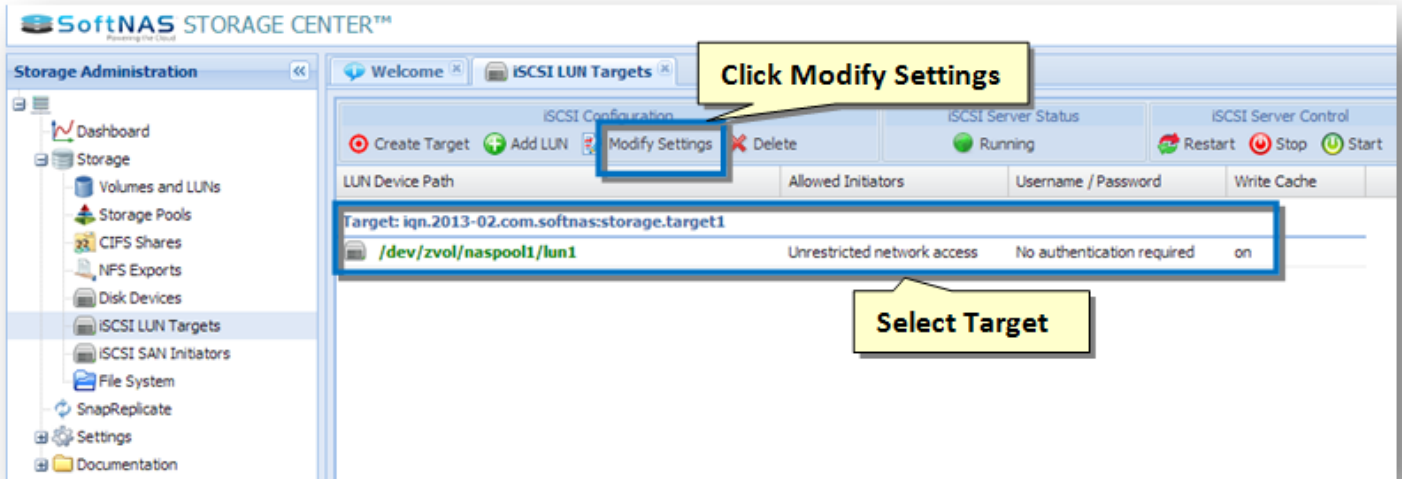
iSCSI Configuration		iSCSI Server Status		iSCSI Server Control			
Create Target	Add LUN	Modify Settings	Delete	Running	Restart	Stop	Start
LUN Device Path	Allowed Initiators	Username / Password	Write Cache				
Target: iqn.2013-02.com.softnas:storage.target1							
/raidpool/LUN_volume1/lundata.dat	Unrestricted network access	No authentication required	on				
/raidpool/LUN_volume2/lundata.dat	Unrestricted network access	No authentication required	on				
Target: iqn.2013-02.com.softnas:storage.target2							
/raidpool/LUN_iSCSI/lundata.dat	Unrestricted network access	No authentication required	on				

Note: Publish any number of block device volumes via a single iSCSI target. However, you can use the **Create Target** button to add new targets as needed.

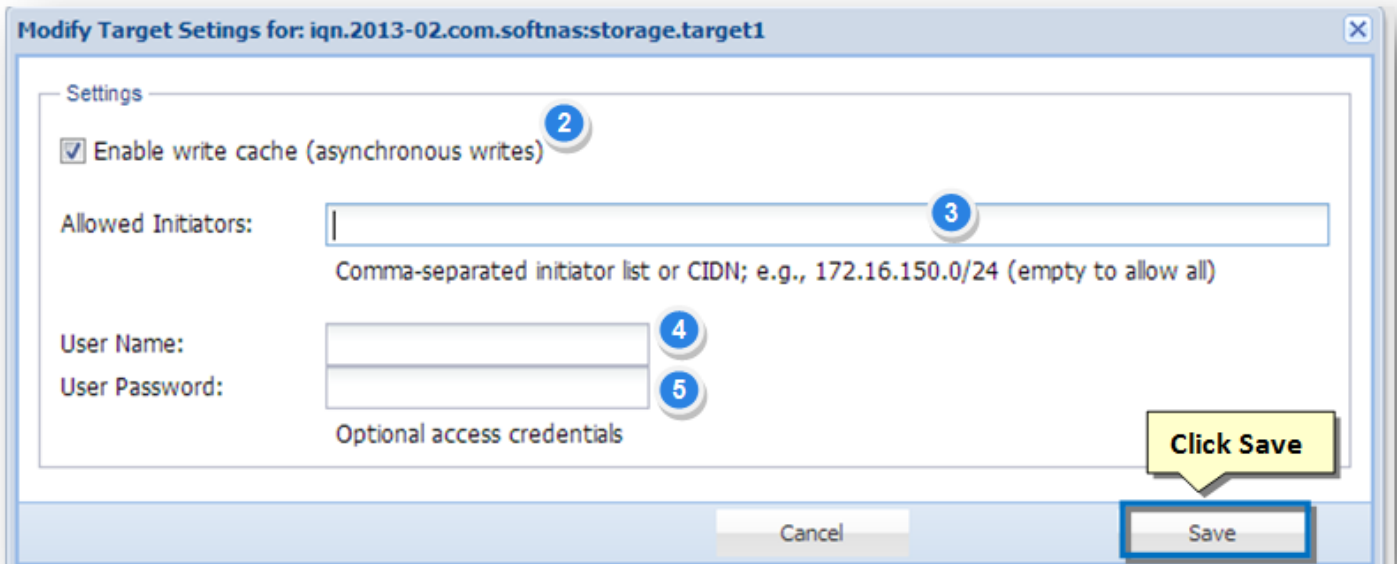
Target Settings and Options

Each **iSCSI** target can be configured to restrict access to one or more **iSCSI client IP** addresses. It can also be configured to require authentication using a user name and password.

1. To do so, on the **iSCSI LUN Targets** panel, select the LUN target and then click the **Modify Settings** option in the tool bar.



The **Modify Target Settings** dialog will be displayed.



2. In the **Settings** section, check the box in the **Enable Write Cache** field. This provides the option to cache incoming iSCSI write requests for faster I/O operations.

3. By default, targets have unrestricted access from any IP address. To restrict which iSCSI initiators are allowed to connect to the target, enter one or more comma-separated IP addresses (or DNS names, if using DNS) in the **Allowed Initiators** text entry box. Use the CIDN notation to provide a range of network addresses; e.g., 172.16.150.0/24 restricts access to iSCSI initiators in the 172.16.150.* subnet only.

4. In order to use login credentials while accessing the target, enter the user name in the **User Name** text entry box.

5. Enter the password in the **User Password** text entry box.

6. Click **Save**.

Note: To skip login credentials to the access target, then simply leave the User Name and User Password fields blank.

7. Once the required changes are made, click **Save**.

8. To enforce the changes, click **Restart** on the **iSCSI LUN Targets** panel.

Accessing the Target and LUN

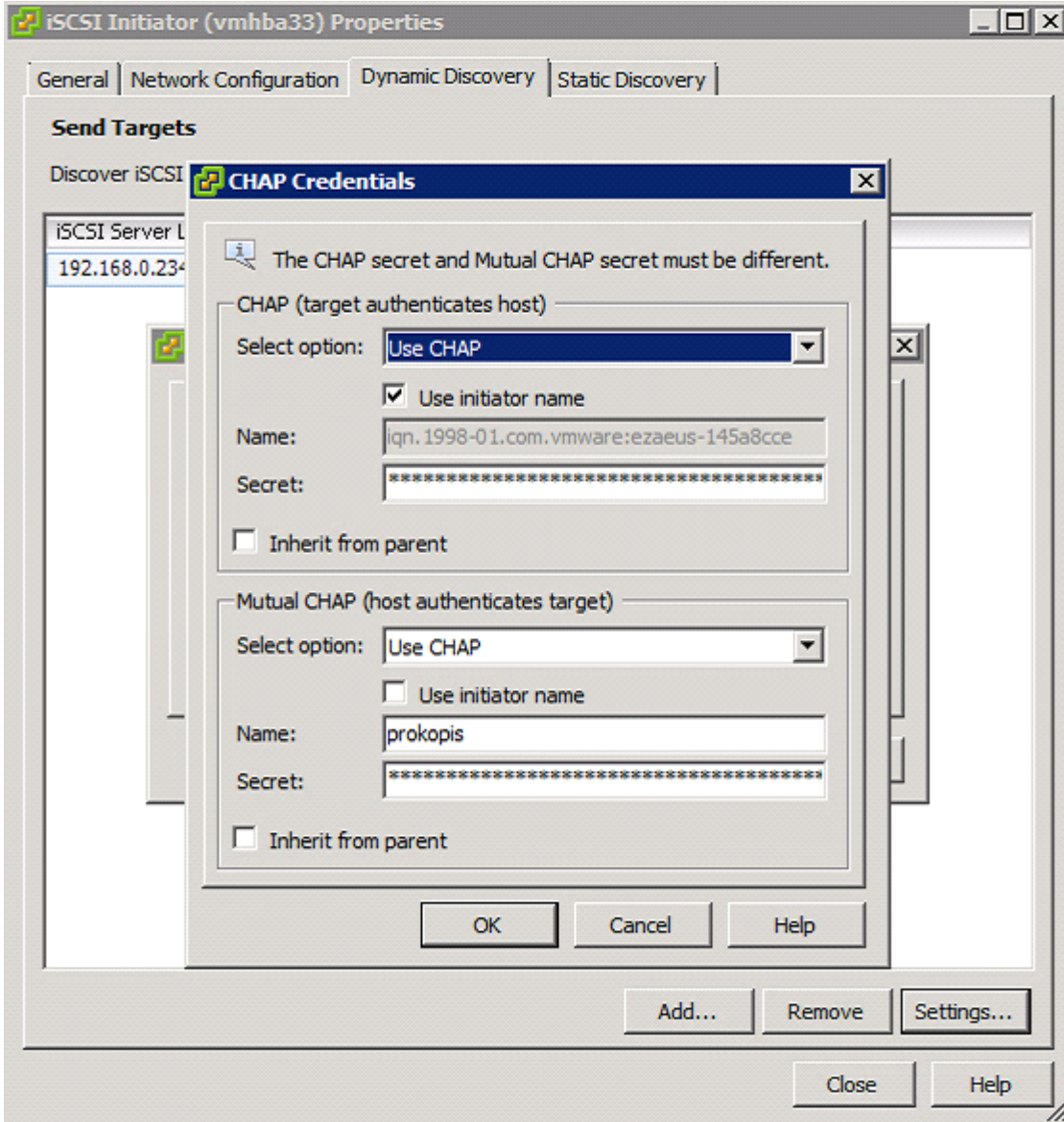
To access the iSCSI target and its LUNs, make use of an SCSI initiator from another system on the network.

For more information, refer to the **SoftNAS Reference Guide** or the operating system reference guide associated with an iSCSI initiator.

iSCSI CHAP Authentication

iSCSI uses CHAP authentication, as shown in the example **VMware vSphere** iSCSI Initiator setup below.









1. After [setting an iSCSI User Name and Password](#) in the iSCSI Target, use the same credentials in the CHAP authentication for the iSCSI initiator.



2. In the **VMware vSphere** ESXi example below, there are several iSCSI datastores.

View: [Datastores](#) [Devices](#)

Datastores [Refresh](#) [Delete](#) [Add Storage...](#) [Rescan All.](#)

Identification	Status	Device	Drive Type
 datastore Le	 Normal	Local ATA Disk (t10.ATA____WDC_WD800JD2D00LSA0____W...	Non-SSD
 HA_VOLUME_1	 Normal	IET iSCSI Disk:1	Non-SSD
 HA_VOLUME_2	 Normal	IET iSCSI Disk (t10.IET____00020001000):1	Non-SSD
 HA_VOLUME_3	 Normal	IET iSCSI Disk (t10.IET____00030001000):1	Non-SSD

Snapshots in StorageCenter

Snapshots

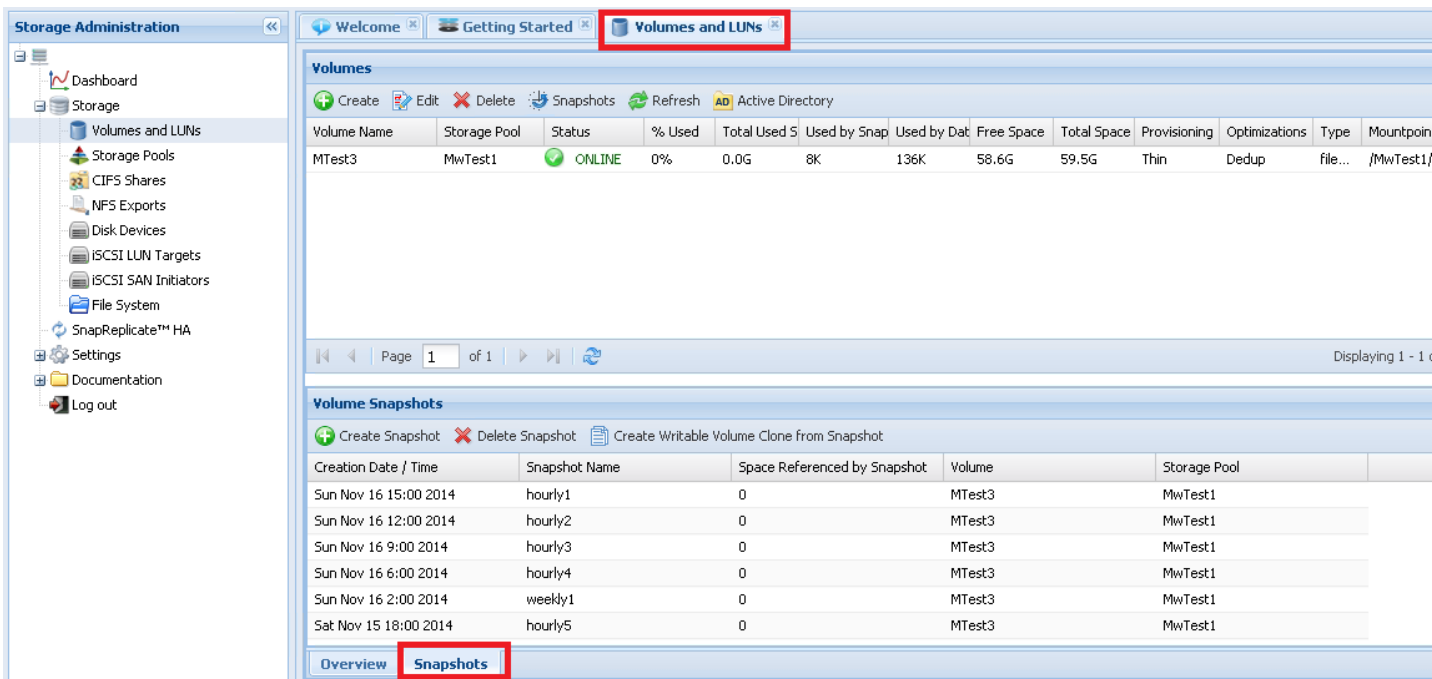
Snapshots to Keep Recovery Copies of Your Data

Use of Snapshots is a great practice to keep archived copies of point-in-time data on your SoftNAS volumes that can be accessed at a later time, if needed from the Snapshot volume.

Snapshots can be taken manually (one at a time, not recommended) or set as part of the local network's regular maintenance settings in **SoftNAS StorageCenter** (recommended best practice).

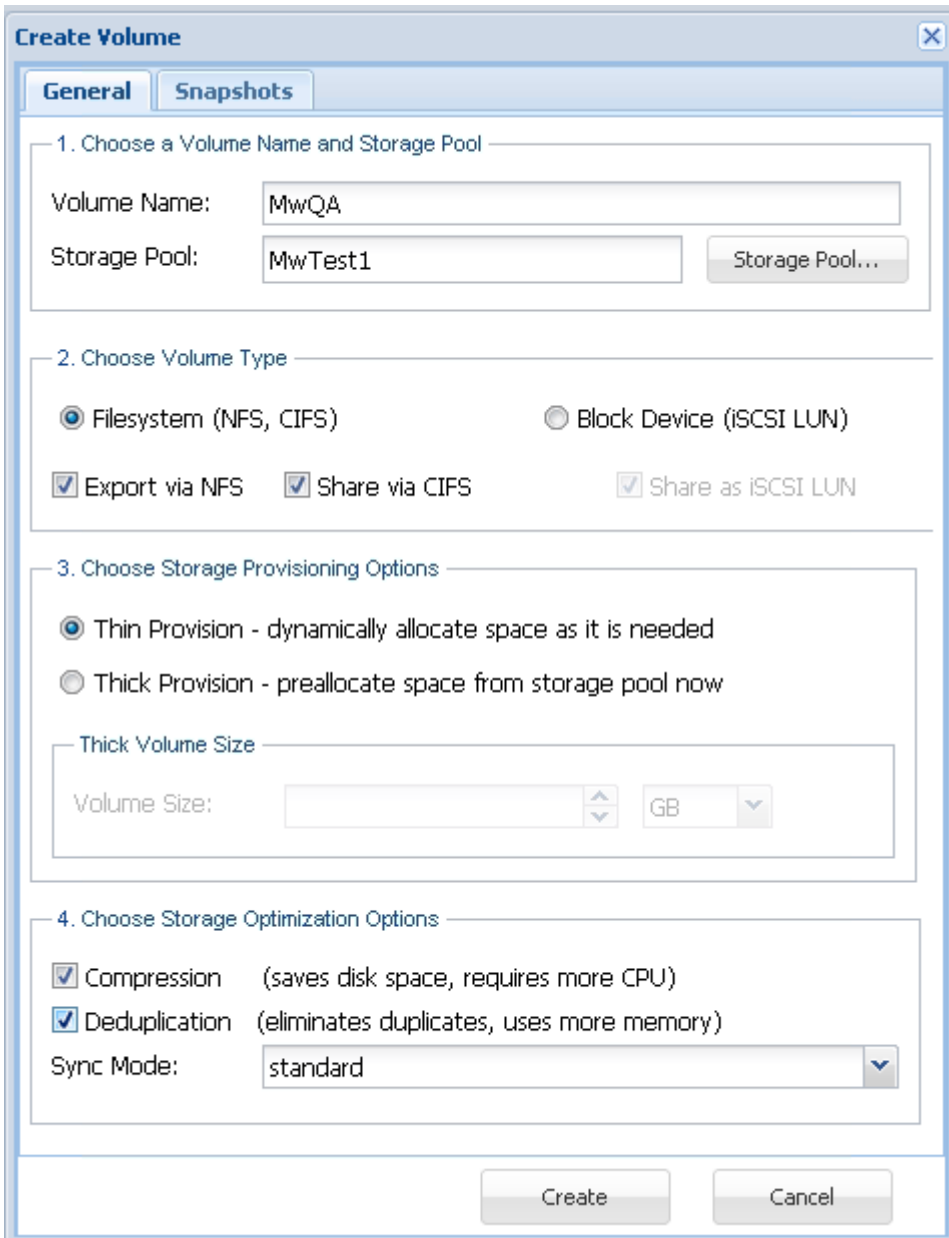
1. In the **Volumes and LUNs** section, click the **Snapshots** tab (at the bottom of the open window).

The **Snapshots** section of the dialog will be displayed.



Volume snapshots are automatically created based upon the chosen schedule. The maximum number of snapshot copies determines when older snapshots are pruned and eliminated.

2. Click **Create** in the **Volumes** (top half) section of the pop-up window. Fill out the required fields before continuing to the **Snapshots** tab.



Create Volume

General | **Snapshots**

1. Choose a Volume Name and Storage Pool

Volume Name:

Storage Pool:

2. Choose Volume Type

Filesystem (NFS, CIFS) Block Device (iSCSI LUN)

Export via NFS Share via CIFS Share as iSCSI LUN

3. Choose Storage Provisioning Options

Thin Provision - dynamically allocate space as it is needed

Thick Provision - preallocate space from storage pool now

Thick Volume Size

Volume Size: GB

4. Choose Storage Optimization Options

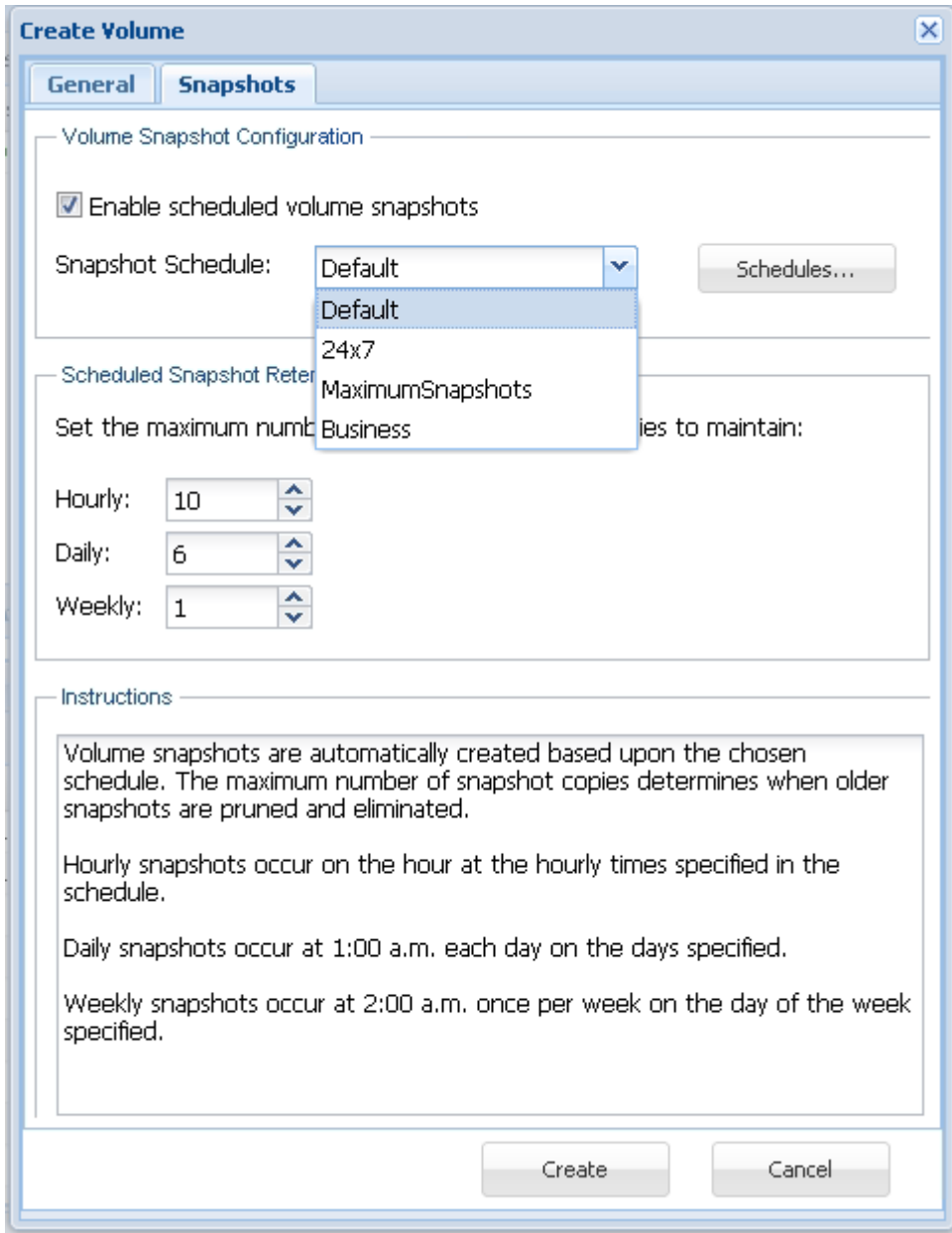
Compression (saves disk space, requires more CPU)

Deduplication (eliminates duplicates, uses more memory)

Sync Mode:

3. Switch to the **Snapshots** tab at the top.

4. In the **Volume Snapshot Configuration** section, check the box in order to enable the scheduling of volume snapshots.



4. In the **Scheduled Snapshot Retention Policy** section, set the maximum number of scheduled snapshot copies to maintain in the **Hourly**, **Daily** and **Weekly** fields by either manually entering the value or by using the scroll bar to increase or decrease the value.

Volumes and LUNs [X]

Create Volume [X]

General | **Snapshots**

Volume Snapshot Configuration

Enable scheduled volume snapshots

Snapshot Schedule: [v]

Scheduled Snapshot Retention Policy

Set the maximum number of scheduled snapshot copies to maintain:

Hourly: [↑][↓]

Daily: [↑][↓]

Weekly: [↑][↓]

Instructions

Volume snapshots are automatically created based upon the chosen schedule. The maximum number of snapshot copies determines when older snapshots are pruned and eliminated.

Hourly snapshots occur on the hour at the hourly times specified in the schedule.

Daily snapshots occur at 1:00 a.m. each day on the days specified.

Weekly snapshots occur at 2:00 a.m. once per week on the day of the week specified.

Note:

- **Hourly snapshots** occur **on the hour** at the hourly times specified in the schedule.
- **Daily snapshots** occur at **1:00 a.m. each day** on the days specified.
- **Weekly snapshots** occur at **2:00 a.m. once per week** on the day of the week specified.

5. Click **Create** at the end.

The new volume is created with preferred **Snapshot** settings.

Advanced/Performance Configuration

Regardless of platform, occasionally higher-quality management tools can only be accessed through Advanced Configurations for Performance considerations. This guide provides instructions and recommendations for value-added support with the **SoftNAS Cloud®** package.

[MTU 9000](#)

[Active Directory Configuration](#)

[Configuring Read Cache and Write Log](#)

MTU 9000

To increase throughput and performance, it is recommended to use **MTU 9000** instead of the default **MTU 1500**. In order to use **MTU 9000**, all network switching and routing elements between the **SoftNAS Cloud® VM** and the client device must support MTU 9000.

Note that for MTU 9000 to work properly, it must be configured on all physical switch ports, routers, host servers and virtual switches (and within **SoftNAS Cloud®** network interfaces). Be sure to verify networking paths and hosts end to end in order to use MTU 9000 (or it can actually reduce performance and potentially cause packet loss or retries if not configured properly).

EC2 Users - Due to the specific ways in which EC2 physical servers and networking infrastructure are configured, some of the physical hosts support jumbo frames, and others do not. On physical hosts that support jumbo frames, AWS will push the 9001 MTU setting through to the virtual machines on that physical host. On the ones that don't, AWS will not push that 9001 MTU setting. This info is tucked away in AWS docs at [Amazon Docs Instance Types](#) "The maximum transmission unit (MTU) for an instance depends on its instance type. The following instance types provide 9001 MTU (jumbo frames): CC2, C3, CG1, CR1, G2, HS1, HI1, I2, and M3. The other instance types provide 1500 MTU (Ethernet v2 frames)."

For example:

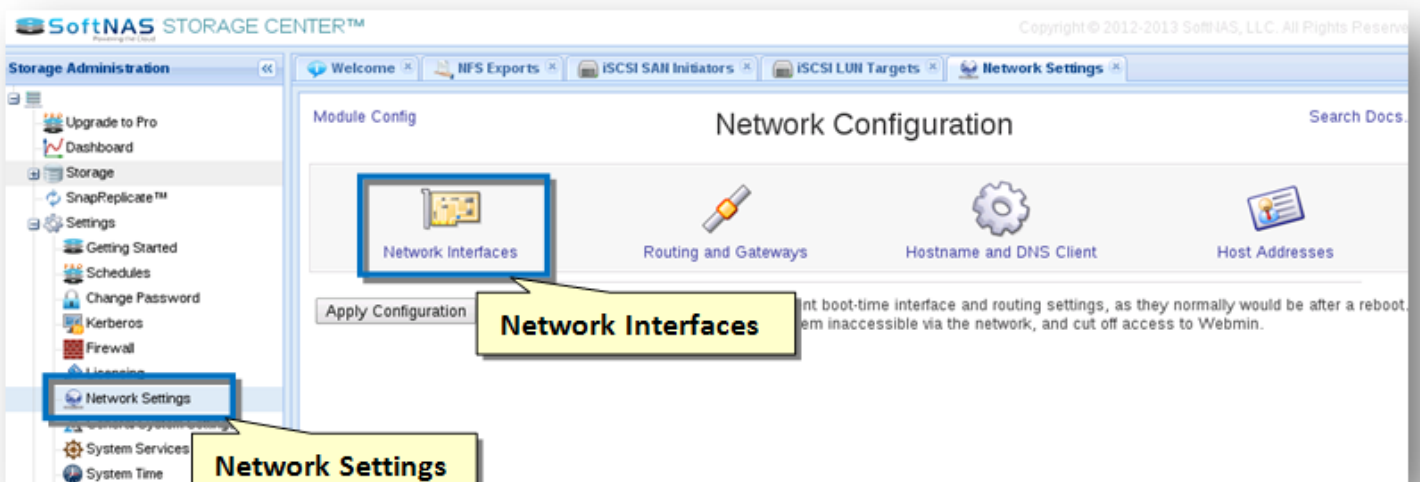
SoftNAS VM, eth1 <=> vSwitch <=> VM host physical NIC <=> Physical switch ports <=> VM host 2 NIC <=> vSwitch 2 <=> Client VM

For MTU 9000 to work, all virtual and physical switch ports must be configured for MTU 9000, as well as the virtual machine client's (or VMkernels, if client is running on VMDK).

Within **SoftNAS Cloud®**, to configure **MTU 9000** to be persistent upon reboot, simply follow the steps given below.

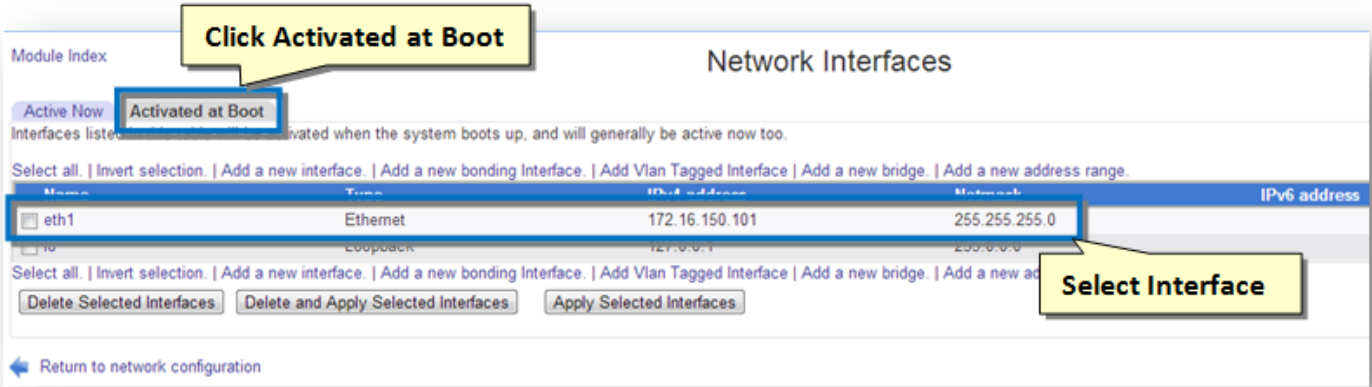
1. Log on to **SoftNAS StorageCenter**.
2. In the **Left Navigation Pane**, select the **Network Settings** option under the **Settings** section.

The **Network Settings** panel will be displayed. Configure and manage all network configuration from here.



3. Click the **Network Interfaces** icon.

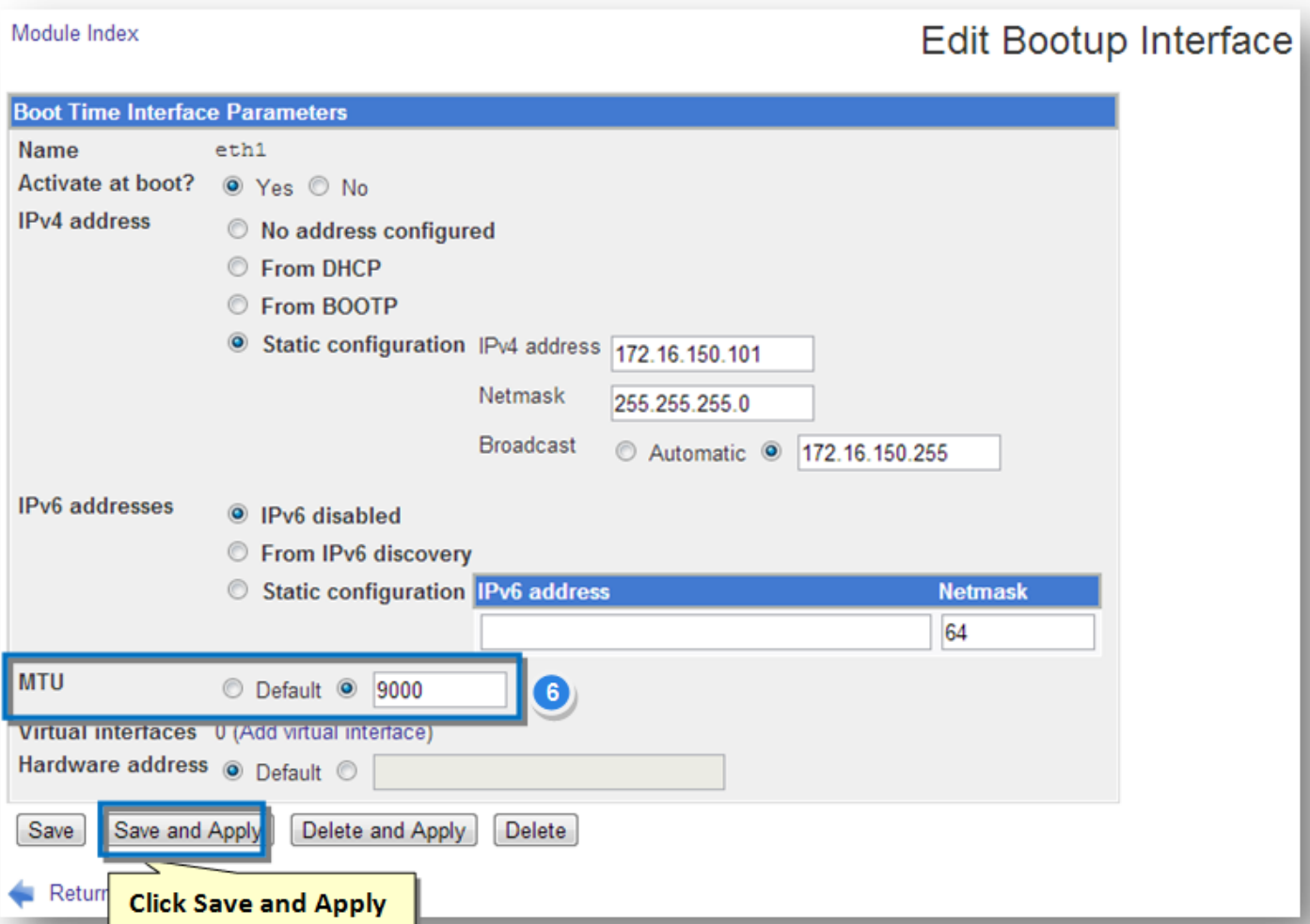
The **Network Interfaces** section of the panel will be displayed.



4. Click the **Activated at Boot** tab.

5. Select the network interface (**eth1**) in the list of the interfaces.

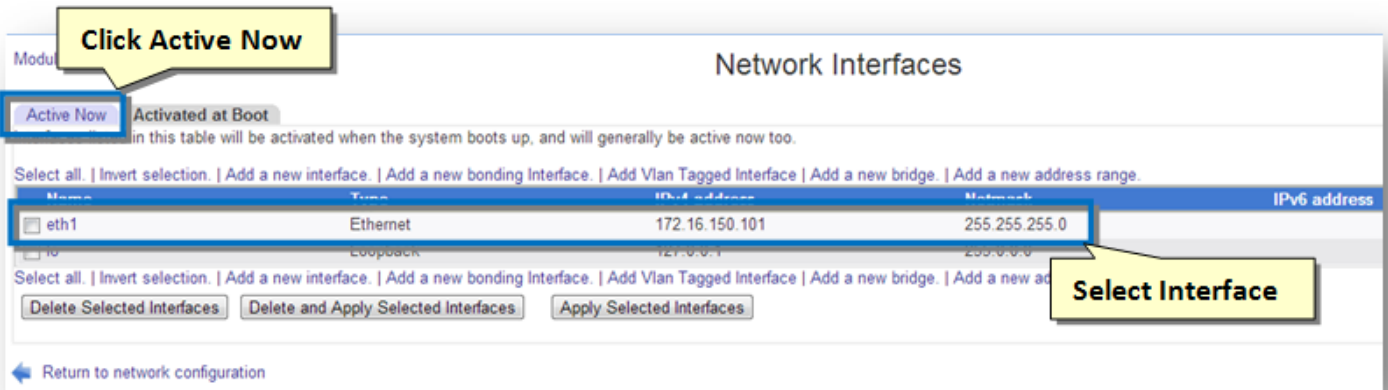
The **Edit Bootup Interface** section of the panel will be displayed.



6. In the **MTU** field, change the value from default to **9000**. In order to do so, check the option for the text entry box and enter the value **9000** in the text box.

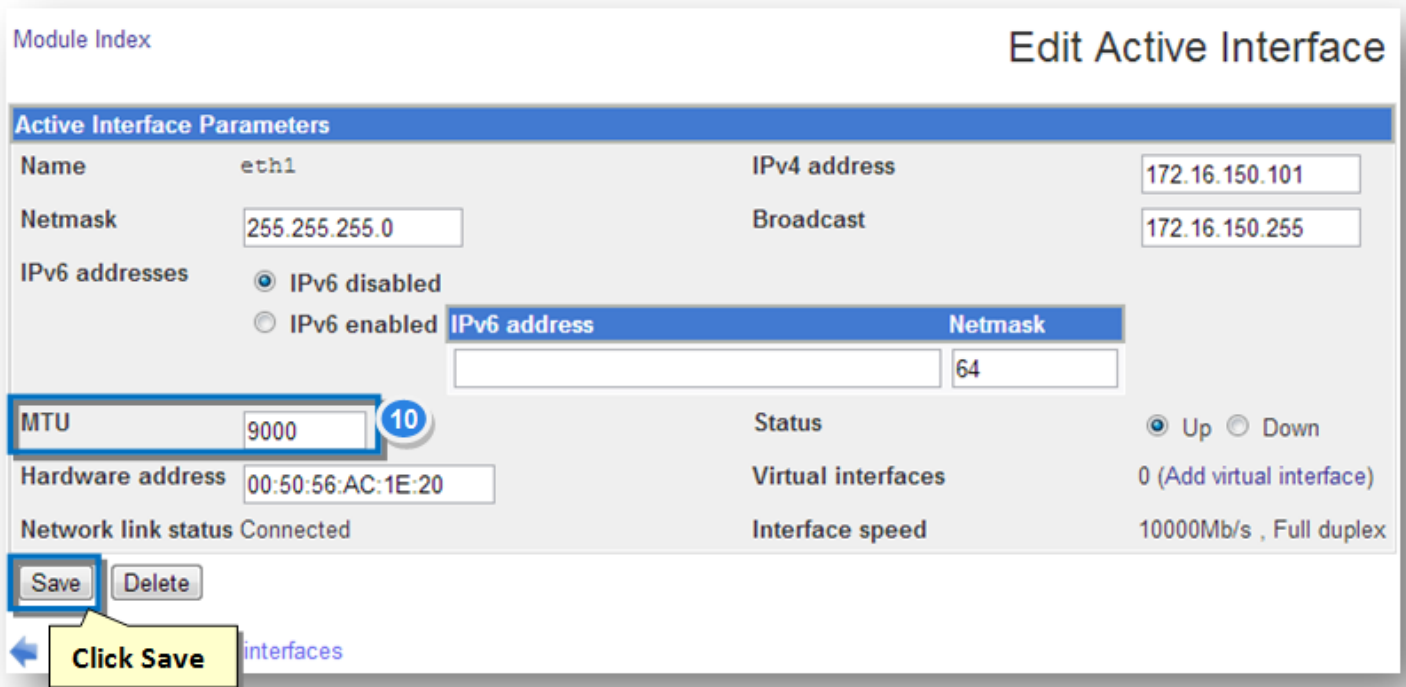
7. Click **Save and Apply**.

8. Back in the **Network Interfaces** panel, click the **Active Now** tab.



9. Select the interface name (**eth1**).

The **Edit Active Interface** section of the panel will be displayed.



10. In the **MTU** field, enter the value as **9000** in the text entry box. This will change the current network interface value to MTU 9000. Be sure that all switching paths are configured to support MTU 9000 before making this change (or risk losing connectivity).

11. Click **Save**.

Configuring VMware vSphere for MTU 9000

Before enabling jumbo frames, ensure the following are true:

- The physical server's network interface card and network switch can support jumbo frames (MTU 9000)
- The switch ports of all routers and switches between **SoftNAS Cloud®** and **VMware vSphere** hosts are properly configured for MTU 9000.

VMWare ESX/ESXi support frames up to 9 Kb (MTU 9000).

In order to use jumbo frames support configuration is required end to end.

These commands are good for ESX/ESXi 5.0 and later:

1. Log into host with the **VMware vSphere** client.
2. Select the physical host to make changes to and click on the host IP.
3. Choose the **Configuration** tab.
4. Select the **Networking** option under **Hardware**.
5. Select properties on the **vSwitch** to be configured.
6. When the **vSwitch** is selected, the MTU set will become visible under **Advanced**.
7. Set Properties. The default is 1500.
8. Click **Edit** on the bottom while the **vSwitch** is selected.
9. On the **General** tab there is a box labeled **Advanced Properties**
10. Change the MTU here from **1500** to **9000** and click **OK**.

Also change the MTU for the VMK (VM kernel).

In the same **vSwitch Properties** box select the first VMK listed.

11. The MAC address and MTU are listed under **NIC Settings**.
12. Click **Edit** for the first VMK
13. On the properties dialogue box that pops up set the MTU in the **NIC settings** box on the **General tab** to **9000** and click OK
14. Repeat this for all VMKs under the virtual switch
15. Close the **vSwitch** properties dialogue and repeat for any remaining **vSwitches**

Be sure to set the **SoftNAS Cloud®** network interface to accept Jumbo Frames / MTU 9000, as described above.

Active Directory Configuration

Overview

Integration of **SoftNAS Cloud®** into **Active Directory** enables domain users to more securely share files and data in a corporate environment. Authentication is managed by Active Directory (AD) via **Kerberos**. Kerberos tickets are issued to users authenticated to AD. When a user accesses a CIFS share managed by **SoftNAS Cloud®**, the ticket is then verified with AD to ensure it is authentic and valid before allowing access to the shares. Windows user IDs and groups (e.g., Domain Users) are transparently and dynamically mapped from AD into **SoftNAS Cloud®** and Linux, making access seamless for Windows users.

When integrated into a domain environment, **SoftNAS Cloud®** becomes another member server of the domain - like any other Windows server joined to the domain.

Authorization and granular access controls are available to manage the level of access available to various users and user groups.

The following sections detail how to configure **SoftNAS Cloud®** for integration with AD and how to troubleshoot and resolve common issues that can arise during AD integration.

On Linux, Samba is used to provide access to CIFS for access from Windows-based systems. Samba uses a program called **winbind**, which binds Windows authentication and identities (e.g., AD users and groups) with Linux, and automatically maps Windows users and groups to Linux users and groups.

Please use the following process to integrate AD with **SoftNAS Cloud®** and Linux with Samba.

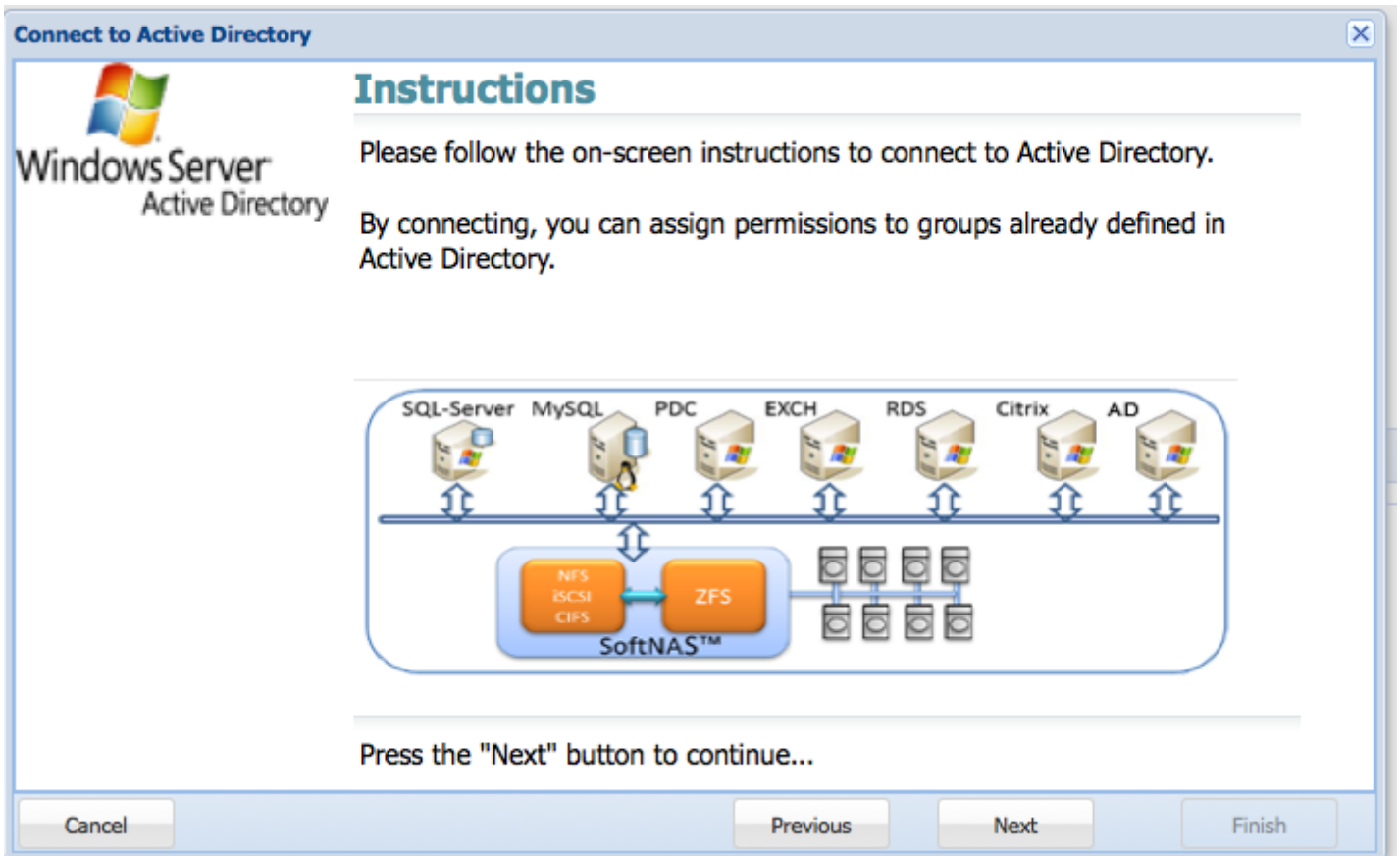
Active Directory Wizard

Configure AD using the **Active Directory Wizard**. This enables integration automation with AD.

After entering some basic networking details to enable **SoftNAS Cloud®** to communicate within the AD environment, **SoftNAS Cloud®** will automatically set up the integration with AD, and will even run a final verification stage to ensure that everything is working smoothly.

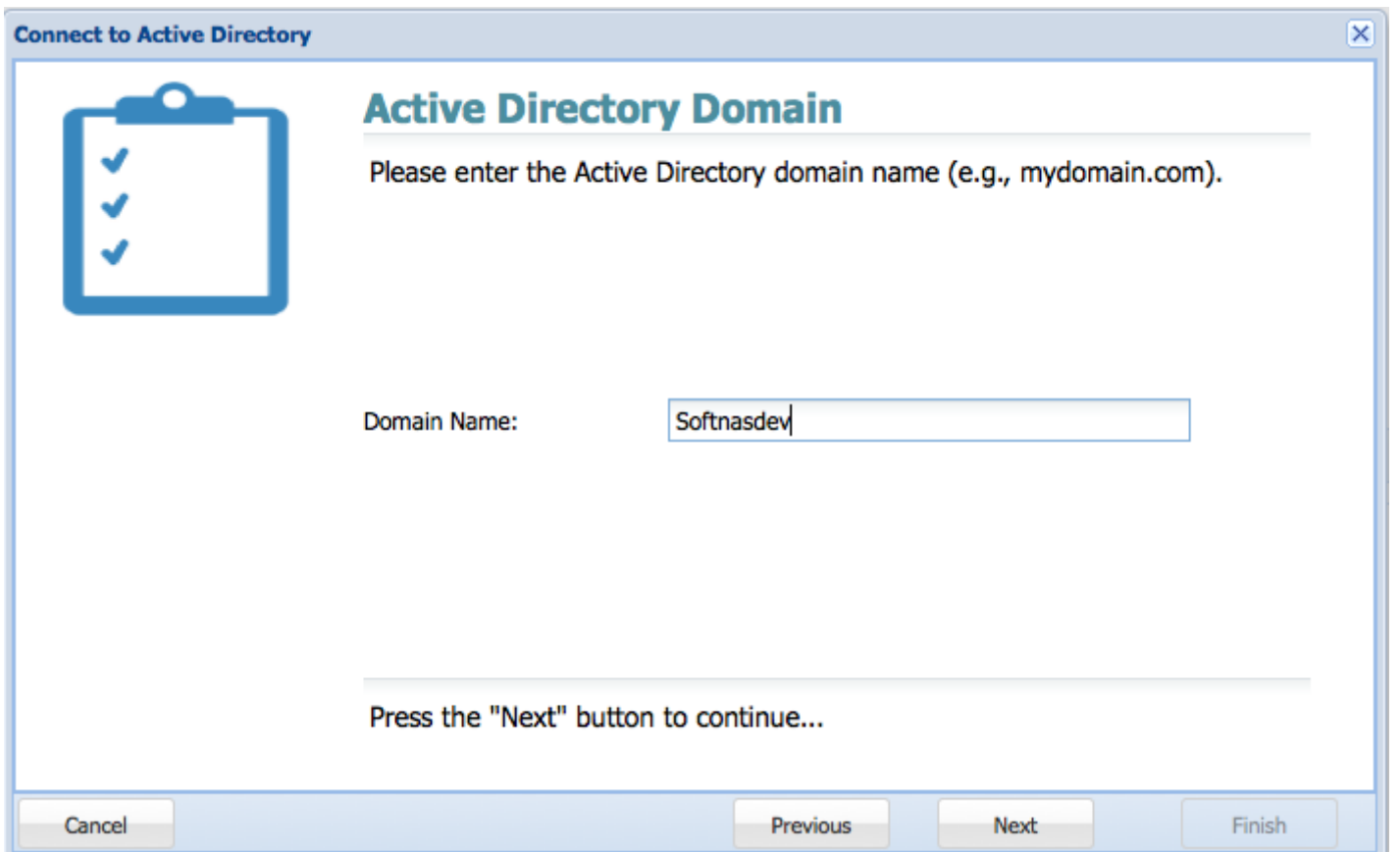
1. From **Volumes and LUNS**, click on **Active Directory**.

The AD Wizard instructions are displayed.



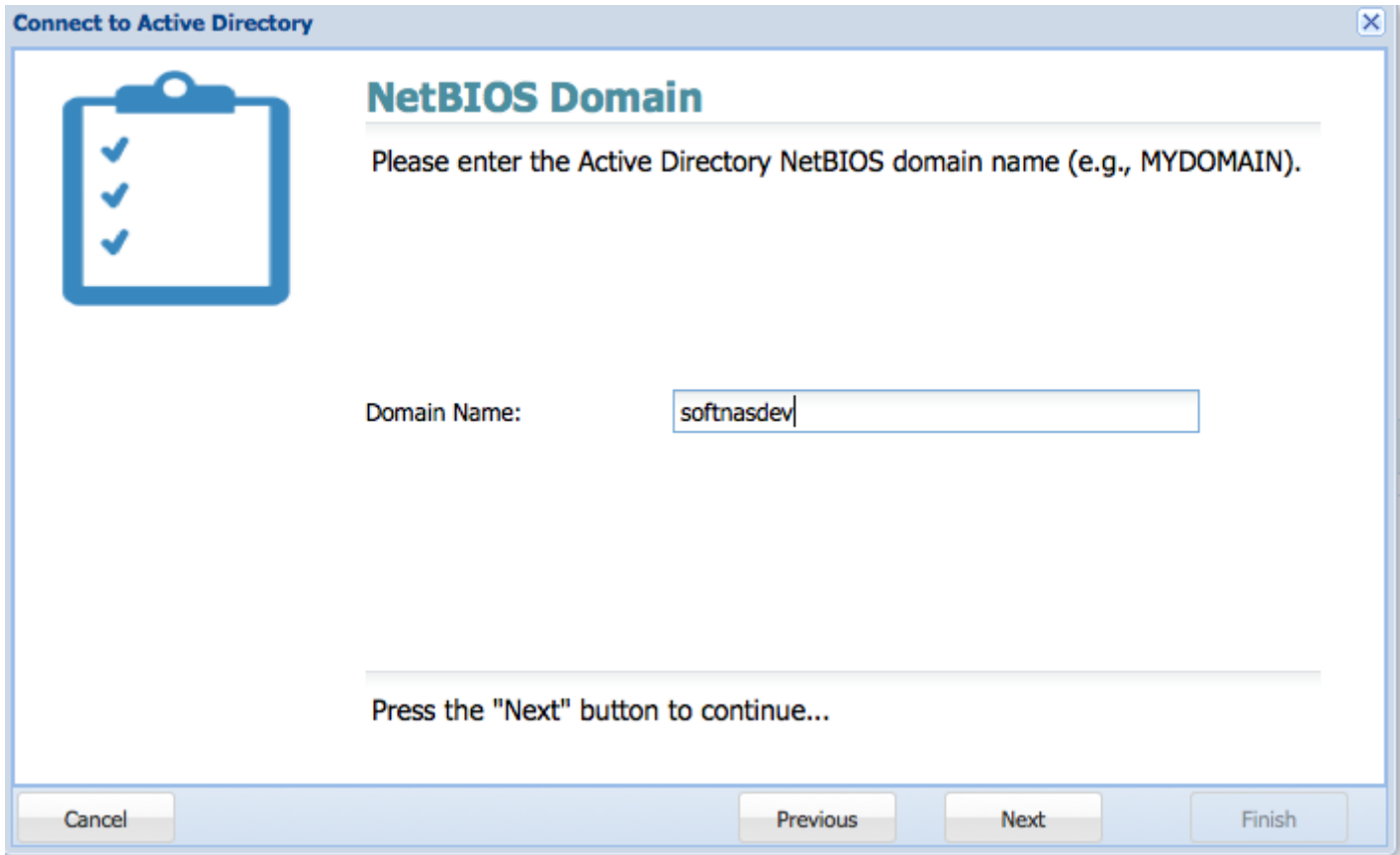
2. Click on **Next**.

3. Provide the domain name of the active directory domain controller, and then click on **Next**.



4. Enter the active directory **NetBIOS Domain**.

Note: The **NetBIOS** domain name is required for interoperability with older computers and services.



Connect to Active Directory

NetBIOS Domain

Please enter the Active Directory NetBIOS domain name (e.g., MYDOMAIN).


Domain Name:

Press the "Next" button to continue...

Cancel Previous Next Finish

5. Enter the **FQDN** of the domain controller.

Connect to Active Directory
✕



Domain Controller Fully Qualified Domain Name


Please enter the Fully Qualified Domain Name (FQDN) of the domain controller (e.g., myhost.mydomain.com).

FQDN:

Press the "Next" button to continue...

6. Provide the AD administrator credentials.

Connect to Active Directory
✕



Domain Administrator Credentials

The Active Directory administrator credentials are needed to access the Active Directory groups.

Please enter and verify the administrator credentials below.

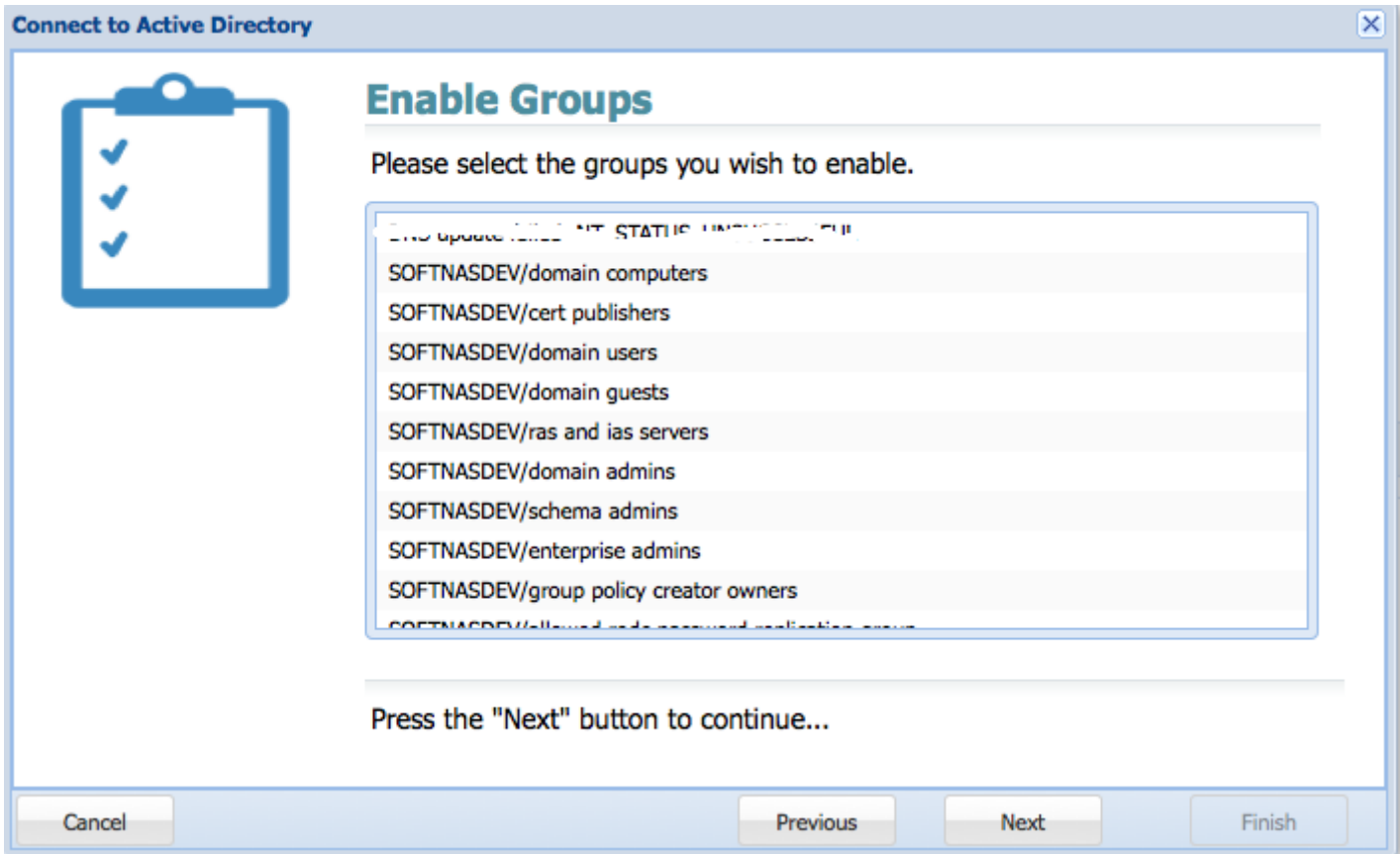
Admin User ID:

Admin Password:

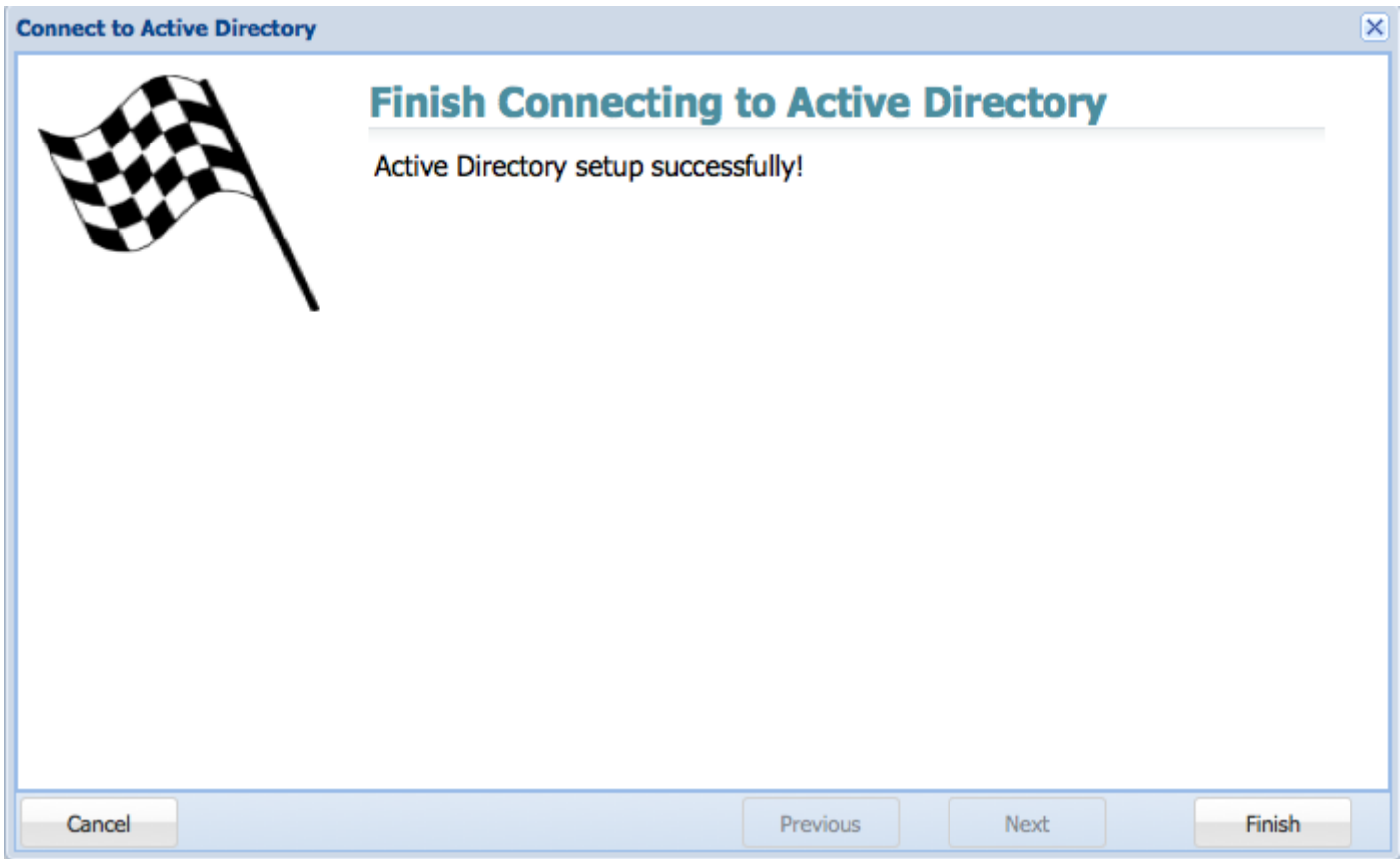
Verify Password:

Press the "Next" button to continue...

7. **Enable** the required groups.



8. Click on **Finish**.



Adding HA pairings to Active Directory

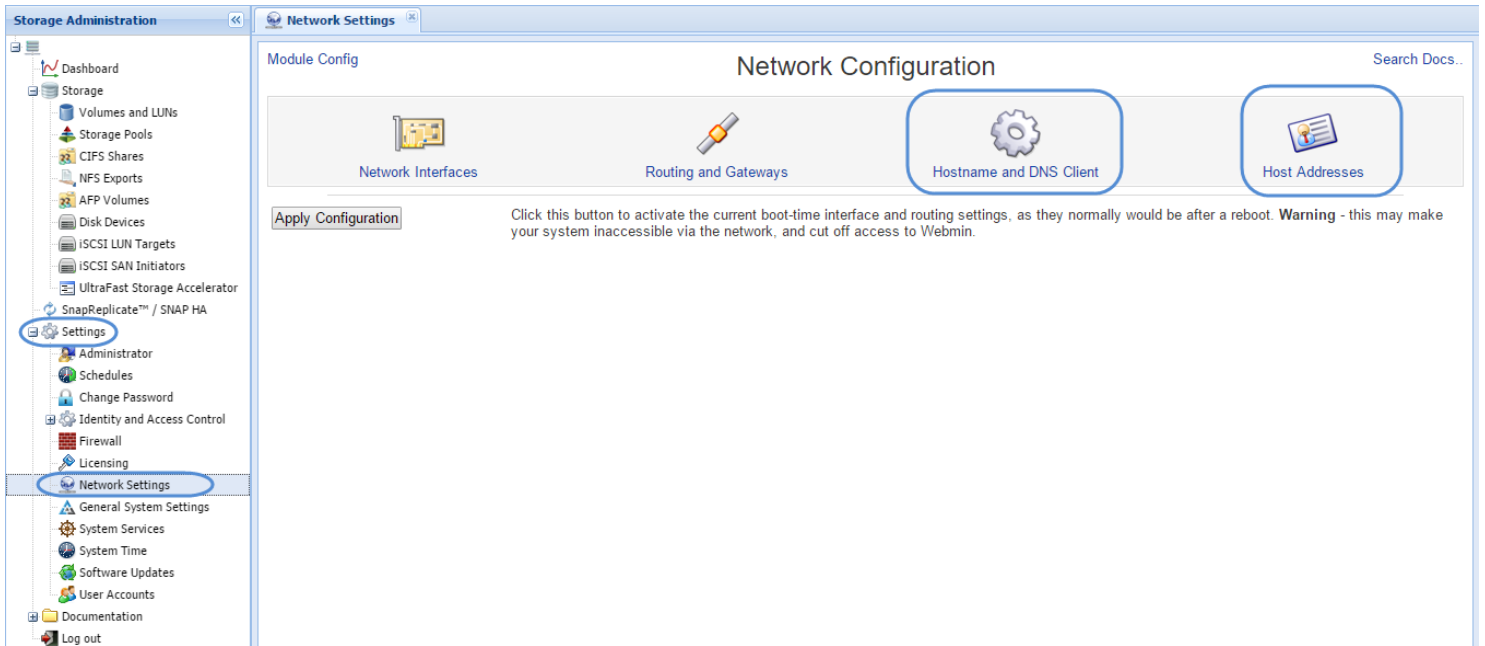
If connecting SoftNAS instances in a High Availability pairing to Active Directory, you must perform the process above twice, once on each node. Active Directory configurations do not carry over to the second node automatically because the target node's NAS services (amongst others) are not running while the node is dormant. Settings cannot be automatically triggered upon takeover. In order for the second instance to remain in Active Directory after a failover the second node must be added as well.

Adding Domain Controllers as DNS Server for SoftNAS

In order to integrate AD with the SoftNAS Linux operating system, the first step is enabling the SoftNAS Linux system to resolve host names into IP addresses for the Active Directory controller, DNS server(s) and the SoftNAS Linux system itself (so you can use host names instead of IP addresses in the following steps).

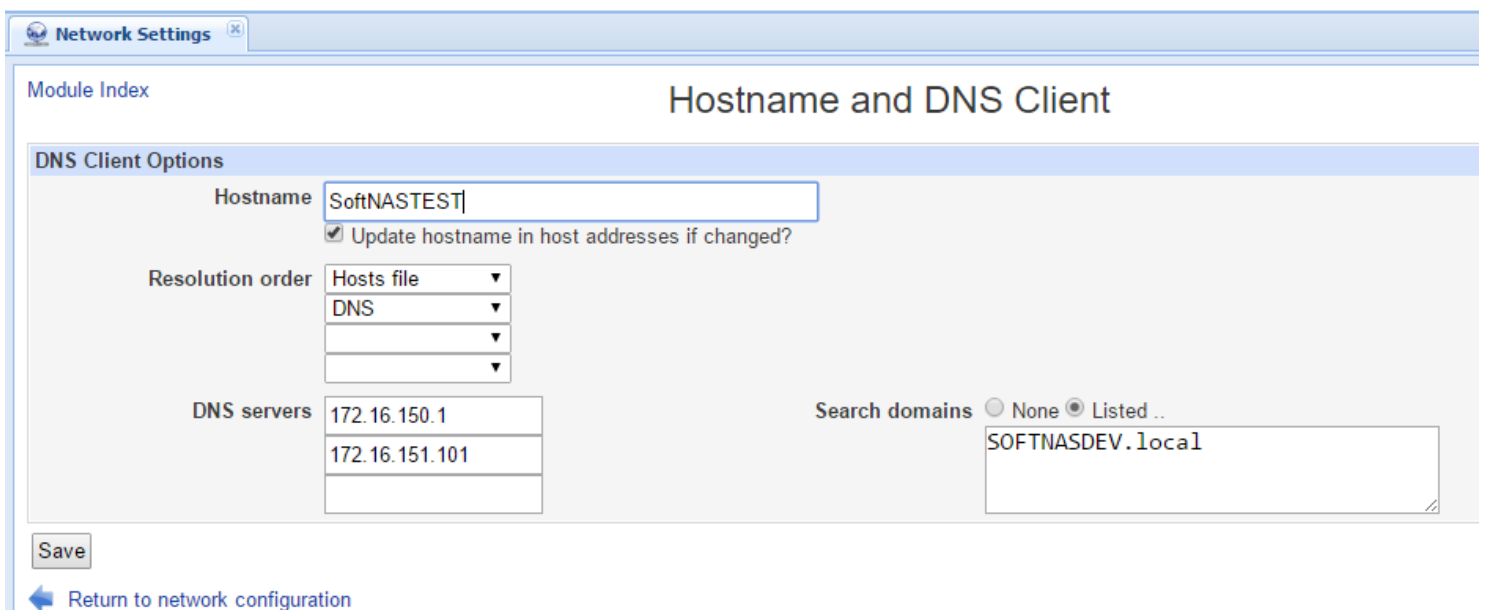
You need to verify that your hostname and DNS are set up correctly:

1. In the Storage Administration Pane on the left, navigate to **General System Settings -> Networking > Network Configuration > Hostname and DNS client** and **Host Addresses**.

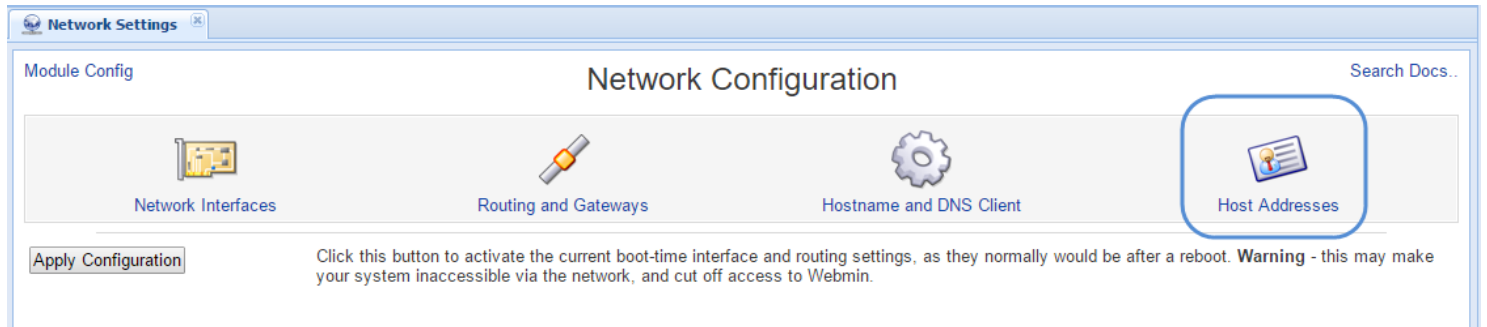


2. The DNS for SoftNAS, when integrated within an Active Directory environment, should be the domain controllers (like any other member server in the domain).

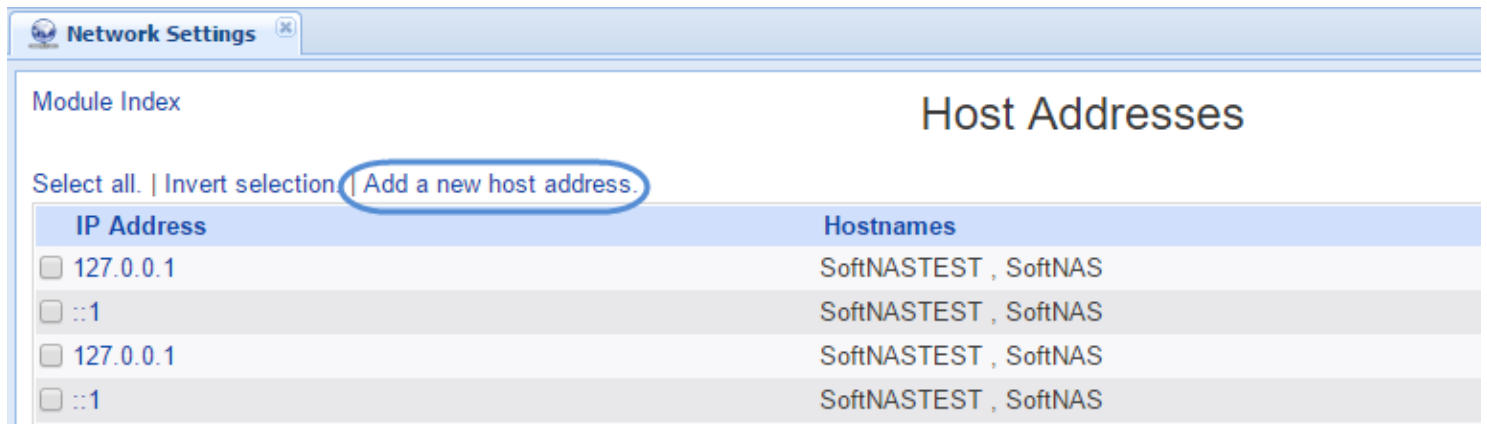
Begin by configuring your **Hostname and DNS Client** lookup for the SoftNAS server. Note that the Hosts file is configured to be used first for name resolution. In our examples, we use a domain name "SOFTNAS.local" and our domain controller and DNS is 172.16.150.1 on the local data center network. Our example host name is "SoftNASTEST".



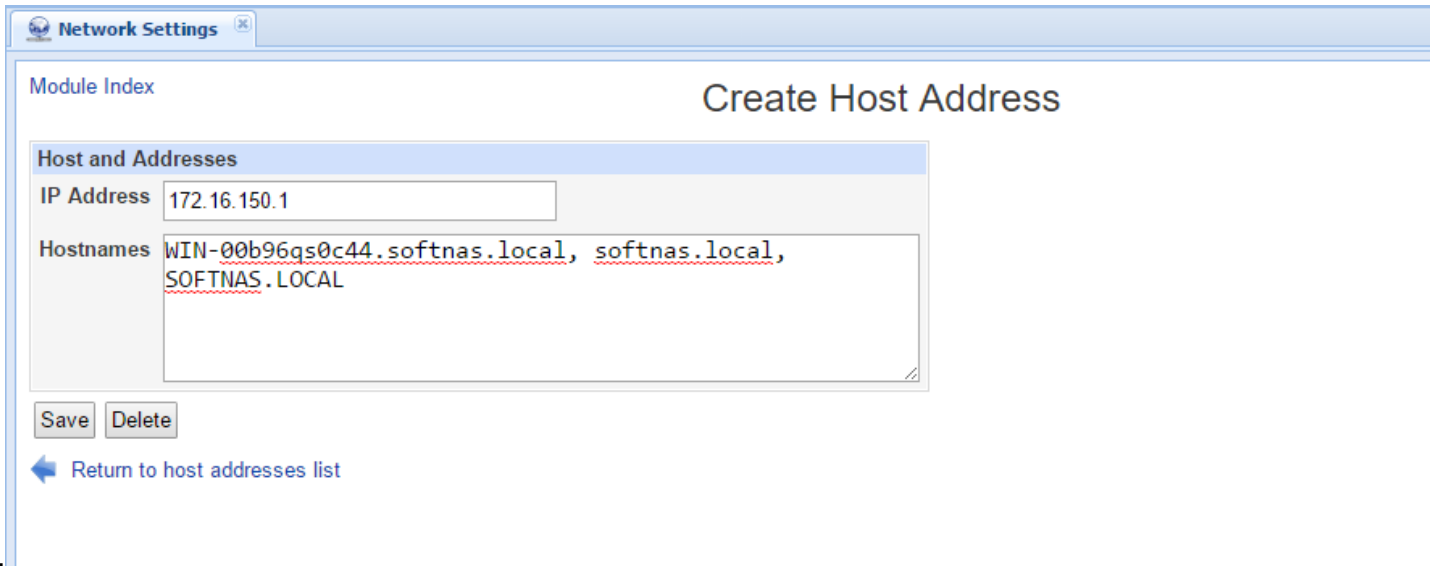
3. Upon clicking Save to set the selected configuration, you will be returned to Network Configuration. Click **Host Addresses**.



4. To create each host table entry, click on the **Add a new host address** link.



5. Fill in the form that appears, then press



Create.

6. Repeat for both the Active Directory and SoftNAS host entries so your final host table looks similar to this:

Select all. | Invert selection. | Add a new host address.

IP Address	Hostnames
<input type="checkbox"/> 127.0.0.1	localhost , localhost.localdomain , localhost4 , localhost4.localdomain4
<input type="checkbox"/> ::1	localhost , localhost.localdomain , localhost6 , localhost6.localdomain6
<input type="checkbox"/> 172.16.150.1	WIN-00B96QSOC44.SOFTNAS.local , softnas.local , SOFTNAS.LOCAL , SOFTNAS
<input type="checkbox"/> 172.16.150.50	softnastest.softnas.local , softnastest , SOFTNASTEST

Select all. | Invert selection. | Add a new host address.

Delete Selected Host Addresses

[Return to network configuration](#)

In the above example, the IP address of the Active Directory controller is 172.16.150.1, so its FQDN is entered (WIN-00B96QSOC44).SOFTNAS.local, along with the "realm" name "SOFTNAS.LOCAL" in lower-case, upper-case and just the domain name "SOFTNAS". The next entry maps the IP address of the SoftNAS Linux host's IP address 172.16.150.50 to FQDN "softnastest.softnasdev.local", "softnastest" and "SOFTNASTEST".

7. Restart the network system to ensure the new DNS resolution rules are in effect.

Note: Anytime you change the DNS or network settings, be sure to either issue a service network restart command as the root user or reboot SoftNAS with a sync; sync; reboot sequence to restart the network subsystem so the new settings will take effect.

8. Verify the host mappings work correctly from a command line (on the SoftNAS host via SSH or a console).

You may also want to verify that your host entries are correct by pinging them with "ping" commands that confirm each mapping is correct. If these host name lookups are incorrect, other steps which follow will fail. Take a moment to verify the host mappings are working as expected for best results.

If you prefer to do this verification via the StorageCenter UI, you can use the following screen to do so. To reach the Command Shell screen, choose **Settings > General System Settings**, which will open a new window with access to the full Webmin console, then choose **Others > Command Shell**.

Be sure to specify the "count" of pings using the "-c 4" switch (or the command will run indefinitely and not return).

Browser address bar: <https://172.16.0.102/webmin/>

Module Config Command Shell

Login: system

- ▶ Webmin
- ▶ System
- ▶ Servers
- ▶ Others
 - Command Shell**
 - Custom Commands
 - File Manager
 - HTTP Tunnel
 - Perl Modules
 - PHP Configuration
 - Protected Web Directories
 - SSH Login
 - System and Server Status
 - Text Login
 - Upload and Download
- ▶ Networking
- ▶ Hardware
- ▶ Cluster
- ▶ Un-used Modules

Search:

- ⚠ View Module's Logs
- 🏠 System Information
- 🔄 Refresh Modules
- 👤 Switch user..

```
> ping 172.16.0.102 c-4
ping: unknown host c-4
> ping 172.16.0.102 -c 4
PING 172.16.0.102 (172.16.0.102) 56(84) bytes of data.
64 bytes from 172.16.0.102: icmp_seq=1 ttl=64 time=0.021 ms
64 bytes from 172.16.0.102: icmp_seq=2 ttl=64 time=0.057 ms
64 bytes from 172.16.0.102: icmp_seq=3 ttl=64 time=0.036 ms
64 bytes from 172.16.0.102: icmp_seq=4 ttl=64 time=0.035 ms

--- 172.16.0.102 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 0.021/0.037/0.057/0.013 ms
```

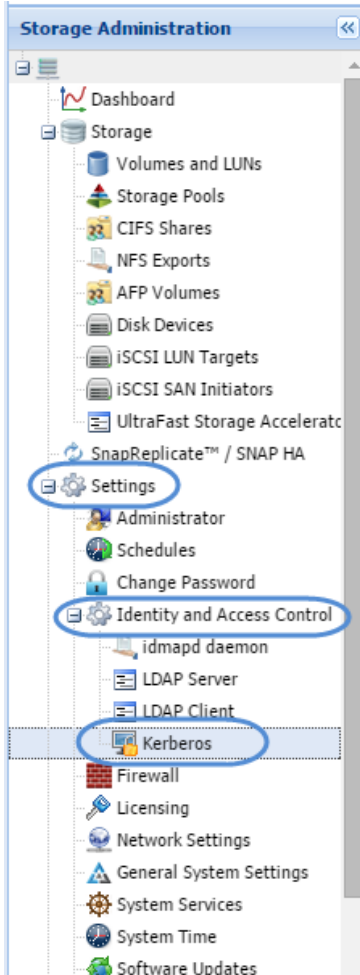
Enter a shell command to execute in the text field below. The cd command may be used to change directory for subsequent commands.

Execute command:

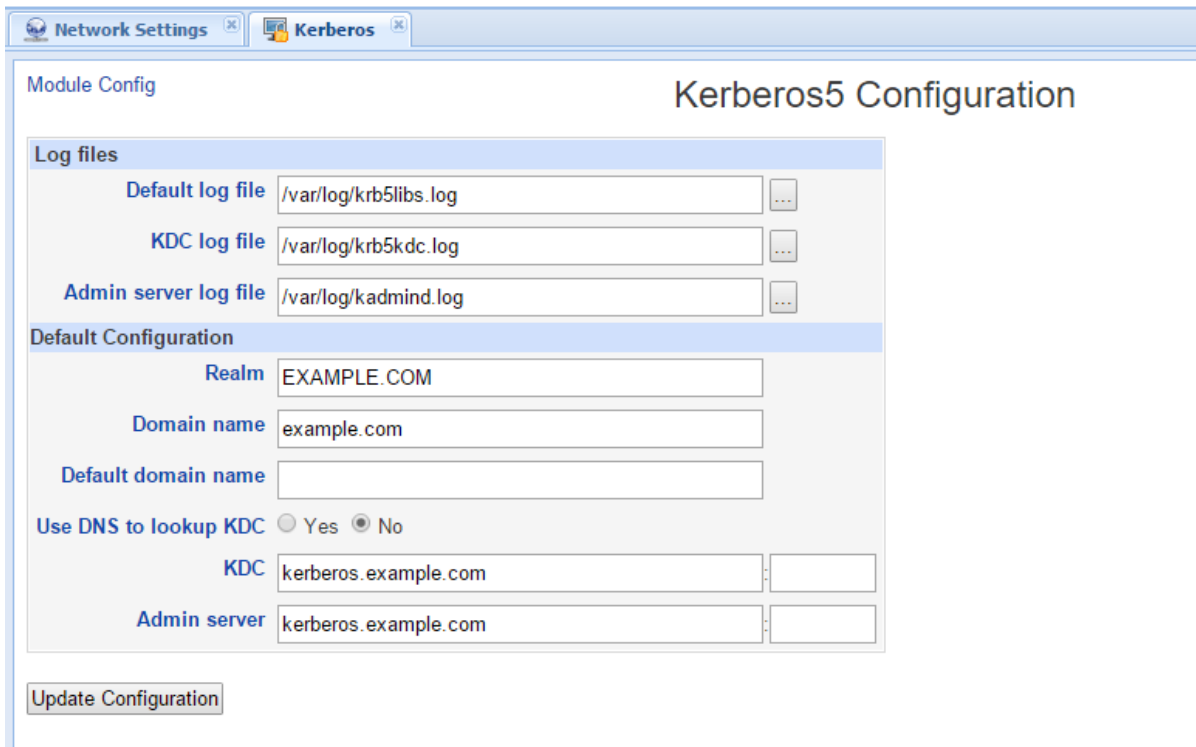
Execute previous command ping 172.16.0.102 -c 4 Edit previous

Configuring Kerberos to Connect to Active Directory

1. Log on to SoftNAS StorageCenter.
2. In the Storage Administration pane on the left, select **Settings > Identity and Access Control > Kerberos**.



The **Kerberos5 Configuration** panel will be displayed.



Module Config Kerberos5 Configuration

Log files

Default log file ...

KDC log file ...

Admin server log file ...

Default Configuration

Realm

Domain name

Default domain name

Use DNS to lookup KDC Yes No

KDC :

Admin server :

3. Enter the the full Active Directory server name in upper case in the **Realm** text entry box; e.g., YOURDOMAIN.COM, MYDOMAIN.LOCAL.

4. Click the **Update Configuration** button.

Verifying Kerberos is Functional

In the above example, SOFTNAS.LOCAL is the full domain name. Log in to a command shell using SSH, SoftNAS Console (VMware) or use the Command Shell. To access the command shell from within the SoftNAS UI, go to **Settings > General System Settings**, which will open a new window with access to the full Webmin console, then choose **Others > Command Shell**.



Once in the command shell, (whichever method you use) issue the following commands:

"kinit" is used to log in as the AD administrator. Note that for best results use the actual domain administrator, not a user with domain admin rights.

```
[root@softnas]# kinit -p administrator
Enter the password for administrator@SOFTNAS.LOCAL
```

Next, list the Kerberos ticket, which proves you successfully logged into AD.

```
[root@softnas]# klist
```

You should see something like:

```
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@SOFTNAS.LOCAL

Valid starting    Expires          Service principal
01/21/13 17:26:12 01/22/13 03:26:20  krbtgt/SOFTNAS.LOCAL@SOFTNAS.LOCAL
renew until 01/22/13 17:26:12
```


Configuring Read Cache and Write Log

SoftNAS Cloud® provides the ability to add **Read Cache** and **Write Log** devices to a storage pool. **Read Cache** provides an additional layer of cache, in addition to RAM memory cache. The **Write Log** provides a cache for incoming writes to be written temporarily to high-speed storage, then later staged to lower-speed spindle-based storage. **SSD** is recommended for both **Read Cache** and **Write Log**.

Important: The **Write Log** becomes a critical element of the storage pool, so it is highly recommended to always use a **RAID 1** mirror for **Write Log** (that way, if a write log device fails, the storage pool won't be at risk of invalidation because the write log is now an integral part of the pool).

Configure Read Cache and Write Log.

1. Click the **Storage Pools** option under the **Storage** section in the **Left Navigation Pane**.

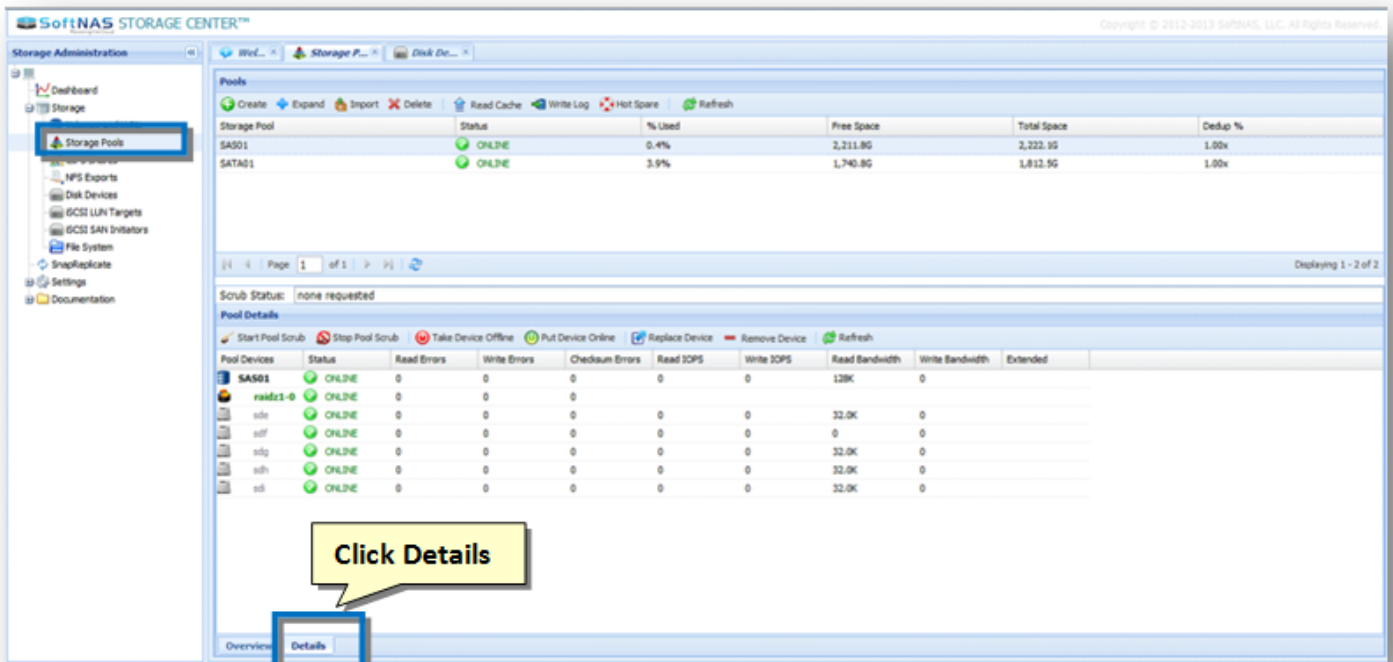
The **Storage Pools** panel will be displayed with the list of all the existing storage pools that are already allocated.

2. Create required storage pools as previously defined.

Creating Storage Pools

3. Verify that disk drives are available that have not been assigned to other storage pools.

Note: These should be high speed drives: SAS or SSD.



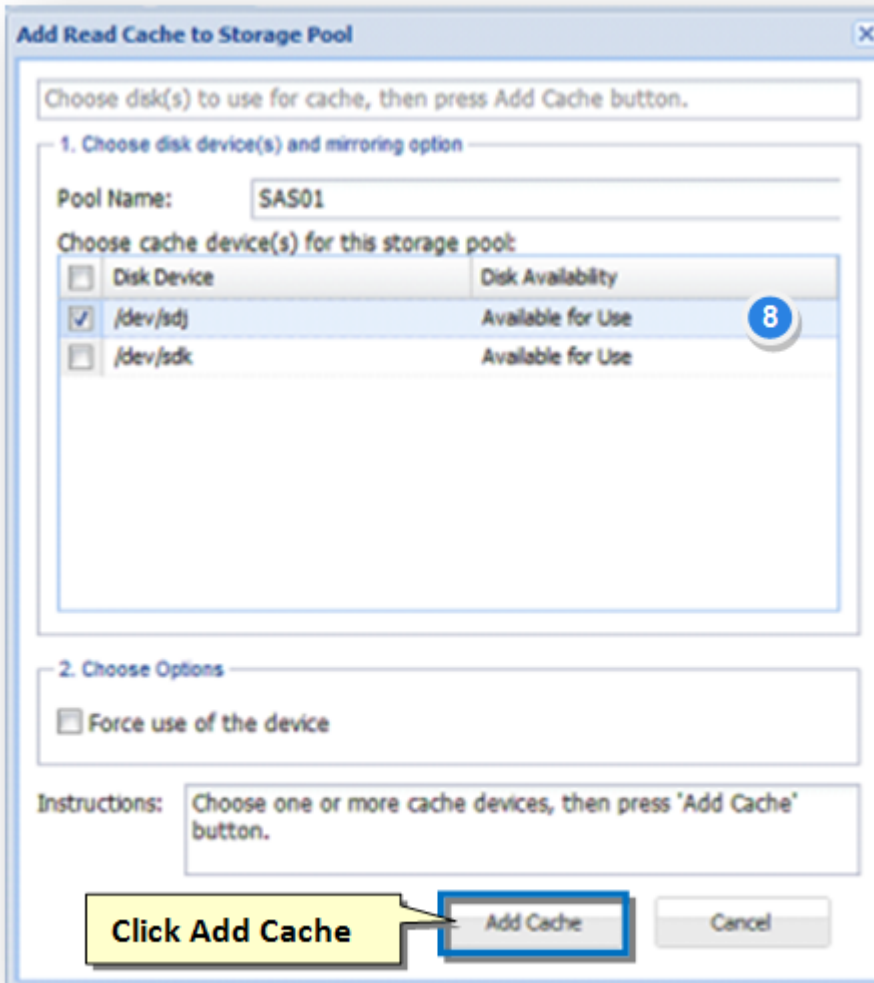
4. On the **Storage Pools** panel, click the **Details** tab in the lower panel.

5. Verify that no log or cache listed under **Pool Devices**.

6. Select the **Storage Pool** to which to add **Read Cache / Write Log**.

7. Click the **Read Cache** option in the toolbar.

The **Add Read Cache to Storage Pool** dialog will be displayed.



8. Select the disk to use for **Read Cache**.

9. Click the **Add Cache** button.

10. For the **Write Log**, select the storage pool and click the **Write Log** option in the toolbar.

Note: Repeat the steps for **Write Log** just like the steps in the **Read Cache**.

View the presence of **Log** and **Cache** devices in the **Storage Pool Detailstab**

The screenshot displays the SoftNAS Storage Center interface. The main area shows the 'Storage Pool Details' for 'SAS01'. The 'Pools' table lists the storage pool and its components. The 'Pool Details' table provides a granular view of each device's status and performance metrics.

Storage Pool	Status	% Used	Free Space	Total Space	Dedup %
SAS01	ONLINE	0.4%	2,211.9G	2,222.1G	1.00x
SATA01	ONLINE	3.9%	1,740.8G	1,812.9G	1.00x

Pool Devices	Status	Read Errors	Write Errors	Checksum Errors	Read IOPS	Write IOPS	Read Bandwidth	Write Bandwidth	Extended
SAS01	ONLINE	0	0	0	0	0	0	0	
raidz1-0	ONLINE	0	0	0	0	0	0	0	
sdg	ONLINE	0	0	0	0	0	0	0	
sdh	ONLINE	0	0	0	0	0	0	0	
sdj	ONLINE	0	0	0	0	0	0	0	
log	ONLINE	0	0	0	0	0	0	0	
cache	ONLINE	0	0	0	0	0	0	0	

How to Migrate Data Disks to a New SoftNAS VM

You may need to migrate data disks, along with their associated storage pools and volumes, from one SoftNAS instance to another. Examples of such cases may be:

- Copy or move data from one SoftNAS VM to a different site or location.
- Copy or move data from one SoftNAS instance on Amazon EC2 to a different region (different data center).
- Restore a data image from backup (not common, but one of the valid use cases one should always be prepared to handle). For example, you may have EBS volume images snapshots saved on Amazon EC2, and want to migrate a backup copy into a new SoftNAS instance.

SoftNAS contains a feature known as Storage Pool Import. The Import feature scans the attached data disks to identify any pools that are currently offline that are eligible to be imported and made active again. This feature is also handy should you ever accidentally delete a pool.

To move one or more storage pools (with its associated volumes) from one SoftNAS instance to another, follow the steps given below.

1. Make sure that there are no active workloads on NFS shares, CIFS shares or iSCSI targets making use of the storage pool and volumes.

Note: Do not attempt to move a volume that's active or data loss could occur.

2. Detach the inactive disk devices from the SoftNAS VM or EC2 instance.

- On Amazon EC2, use the Detach option for each EBS volume that you want to move. Refer to the Attaching and Detaching Volumes section for more information.
- On VMware, remove each virtual hard disk from the VM using the Settings dialog.

3. Copy or move the disks (as appropriate) to the destination (if required).

4. Attach the disk devices to the new SoftNAS VM or EC2 instance.

- On Amazon EC2, use the Attach option for each EBS volume. Refer to the Attaching and Detaching Volumes section for more information.
- On VMware, add each virtual hard disk to the VM using the Settings dialog

5. Log into the destination SoftNAS StorageCenter user-interface.

6. In the Left Navigation Pane, select the Storage Pools option under the Storage section.

7. Click the Import option in the toolbar.

The **Import Pools** dialog will be displayed.

It has two sections labeled **Deleted Pools Available for Import** and **Foreign Pools Available for Import**.

The **Foreign Pools** listed (if any are present) are storage pools created on a different SoftNAS system.

8. If the pools are ready to import, there will be a button labeled **Import <poolname>**, where poolname will be the pool that's available to import. Click that button.

9. You will need to select the **Force Import** checkbox, to force the system to import foreign pools from another system.

10. For each volume, configure the volume's **Snapshots** to use the desired schedule.

Note: They are not imported automatically, but can be manually copied from the old system by copying the **snapshots.ini** and **schedules.ini** files in the **/var/www/softnas/snsnserver** folder.

11. For each NFS and CIFS share you want, create the appropriate NFS exports and CIFS shares (they are not imported automatically.)

12. For each iSCSI target (if any), define the appropriate iSCSI devices and targets.

Note: They are not imported automatically, but can be manually copied from the old system by copying the **file / etc/tgt/targets.conf** to the new system, then restart the iSCSI Server.

The data disks will now be ready for use.

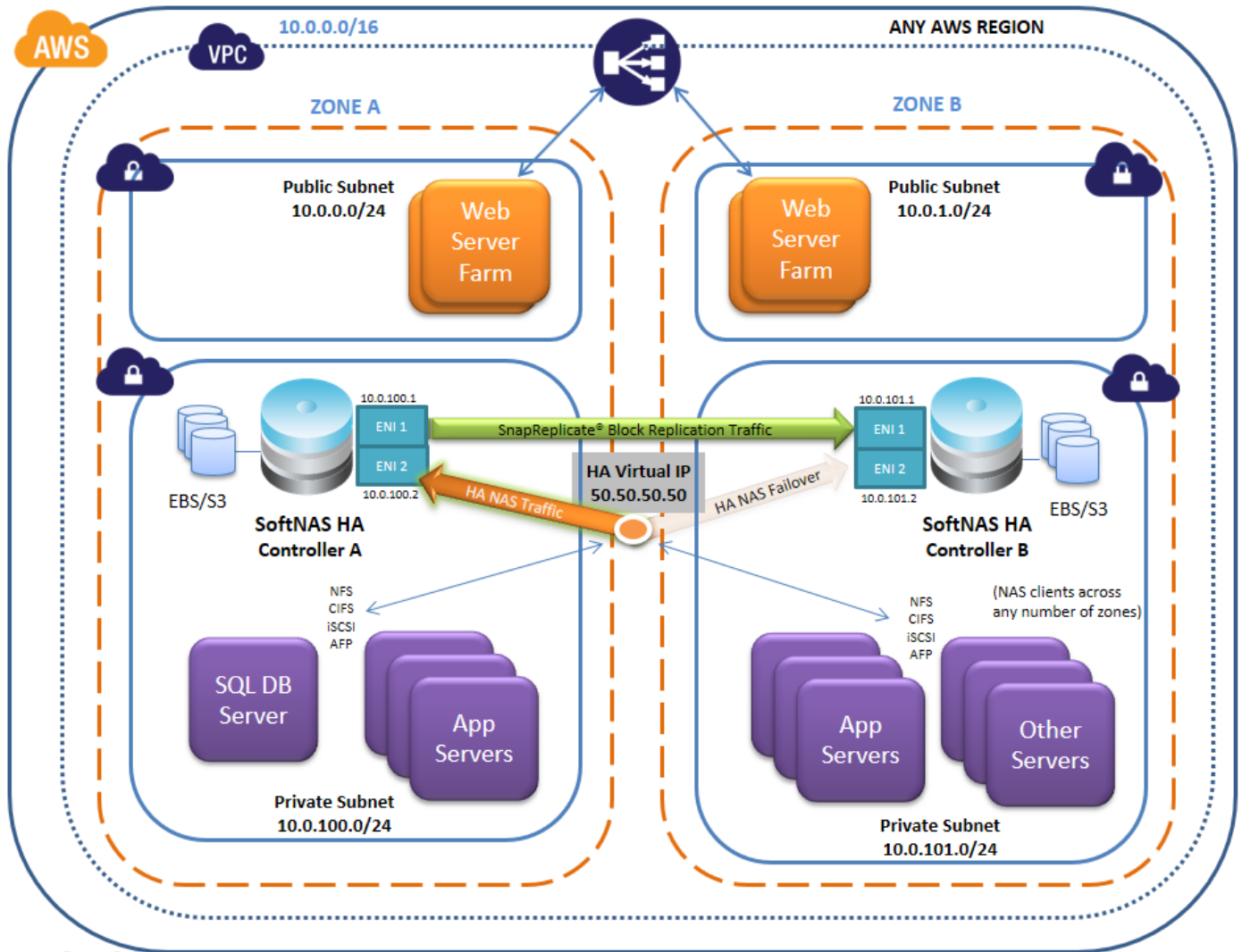
13. Click the **Refresh** button on the **Storage Pools** panel.

14. Similarly, navigate to the **Volumes and LUNs** panel and view the volumes.

Setting Up SnapReplicate and SNAP HA™

About SoftNAS SnapReplicate and SNAP HA™

Setting up **SnapReplicate** provides replication of data between **SoftNAS Cloud®** instances for greater redundancy. **SNAP HA™**, on the other hand, adds an additional layer of protection by providing load balancing between **SoftNAS Cloud®** instances.



For in-depth information on **SoftNAS High Availability** functions, consult [SoftNAS High Availability Guide](#)

Overview

The following are required for a successful **SNAPReplicate** and **SNAP HA™** setup.

If setting up SNAPReplicate using Elastic IP addresses:

- Create virtual network (public and private subnets)
- Deploy 2 instances into the private subnets (into different regions for greater redundancy)

If setting up SNAPReplicate using Virtual IP addresses:

- Create virtual network (create separate private subnets.)
- Deploy 2 instances into the private subnets (into different regions for greater redundancy)

[Launching SoftNAS Cloud® Platforms](#)

- Configure **SoftNAS SnapReplicate**.

Setting Up For SnapReplicate

The following is required for a standard **SoftNAS SnapReplicate** and **SNAP HA™** implementation:

If setting up SNAPReplicate using Elastic IP addresses:

- Create virtual network (public and private subnets)
- Deploy 2 instances into the private subnets (into different regions for greater redundancy)

If setting up SNAPReplicate using Virtual IP addresses:

- Create virtual network (create separate private subnets.)
- Deploy 2 instances into the private subnets (into different regions for greater redundancy).

[Launching SoftNAS Cloud® Platforms](#)

- Configure **SnapReplicate** and **SNAP HA™** using **SoftNAS StorageCenter**.

Configuring StorageCenter

Once the **StorageCenter** interface has been accessed, set up the [Disk Devices](#), [Storage Pools](#), and [Volumes](#) that will be required for HA.

[SoftNAS Cloud® Configuration](#)

Note: When setting up storage pools for replication, they have to have the same name. Otherwise, replication will not work properly. Also, create a volume on the source-side node.

For more in depth setup information on setting up SnapReplicate, see [SnapReplicate](#).

To review how to set up SNAP HA™, see [SNAP HA™](#).

SnapReplicate

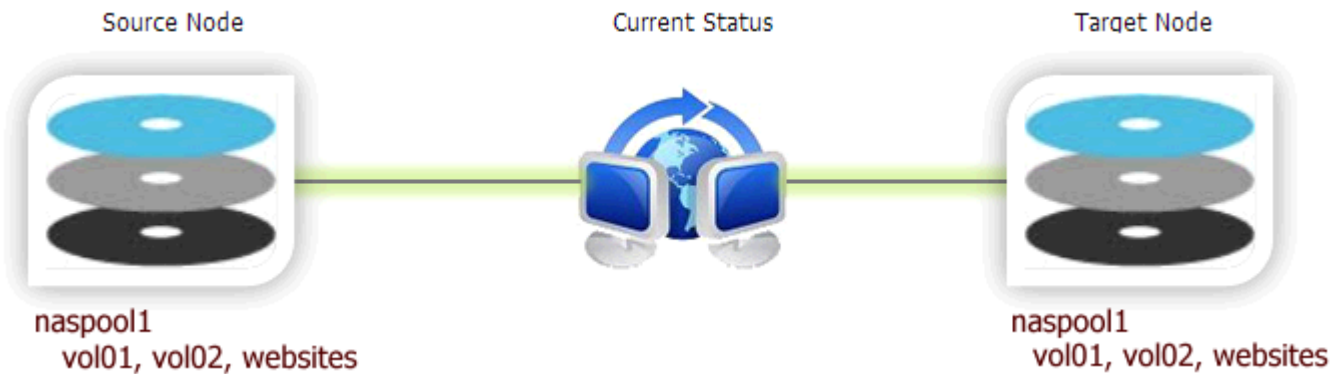
Preparing the SnapReplicate Environment

The first step in preparing a **SnapReplicate** deployment is to install and configure two **SoftNAS Cloud®** controller nodes. Each node should be configured with a common set of storage pools with the same pool names.

Note: Only storage pools with the same name will participate in **SnapReplicate**. Pools with distinct names on each node will not be replicated.

For best results, it is recommended (but not required) that pools on both nodes be configured identically (or at least with approximately the same amount of available total storage in each pool).

In the following example, we have a storage pool named **naspool1** on both the nodes, along with three volumes: **vol01**, **vol02** and **websites**. In such cases, the **SnapReplicate** will automatically discover the common pool named **naspool1** on both nodes, along with the source pool's three volumes, and will auto-configure the pool and its volumes for replication. This means you do **not** have to create duplicate volumes (**vol01**, **vol02**, and **websites**) on the replication target side, as **SnapReplicate** will perform this action.



Other important considerations for the **SnapReplicate** environment include:

- Network path between the nodes
- NAT and firewall paths between the nodes (open port 22 for SSH between the nodes)
- Network bandwidth available and whether to configure throttling to limit replication bandwidth consumption

Note that **SnapReplicate** creates a secure, two-way SSH tunnel between the nodes. Unique 2048-bit RSA public/private keys are generated on each node as part of the initial setup. These keys are unique to each node and provide secure, authenticated access control between the nodes. Password-based SSH logins are disabled and not permitted (by default) between two **SoftNAS** nodes configured with **SnapReplicate**. Only PKI certificate-based authentication is allowed, and only from **known hosts** with pre-approved source IP addresses; i.e., the two **SnapReplicate** nodes (and the configured administrator on **Amazon EC2**).

After initial setup, SSH is used for command and control. SSH is also used (by default) as a secure data transport for authenticated, encrypted data transmission between the nodes.

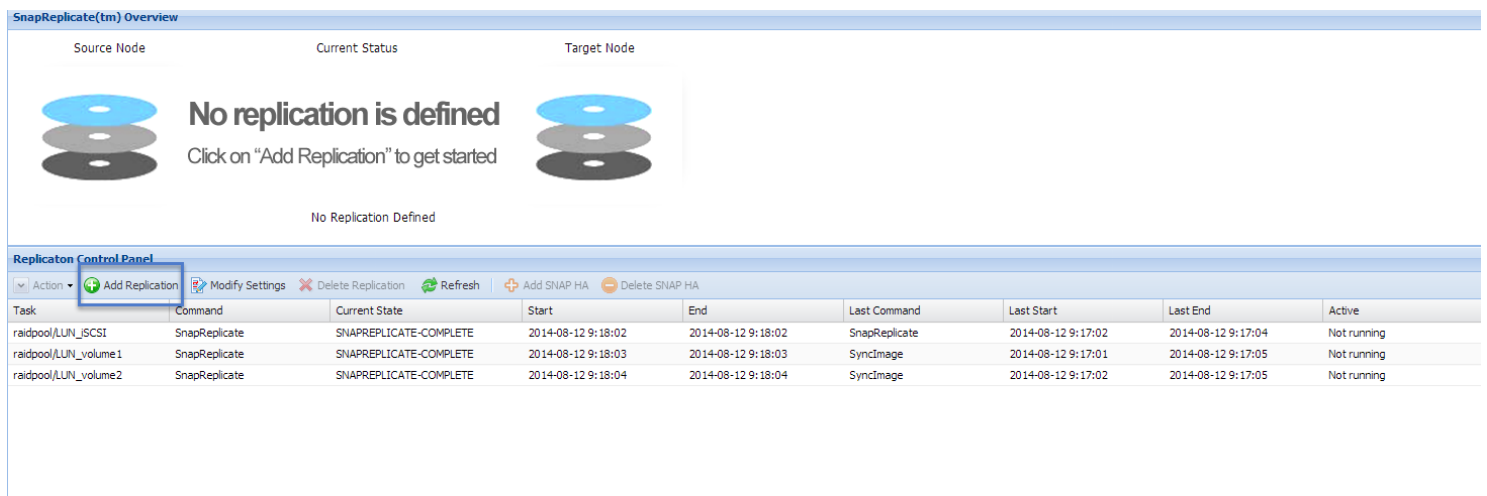
Establishing a SnapReplicate Relationship

Be prepared with the IP address (or DNS name) of the target controller node, along with the **SoftNAS StorageCenter** login credentials for that node.

To establish the secure **SnapReplicate** relationship between two **SoftNAS Cloud®** nodes, simply follow the steps given below.

1. Log into the source controller's **SoftNAS StorageCenter** administrator interface using a web browser.
2. In the **Left Navigation Pane**, select the **SnapReplicate** option.

The **SnapReplicate** page will be displayed.



SnapReplicate(tm) Overview

Source Node Current Status Target Node

No replication is defined
Click on "Add Replication" to get started

No Replication Defined

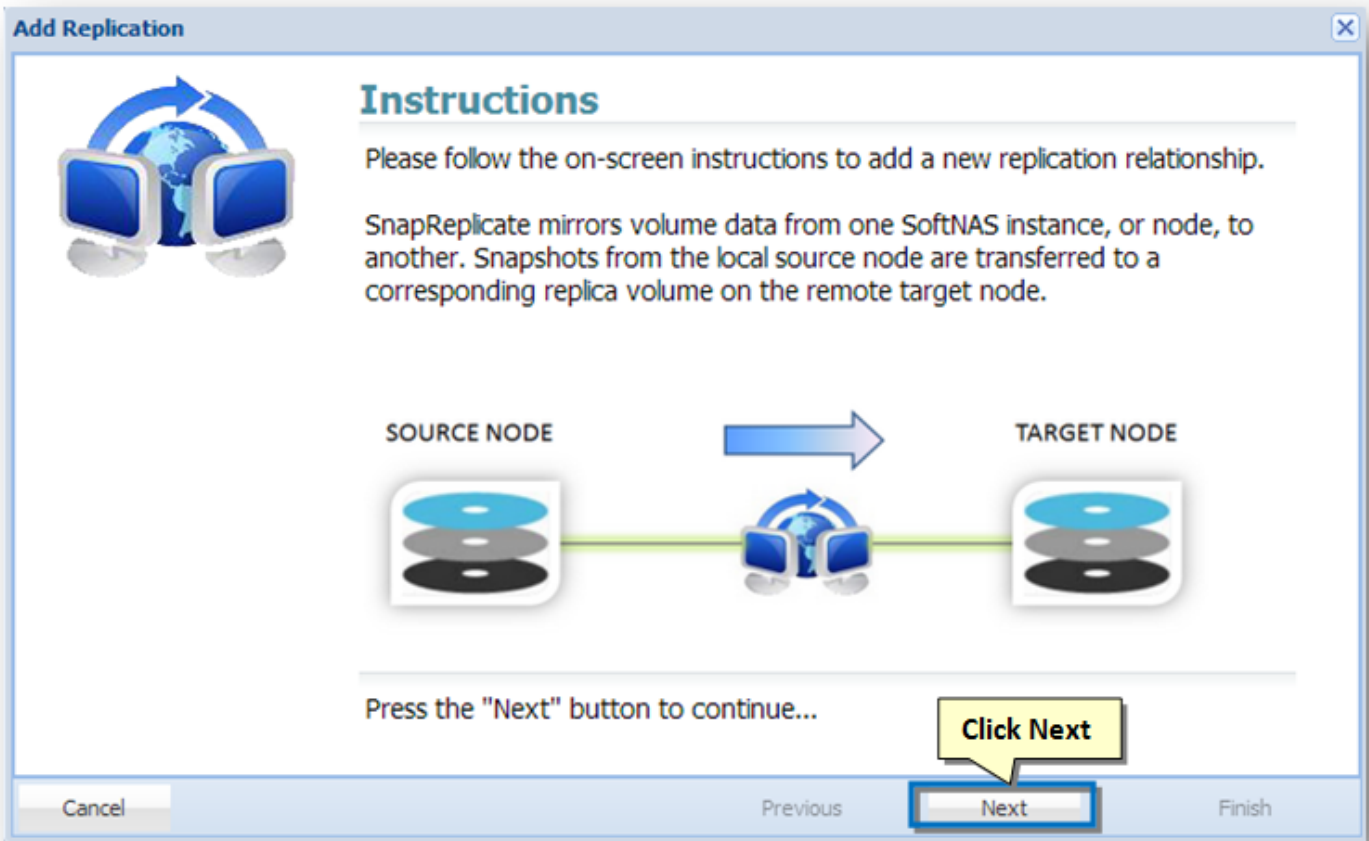
Replication Control Panel

▼ Action
➕ Add Replication
⚙️ Modify Settings
✖ Delete Replication
🔄 Refresh
➕ Add SNAP HA
➖ Delete SNAP HA

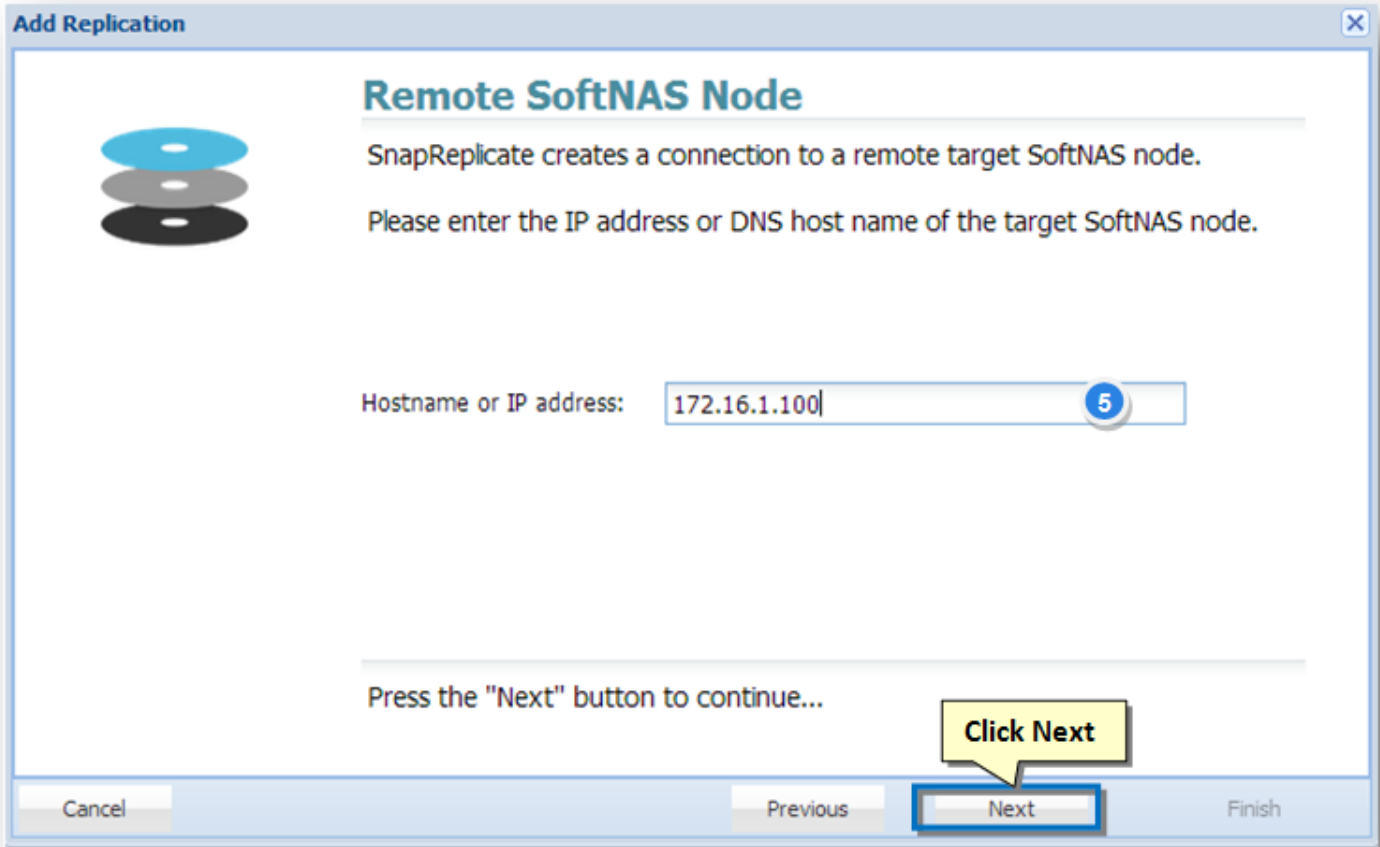
Task	Command	Current State	Start	End	Last Command	Last Start	Last End	Active
raidpool/LUN_ISCSI	SnapReplicate	SNAPREPLICATE-COMPLETE	2014-08-12 9:18:02	2014-08-12 9:18:02	SnapReplicate	2014-08-12 9:17:02	2014-08-12 9:17:04	Not running
raidpool/LUN_volume1	SnapReplicate	SNAPREPLICATE-COMPLETE	2014-08-12 9:18:03	2014-08-12 9:18:03	SyncImage	2014-08-12 9:17:01	2014-08-12 9:17:05	Not running
raidpool/LUN_volume2	SnapReplicate	SNAPREPLICATE-COMPLETE	2014-08-12 9:18:04	2014-08-12 9:18:04	SyncImage	2014-08-12 9:17:02	2014-08-12 9:17:05	Not running

3. Click the **Add Replication** button in the **Replication Control Panel**.

The **Add Replication** wizard will be displayed.



4. Read the instructions on the screen and then click the **Next** button.



5. In the next step, enter the IP address or DNS name of the remote, target **SoftNAS Cloud®** controller node in the **Hostname or IP Address** text entry box. Note that by specifying the replication target's IP address, you are specifying the network path the SnapReplicate traffic will take.

There are two ways to set up AWS EC2 nodes for high availability. Previously, only Elastic IPs could be used. Private HA is now supported, using Virtual IPs. A Virtual IP is a HUMAN ALLOCATED IP address outside of the CIDR (Classless Inter-Domain Routing) range. For example, if you have a VPC CIDR range of 10.0.0.0/16, one can use 20.20.20.20. This will then be added to the VPC Route Table, and will be pointed to the ENI device (NIC) of one of the SoftNAS HA Nodes. A private high availability setup is recommended, as it allows you to host your HA setup entirely on an internal network, without a publically accessible IP. In order to access your high availability EC2 cluster, an outside party would need to access your network directly, via a jumpbox, or VPN, or other solution. This is inherently more secure than a native Elastic IP configuration.

To connect the nodes, the source node must be able to connect via HTTPS to the target node (similar to how the browser user logs into **StorageCenter** using HTTPS). HTTPS is used to create the initial **SnapReplicate** configuration. Next, several SSH sessions are established to ensure two-way communications between the nodes is possible. SSH is the default protocol that is used for **SnapReplicate** for replication and command/control.

Whether using a Virtual or Elastic IP setup to create a **SnapReplicate** relationship between two EC2 nodes, the source node must be able to connect via HTTPS to the target node (similar to how the browser user logs into **StorageCenter** using HTTPS). HTTPS is used to create the initial **SnapReplicate** configuration. Next, several SSH sessions are established to ensure two-way communications between the nodes is possible. SSH is the default protocol that is used for **SnapReplicate** for replication and command/control. When connecting two **Amazon EC2** nodes, **use the internal instance IP addresses** (not the the human allocated virtual IP outside the CIDR range mentioned above, or the Elastic IP, which is a public IP). That's because the traffic gets routed internally by default between instances in EC2 by default. Be sure to put the internal IP addresses of both EC2 instances in the Security Group to enable both HTTPS and SSH communications between the two nodes.

To view the internal IP address of each node, from the EC2 console, select **Instances**, then select the instance - the **Private IPs** entry shows the instance's private IP address used for **SnapReplicate**.

For example:

Node 1 - Virginia, East (zone 1-a) Private IP: 10.120.1.100 (initial source node)

Node 2: Virginia, East (zone 1-b) Private IP: 10.39.270.23 (initial target node)

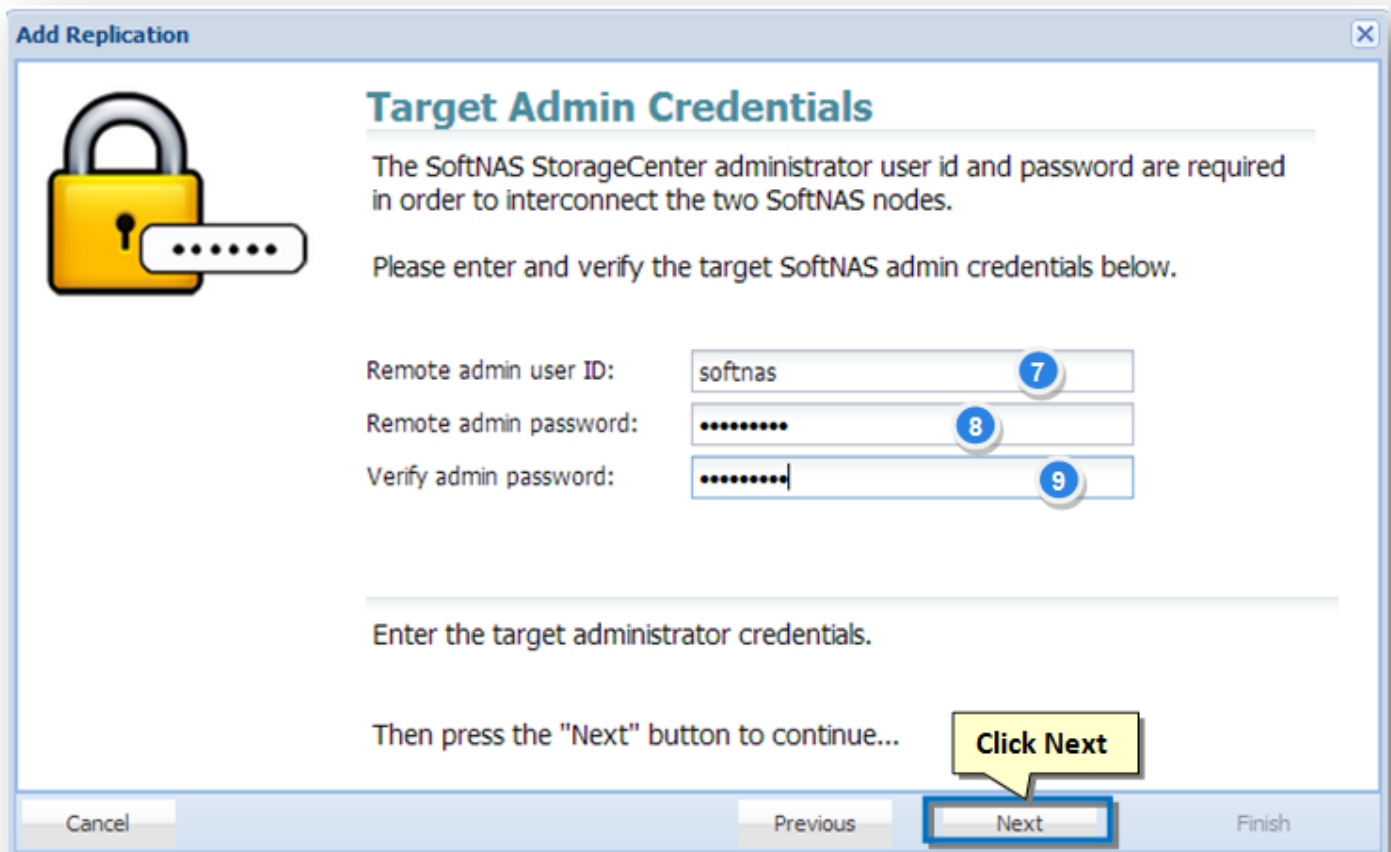
Add the following Security Group entries:

Type	Security Group Entry
SSH	10.120.1.100/32
SSH	10.39.270.23/32
HTTPS	10.120.1.100/32
HTTPS	10.39.270.23/32

VMware: Similarly, it is important to understand the local network topology and the IP addresses that will be used - internal vs. public IP addresses when connecting the nodes. ALWAYS USE THE **INTERNAL/PRIVATE IP ADDRESS**.

6. Click the **Next** button.

In the next step, provide the target node's admin credentials.



Add Replication

Target Admin Credentials

The SoftNAS StorageCenter administrator user id and password are required in order to interconnect the two SoftNAS nodes.

Please enter and verify the target SoftNAS admin credentials below.

Remote admin user ID: 7

Remote admin password: 8

Verify admin password: 9

Enter the target administrator credentials.

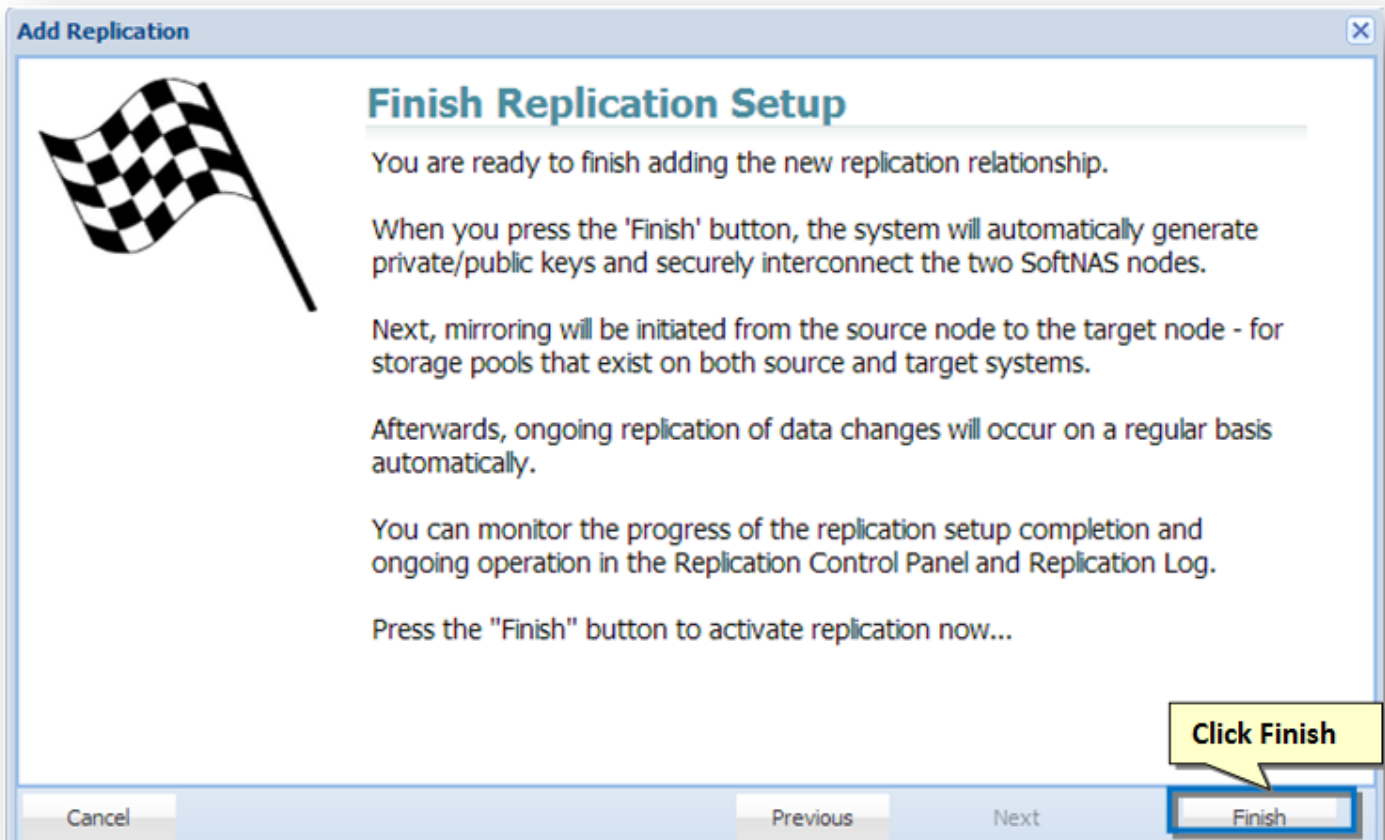
Then press the "Next" button to continue...

Click Next

Cancel Previous **Next** Finish

7. Enter the administrator's email id for the target node in the **Remote Admin User ID** text entry box.
8. Enter the administrator's password for the target node in the **Remote Admin Password** text entry box.
9. Re-enter the administrator's password for the target node to confirm the same, in the **Verify Admin Password** text entry box.
10. Click the **Next** button.

The IP address/DNS name and login credentials of the target node will be verified. If there is a problem, an error message will be displayed. Click the **Previous** button to make the necessary corrections and then click the **Next** button to continue.



11. In the next step, read the final instructions and then click the **Finish** button.

The **SnapReplicate** relationship between the two **SoftNAS Cloud®** controller nodes will be established. The corresponding **Synclmage** of the **SnapReplicate** will be displayed.

The **Synclmage** compares the storage pools on each controller, looking for pools with the same name. For example, let's say we have a pool named "naspool1" configured on each node. Volume discovery will automatically add all volumes in "naspool1" from the source node to the replication task list.


For each volume added as a **Synclmage** task, that volume will be created on the target node (if it exists already, it will be deleted and re-created from scratch to ensure an exact replica will be created as a result of **Synclmage**). The **Synclmage** then proceeds to create exact replicas of the volumes on the target.

After data from the volumes on the source node is mirrored to the target, once per minute **SnapReplicate** transfers keep the target node **hot** with data block changes from the source volumes.

The tasks and an event log will be displayed in the **SnapReplicate Control Panel** section.


SnapReplicate(tm) Overview

Source Node




10.61.175.18

Current Status









Source Node (Primary)

Target Node



10.218.173.74

Replicaton Control Panel

Action ▾
 Add Replication
 Modify Settings
 Delete Replication
 Refresh
 Add SNAP HA
 Delete SNAP HA

Task	Command	Current State	Start	End	Last Command	Last Start	Last End	Active
raidpool/LUN_ISCSI	SyncImage	MIRROR-COMPLETE	2014-08-12 9:20:20	2014-08-12 9:20:21				Not running
raidpool/LUN_volume1	SyncImage	MIRROR-COMPLETE	2014-08-12 9:20:21	2014-08-12 9:20:23				Not running
raidpool/LUN_volume2	SyncImage	MIRROR-COMPLETE	2014-08-12 9:20:22	2014-08-12 9:20:23				Not running

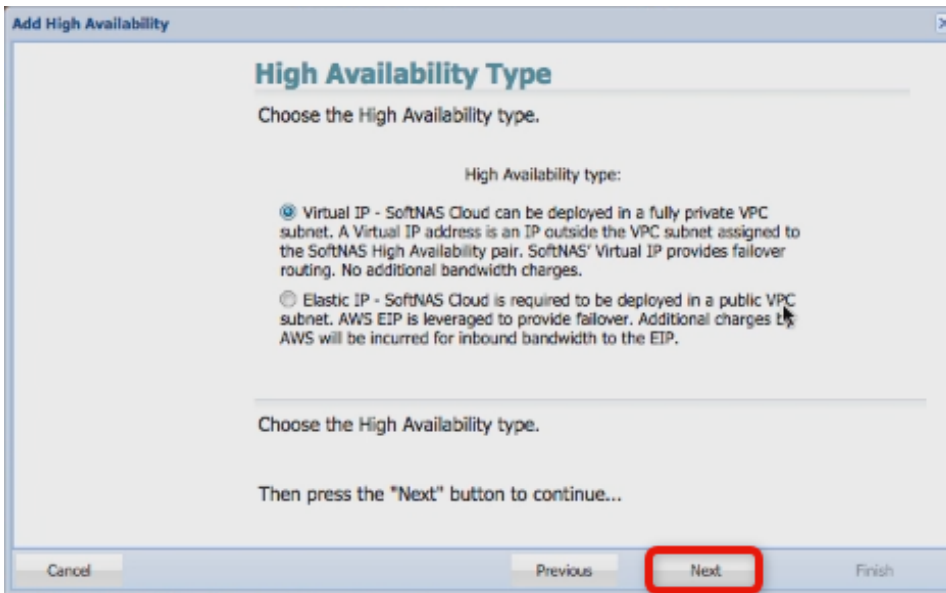
This indicates that a **SnapReplicate** relationship is established and the replication should be taking place.

SNAP HA™

Before setting up SNAP HA™, set up SnapReplicate according to the guidance in [Setting up SnapReplicate](#). For more detailed setup instructions, check [SNAPReplicate](#).

Setting Up SNAP HA™

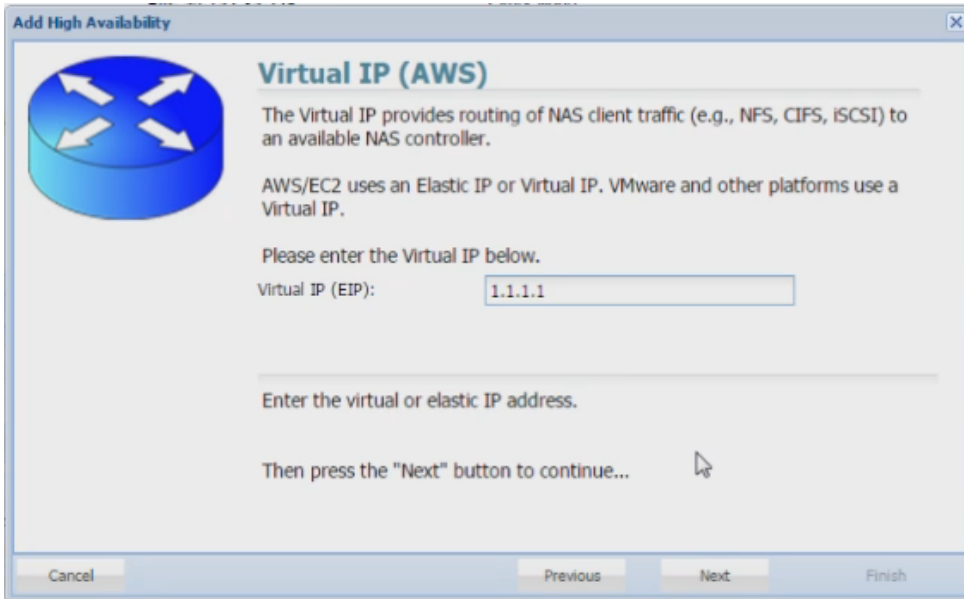
1. From the **SoftNAS SnapReplicate** panel, click on **Add SNAP HA™**.
2. Click **Next** on the Welcome screen.
3. Select the type of High Availability type to be used.



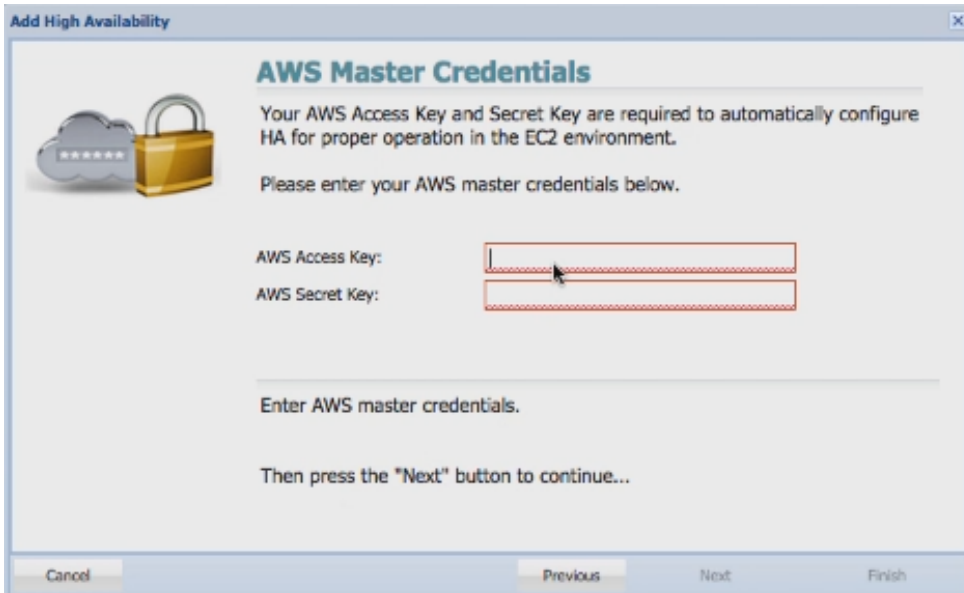
- **Virtual IPs:** SoftNAS Cloud® is now deployable in a fully private VPC subnet. This configuration has two advantages - no public facing IP addresses makes storage more secure, and no inbound bandwidth charges from AWS. This is the recommended setup for a more secure deployment.

- **Elastic IPs:** This is the traditional method of connecting AWS SNAP HA™. If using EIPs, SoftNAS Cloud® can only be deployed in a public VPC subnet. AWS EIPs are leveraged to provide failover. Additional charges by AWS are incurred for inbound bandwidth.

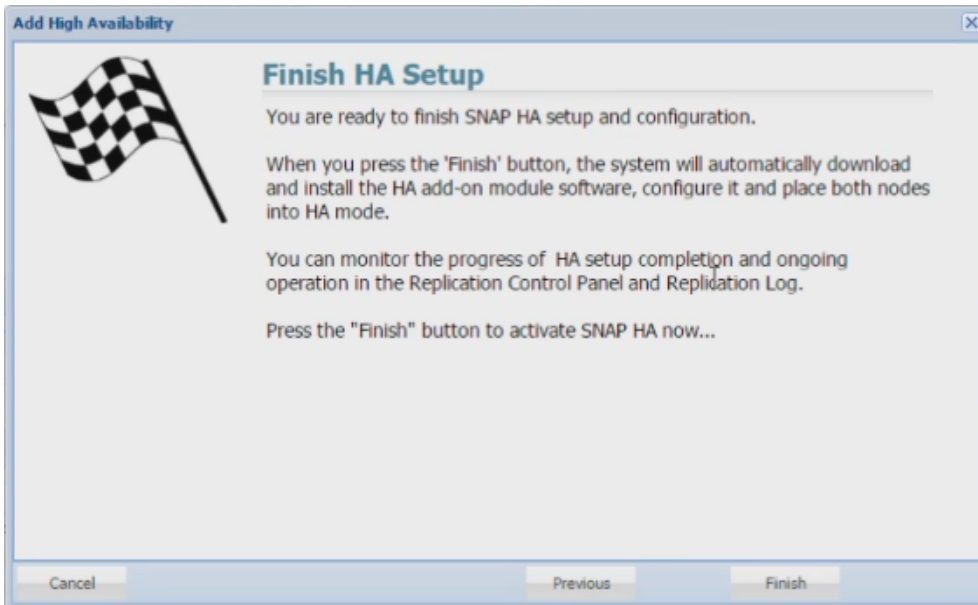
4. Add the Elastic or Virtual IPs of both the primary and secondary instances when prompted by the **SnapReplicate** interface. As the Virtual IP option is recommended, it is shown below. The screen will be nearly identical for Elastic IPs. When creating your Virtual IP, be sure that the IP chosen lies outside the chosen CIDR block selected for the two replication nodes.



5. Provide the administrator credentials if prompted.



6. Click on **Finish**.



At this point **SoftNAS Cloud®** will do all of the heavy lifting that is required to establish HA, without the need for any user intervention. The process may take several minutes. After completion, the High Availability **SoftNAS Cloud®** pair has been successfully set up across Availability Zones.

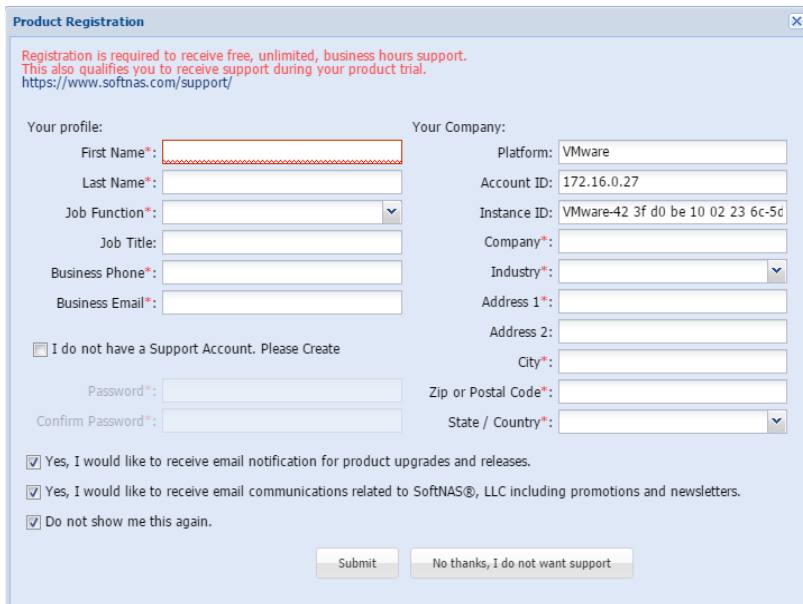
Registering SoftNAS Cloud®

Optimized Support

Registering the **SoftNAS Cloud®** product provides access to free, unlimited support during business hours. multiple levels of support services to meet all levels of storage management needs. Upon initial sign-in, a pop-up will prompt the user for account information required for support levels. Consult [SoftNAS Support Page](#) for the most up-to-date information on support levels.

Registration Details

On the seventh day after deployment, the customer will be prompted to register their SoftNAS instance. The prompt will appear as shown below. While he or she is not prompted after deployment, the user can register at any time by clicking the red link in the upper right corner. If you do not register after seven days, the prompt to register will begin to appear upon each login. However, you can select the **"Do not show me this again"** option to prevent future registration prompts. Remember though, that foregoing registration means you will not receive our free, unlimited business hours support. The red asterisks (*) denote fields required for a successful registration; this menu may be returned to later. The business email address entered here will be the contact information used for **SoftNAS Cloud®** [monitoring reports](#).



Product Registration

Registration is required to receive free, unlimited, business hours support.
This also qualifies you to receive support during your product trial.
<https://www.softnas.com/support/>

Your profile:		Your Company:	
First Name*:	<input type="text"/>	Platform:	<input type="text" value="VMware"/>
Last Name*:	<input type="text"/>	Account ID:	<input type="text" value="172.16.0.27"/>
Job Function*:	<input type="text"/>	Instance ID:	<input type="text" value="VMware-42 3f d0 be 10 02 23 6c-5c"/>
Job Title:	<input type="text"/>	Company*:	<input type="text"/>
Business Phone*:	<input type="text"/>	Industry*:	<input type="text"/>
Business Email*:	<input type="text"/>	Address 1*:	<input type="text"/>
<input type="checkbox"/> I do not have a Support Account. Please Create		Address 2:	<input type="text"/>
Password*:	<input type="text"/>	City*:	<input type="text"/>
Confirm Password*:	<input type="text"/>	Zip or Postal Code*:	<input type="text"/>
		State / Country*:	<input type="text"/>

Yes, I would like to receive email notification for product upgrades and releases.
 Yes, I would like to receive email communications related to SoftNAS®, LLC including promotions and newsletters.
 Do not show me this again.

Manual Registration Request

To return to the registration window after bypassing it at login, or to register immediately (prior to the prompts provided on the seventh day and thereafter), click the hyperlink at the top right of the **StorageCenter** UI for **Product Registration**.

Note: Once the product has been successfully registered, this button will be disabled. Make use of the **Feature Request** hyperlink for product suggestions.

The screenshot displays the SoftNAS Cloud administration interface. On the left is a navigation menu with the following items: Dashboard, Storage, Volumes and LUNs, Storage Pools, CIFS Shares, NFS Exports, AFP Volumes, Disk Devices, iSCSI LUN Targets, iSCSI SAN Initiators, SnapReplicate™ / SNAP HA, Settings, Documentation, and Log out. The main header area contains the text 'SoftNAS Cloud®, version 3.4.0 host SoftNAS'. To the right of the header are two buttons: 'Product Registration - unregistered product' and 'Feature Request'. Two callout boxes are present: one labeled 'Product Registration' pointing to the first button, and another labeled 'Feature Request' pointing to the second button.

Microsoft Azure

Overview

Microsoft Azure is an Internet-scale computing and services platform hosted in data centers managed or supported by Microsoft. It includes many separate features with corresponding developer services which can be used individually or collaboratively.

SoftNAS Cloud® provides the network storage backbone needed for business critical cloud applications.

SoftNAS Cloud® for Microsoft Azure leverages the underlying storage devices of Azure. Multiple devices are then organized into RAID configurations, increasing performance and throughput, and providing the ability to recover from underlying physical disk failures. **SoftNAS Cloud®** provides the most durable, highest performance NAS solution available for **Microsoft Azure**, and is the only Azure storage product that supports up to 16 PB of Blob storage and high availability with a **No Downtime Guarantee SLA**.

Product and Installation Options

SoftNAS Cloud® provides the following applicable products:

- SoftNAS Cloud® **Express** (1TB of storage)
- SoftNAS Cloud® **Standard** (16 PB of storage)*
- SoftNAS Cloud® **BYOL** (Bring Your Own License)

Product	Storage	Purchase	License
SoftNAS Cloud® Express	1 TB	Subscribe via Azure Marketplace .	Embedded in platform subscription or BYOL available from SoftNAS .
SoftNAS Cloud® Standard	16 PB	Subscribe via Azure Marketplace .	Embedded in platform subscription or BYOL available from SoftNAS .

- SoftNAS SNAP HA™ included with each product.

*When leveraging Azure Blob storage and multiple blob storage accounts.

	Recommended	Configuration Note
Compute		
General Purpose	DS4v2 Standard / 8 cores	Standard: A good starting point in regards to memory and CPU resources. This category is suited to handle the processing and caching with minimal requirements for network bandwidth.
High	DS5v2 Standard / 16 cores	Medium: Good for workloads that are read intensive and will benefit from the larger memory-based read cache for this category. The additional CPU will also provide better performance when deduplication, encryption, compression and/or RAID is enabled.
Extreme	DS15v2 / 20 cores	High: This category can be used for workloads that require a very high speed network connection due to the amount of data transferred over a network connection. In addition to the very high speed network, this level of instance gives you a lot more storage, CPU and memory capacity.
Memory		
Base RAM - General Purpose	28 GB /DS4v2 Standard/ Premium	Premium or Standard storage
Base RAM - High	56 GB /DS5v2 Standard/ Premium	Premium or Standard storage
Base RAM - Extreme	140GB / DS15v2 Standard/ Premium	Local SSD, large-scale use with increased RAM caching, premium or standard storage
Additional RAM	1 GB per 1 TB of deduplicated storage. e.g.: 50 TB deduplicated storage = 50 *additional* GB for deduplication tables for best performance.	Recommended for best performance
Storage		
Boot Disk	30 GB Hard disk for Linux boot and system disk (included)	
Data Disk - General	Standard Azure Data Disks (DS Standard Series)	
High IOPS	Azure Premium Storage (DSv2 Standard Series)	
RAID 10	Recommended for I/O-intensive applications and databases	
RAID 5/6	Recommended for best space utilization (tradeoff: slower write performance)	
Network		
Up to 120 MB/sec - 1GbE	Less overhead cost	
500+ MB/sec - 10 GbE	Better performance (requires more resources)	Consider MTU 4000 configuration for optimal performance

Note: As of version 3.4.8 SoftNAS does not support launching SoftNAS Cloud VMs on the classic portal. The Azure Resource Manager (ARM) is the only supported platform.

SoftNAS Cloud® System Capacities

Listed below is a table representing the capabilities of the **SoftNAS Cloud®** for **Microsoft Azure**.

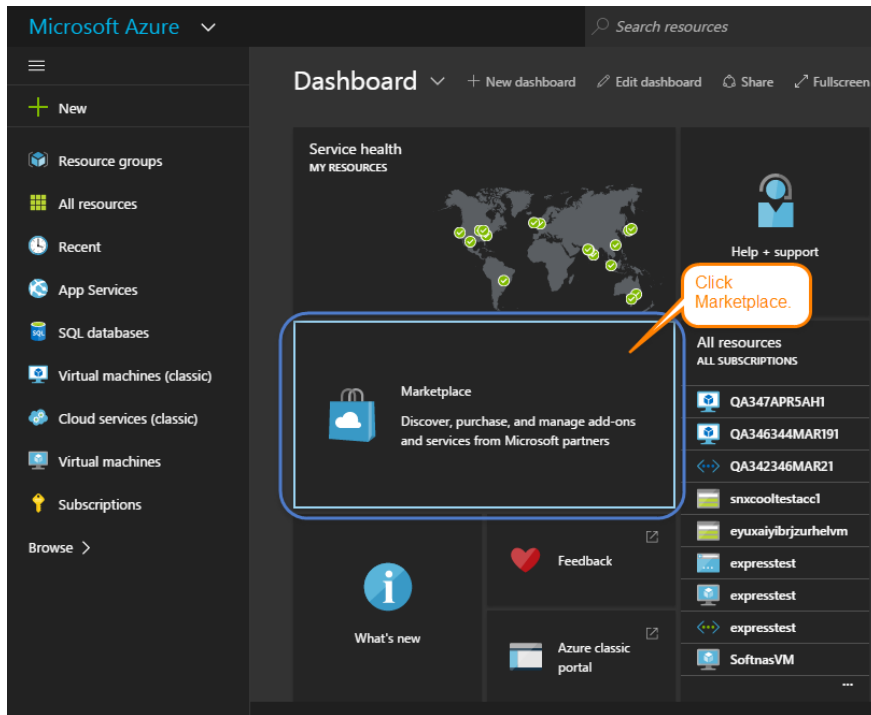
	SoftNAS Cloud® Capacity	Configuration Note
Editions		
SoftNAS Cloud® Express	1TB	Available as Azure subscription and BYOL from SoftNAS .
SoftNAS Cloud® Standard	16 PB	Available as Azure subscription and BYOL from SoftNAS .
Free Tier	DS3 Standard (100GB)	Limited performance and functions. Advanced capabilities such as SnapReplicate and SNAP HA™ are not available.
Memory		
RAM Cache	1 GB to 100 GB	Defaults to 50% total RAM for read cache
SSD Cache	low-speed level 2 cache	Optional
Ephemeral Cache	low-speed level 2 cache	Optional for read cache
Storage		
Maximum Storage	16 TB/16PB	16 TB - Maximum usable block storage capacity on Azure Marketplace , contingent on instance type. 16PB - Can be extended up to 16 petabytes by leveraging multiple Azure Blob storage accounts.
# of Storage Pools	Unlimited	
# of Volumes	Unlimited	
# of Snapshots	Unlimited	
# of Snapshot Clones	Unlimited	
SnapReplicate	Unlimited Pools & Volumes	
SnapReplicate Throttle	56Kb/sec to Unlimited bandwidth	
Active Directory	Kerberos Integration	
Files and Directories	Unlimited	
Network		
Schedules	Unlimited	
NFS Exports:	Linux Default	
iSCSI Targets	Linux Default	
CIFS Shares	Linux Default	
Firewall Ports:	22 (ssh), 443 (https)	Plus NFS, iSCSI, and CIFS, and AFP as required
IP Tables Firewall	Off by default	May be configured, but is not required. Use an alternative method to set Security Groups unless added firewall protection on SoftNAS Cloud® instance is required.

Create & Configure a Virtual Machine in Azure

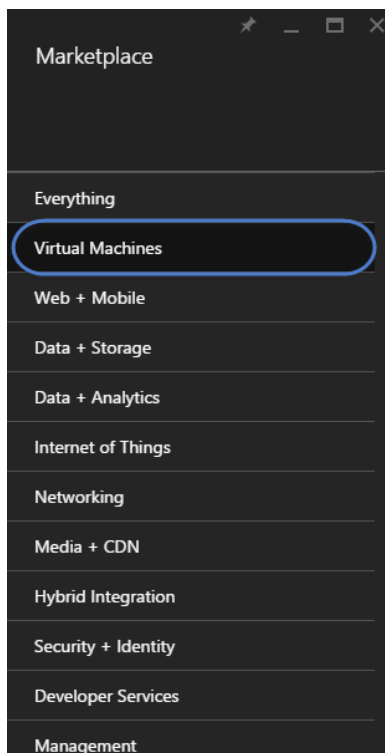
Add the SoftNAS Cloud® VM from within the **Microsoft Azure Management Portal**, and associate it to a virtual network.

Create the SoftNAS Cloud® VM

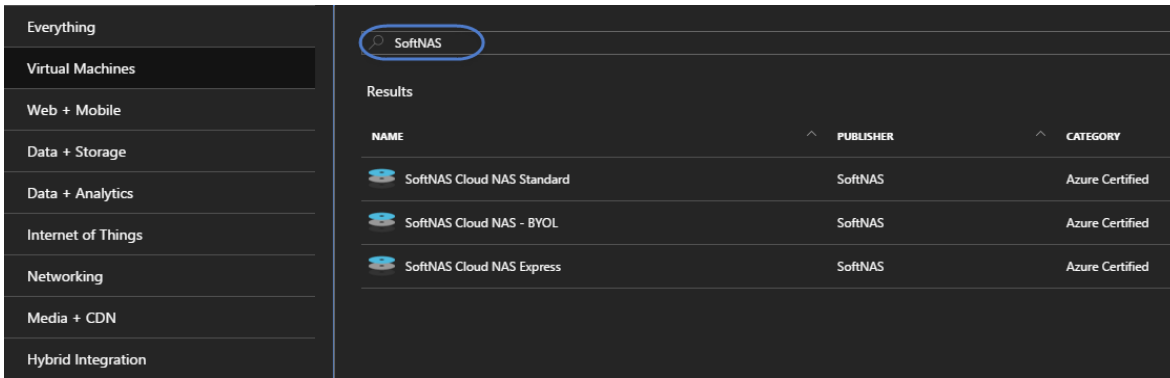
1. From the **Azure Management Portal**, click on **Marketplace**.



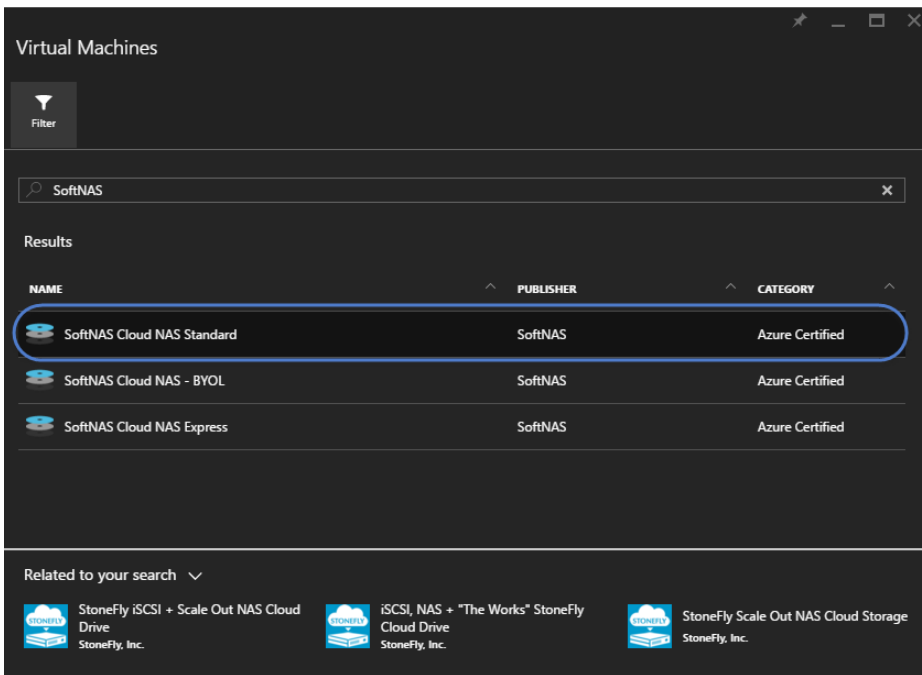
2. Click **Virtual machines**. The Virtual machines dialog is displayed.



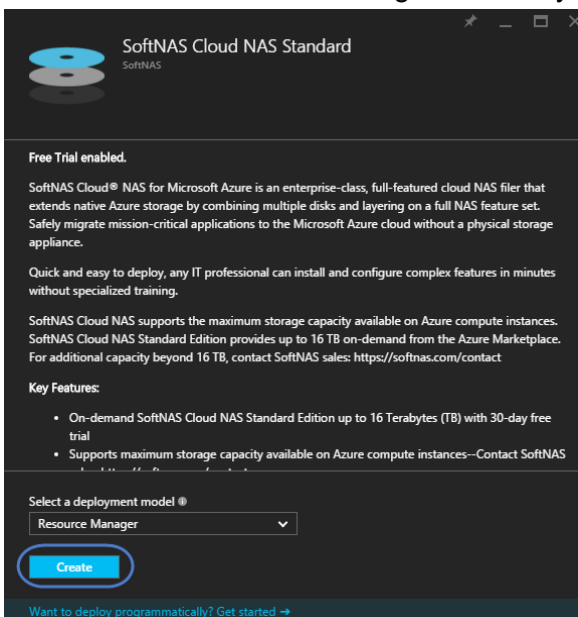
3. The next step is to **Choose an Image**. Search for **SoftNAS** in the provided field. Choose the available **SoftNAS Cloud®** release version that best fits the deployment scenario and IT budget.



4. Choose the available **SoftNAS Cloud®** release version that best fits the deployment scenario and IT budget.



5. Ensure the Resource Manager deployment model is selected, as it is required in order to provide for SoftNAS' advanced features, such as high availability. Click **Create**.



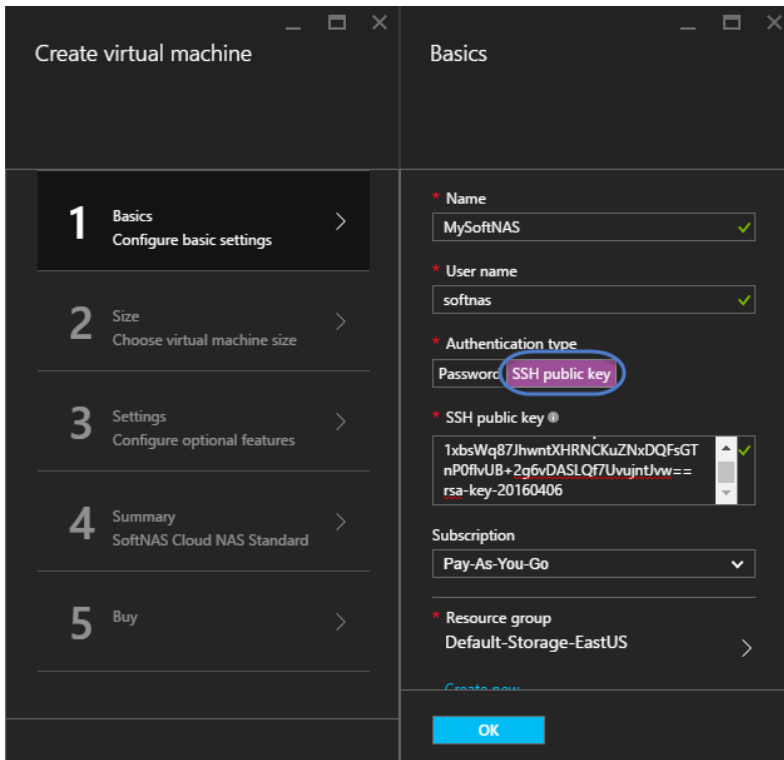
Note: As of version 3.4.8 SoftNAS does not support launching SoftNAS Cloud VMs on the classic portal. The Azure Resource Manager (ARM) is the only supported platform.

Configuring VM Name/User Name and Authentication

Here the appropriate VM Name, user name, password, or public SSH key will be set. The user name must be set as 'softnas' or you will be unable to log into your instance. Other users can be created after initial login. If security is a top concern, SSH should be used later to access the **SoftNAS Cloud®** instance with a Linux login to set the password for User Name **softnas**. Additional users can be created within the SoftNAS UI after initial configuration.

To make the required settings, configure the network settings as described in the table below.

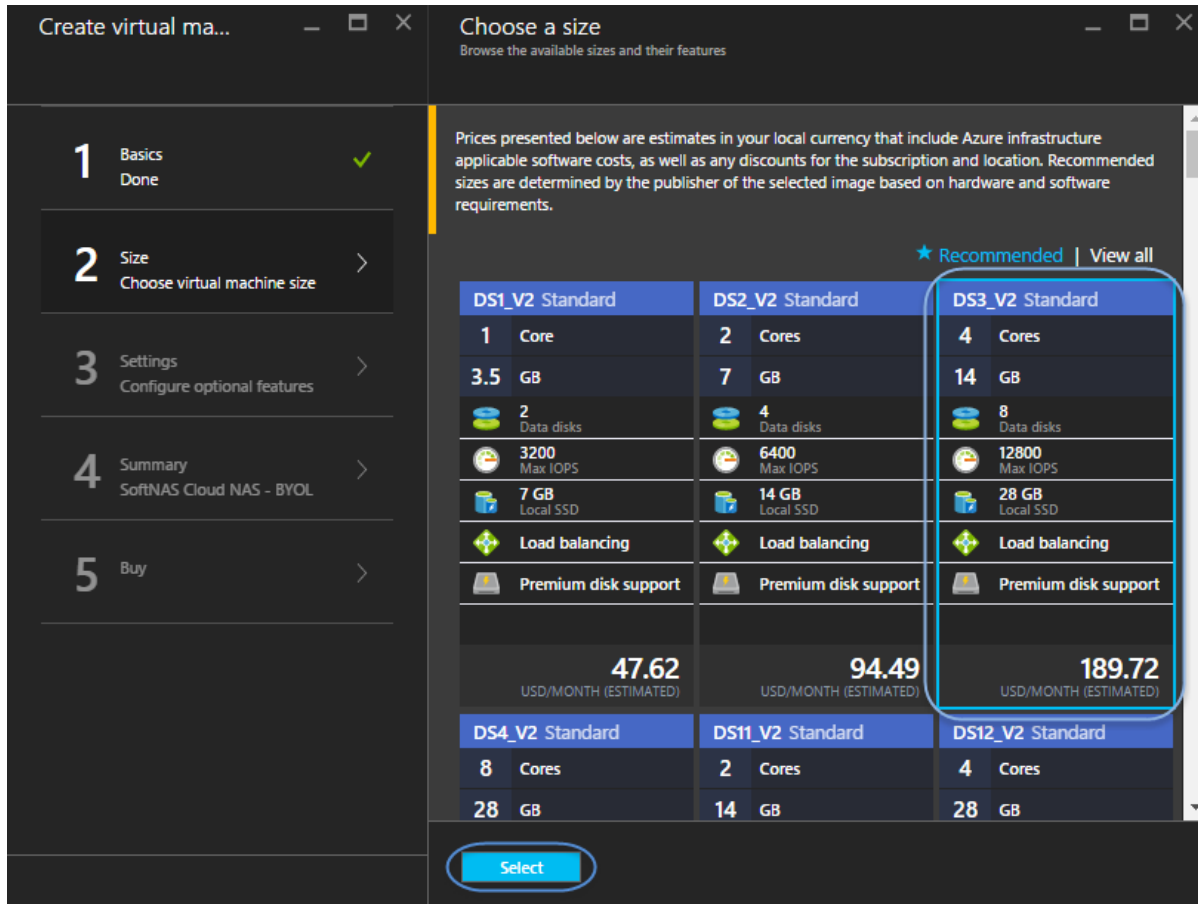
Parameter	Description
Host Name	Provide a unique name for the Host.
User Name	Set to softnas . The User Name of softnas is required to login to the virtual machine. Note: As best practice for security, the password for the softnas account should not be set through the Azure interface. SSH will be used to access the SoftNAS Cloud® VM as a Linux login. The password will be created then.
Password	You can set the Authentication type to Password , and provide a simpler password for your initial SoftNAS login, but this is not as secure a method.
SSH	Paste in the public key for an SHH key pair. For example, use ssh-keygen on Linux or OS X, or Putty on Windows. For more information, see section Generating SSH Keys .



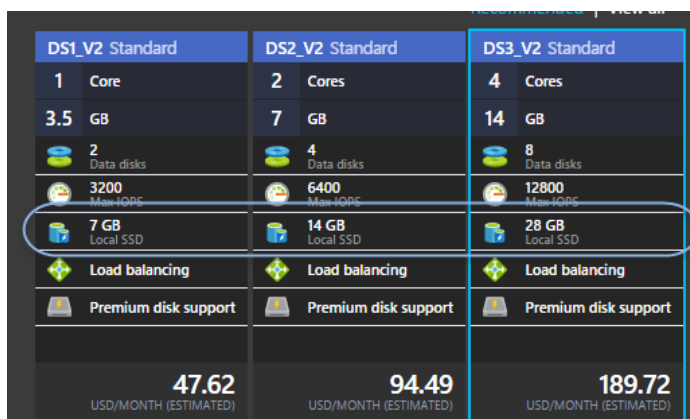
Setting Size

Microsoft Azure includes a variety of pricing tiers designed to group compute resources together in bundles. SoftNAS Cloud® provides recommendations of 3 commonly used **Sizes** for best possible product experience. Other **Sizes** may be used based on user preference. Note that the A0 Size can be used as a perpetually free offering with production limitations.

1. Click on Size. The Size screen is displayed.



Note: Ephemeral storage offered on Azure is for caching purposes only, NOT for storage. When planning your deployment, do not consider ephemeral storage as part of your storage requirement calculations. Ephemeral storage is used to improve read and write-cache performance for your instance. Ephemeral storage is listed as Local SSD in a given VM Size.

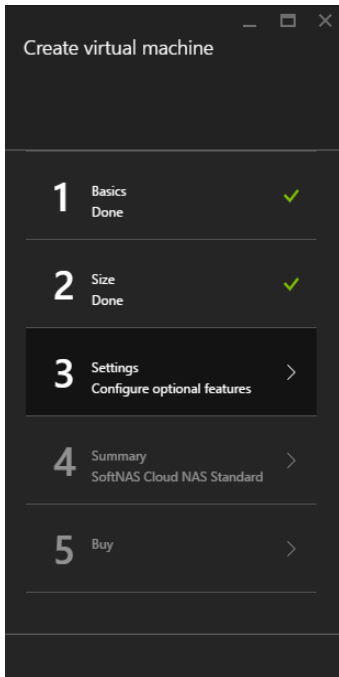


2. Use one of the suggested **Size**, or browse other pricing tiers to meet budgetary and data needs. Click **Select** when your selection is made.

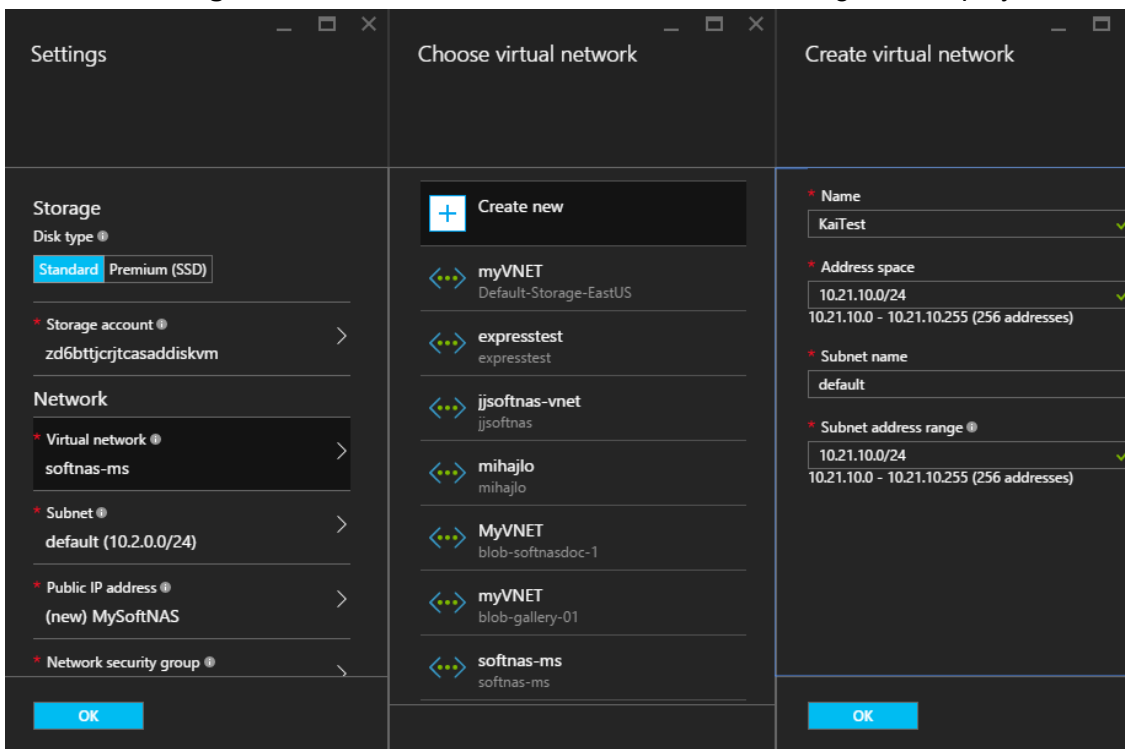
Optional Features (Settings)

You can now apply optional settings, including **Disk Type**, **Storage Account**, **Network**, and more. Here you can associate the **SoftNAS Cloud® VM** to an existing virtual network or create a new virtual network specifically for the **SoftNAS Cloud® VM**.

1. From the **Create VM Blade**, click on **Settings**.



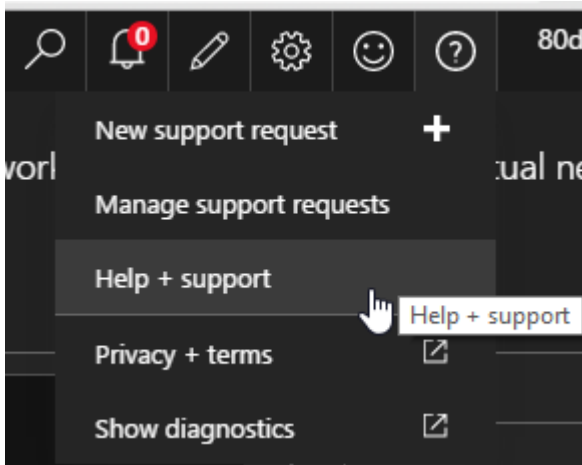
2. Under **Settings**, click on **Virtual Network**. The network settings are displayed.



3. Associate the **SoftNAS Cloud® VM** to an existing virtual network, or create a new virtual network.

Note: If creating a new network, simply provide a name for the virtual network. It is feasible to use the default CIDR block and to use the default **Microsoft Azure** DNS server.

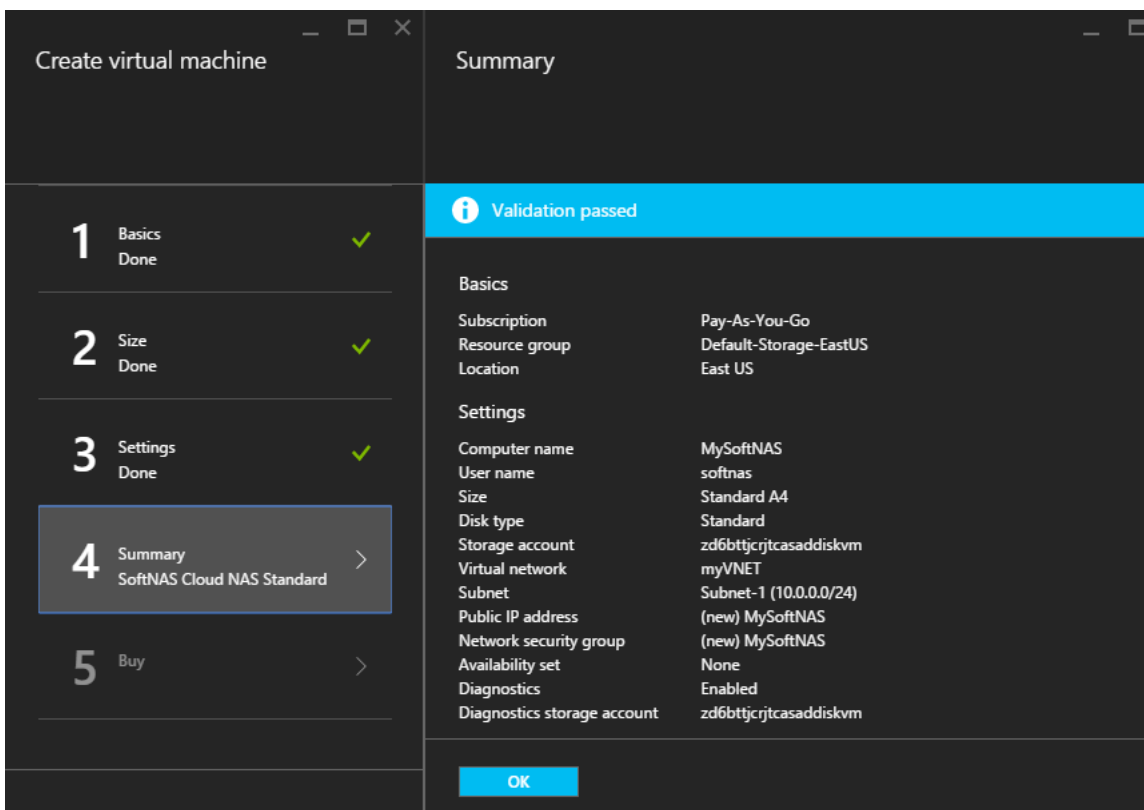
In addition to naming your Virtual Network and assigning a CIDR block, you can also apply a subnet, a public IP Address, a security group, etc. The menus are very similar in layout, and highly intuitive to use. Configure your instance as required, using **Azure Help Menu** if you have any problems or questions.



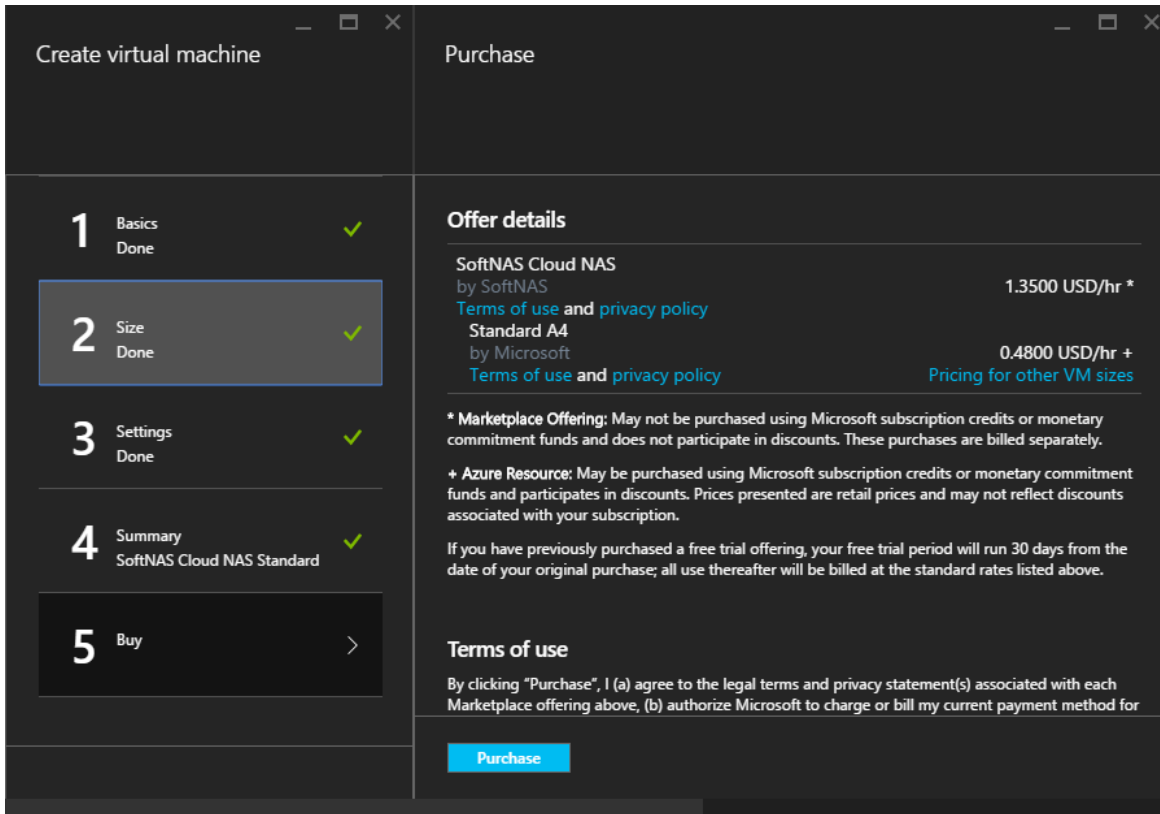
Purchase

After performing optional configuration, validate and purchase the VM.

1. Click **OK** to accept any settings changes, and click **OK** again to validate the settings in **Summary**.



2. On the next screen, review the purchase details and then click **Purchase**.



The screenshot displays two side-by-side windows from the Azure portal. The left window, titled 'Create virtual machine', shows a progress bar with five steps: 1. Basics (Done), 2. Size (Done), 3. Settings (Done), 4. Summary (SoftNAS Cloud NAS Standard), and 5. Buy. The right window, titled 'Purchase', shows the offer details for 'SoftNAS Cloud NAS by SoftNAS' at 1.3500 USD/hr and 'Standard A4 by Microsoft' at 0.4800 USD/hr + Pricing for other VM sizes. It includes terms of use and a 'Purchase' button.

Create virtual machine

- 1 Basics Done ✓
- 2 Size Done ✓
- 3 Settings Done ✓
- 4 Summary SoftNAS Cloud NAS Standard ✓
- 5 Buy >

Purchase

Offer details

SoftNAS Cloud NAS
by SoftNAS 1.3500 USD/hr *

[Terms of use and privacy policy](#)

Standard A4
by Microsoft 0.4800 USD/hr +
[Pricing for other VM sizes](#)

*** Marketplace Offering:** May not be purchased using Microsoft subscription credits or monetary commitment funds and does not participate in discounts. These purchases are billed separately.

+ Azure Resource: May be purchased using Microsoft subscription credits or monetary commitment funds and participates in discounts. Prices presented are retail prices and may not reflect discounts associated with your subscription.

If you have previously purchased a free trial offering, your free trial period will run 30 days from the date of your original purchase; all use thereafter will be billed at the standard rates listed above.

Terms of use

By clicking "Purchase", I (a) agree to the legal terms and privacy statement(s) associated with each Marketplace offering above, (b) authorize Microsoft to charge or bill my current payment method for

Purchase

A new **SoftNAS Cloud®** instance will launch into **Microsoft Azure**.

Adding Administrative Accounts

Service Administrator Account

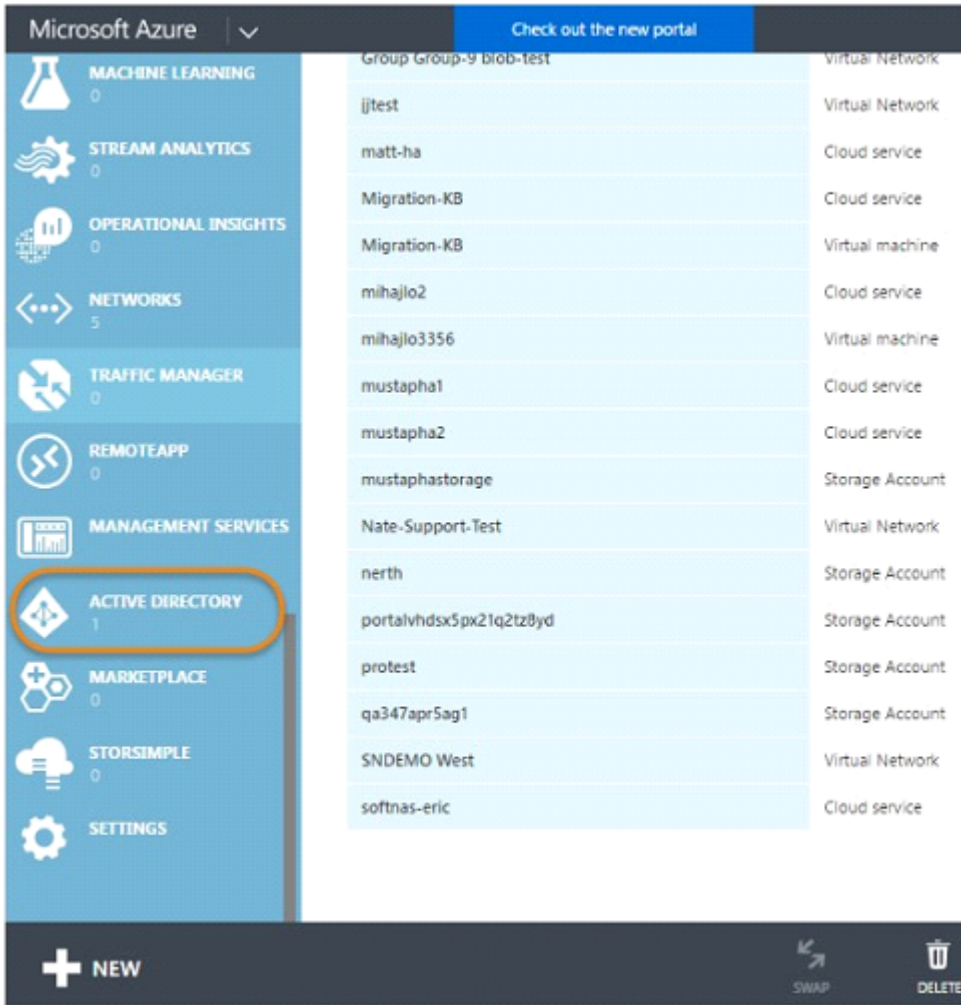
Before adding block storage, it is important to note that you will require a properly configured service administrator account in order to connect storage from within the UI. Without these credentials, the storage accounts you require will not be available.

To create an administrative Server account

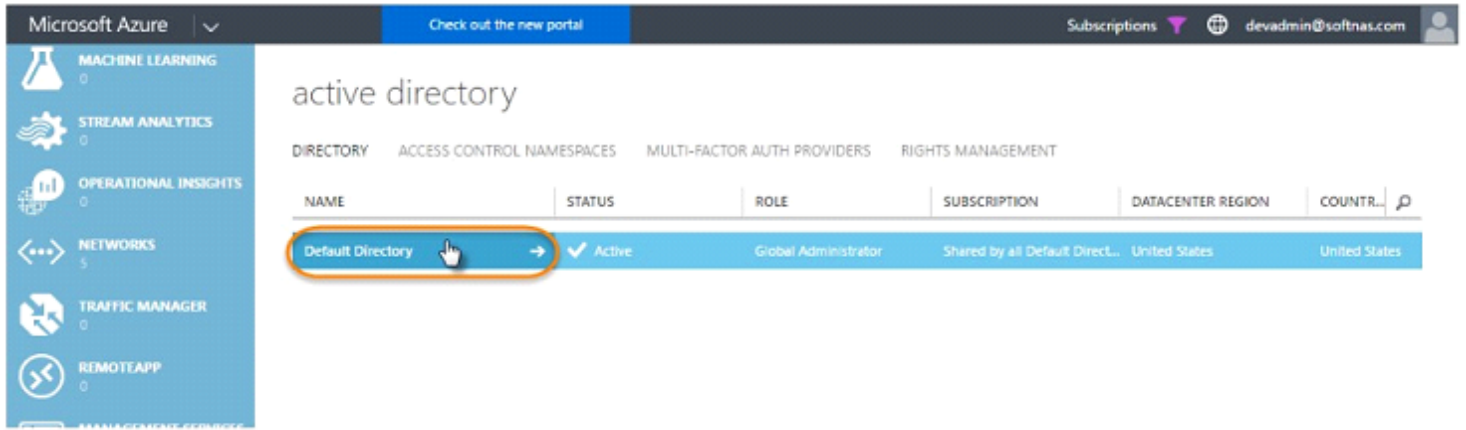
1. To ensure you have a valid service administrator account, log into the classic Azure Management Portal with administrative credentials:

<https://manage.windowsazure.com>

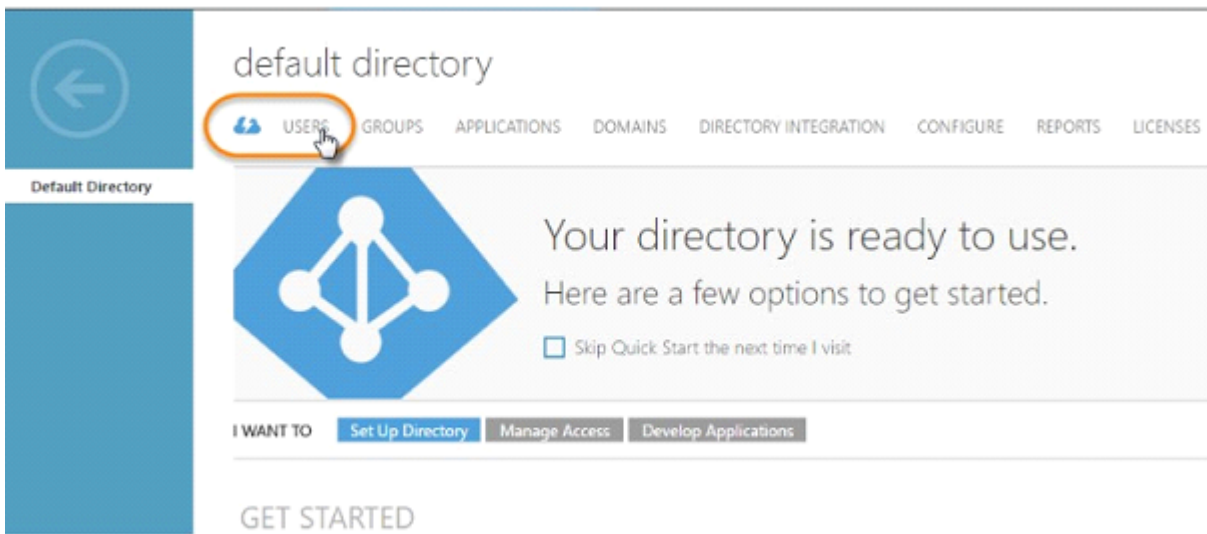
2. Once logged in, select **Active Directory** from the left-side menu.



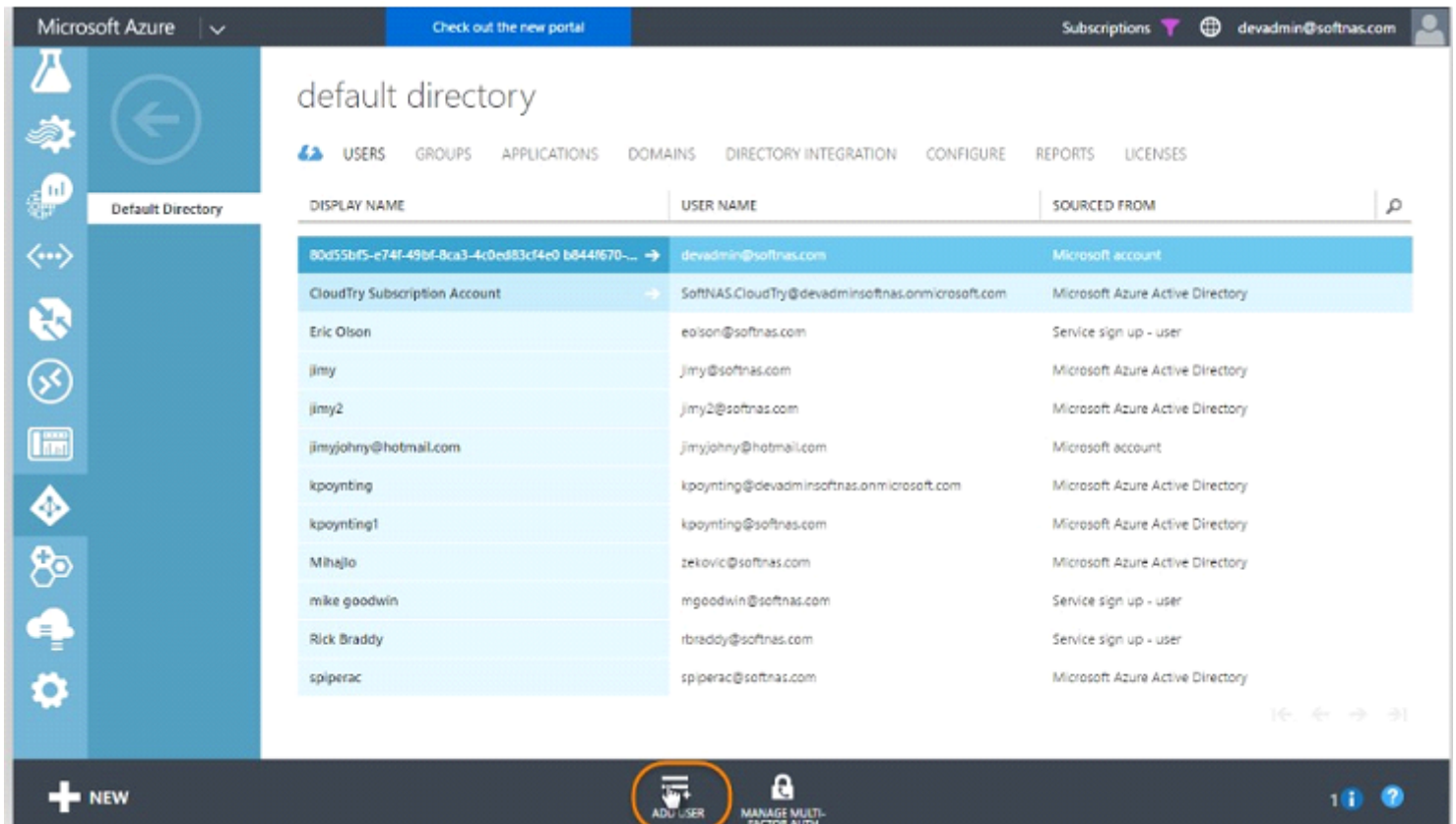
3. Find **Default Directory** (or the directory you are using) and select it as shown below.



4. From **Default Directory**, select **Users**.



5. Find **Add User** at the bottom of the screen. Select it.



6. A wizard will open. Enter your desired email and click the **Next Arrow**.
 In the **User Profile** screen of the wizard, do the following:
- a. Enter your name and a display name.
 - b. Specify the role of the user. Select Service Admin.
 - c. Click the Next Arrow.

ADD USER ×

user profile

FIRST NAME LAST NAME **a**

DISPLAY NAME

ROLE ? **b**

MULTI-FACTOR AUTHENTICATION ?

Enable Multi-Factor Authentication

c

← →

1

7. Click **Create**.

ADD USER ×

Get temporary password

The new user 'someone@devadminsoftnas.onmicrosoft.com' will be assigned a temporary password that must be changed on first sign in. To display the temporary password and to create the account, click Create.

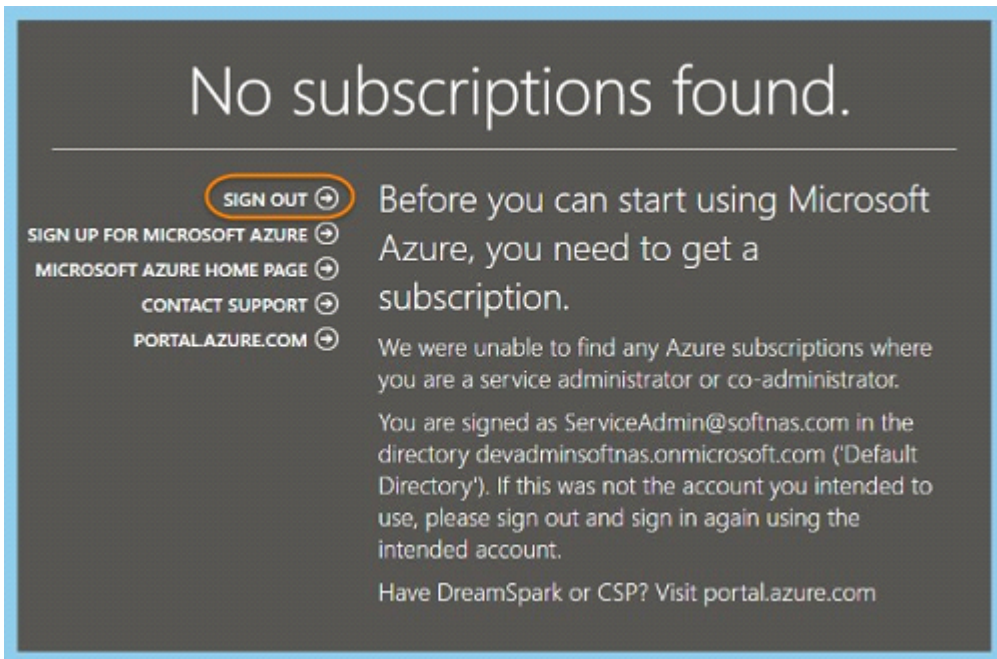
← ✓

8. Copy the temporary password, and click the check mark.

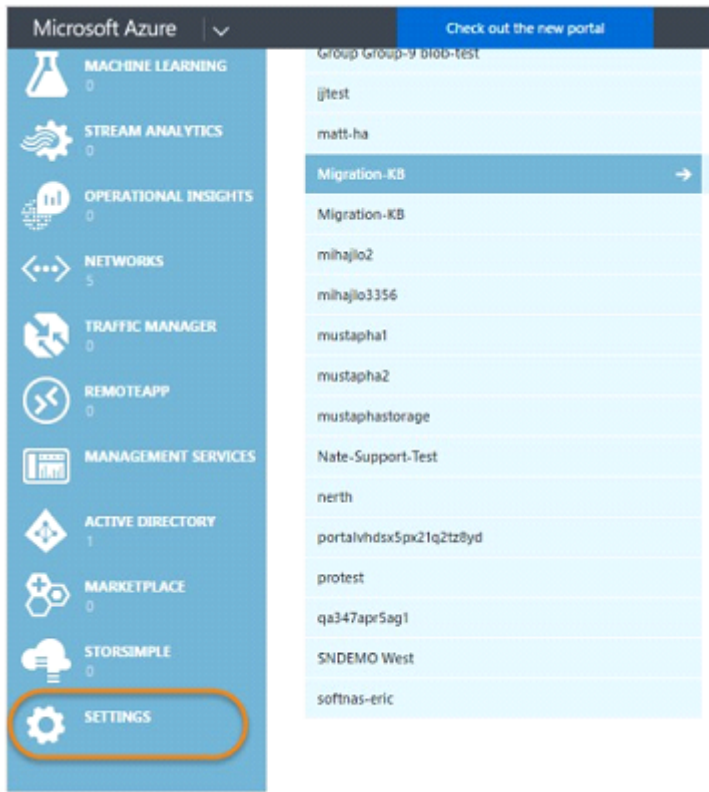
9. Log out of the administrative account, then log back in with the new user and temporary password. You'll be prompted to create your own password. Sign in to establish the new password as shown below.

Update password and sign in

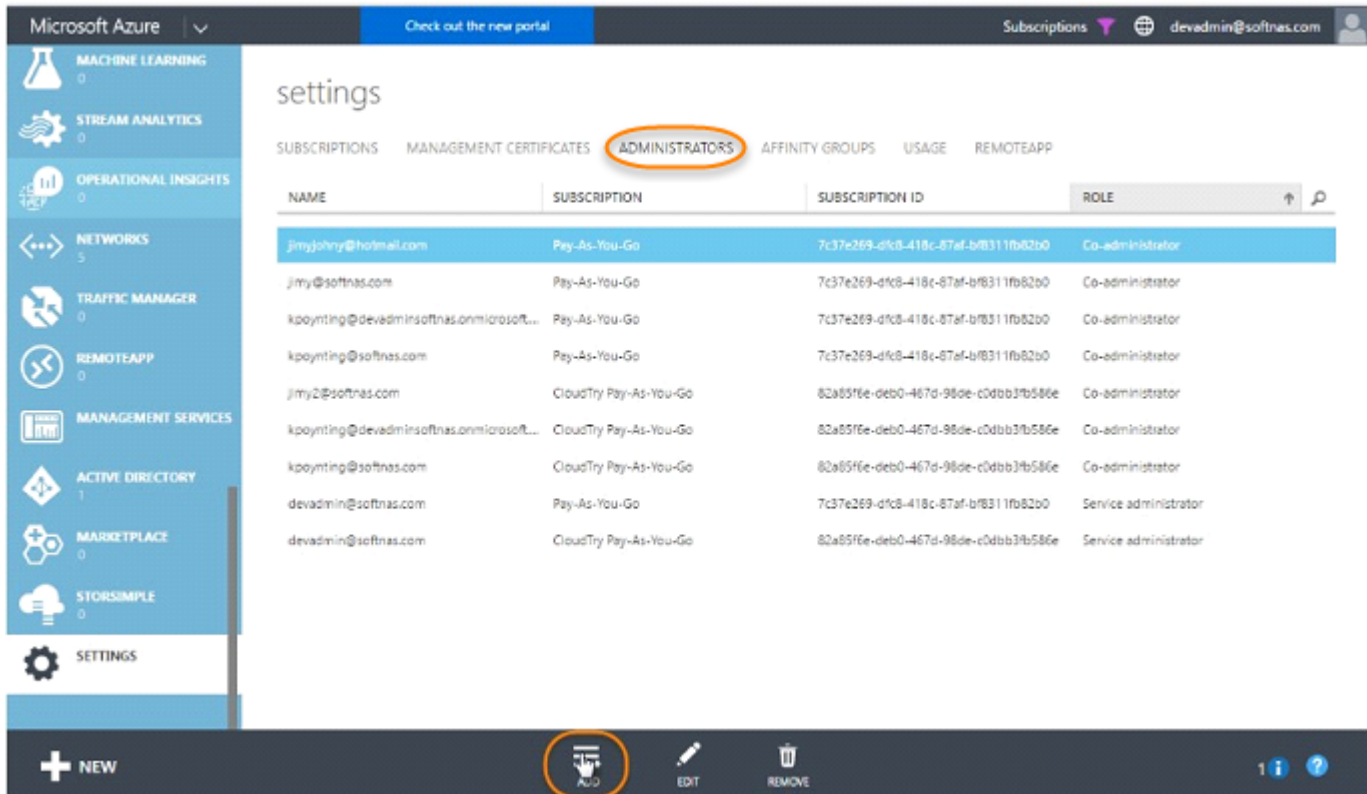
10. As you can see, you will need a subscription added to your new account. Sign out, then sign in once more with your original administrative account.



11. Once logged back in, go to **Settings** from the left-side menu.



12. Select **Administrators**, and click **Add**.



13. Type the email address. This will call up the account. Ensure the subscriptions you will need are checked off, and click **Next**.

ADD A CO-ADMINISTRATOR x

Specify a co-administrator for subscriptions

Co-administrators can fully manage the services within a subscription. Enter a valid email address, and then select at least one subscription.

EMAIL ADDRESS

✔  Default Directory

SUBSCRIPTION	SUBSCRIPTION ID	
<input checked="" type="checkbox"/> CloudTry Pay-As-You-Go	82a85f6e-deb0-467d-98de-c0dbb3fb586e	
<input checked="" type="checkbox"/> Pay-As-You-Go	7c37e269-dfc8-418c-87af-bf8311fb82b0	



14. Now that we know we have a service account properly configured, we can now access the storage accounts needed to add block storage from within the SoftNAS UI.

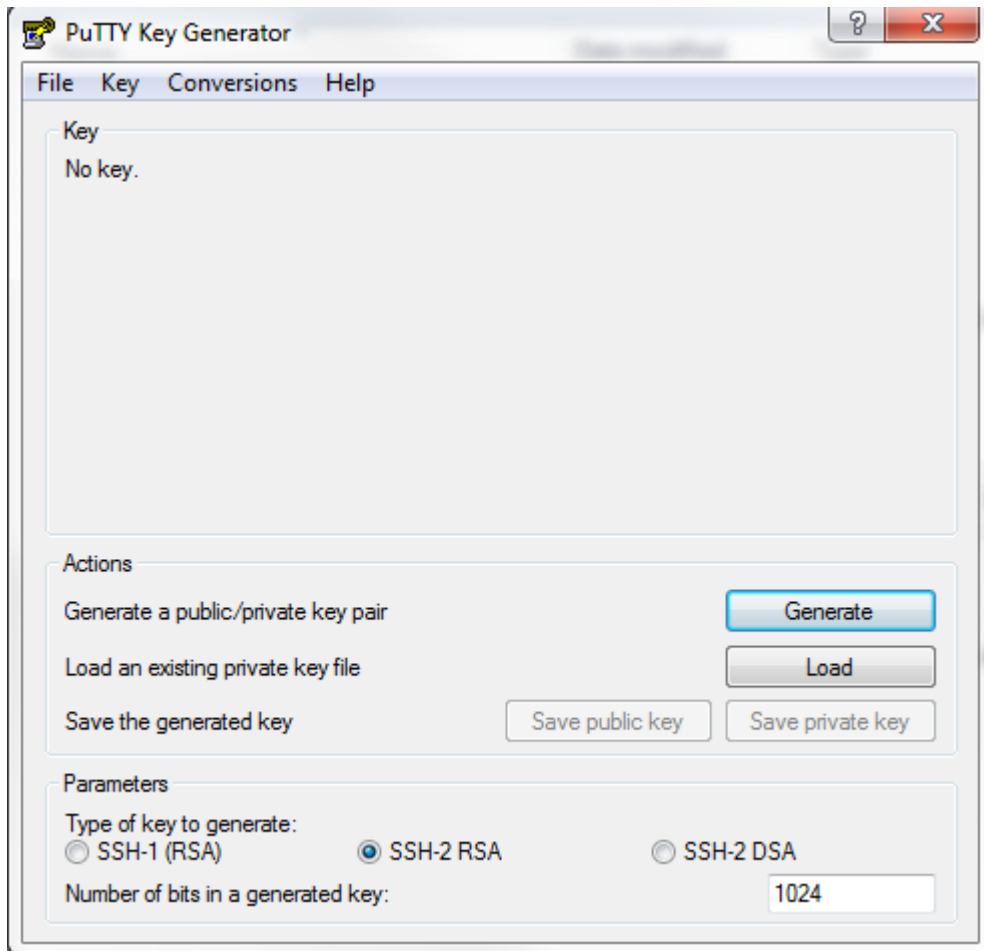
Generating SSH Keys

Using PuTTY to Generate SSH Keys in Windows

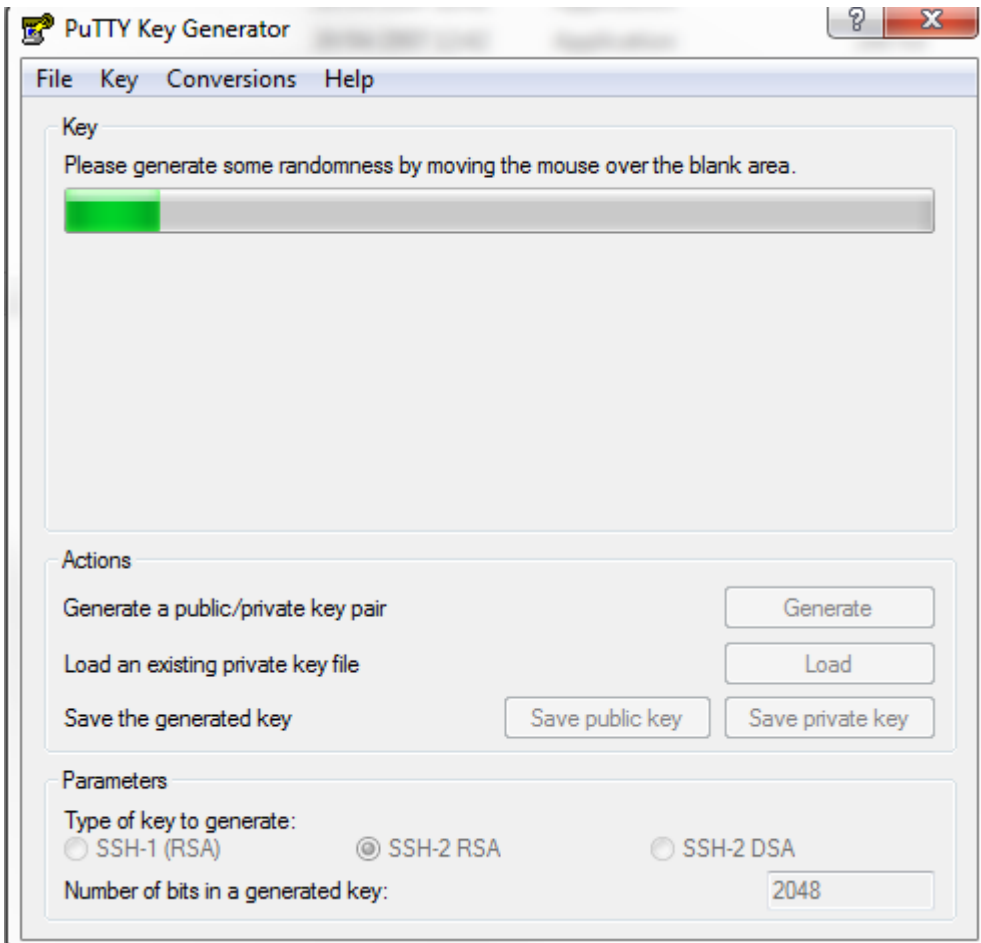
Use [PuTTYGen](#) on Windows to generate private/public key pairs for SSH authentication.

Once PuTTYGen has been downloaded, use the following procedure to generate a SSH key for a **SoftNAS Cloud®** instance in **Microsoft Azure**.

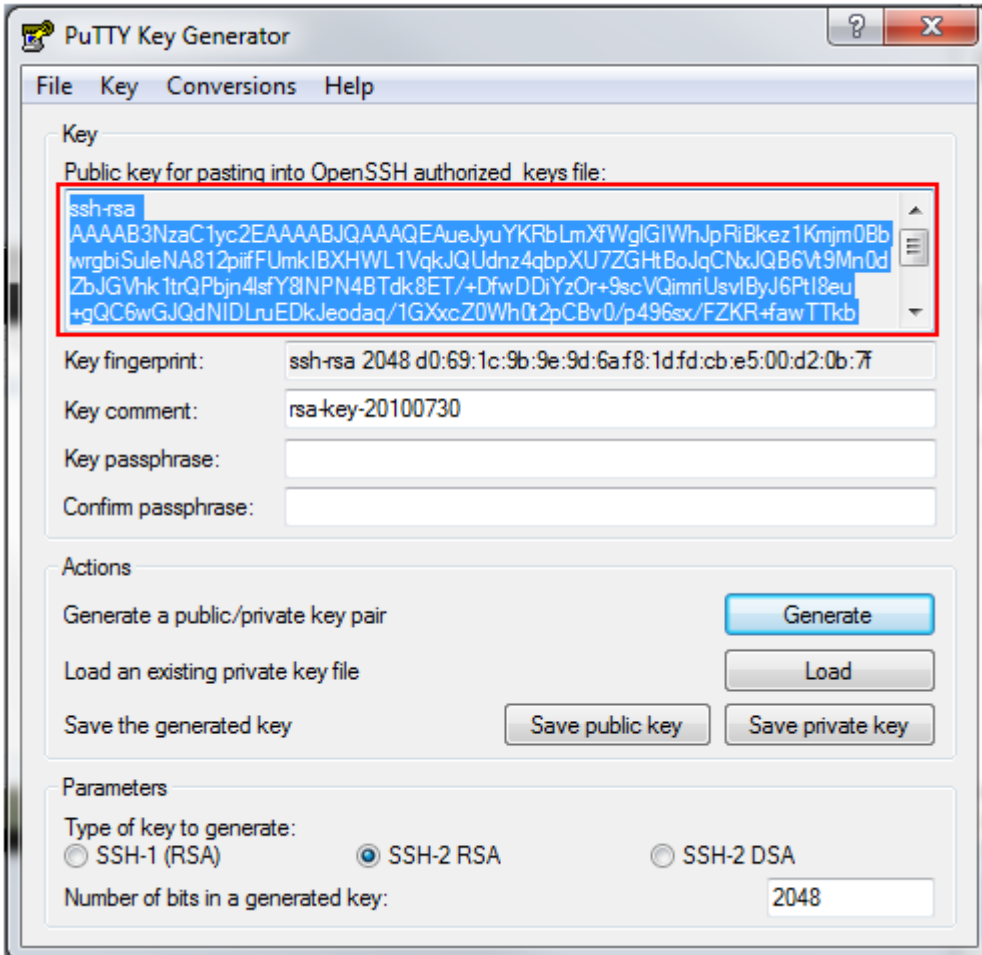
1. Open PuTTYGen and click **Generate** to generate new public/private keys.



2. Generate randomness by moving the mouse when prompted.



3. Copy the public key, which will be used for the **SoftNAS Cloud®** instance in **Microsoft Azure**.



Note: Save both the **private** and **public** keys.

Using OpenSSH to Generate SSH Keys in Linux

To set up SSH access, the following is required:

- Create a public/private key pair.
- Copy the public key that will be uploaded to the remote server.

Create the Key Pair

1. Open a new terminal session.
2. Run the **ssh-keygen** command to create a new public/private key.

Select a location on the local machine (default location is recommended). Also, provide a passphrase to protect the private key at this time, if required.


```

$andrewjmacbook3:~ andrewjohnston$ ls -al ~/.ssh
-bash: $: command not found
andrewjmacbook3:~ andrewjohnston$ ls -al ~/.ssh
total 24
drwx-----  5 andrewjohnston  staff   170  1 Mar 10:04 .
drwxr-xr-x+ 39 andrewjohnston  staff  1326 28 Aug 11:05 ..
-rw-----  1 andrewjohnston  staff  1766  1 Mar 10:04 github_rsa
-rw-r--r--  1 andrewjohnston  staff   407  1 Mar 10:04 github_rsa.pub
-rw-r--r--  1 andrewjohnston  staff  1643 21 Aug 14:27 known_hosts
andrewjmacbook3:~ andrewjohnston$ ssh-keygen -t rsa -C "gentleman1@gmail.com"
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/andrewjohnston/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /Users/andrewjohnston/.ssh/id_rsa.
Your public key has been saved in /Users/andrewjohnston/.ssh/id_rsa.pub.
The key fingerprint is:
69:55:4b:63:ff:e5:b4:9c:f8:4f:9f:66:ac:32:a8:88 gentleman1@gmail.com
The key's randomart image is:
+--[ RSA 2048]-----+
|           =         |
|          ++        |
|         . . . o    |
|          o   o++   |
|         S   .+o    |
|          .   .     |
|         .   ...    |
|         . . . o   =+|
|        E . . . o.+o|
+-----+
andrewjmacbook3:~ andrewjohnston$

```

Adding the Key to the Remote Server

Note: Add the newly created public key to the **SoftNAS Cloud®** instance in **Microsoft Azure**. In order to do this, copy the key from Terminal and then paste it into the **SoftNAS Cloud® VM** at time of creation.

1. From Terminal, run the following command

```
cat ~/.ssh/id_rsa.pub
```

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQBNqqi1mHLnryb1FdbePrSZQdmXRZxGZbo0gTfglysq6KMNUNY2VhzmYNS
```

2. Copy the entire output, including **ssh-rsa**. This is the public key that needs to be pasted into the appropriate field at **SoftNAS Cloud® VM** creation.

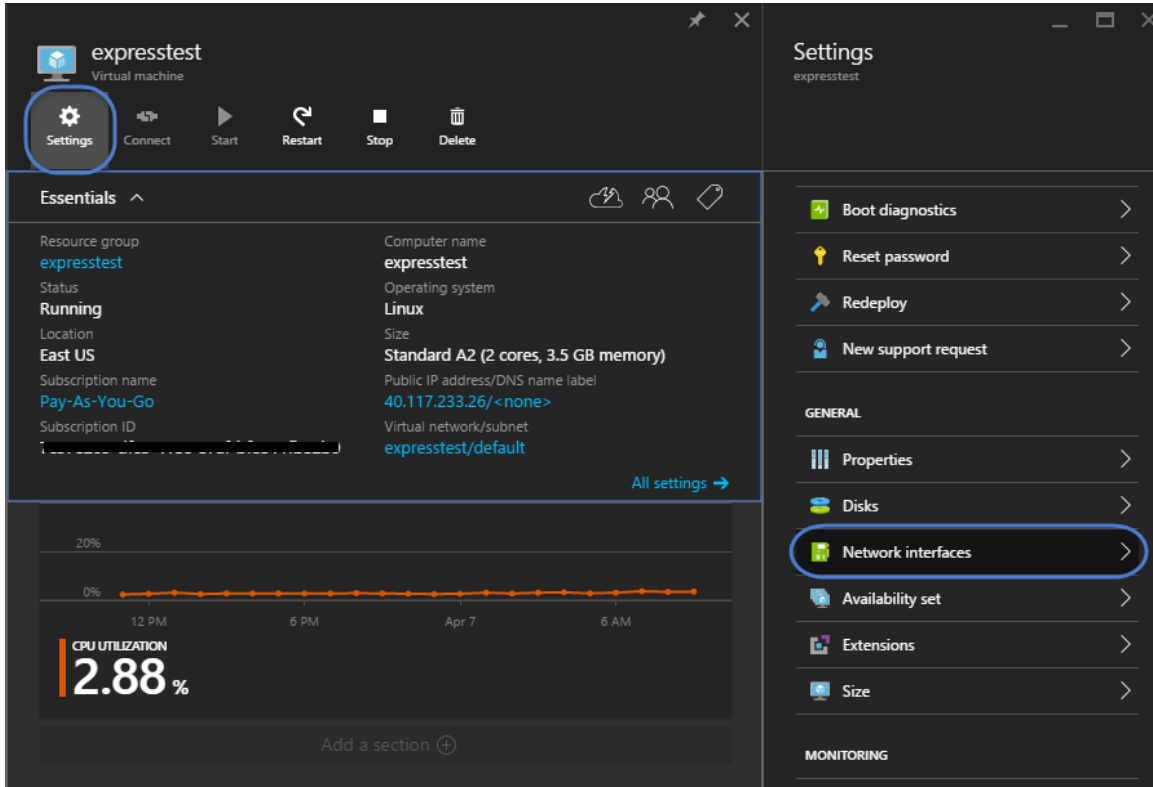
Move on to complete section [Create & Configure Virtual Machine](#).

Managing Network Settings

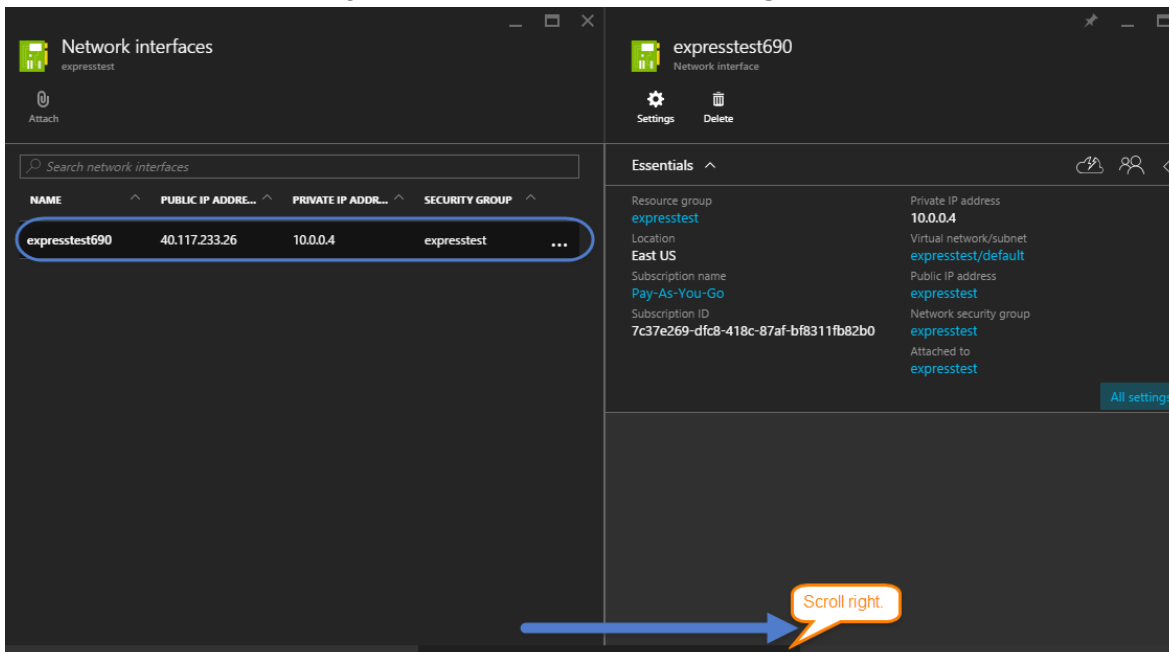
Network Settings

Network settings, including inbound and outbound rules are very important to the success of your deployment, and will differ based upon the use case. Managing Network Settings at the Azure VM level is important to the success of your deployment. To change your network settings:

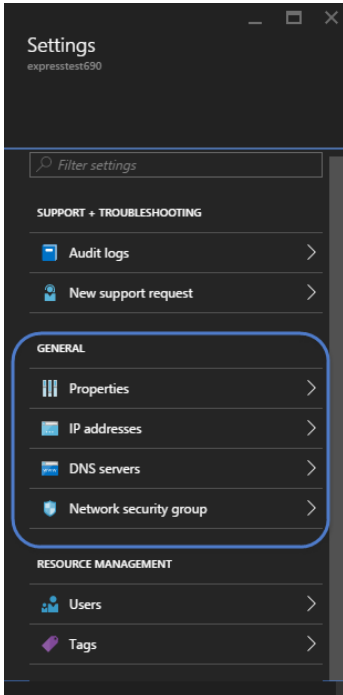
1. From the Virtual machines screen, click on the preferred SoftNAS Cloud® VM.
2. Click on **Settings > Network Interfaces**.



3. Select the available network interface. This will open a new **Settings** menu, allowing you to configure your network interface. Scroll right to reach the **Network Settings** menu.

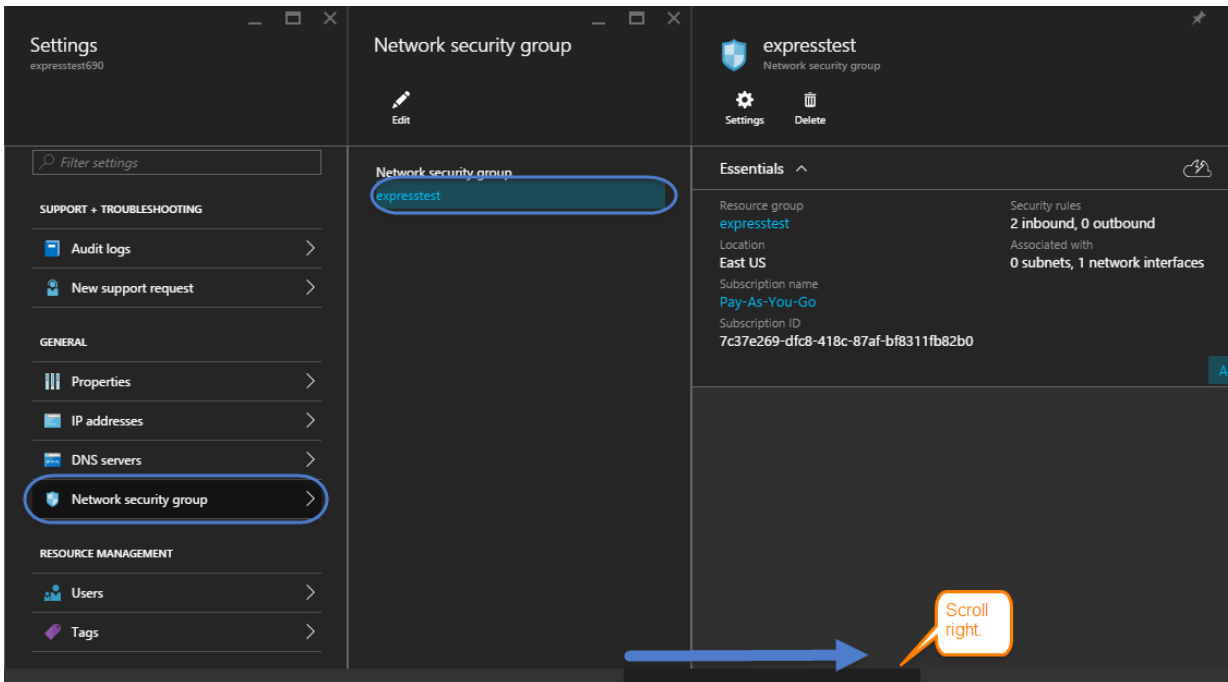


4. In the Network Setting Menu, under General, you can view network interface properties, manage IP addresses, provide DNS settings, and apply a **Network Security Group**. The IP address supplied for the network interface will be used to connect to your SoftNAS Cloud on Azure instance.



Network Security Group

Azure manages inbound and outbound rules in a similar fashion to AWS, by tying them to a **Network Security Group**. To view and change the Network Security Group settings, select **Network Security Group**.



In the Settings Menu for the selected Network Security Group, you can view the defaults, and make any required changes to both your inbound and outbound security rules, as well as subnets.

The screenshot displays the 'Settings' window for 'expresstest' in SoftNAS Cloud. The main area is titled 'Inbound security rules' and contains a table with the following data:

PRIORITY	NAME	SOURCE	DESTINATION	SERVICE	ACTION
1010	SSH	Any	Any	TCP/22	Allow
1020	HTTPS	Any	Any	TCP/443	Allow

The left sidebar includes sections for 'SUPPORT + TROUBLESHOOTING' (Audit logs, New support request), 'GENERAL' (Properties, Inbound security rules, Outbound security rules, Network interfaces, Subnets), and 'MONITORING' (Diagnostics).

Adding Storage in Microsoft Azure

There are three basic methods of adding disks (storage) to your SoftNAS instance on Azure. Each method is a fairly simple task, but there are some considerations before adding your storage, or even selecting your method. One of the key decisions you will need to make is whether to deploy and use block or object storage.

Note: Whichever type of storage you choose, it will require set up of storage accounts.

- [Creating Storage Accounts](#)

Block Storage

Block storage provides fixed size raw storage capacity within your VM. In Azure, these are referred to as virtual hard disks. Within the SoftNAS UI, these are referred to as **Microsoft (MSFT) Disks**. Each volume added is treated as an independent disk drive. Block storage disks are only accessible when attached to an OS, such as the linux-based SoftNAS framework we offer. They are typically formatted with a file system, such as FAT32, NTFS, EXT3, or EXT4. They are also easily configured into software RAID configurations.

Note: In SoftNAS, object storage can also be leveraged into RAID configurations.

Block storage is typically used for applications, particularly databases and mission critical apps, such as SQL, Exchange, or Sharepoint, etc...anything that requires high performance benchmarks and low latency.

There are two methods to add block storage for SoftNAS on Azure:

- [Adding Disks Via the Microsoft Azure Portal](#)
- [Adding Block Storage via the SoftNAS UI](#)

Object (Blob) Storage

Object storage (called Blob storage in Azure), is directly accessible through an API or HTTP/HTTPS and can store any type of data. The data is guaranteed not to be lost and can be replicated across data centers. It offers web service interfaces for easy access.

Typical uses for Object (Blob) storage includes unstructured data such as repositories of music, image, and video files. It is also used for log files, backup files, and data dumps. Blob storage provides large capacity for large data sets and archive files. It can be used to replace local tape drives. While these are typical use cases, SoftNAS offers the ability to treat object storage as independent disks, much like block storage, allowing it to be configured into RAID configured volumes.

To add object storage to your SoftNAS instance:

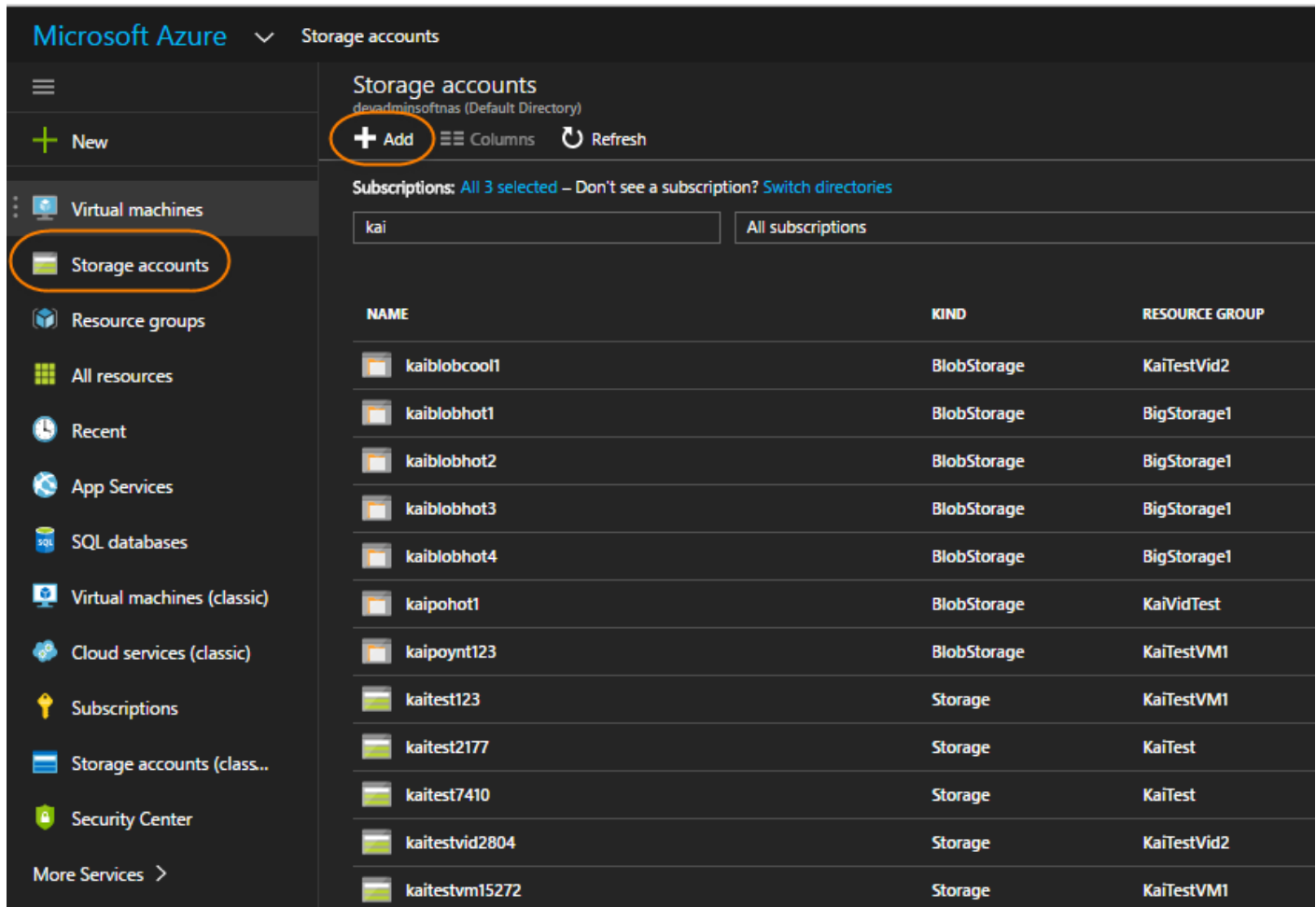
- [Adding Object Storage via the SoftNAS UI](#)

Creating Storage Accounts

In order to add storage disks of any variety to your SoftNAS instance, you will need to create at least one storage account. Creating MSFT or Blob disks require different storage account types. In order to leverage more than the 500 TB per storage account limit, you will need to create several blob storage accounts. When creating your multiple blob storage accounts, you must then decide whether to leverage hot or cold storage. You cannot mix hot and cold storage within a pool, but you can provide more than one pool. In other words, you will need to know what configuration you intend to create, and plan your storage accounts accordingly. One SoftNAS on azure instance can potentially require many storage accounts.

To add a storage account:

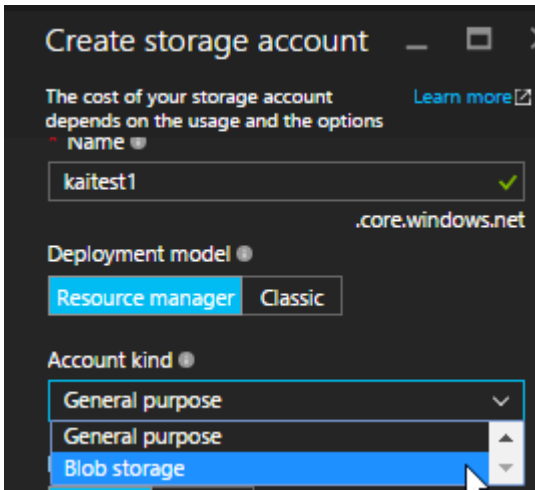
1. Log into the Azure Portal.
2. Select **Storage Accounts**. Click **Add**.



The screenshot shows the Microsoft Azure portal interface for 'Storage accounts'. The left-hand navigation pane has 'Storage accounts' highlighted with an orange circle. In the main content area, the '+ Add' button is also circled in orange. Below the navigation pane, a table lists existing storage accounts with columns for NAME, KIND, and RESOURCE GROUP.

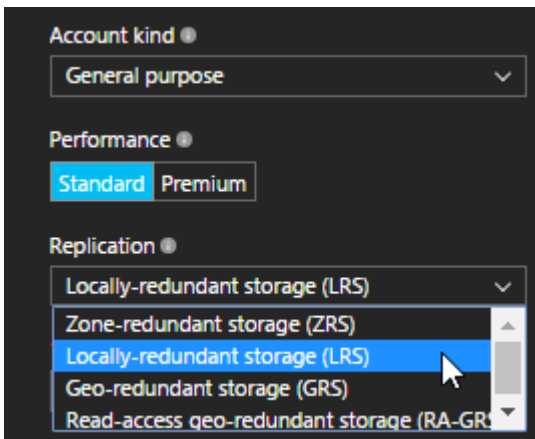
NAME	KIND	RESOURCE GROUP
kaiblobcool1	BlobStorage	KaiTestVid2
kaiblobhot1	BlobStorage	BigStorage1
kaiblobhot2	BlobStorage	BigStorage1
kaiblobhot3	BlobStorage	BigStorage1
kaiblobhot4	BlobStorage	BigStorage1
kaipohot1	BlobStorage	KaiVidTest
kaipoyn123	BlobStorage	KaiTestVM1
kaitest123	Storage	KaiTestVM1
kaitest2177	Storage	KaiTest
kaitest7410	Storage	KaiTest
kaitestvid2804	Storage	KaiTestVid2
kaitestvm15272	Storage	KaiTestVM1

Provide a name for the storage account, select the deployment model, and determine what type of account you wish to create, **General Purpose**, or **Blob storage**.

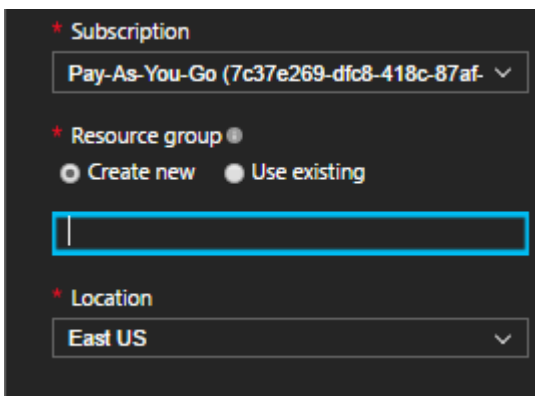


If you select General Purpose, you have the option to select Premium Storage. Blob Storage accounts only provide Standard. Premium storage accounts are backed by solid state drives and offer consistent, low-latency performance. They can only be used with Azure virtual machine disks, and are best for I/O-intensive applications, like databases. This setting can't be changed after the storage account is created. Note as well that Premium storage comes in set disk sizes - 128 GB, 512 GB, and 1024GB. Determine the best option based on your needs.

For Replication, select **Locally-redundant storage**. Other options will likely work, but have not been fully tested, and may result in latency issues as data can span multiple locations.



Finally, if you have more than one subscription, select the correct one. Determine whether to create a new resource group, or add the new account to an existing group. If using an existing group, select from the dropdown, and location will be auto-populated. If creating a new resource group, type the name and select the location. Click **Create** when your selections have been made.



You now have a new storage account, whether Blob storage or General Purpose.

- [Hot and Cool Storage](#)
- [Adding Disks via the Microsoft Azure Portal](#)
- [Adding Block Storage via the SoftNAS UI](#)
- [Adding Object Storage via the SoftNAS UI](#)

Hot and Cool Storage

There are two general types of storage accounts for Azure:

- **General Purpose**
- **Blob Storage Accounts**

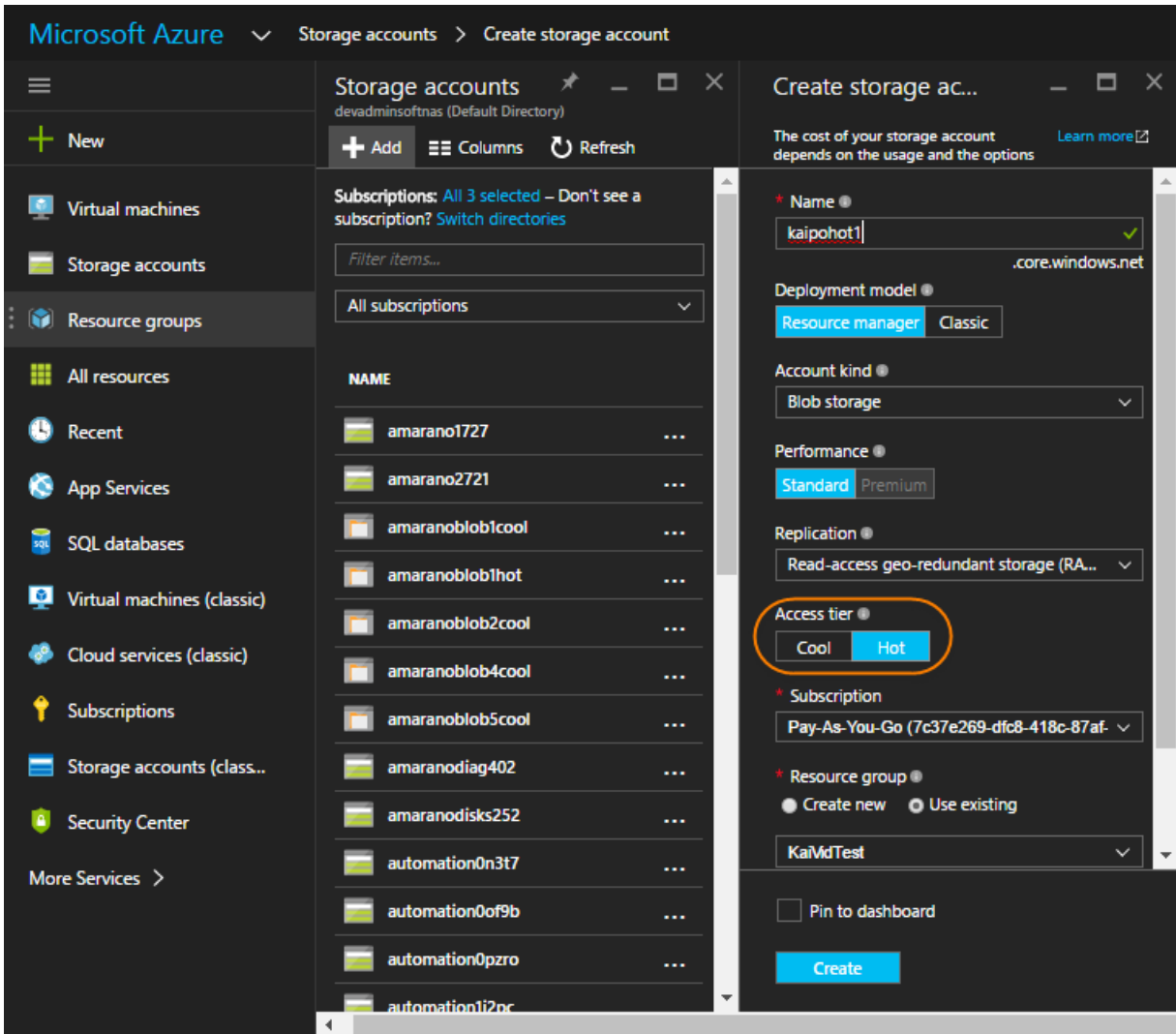
General purpose accounts are used for block storage, or Azure Virtual Machine Disks.

If deciding to add Azure object storage (otherwise known as Blob storage), you will need to have a Blob storage account set up, or you will not be able to call upon the storage within the SoftNAS UI. When creating your Blob Storage account, you will also have another decision to make - whether you will leverage hot or cool storage for Azure. SoftNAS offers full support for both options:

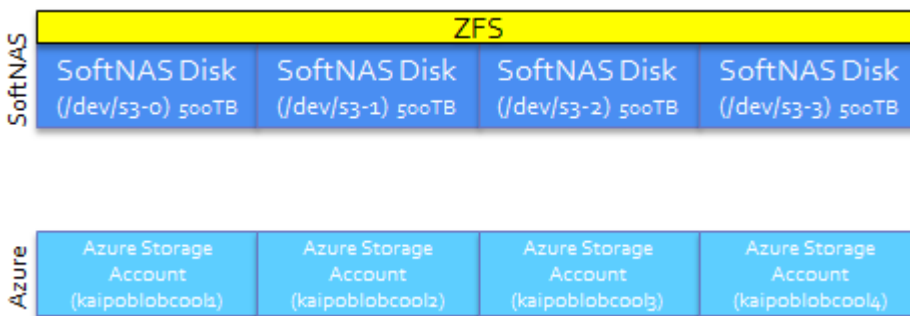
- **Azure Cool Storage** - Object storage that allows economical safe-keeping of less frequently accessed file data.
- **Azure Hot Storage** - Object storage that optimizes frequently accessed stored data to enable continuous IO.

Note: You cannot mix hot and cool storage disks in a RAID configured pool. A decision must be made on storage type for each pool. As storage type is determined at the blob storage account level, you must be aware of the type of account created. SoftNAS recommends labelling them with Hot or Cool in the names to avoid confusion.

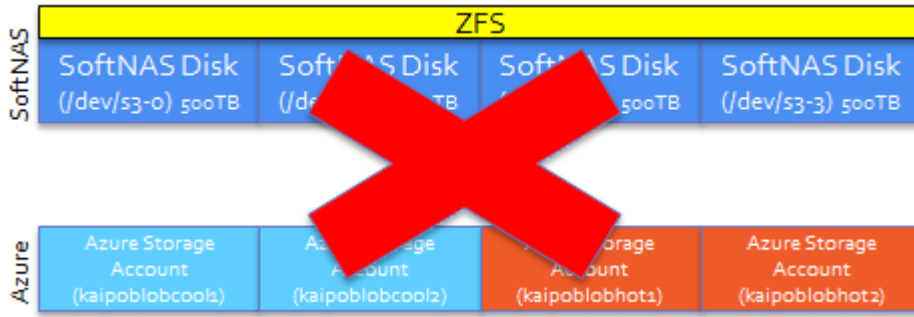
When creating your Azure blob account, you will see an option to determine the '**Access tier**' with two available options, **Hot** and **Cool**. This setting determines what type of blob storage the account in question will provide. If Hot, this storage account will only provide Hot storage to your instance. If creating a separate pool of Cool disks, another blob storage account will need to be provided.



In a given pool, you can add any number of azure blob storage disks, by first creating blob storage accounts. It is recommended to name them in sequence with clues as to which type of storage they provide.

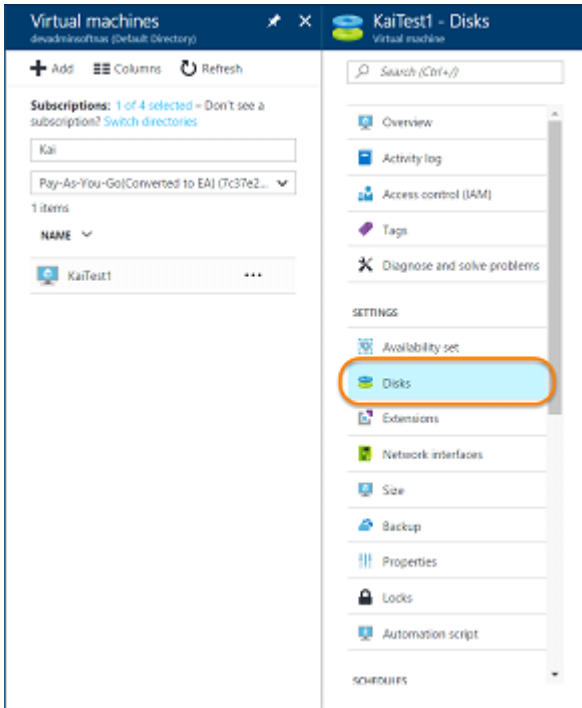


Never mix blob storage accounts within the same pool. SoftNAS will alert you should this occur accidentally.

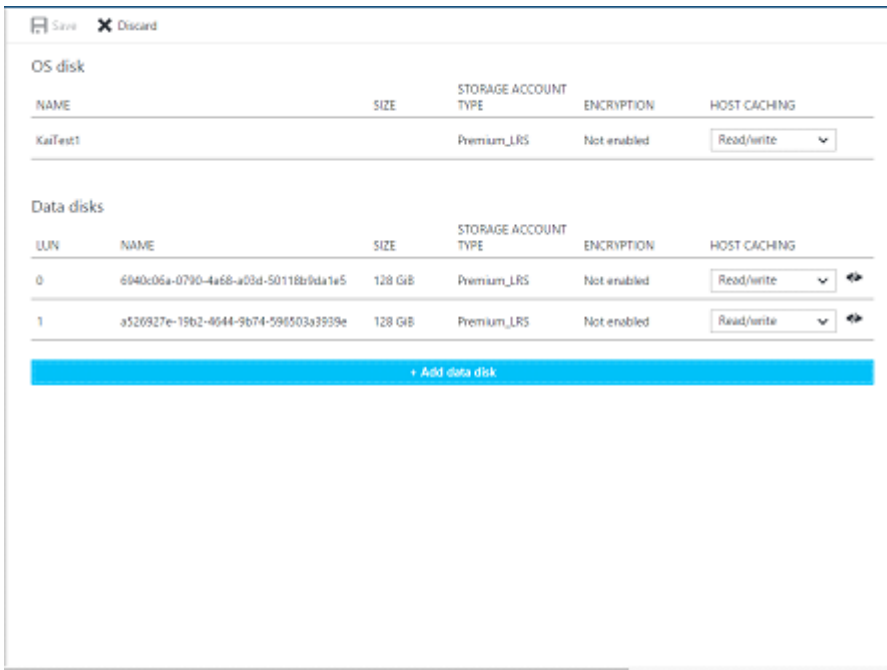


Adding Disks via the Microsoft Azure Portal

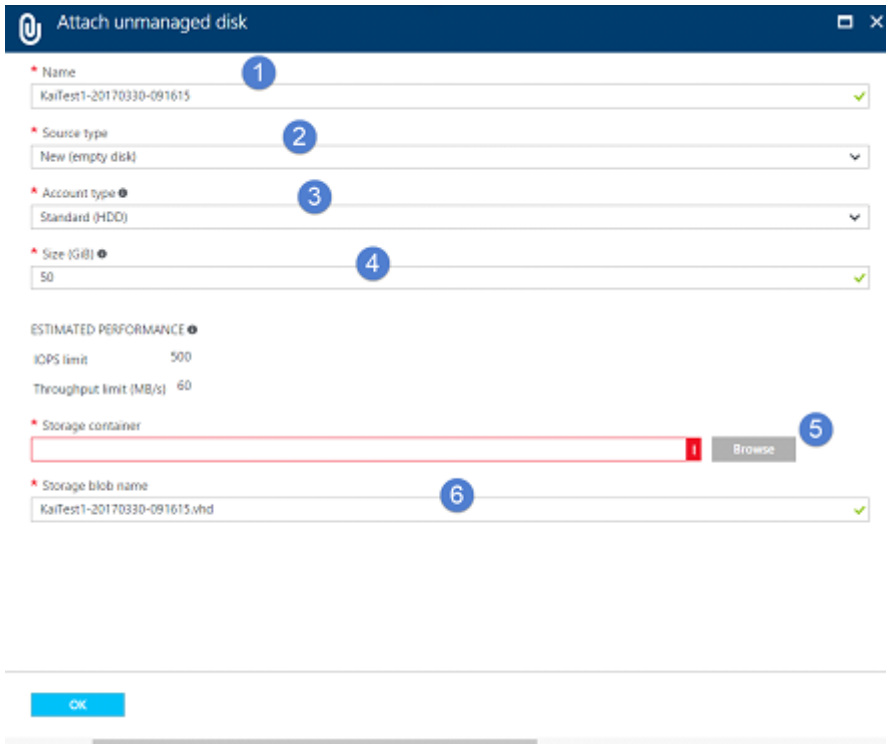
Navigate to the SoftNAS Cloud® instance. Click **Settings**. In the **Settings** blade, select **Disks**.



In the **Disks** blade, select **Add Data Disk**.



You will be taken to the **Attach unmanaged disk** blade.



The screenshot shows a dialog box titled "Attach unmanaged disk" with the following fields and callouts:

- 1**: Name field containing "KaliTest1-20170330-091615".
- 2**: Source type dropdown menu set to "New (empty disk)".
- 3**: Account type dropdown menu set to "Standard (HDD)".
- 4**: Size (GiB) field set to "50".
- 5**: Storage container field with a red border and a "Browse" button.
- 6**: Storage blob name field containing "KaliTest1-20170330-091615.vhd".

Below the fields, there is an "ESTIMATED PERFORMANCE" section showing "IOPS limit" as 500 and "Throughput limit (MB/s)" as 60. An "OK" button is located at the bottom left.

1. Provide a name for the disk.

Note: Retaining the default Disk File Name is possible.

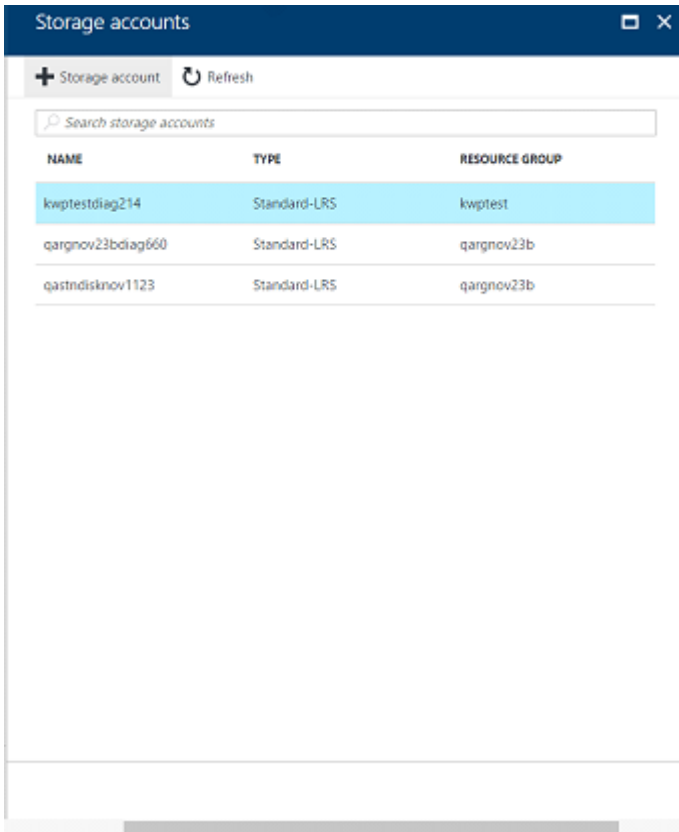
2. Select the source type as new disk. (You can select Existing blob if you have an existing disk.)

3. Specify the account type, Standard (HDD), or Premium (SSD).

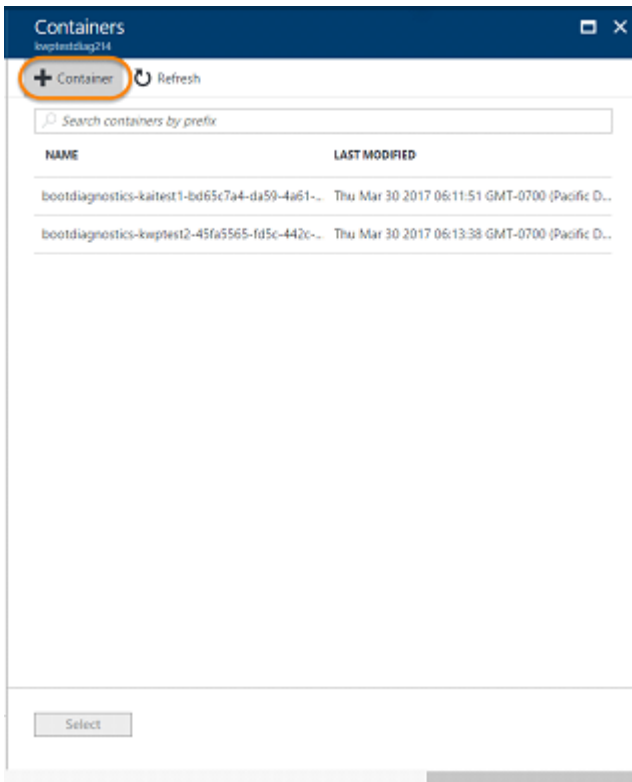
4. Specify the size of the disk – if Standard, this can be any number you like. If Premium, the disk size must match the available SSD disk sizes: 128 GB, 512GB, and 1024GB.

5. Next you will need to select a storage container or create one – if you have an existing container, provide the info in the box provided. If creating one, or if you need to find the existing container, select **Browse**.

a. If searching for an existing container, select the storage account it resides under. If creating one, select the storage account you wish the container to be under. Create one if necessary.



b. Once the storage container is selected (or created, then selected), then select the container from the available options, or create one. Click **+Container** to create one.



c. Provide a name for the container if a new one is being created, and determine access type. By default, access is private. Use Blob for public read access, and Container for public read and list access. Click **Create**.

- d. Select the container, created or existing.
 6. Provide an alternate name for the vhd, if you so choose. Again, the default is acceptable.
 7. Click **OK**, and the disk will be added.
- Now you can create pools and volumes. This process is identical across Cloud platforms.

[Creating Storage Pools](#)

[Configuring Volumes](#)

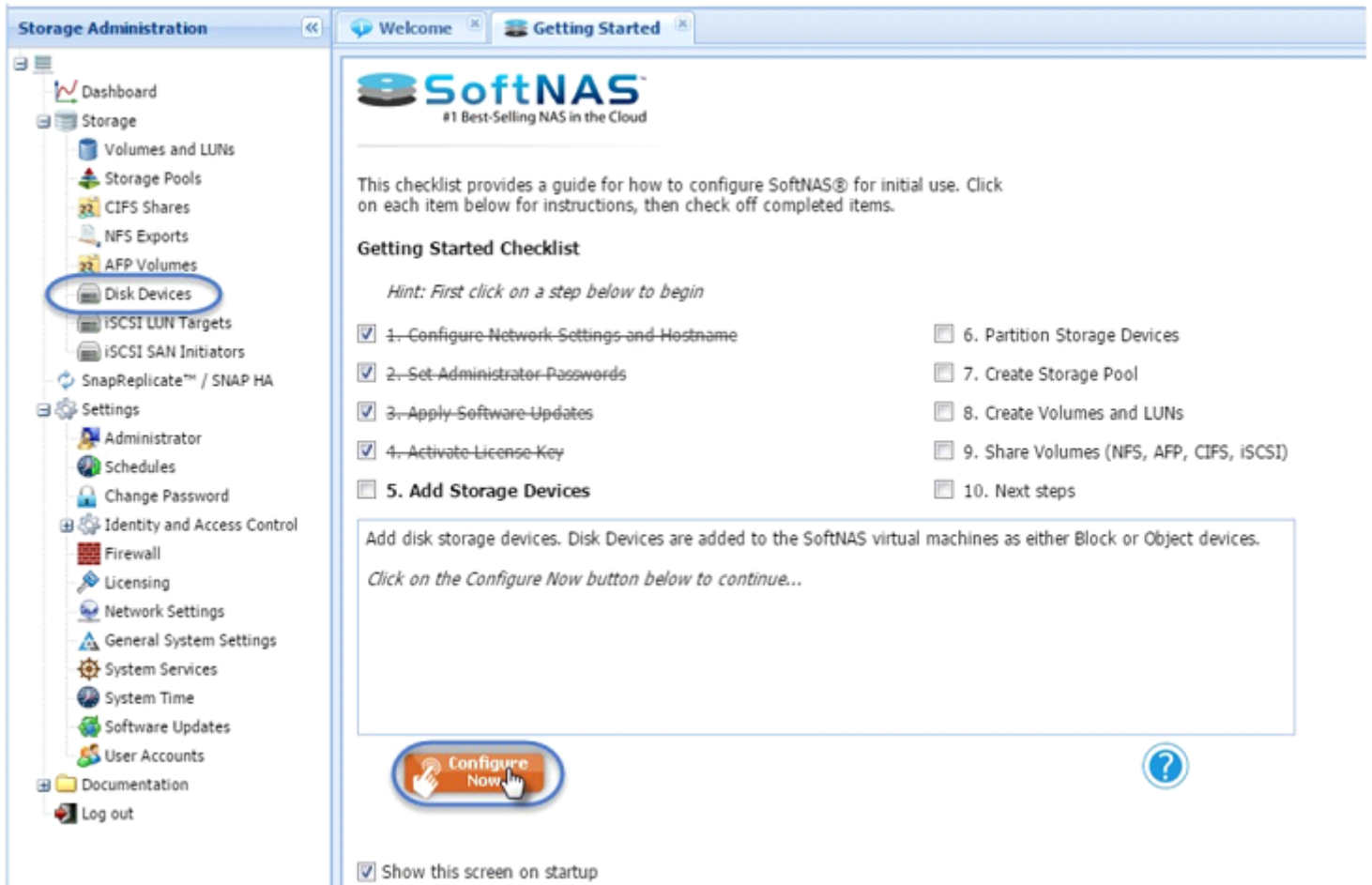
Adding Block Storage via the SoftNAS UI

You can not only add disks from within the Azure Portal, but also quickly and easily from the SoftNAS UI. Users can add Microsoft block storage disks, allowing you to leverage them for pools and volumes.

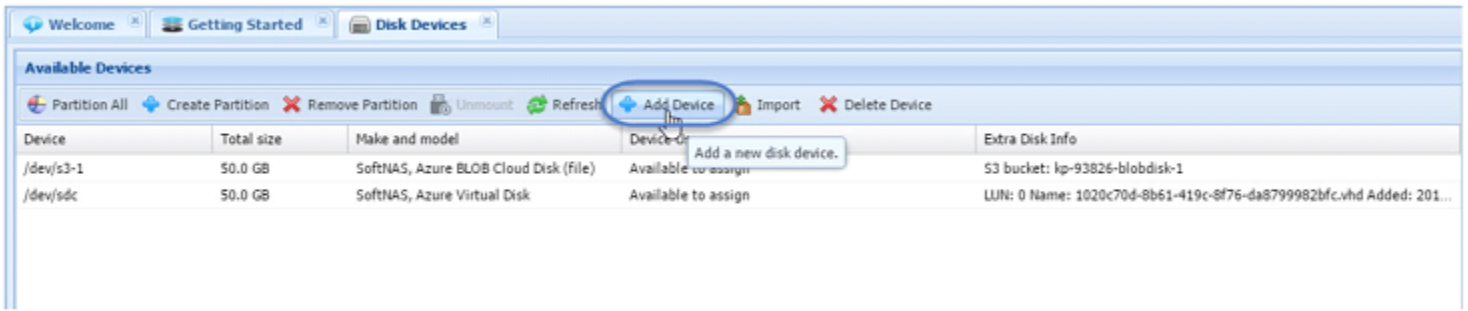
1. Enter the IP address of your instance in order to call upon the SoftNAS login screen.
2. Enter your username and password and click **Login**.



SoftNAS StorageCenter will open. If this is your first login, you will be greeted by the End User License Agreement, then the **Getting Started Checklist**. To add storage, select **Add Storage Devices** from the checklist, then click **Configure Now**, or select **Disk Devices** from the **Storage Administration** pane.



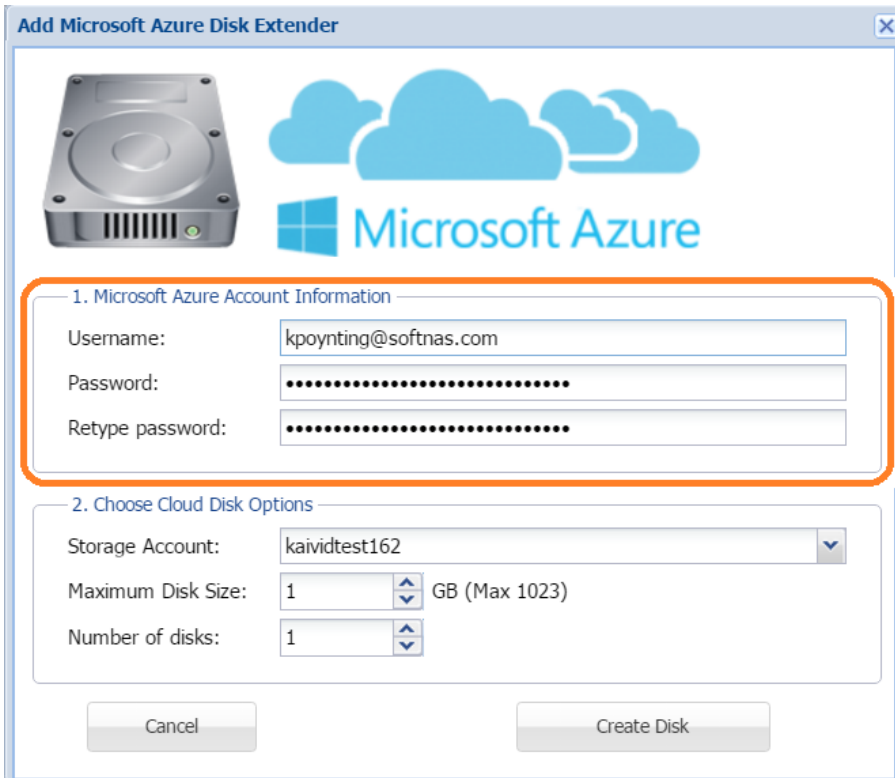
3. The Disk Devices tab will open (if it does not, select it). Click **Add Device**.



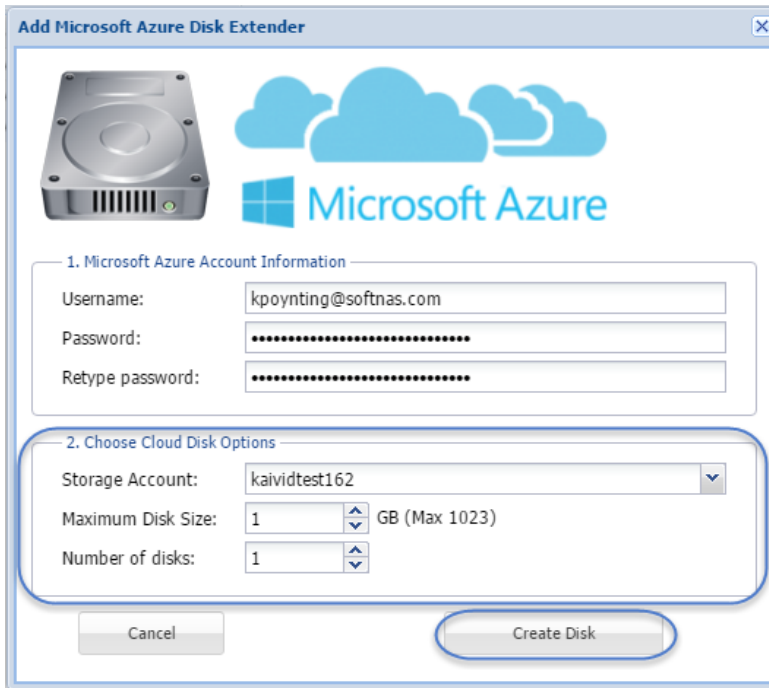
From the Add Disk Device wizard, select the second option, **Microsoft Cloud Disk Extender**. Click **Next**.



4. Provide the service administration account with access to the appropriate subscriptions.



5. Select the appropriate storage account, then set the disk size, and the number of disks you wish to create.



6. Click **Create Disk**.

Note: SoftNAS displays "Creating..." in the Device Usage column until the Adding Disk process is complete. The process is complete when Device Usage reads 'Available to Assign'.

Available Devices

Device	Total size	Make and model	Device Usage	Extra Disk Info
/dev/sdc	25.0 GB	SoftNAS, Azure Virtual Disk	Used in pool pool1	LUN: 1 Name: 038e780c-0060-41bd-b2e3-1c0b1c1d626a.vhd Added: 2016.08.15 ...
/dev/sdd	25.0 GB	SoftNAS, Azure Virtual Disk	Used in pool pool1	LUN: 2 Name: 9a7cfb5e-3df6-4293-9a1b-a53792ff7406.vhd Added: 2016.08.15 1...
/dev/sde	1.0 GB	SoftNAS, Azure Virtual Disk	Creating.....	Azure

Available Devices

Device	Total size	Make and model	Device Usage	Extra Disk Info
/dev/sdc	25.0 GB	SoftNAS, Azure Virtual Disk	Used in pool pool1	LUN: 1 Name: 038e780c-0060-41bd-b2e3-1c0b1c1d626a.vhd Added: 2016.08.15 ...
/dev/sdd	25.0 GB	SoftNAS, Azure Virtual Disk	Used in pool pool1	LUN: 2 Name: 9a7cfb5e-3df6-4293-9a1b-a53792ff7406.vhd Added: 2016.08.15 1...
/dev/sde	1.0 GB	SoftNAS, Azure Virtual Disk	Available to assign	LUN: 3 Name: 1e95ee54-2663-4359-a14a-99a74bda69c.vhd Added: 2016.08.17 ...

It is very simple to add a new disk to your SoftNAS instance using the SoftNAS UI. You can now use your newly added disks to create pools and volumes.

[Create a Storage Pool](#)

[Create & Configure Volumes](#)

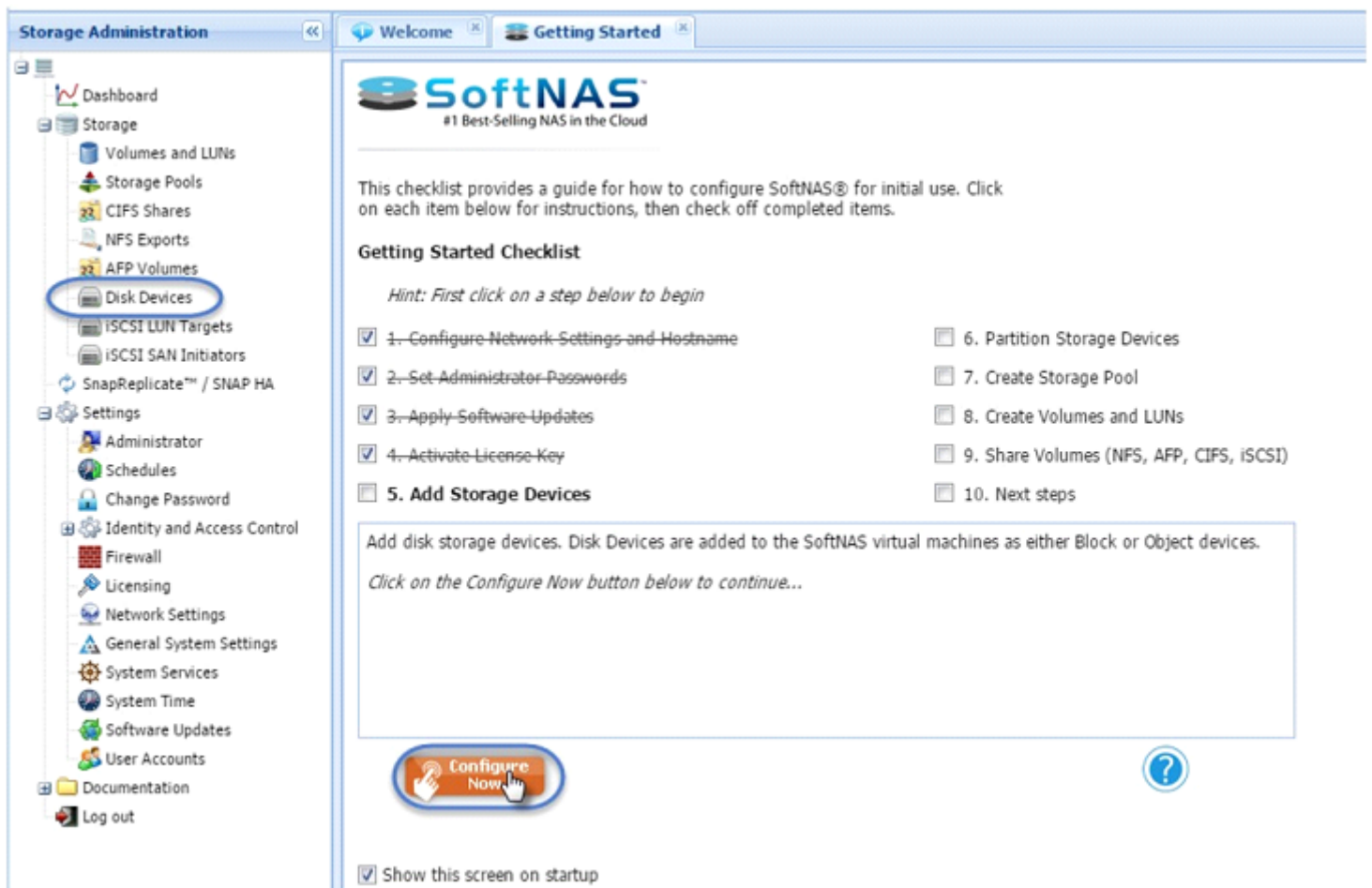
Adding Object Storage via the SoftNAS UI

If deciding to add Azure object storage (otherwise known as Blob storage), you will need to have a Blob storage account set up, or you will not be able to call upon the storage within the SoftNAS UI.

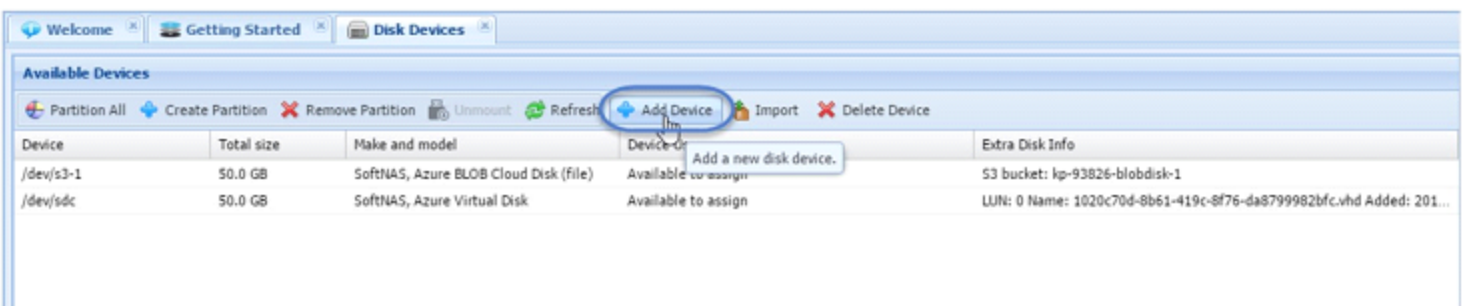
Create Blob Storage in SoftNAS Azure

Once you have the blob storage account, we can add object storage.

1. Log in to the SoftNAS UI, by going to the URL of the VM instance and enter the username and password.
2. If this is your first login to the SoftNAS UI, after accepting the End User License Agreement, you are greeted by our Getting Started Checklist. The first four items are typically taken care of in the creation of the VM from the Azure Portal. Feel free to check them off, as shown below.
3. Select Add Storage Devices and click **Configure Now**. Configure Now will take you directly to Disk Devices. It can also be reached from the **Storage Administration** pane on the left.



4. Select **Add Device**.

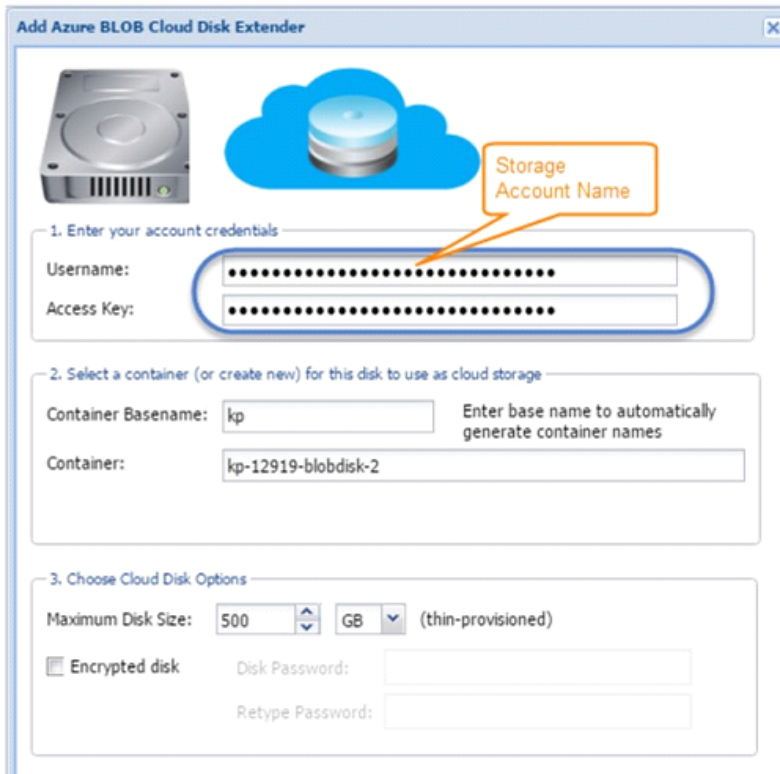


5. In the **Add Disk Device** wizard, you will notice two options, **Cloud Disk Extender**, and **Microsoft Cloud Disk Extender**. For object storage, select the first option. Here you can add object storage options from AWS, CenturyLink and many other vendors. These options are all added in exactly the same method described in [Adding Cloud Disk Extenders](#). Azure Blob is accessed in a similar manner, but has a few differences.

6. In the dropdown, select Azure Blob.

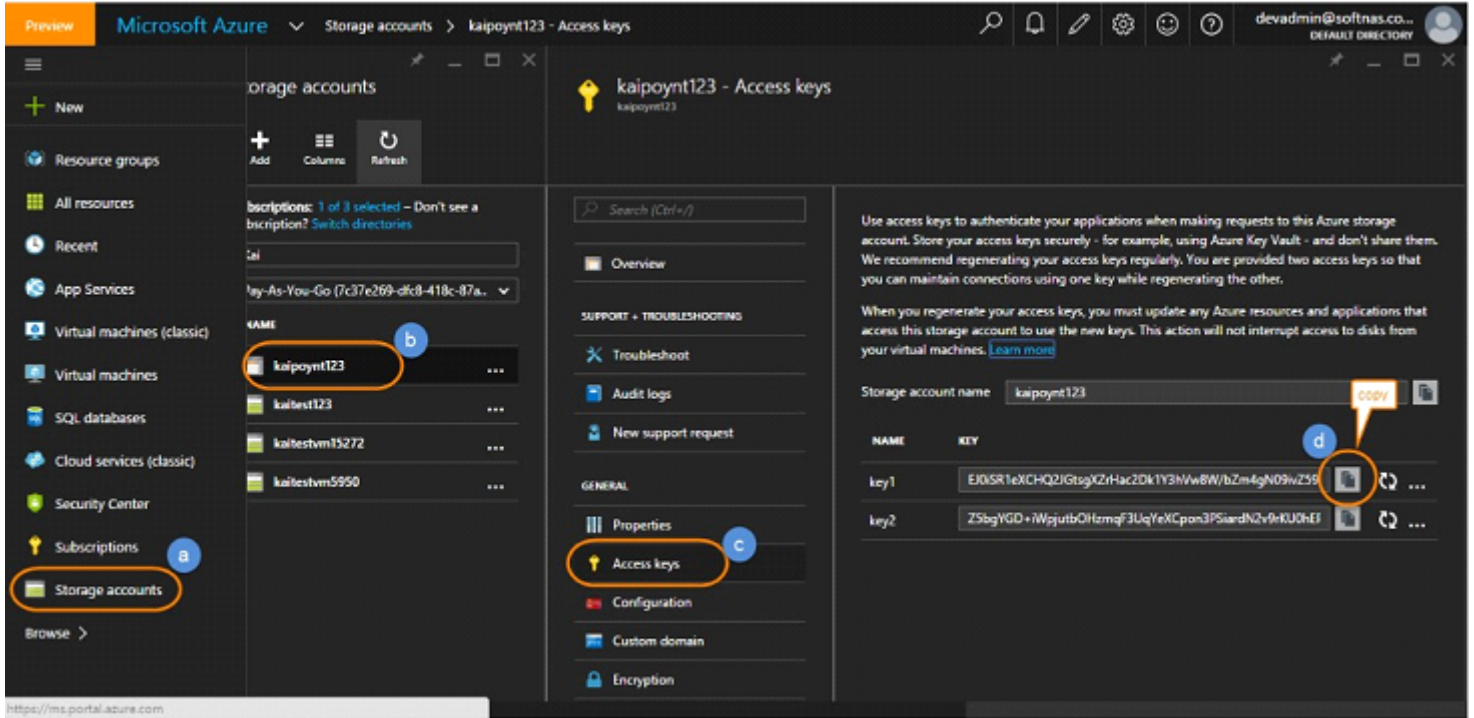


7. The **Add Azure BLOB Cloud Disk Extender** screen will display. This is where you will need the blob storage account we provided instructions for in [Creating Storage Accounts](#). Enter the name of the storage account, and provide the access key for it.



8. If you don't have the storage account and access key handy, go to the azure portal.
- a. Select Storage Accounts.
 - b. Select your blob storage account.
 - c. Under General, select Access Keys.

d. Copy the key.



9. Enter the blob storage account name and access key in the field provided in the **Add Device** wizard.

10. Select the desired size of your instance, up to 500 TB.

11. Click **Create Cloud Disk**.

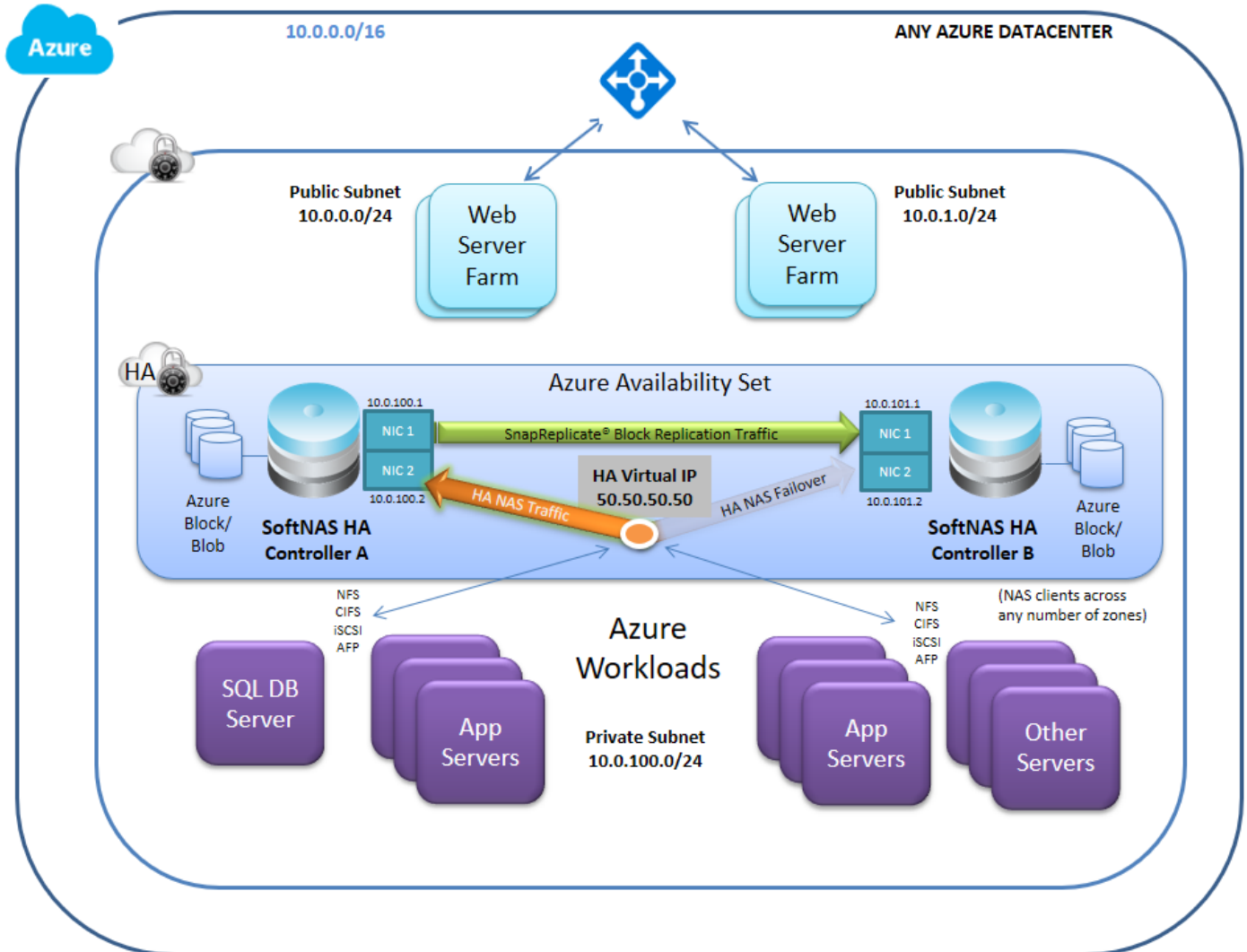
You now have an azure blob disk, configurable into a storage pool and later a volume. Remember that an Azure Blob Storage account can be configured to provide Hot or Cool storage. Each storage account can provide up to 500TB of data. If you need more than this, you will need to leverage additional blob storage accounts. Hot or Cool Storage is applied at the storage account level, and you must be aware of which accounts provide which type. You cannot mix storage types in the same pool. For more information, see [Hot and Cool Storage](#).

To create a pool and volume with your Azure blob disk, see:

- [Create a Storage Pool](#)
- [Create & Configure Volumes](#)

High Availability in Azure SoftNAS

Configuring high availability in SoftNAS Cloud NAS on Azure is a simple process. As with AWS, it involves two nodes with defined IP addresses, and a third human-configured virtual IP to establish a heartbeat between the two instances. However, in order to provide our customers with our No Downtime Storage Guarantee, your two instances will need to be set into an Azure Availability set. We will cover this and more in the sections to follow.

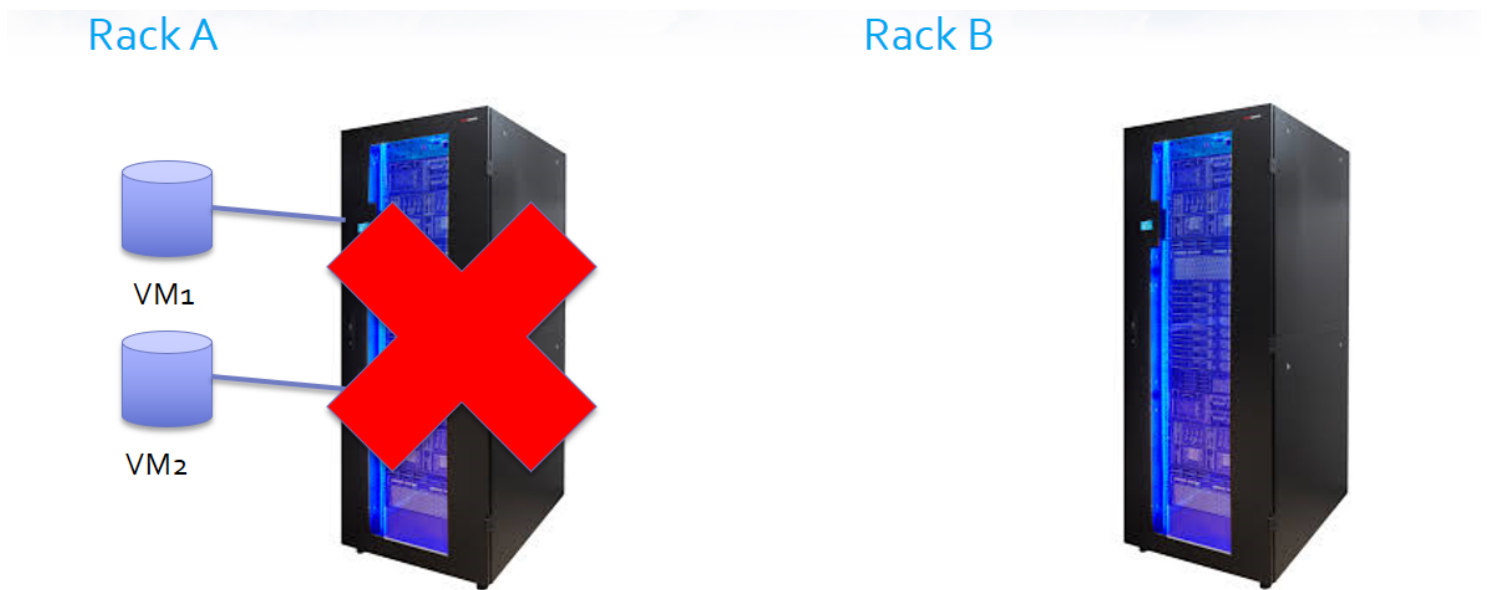


[Azure Availability Sets](#)
[SnapReplicate on Azure](#)
[SNAP HA™ on Azure](#)

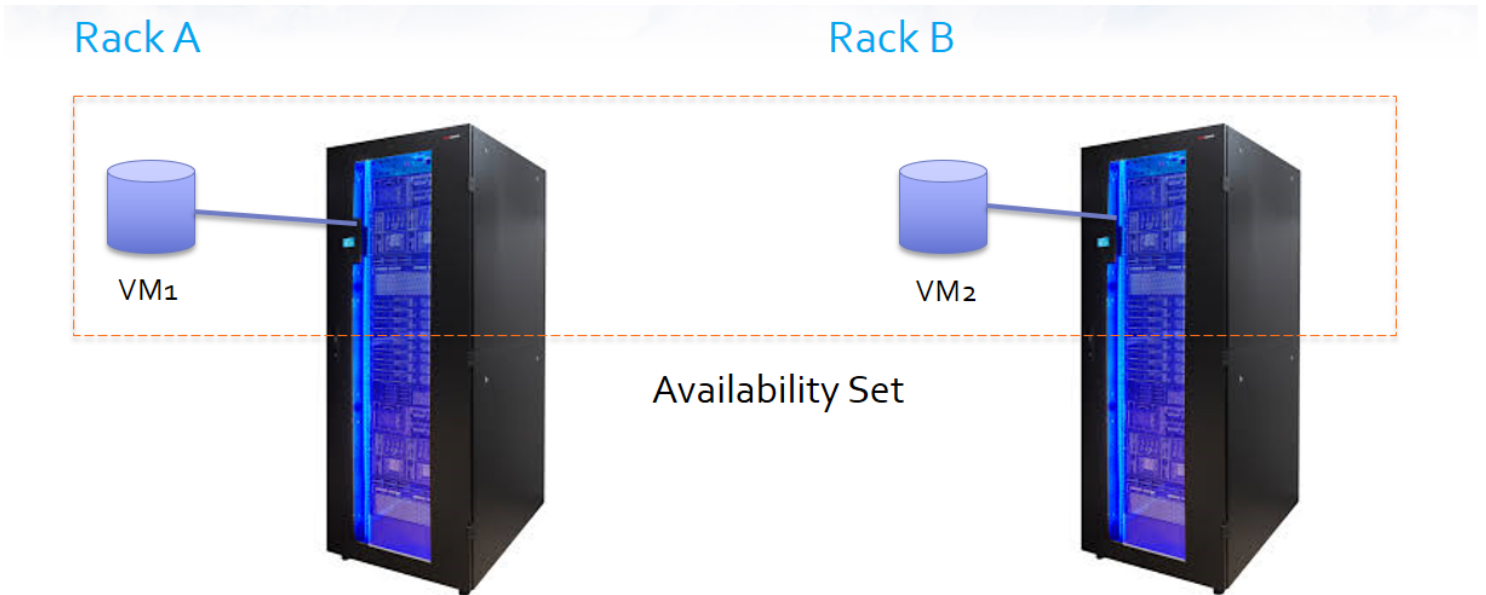
Azure Availability Sets

What is an Availability Set?

Availability Sets make use of two key concepts - Fault Domains, and Update Domains. At its core, Azure consists of racks upon racks of servers. Each rack can host any number of virtual machines. When creating a highly available pairing, you want to be sure that there is no single point of failure, that your workload will still be provisioned by one virtual machine if the other is under maintenance. Unfortunately, if you do not specify otherwise, there is no guarantee that your VMs will not be placed on the same rack, or the same 'Fault Domain'. In essence, a fault domain can be considered a rack within Azure. Every VM on the rack is subject to that rack's power and network connections. A rackwide failure, or a rackwide maintenance window will take down all VMs hosted on this single point of failure. When Azure refers to a fault domain, consider each fault domain a single point of failure.



An Availability Set distributes highly available workloads across multiple Fault Domains, thereby eliminating any single point of failure. Unless the entire data center is down, your workload will keep running. In essence, your workload is split between two or more racks, leveraging the redundant power supplies, network switches, etc, of each.



Grouping VMs in an availability sets also gives the Windows Azure Fabric Controller (FC) the information it needs to intelligently update the host OSs that your guest VMs are running on. Without availability sets the FC would have no idea that two machines were serving the same purpose and could reasonable take them both down for host OS updates.

An Availability Set also makes use of Update Domains. This allow you to determine how many of the workloads are down at any given time. You can set a priority order for shutting down the VMs and the number of update domains determines how many machines will be involved in the shutdown. In the image below, we see an Availability Set with 16 virtual machines, and four update domains. This means that a maximum of four VMs can be down for maintenance at a given time, allowing the other 12 to carry the load. Once the first four return to service, another group will be available for maintenance. In conjunction with Fault Domains, this allows an Availability Set to ensure that undue burden is not placed on either rack.

Availability Set 1

Update Domain 1	Update Domain 2	Update Domain 3	Update Domain 4
VM1 – updating	VM2	VM3	VM4
VM5 – updating	VM6	VM7	VM8
VM9 - updating	VM10	VM11	VM12
VM13 - updating	VM14	VM15	VM16

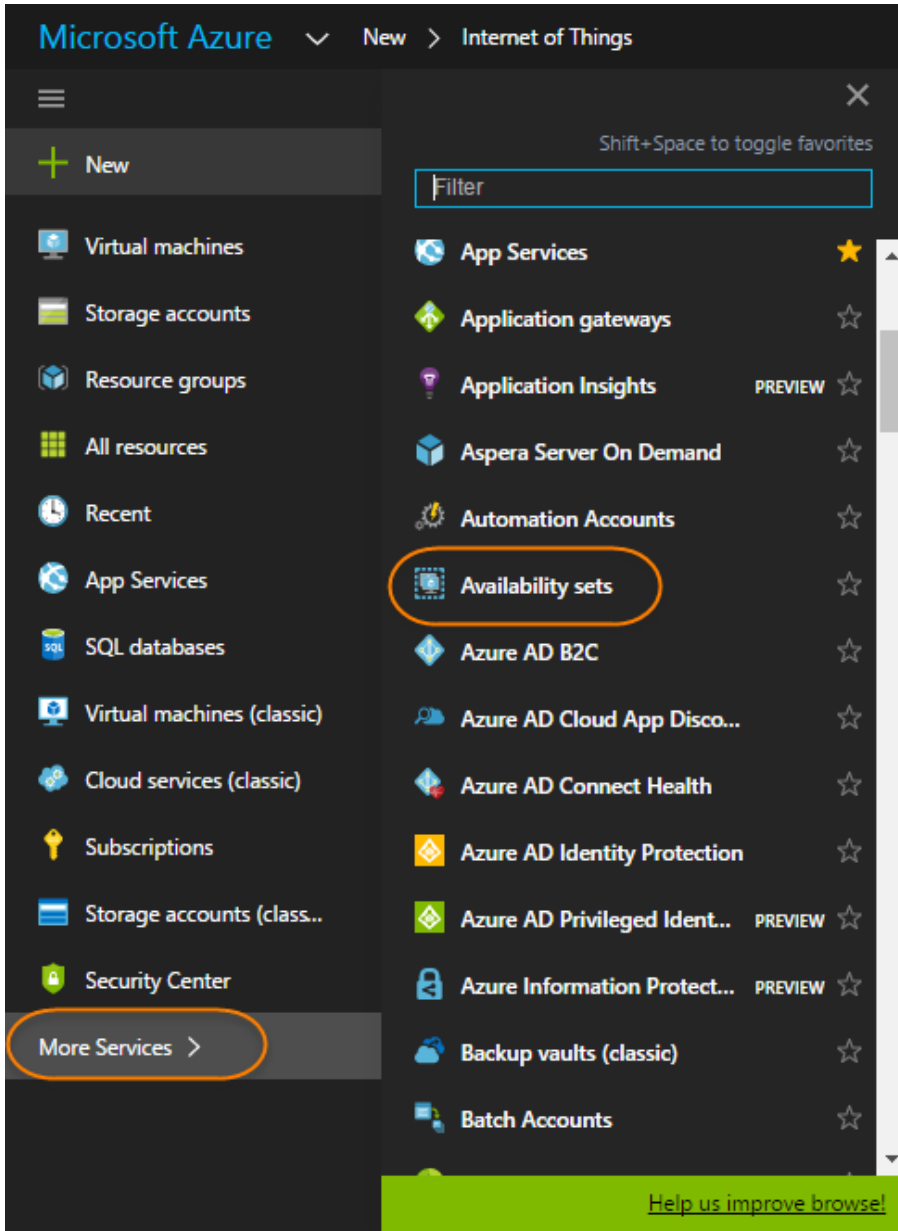
When considering your use case, including the number of VMs you want to create and the number of Availability Sets you will need to create, remember that as a rule, you want one Availability Set per workload. A workload can be considered any virtual machines working together towards a common single purpose. Therefore, two highly available SoftNAS VMs to perform a single function would constitute a workload.

Creating An Availability Set

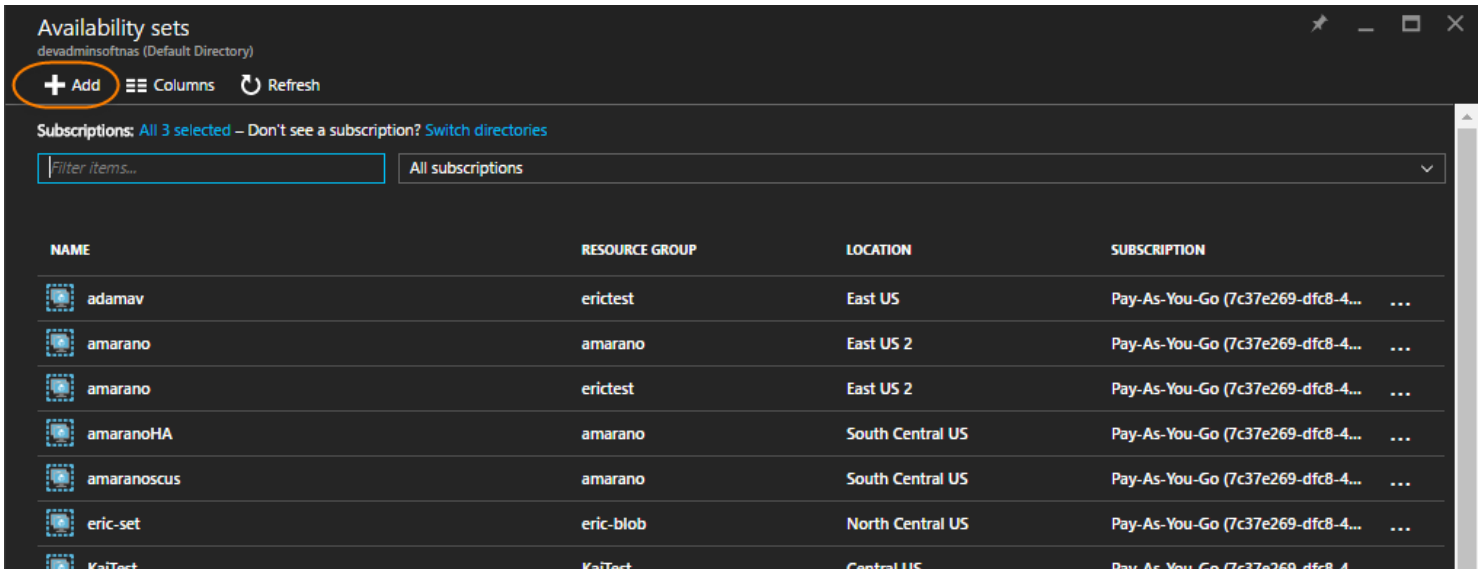
Creating an Availability Set in the Azure Portal can be done in one of two ways - while creating your VM, or separately.

Creating Separately

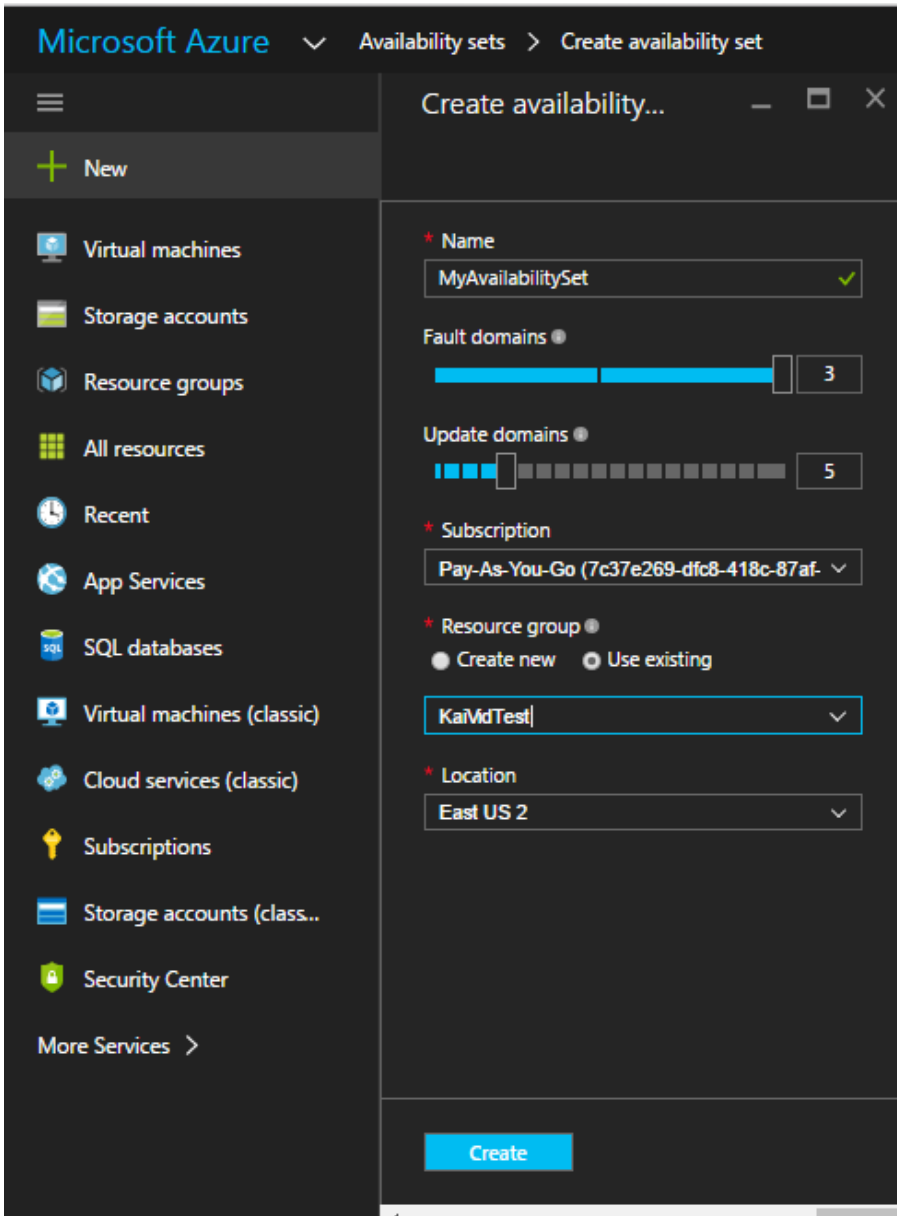
To create an Availability Set prior to creating your virtual machines, select **More Services**, then **Availability Sets** from the listed options.



Click **Add**.



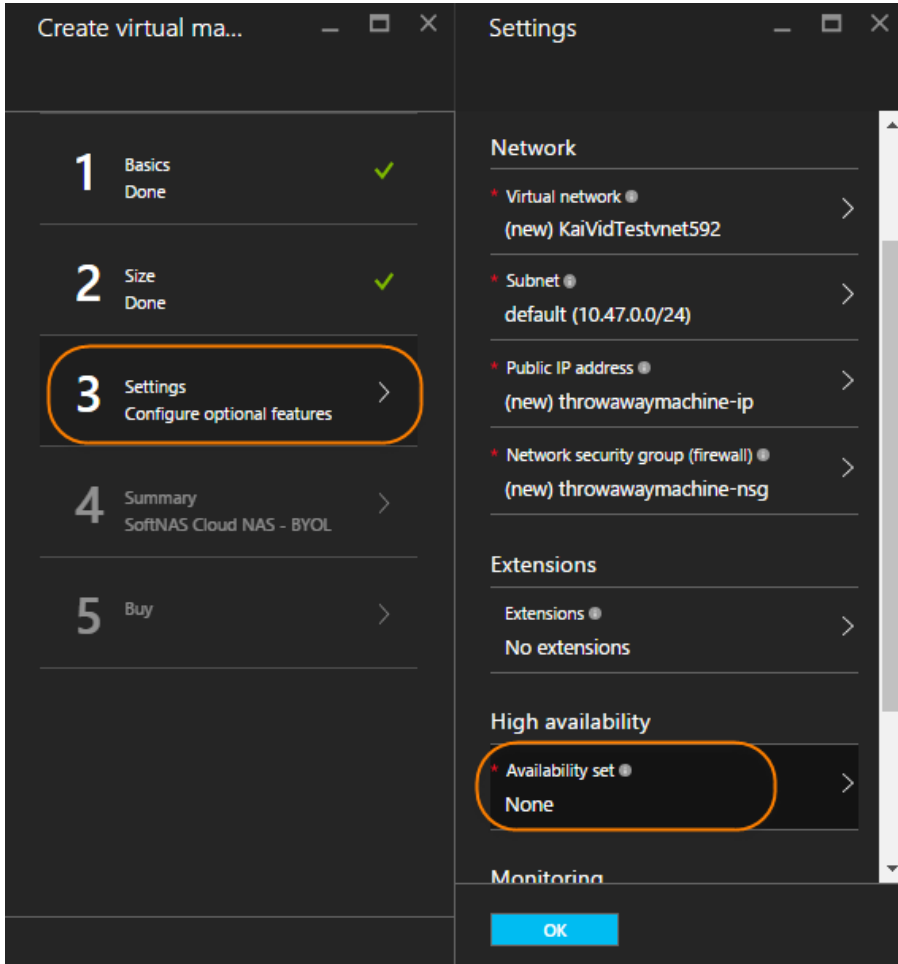
Provide a name, the subscription that the Availability Set belongs to, the number of Fault Domains and Update Domains you require for your particular purpose, and create or select an existing resource group. Finally, select a location.



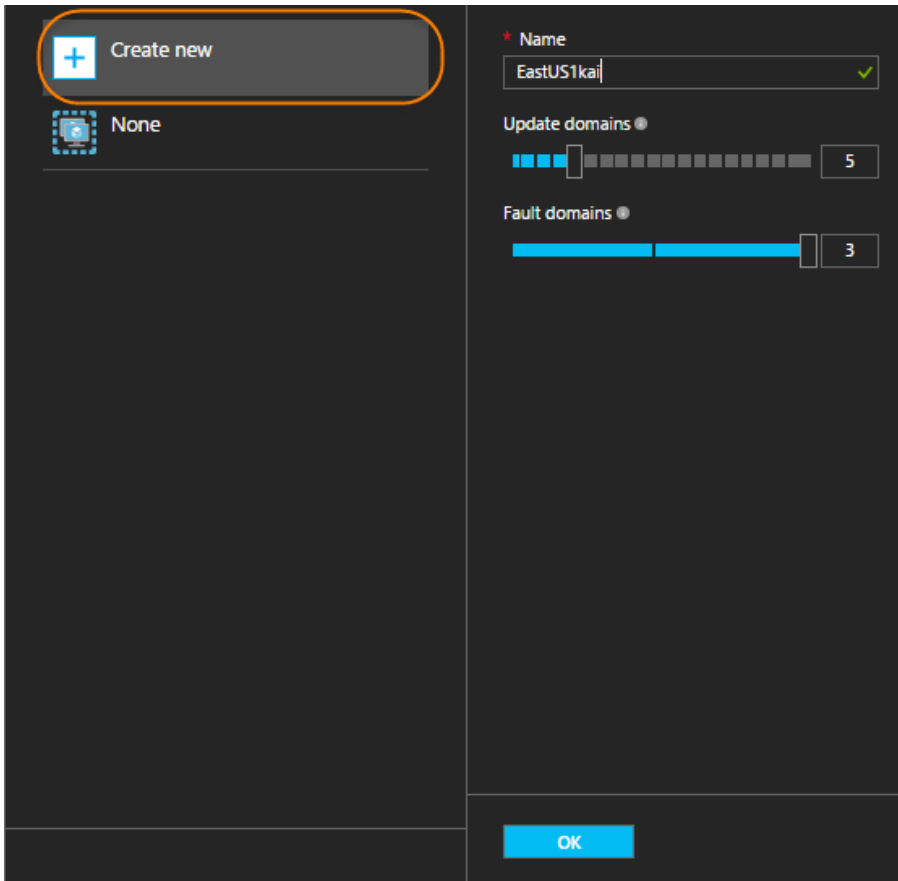
During VM creation

If creating a VM, it is possible to select an existing Availability Set, or to create one for your instance. When adding your virtual machine within an Availability set, or creating one, remember that for a given workload, both must be in the same Availability Set. A virtual machine cannot be moved from one availability set to another after creation.

Creating your virtual machine is well documented in [Create and Configure a Virtual Machine in Azure](#), so we will not cover the topic in detail. It is in the third part of VM creation, **Settings**, in which your Availability Set can be created or selected.

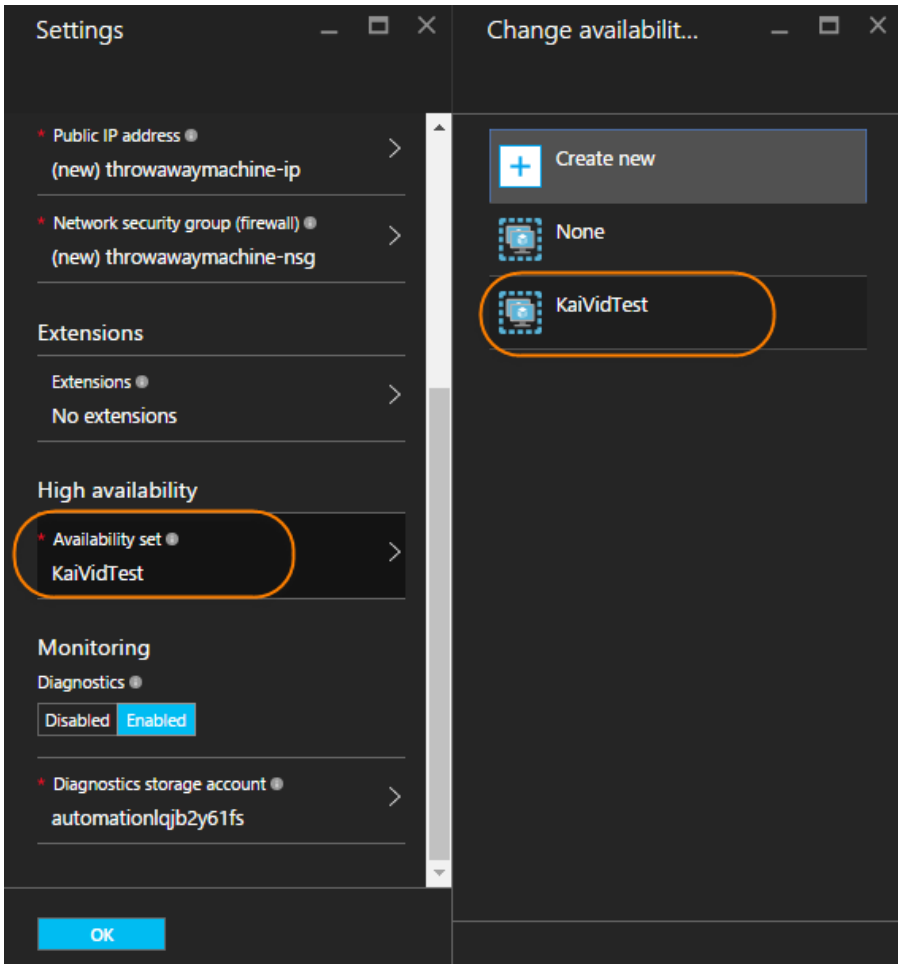


Once Availability Set has been selected, you will have the option to create a new Availability Set, or select from existing if available within the current resource group and location. To create a new Availability Set, click **Create New**.



Note that the menu here is much simplified, as your resource group and location were already determined when establishing the 'Basics' for your VM. These settings are automatically applied to your Availability Set using this method.

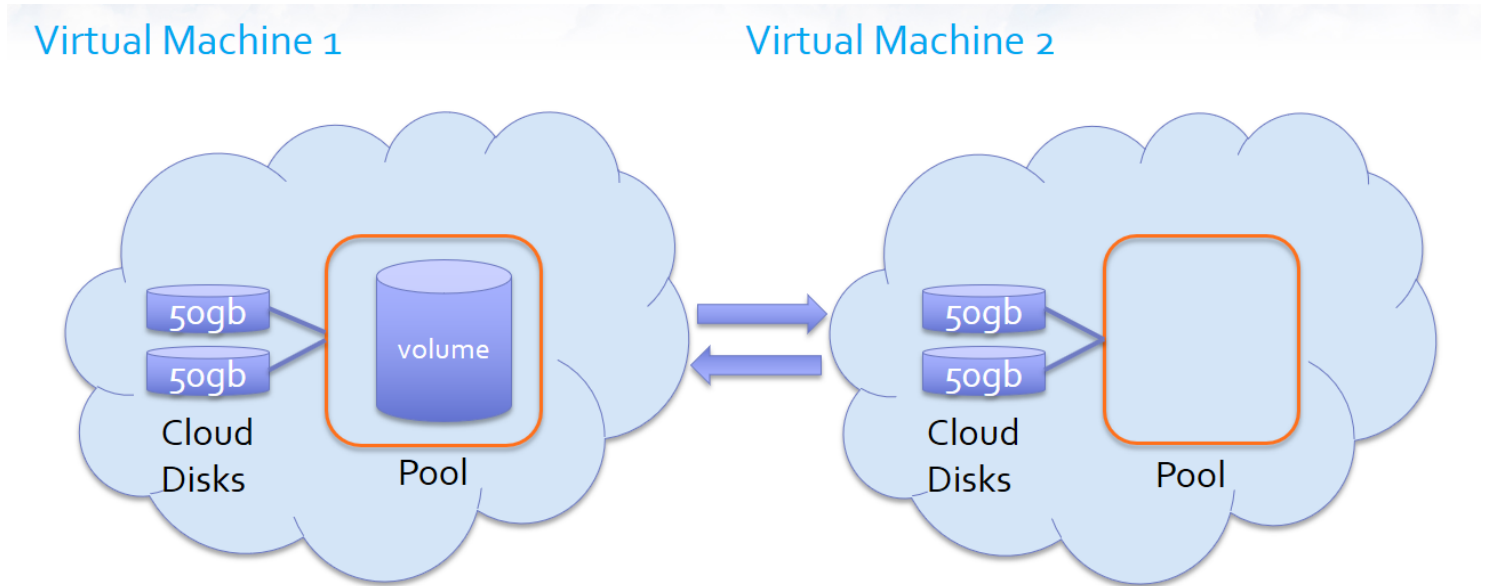
If a pre-existing Availability Set is available, simply select it, and it will be applied to your VM.



Remember again, if you create or add an availability set to the first VM of your HA pairing, the second ***must*** be added to the same availability set.

SnapReplicate™ on Azure

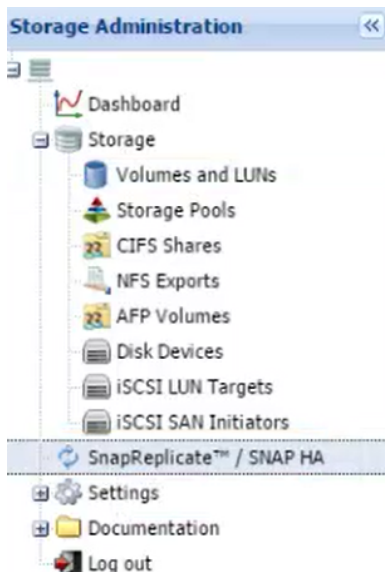
SnapReplicate™ provides quick and easy replication between two paired SoftNAS Cloud NAS instances. This requires some basic preliminary setup, including adding storage, creating a pool, and creating a volume on the first instance, then mirroring that configuration, minus the volume, on the second instance. In essence, you must create a landing strip for the volume on the target instance.



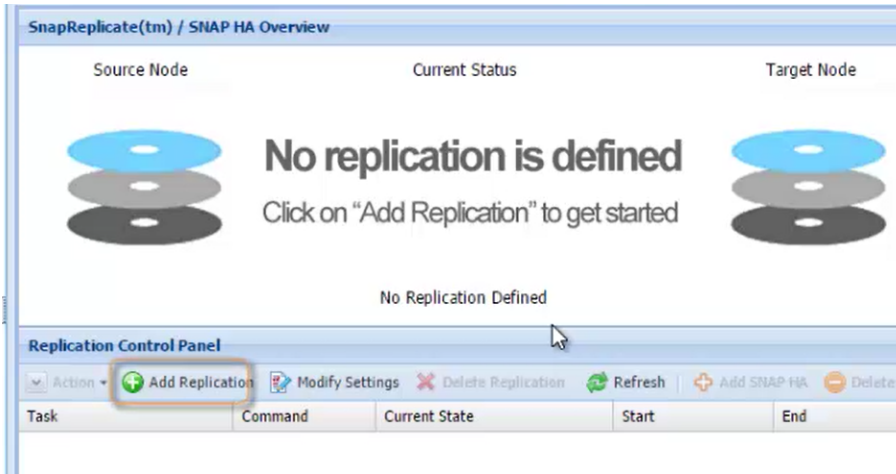
The above is a very basic representation, illustrating two cloud disks in a RAID configuration (any RAID configuration of at least two disks) forming a pool, with a volume created on the source instance. On the target instance, disks of the same size and RAID configuration are set into a pool of the same name. This basic configuration is used for each platform upon which SoftNAS is available, including AWS and VMware. Provided disks and pools are in a mirrored configuration, the volume or volumes in the pools can be replicated.

Once the above configurations have been established, setting up SnapReplicate™ for Azure is a simple process.

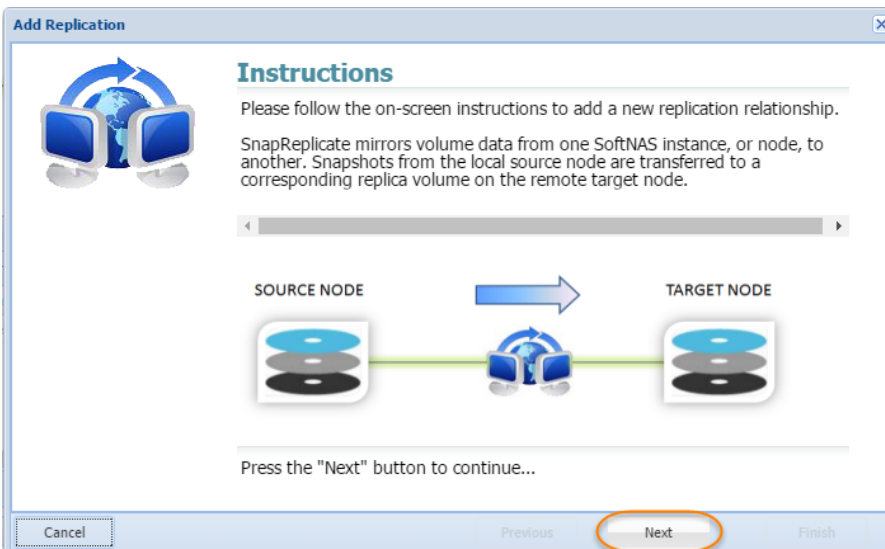
1. Log into the source instance (via the IP address in your browser.)
2. Select **SnapReplicate™/SNAP HA** from the **Storage Administration** pane.



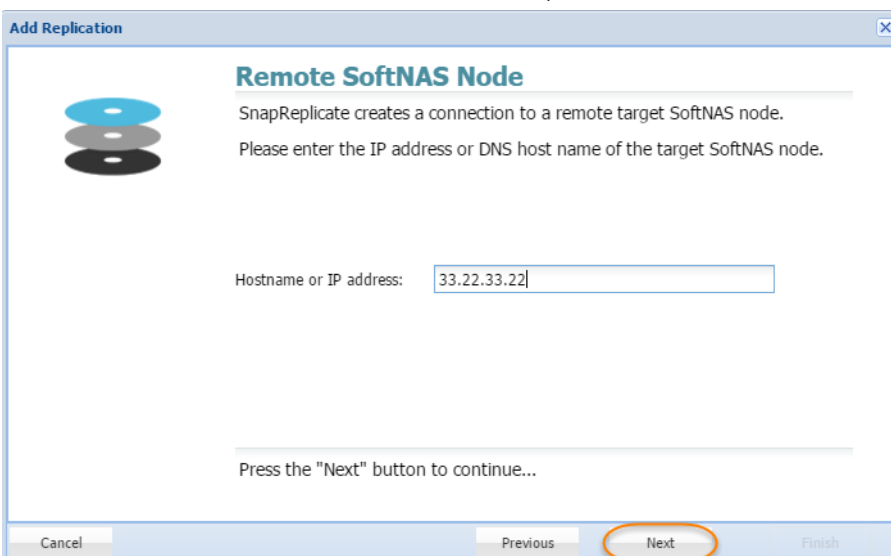
3. The **SnapReplicate/SnapHA** window opens. Click **Add Replication**.



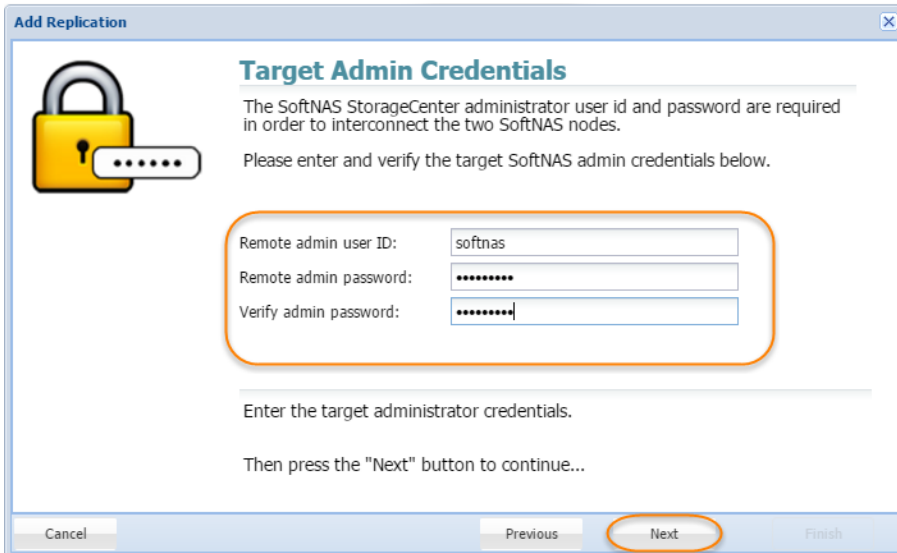
4. The **Add Replication** wizard will open. Click **Next**.



5. In the **Remote SoftNAS Node** window, enter the IP Address of the Target Node. Click **Next**.



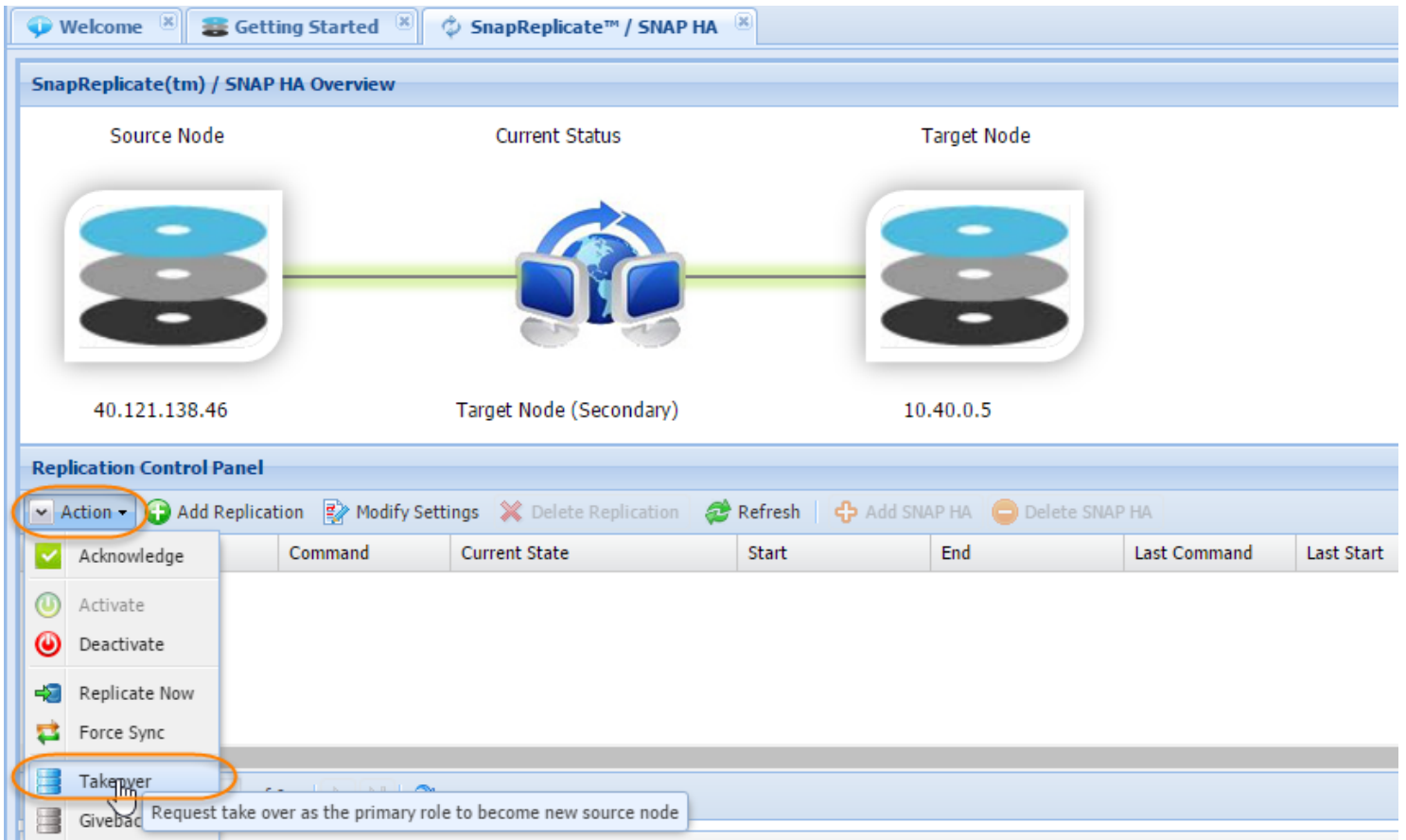
6. Enter the credentials for the target softNAS node (by default this will be a username of softnas, and the password established in setup, unless alternate credentials were created). Click **Next**.



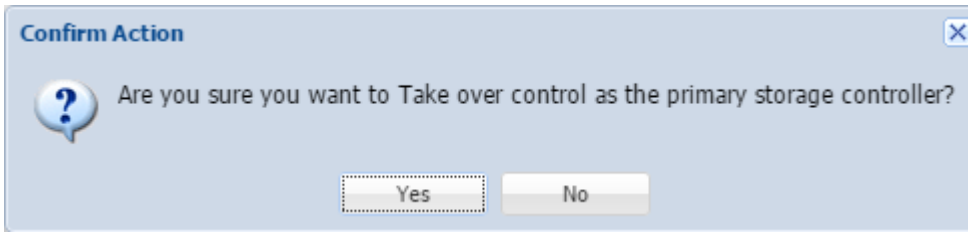
7. Click **Finish**, to complete the wizard.

Testing Replication

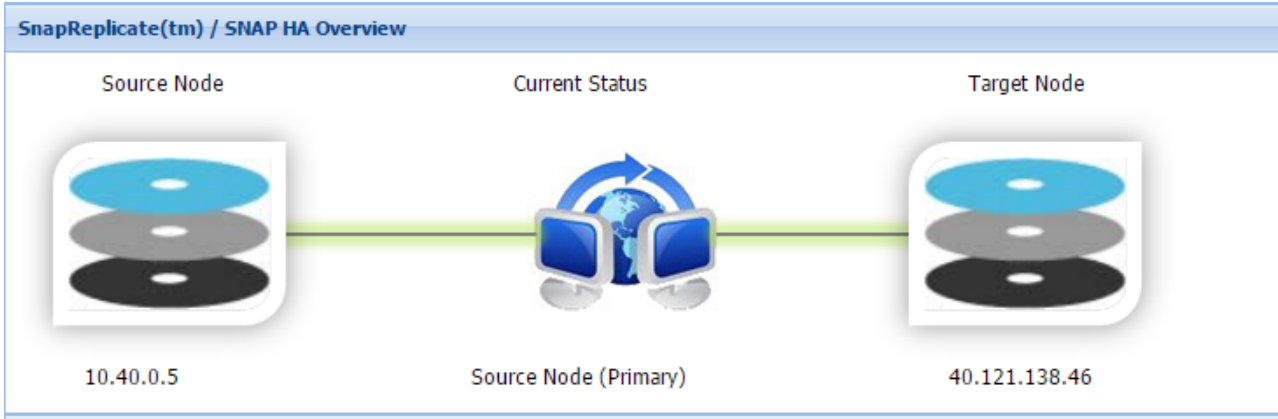
1. To test the replication, move to the target node, and confirm that the volume from the source node is replicated to **Volumes and LUNS**.
2. Still on the target node, return to SnapReplicate/SNAP HA, and click **Actions** and then **Takeover**.



3. Click **Yes** on the confirmation prompt.



4. The target node will become the primary.

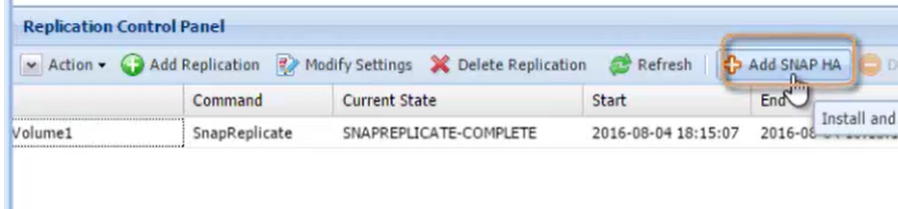


5. Return to the former source node. Click **Actions** and **Takeover** to restore the source node as Primary.

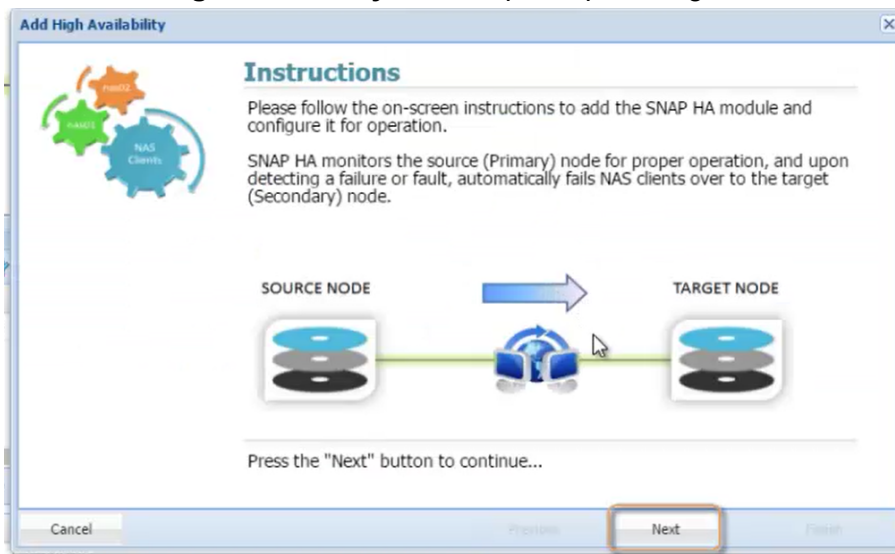
SNAP HA on Azure

SnapReplicate™ allows for manual replication of volumes to another node in the event of a problem or a planned maintenance. SNAP HA allows replication to be triggered automatically in such a case, by establishing a heartbeat between linked instances. If the heartbeat fails to register for more than a few moments, the other instance takes over, ensuring seamless access to the provisioned data.

1. To set up SNAP HA, start the process by clicking **Add SNAP HA**.

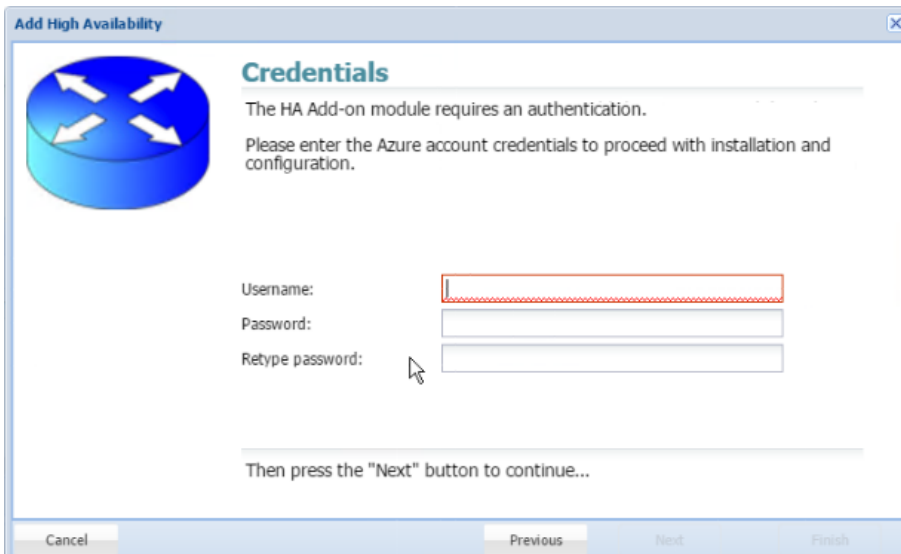


2. The **Add High Availability** wizard opens, providing an Instruction window. Click **Next**.



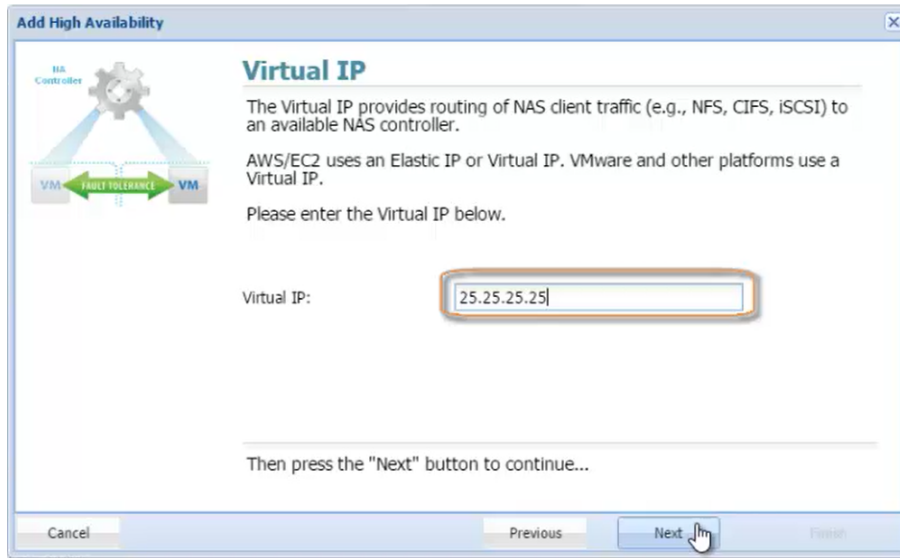
3. The next screen depends upon whether your storage pool has made use of MSFT disks added from within the SoftNAS UI (as explained in [Adding Block Storage via the SoftNAS UI](#)), or if you added [Azure Blob Storage](#) disks, or added your [block storage disks through the Azure Portal](#).

If you added Azure Blob Storage or used the Azure Portal to add your disks, then you would first have to provide Azure account credentials before being prompted to enter your Virtual IP Address.

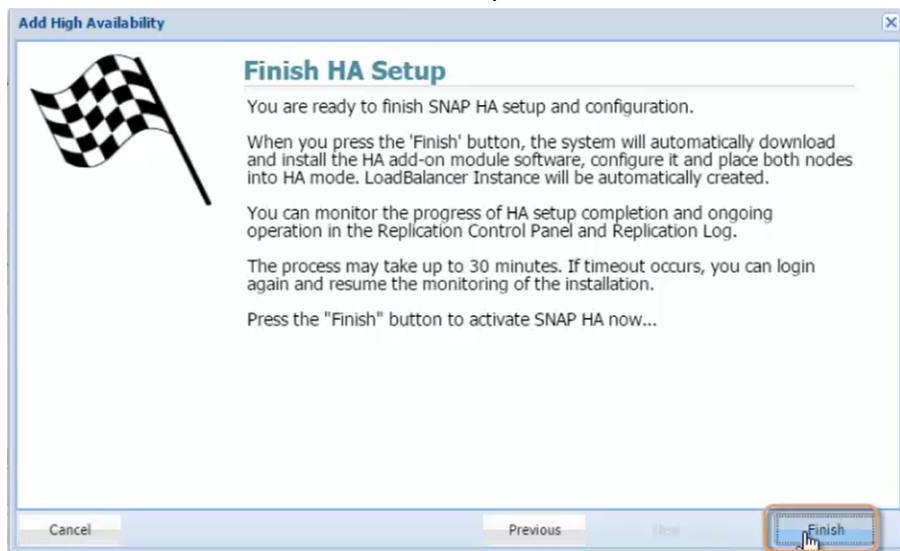


4. If you added Microsoft disks using the SoftNAS UI, you will have supplied Azure credentials already. In this case, the wizard will skip ahead to the Virtual IP screen. This is because your credentials would be cached in order to speed up the process.

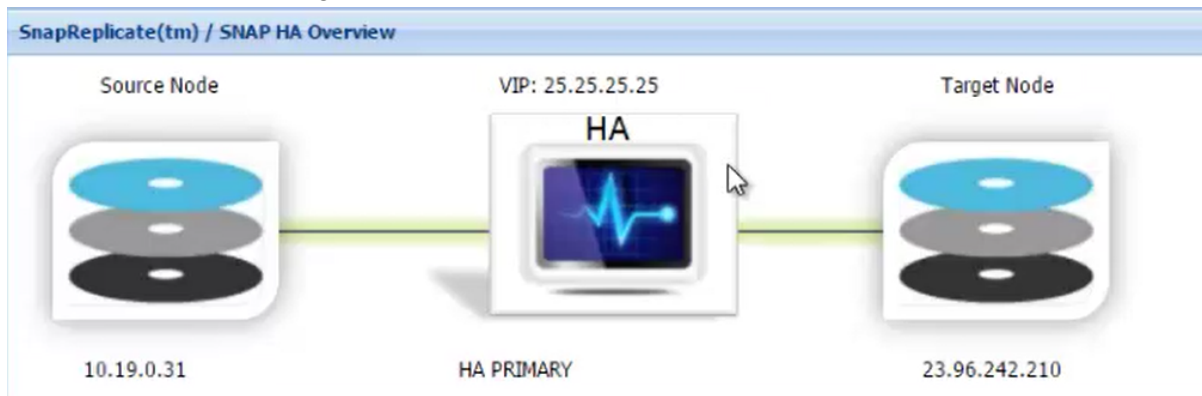
Here you will create and add an IP Address that is not in the same CIDR block as the instances. (In simplest terms, ensure that the IP address does not start with the same numbers as the two instances.) Click Next.



5. Click **Finish** on the Finish HA Setup screen.



6. Your SNAP HA pairing is created.



To test, shut down one of the instances. The other will become primary after a few moments. Alternatively, select **Actions**, and **Takeover** to simulate a failover.

Connecting to the SoftNAS StorageCenter

Once the **SoftNAS Cloud®** instance in **Microsoft Azure** has been created, it can be connected to via **StorageCenter** for administrative tasks.

- Connect Via SSH to create the **SoftNAS Cloud®** password.
- Connect to **SoftNAS StorageCenter** using the domain name of the **SoftNAS Cloud®** instance, such as **softnastest.cloudapp.net**

Set the SoftNAS Cloud® Password

Set the **SoftNAS Cloud®** password from either Windows command line or using Linux/OS X Terminal (Terminal).

Create the Password Using Terminal

1. Open Terminal and run the following command

```
ssh -i [softnasazure] softnas@softnastest.cloudapp.net
```

Where *[softnasazure]* is the pathname to the [private key file on the host](#)

Upon the following message:

```
Last login: Wed Oct 22 10:36:52 on ttys000
Mark's-MBP:~ markbic$ ssh -i softnasazure softnas@byol.cloudapp.net
The authenticity of host 'byol.cloudapp.net (104.45.239.12)' can't be established.
RSA key fingerprint is 4a:b0:cf:e0:c9:a2:b1:00:64:7c:d0:21:62:bf:c1:57.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'byol.cloudapp.net,104.45.239.12' (RSA) to the list of known hosts.
Last login: Wed Oct  1 12:53:00 2014 from 202.88.235.51
```

2. Select **Yes** to continue connecting to the remote server.

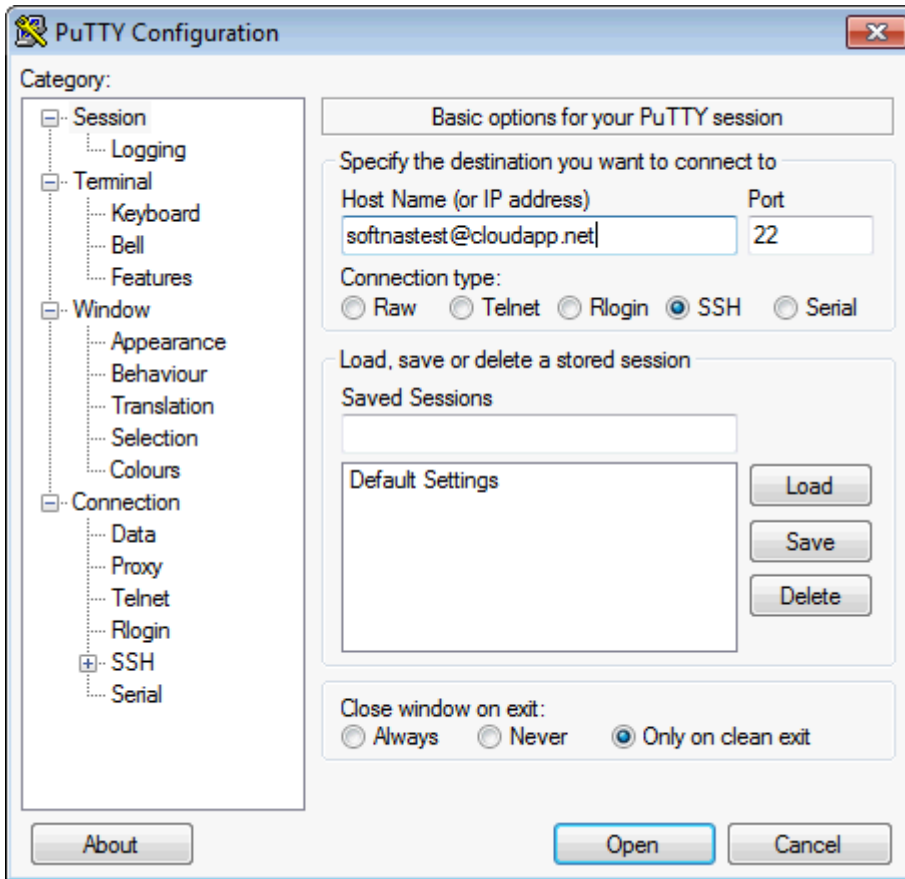
3. From Terminal run the following command:

```
sudo passwd softnas
```

Enter a new password and confirm the password.

Creating the Password from Windows (PuTTY)

1. Open PuTTY and connect to the **SoftNAS Cloud®** domain name on port 22.



2. From PuTTY terminal run the following command

```
sudo passwd softnas
```

Enter a new password and confirm the password.

Connecting to StorageCenter

1. From the **Microsoft Azure Management Portal**, click on **Virtual Machines > Settings > Properties**.

2. Take note of the domain name for the **SoftNAS Cloud®** instance. e.g., softnastest.cloudapp.net

Note: This will be the domain name used to connect to **SoftNAS Cloud®**.

3. Navigate a web browser to the **SoftNAS Cloud® VM** domain name.

The **StorageCenter** login screen is displayed.



Log in to SoftNAS StorageCenter™

2. Enter the following credentials:

- For username: **softnas** (set in the Azure store during VM creation).
- For password: Provide the [password set via SSH](#) or modified above.

Upon a successful connection, the **StorageCenter** GUI is displayed. Continue to [SoftNAS Cloud® Configuration](#).

CenturyLink

SoftNAS has partnered with CenturyLink, allowing SoftNAS Cloud® instances to be deployed on CenturyLink cloud storage. CenturyLink is a widely respected player in the internet, cloud services and data management industries, with clients all over North America, from residential to enterprise. SoftNAS has provided a Virtual Appliance - what CenturyLink calls a Partner Template - that can be deployed to your CenturyLink Cloud account via a Service Task.

This deployment process for Partner Templates currently requires manual interaction via the Service Task process, but will be further automated in future releases of the CenturyLink Cloud Platform.

See "[Setting up SoftNAS on CenturyLink](#)" for more detailed instructions on setting up your CenturyLink with SoftNAS instance.

SoftNAS Cloud® System Requirements

Listed below is a table to assist with the setup decisions during the configuration required to accomplish various tasks and goals.

	Recommended
Compute	
Regular Tier	Under 15000 iOPS
Hyper-scale	Over 15000 iOPS
Memory	
Configurable	1GB -128 GB
Storage	
Boot Disk	30 GB Hard disk for Linux boot and system disk
Data Disks	Native Storage Devices 1Gb to 1 Terabyte volumes, up to 4 Terabytes per instance (4x1 terabyte volumes). Also compatible with S3 storage spots.
Software RAID	Recommended to configure EBS disks using SoftNAS software RAID for increased performance and data durability.
Networking	
High Speed Connectivity	All CenturyLink VMs operate at 10 GbE inter-connectivity.
HA Networking	Supported on same 10 GbE interfaces
HA Host Failover	Configure multiple redundant SoftNAS Cloud® instances in separate availability zones or different geographic regions.

Note: Refer to CenturyLink's documentation for storage tiering SSD performance metrics.

SoftNAS Cloud® System Capacities

Listed below is a table representing the capabilities of the **SoftNAS Cloud®** for **CenturyLink**.

	SoftNAS Cloud® Capacity	Configuration Note
Editions		
SoftNAS Cloud® Express	1 TB	

SoftNAS Cloud® Standard	20 TB	
SoftNAS Cloud® Enterprise	16 TB	
Memory		
RAM Cache	1 GB to 100 GB	Defaults to 50% total RAM for read cache
SSD Cache	low-speed level 2 cache	Optional
Ephemeral Cache	low-speed level 2 cache	Optional for read cache
Storage		
Maximum Storage	16 TB	Maximum usable storage capacity with SoftNAS Cloud®, contingent on instance type.
# of Storage Pools	Unlimited	
# of Volumes	Unlimited	
# of Snapshots	Unlimited	
# of Snapshot Clones	Unlimited	
SnapReplicate	Unlimited Pools & Volumes	
SnapReplicate Throttle	56Kb/sec to Unlimited bandwidth	
Active Directory	Kerberos Integration	
Files and Directories	Unlimited	
Network		
Schedules	Unlimited	
NFS Exports:	Linux Default	
iSCSI Targets	Linux Default	
CIFS Shares	Linux Default	
Firewall Ports:	22 (ssh), 443 (https)	Plus NFS, iSCSI, and CIFS as required by network
IP Tables Firewall	Off by default	May be configured, but is not required. Use an alternative method to set Security Groups unless added firewall protection on SoftNAS Cloud® instance is required.

SoftNAS Cloud® for CenturyLink Installation Options

SoftNAS Cloud® provides the following applicable products:

- SoftNAS Cloud® **Express** (1TB of storage)
- SoftNAS Cloud® **Standard** (20TB of storage)
- SoftNAS Cloud® **Enterprise** (up to 16 PB of storage)

Product	Storage	Purchase	License
SoftNAS Cloud® Express	1 TB	Purchased from SoftNAS.	Monthly and Annual Options

SoftNAS Cloud® Standard	20 TB	Purchased from SoftNAS.	Monthly and Annual Options
SoftNAS Cloud® Enterprise	16 PB	Purchased from SoftNAS.	Monthly and Annual Options

- **SoftNAS SNAP HA™** included with each product.

Setting up SoftNAS on Century Link

Setting up SoftNAS on CenturyLink

SoftNAS deploys in a virtual appliance model, as a CenturyLink Cloud "Partner Template". Follow these step by step instructions to deploy a SoftNAS solution in to your CenturyLink Cloud account:

Prerequisite

In order to set up a SoftNAS instance using CenturyLink Cloud, you will need:

- access to the CenturyLink Cloud platform as an authorized user.
- to identify a Network VLAN you want the SoftNAS instance to reside on.

The Support Email

In order to integrate SoftNAS with Century Link, it all starts with an email. CenturyLink support needs to know what sort of instance you wish to setup. The email should be formatted roughly as seen below, with information matching your organizational requirements. Open a service task request ticket via email to servicetasks@ctl.io with the following details:

Note: You will need to edit some of the information below.

TO: servicetasks@ctl.io

EMAIL SUBJECT: Ecosystem Partner Template Import Request

CLC Support Team, please create a ticket to import the Ecosystem Partner Template image referenced below to my CenturyLink Cloud Account:

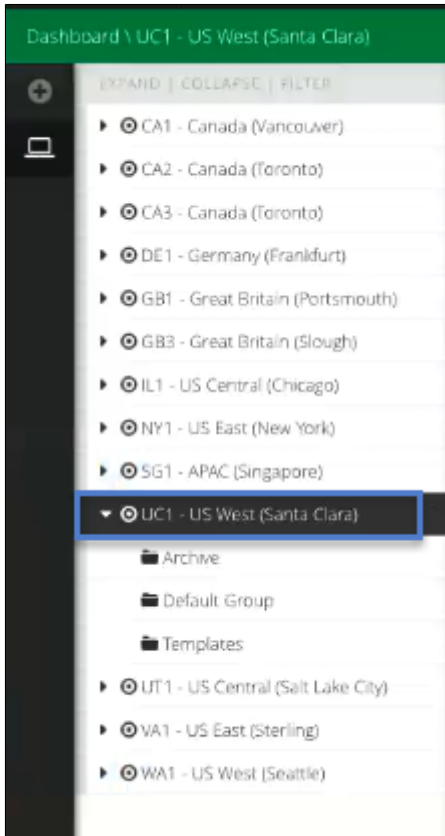
- *Import CenturyLink Ecosystem Partner Source Image: SoftNAS OVA*
- *My CenturyLink Cloud Account Alias: #####*
- *Data Center to import image to: ###*
- *Server Name to import image as: #####*
- *VLAN in the account to add the Server to: #####*
- *Additional Notes or work to be done: IMPORTANT: Please make sure that the IP shows up in Control so that the user can add a Public IP through Portal if desired.*

Please let me know if you have any questions or issues. Kindly send me a reply once the work has been completed and let us know the IP address of the server where this technology has been deployed.

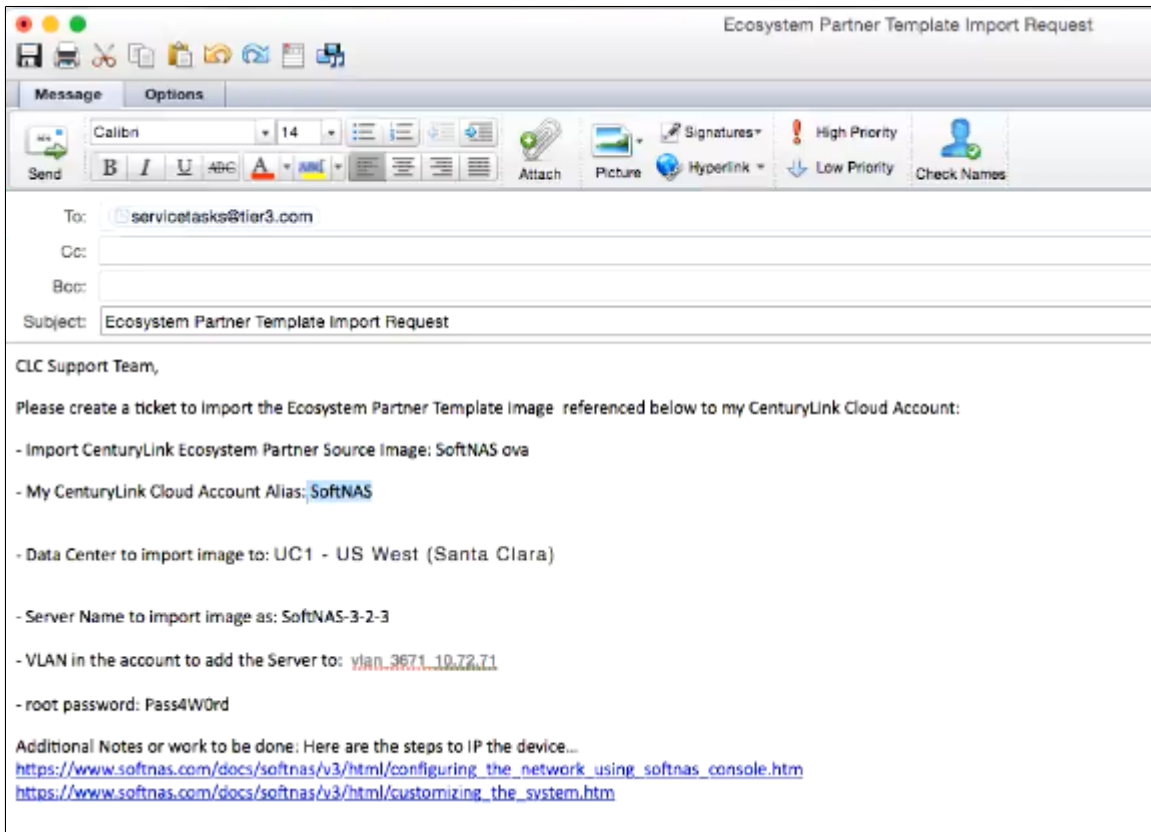
*Thank you very much,
Your_Name_and_Contact_Info_Here*

In the template above, the key information required is as seen below:

- Import CenturyLink Ecosystem Partner Source Image: SoftNAS OVA
- A Century Cloud Account Alias: Your Alias
- Data center to import an image to: - type or copy and paste the name of the desired Data Center. In the example below, this is UC1 - US West (Santa Clara)



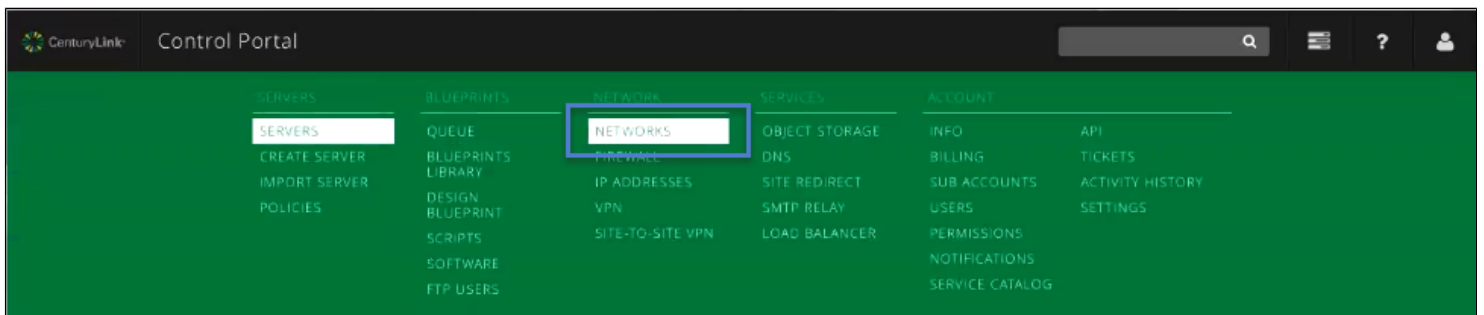
- The Server name to import the image as: specify the desired name - in the image below SoftNAS 3-2-3.
- The remaining information can be created/set by CenturyLink (VLAN, Password etc), but if included in the email, the instance will be that much quicker to create.
- Of course, your contact info must be provided as well. Contact info is removed from the example screenshot shown below, in order to preserve privacy, but your name, email and phone number are required for Century Link to begin their efforts.



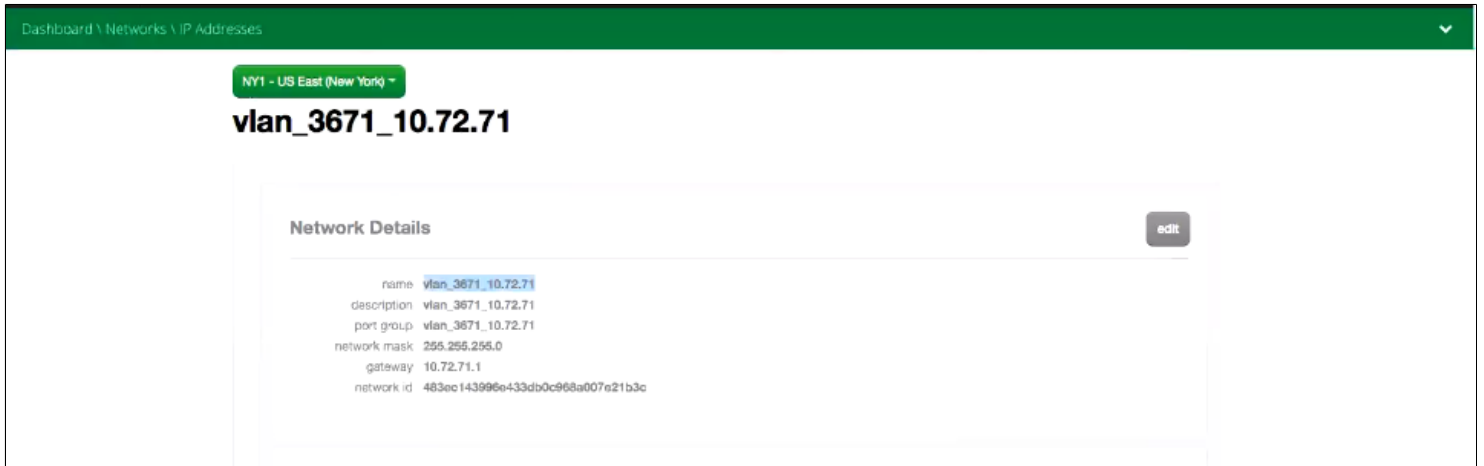
Copying the VLAN from an existing instance

If you are an existing customer and would like to match your new instance's VLAN to that of another instance on the same Data Center, you can help the service desk by providing the network settings from within the CenturyLink console. Simply log in with the information provided by CenturyLink for your prior instance.

1. To obtain your network settings, log into CenturyLink.
2. Click on Networks, under the Network tab.



3. Click the desired VLAN, and copy and paste the information from the Networks Dashboard.



4. Add the information to the email.

If this is your first instance, CenturyLink can create a VLAN for you, allowing you to edit it as desired once logged in to your instance. To edit your VLAN info, simply click the Edit button.

CenturyLink will reply with your credentials and all required server information once setup is complete.

Launching the Instance

CenturyLink will reply with credentials and all required data when the provisioning is done, based on the contact information you provide them. Log into CenturyLink, and select the Data Center that you requested the instance be built on. The instance you requested will display under the Data Center. Simply power it up.

Dashboard \ NY1 - US East (New York) \ Default Group \ NY1SOFTSOFTNA01

EXPAND | COLLAPSE | FILTER

- CA1 - Canada (Vancouver)
- CA2 - Canada (Toronto)
- CA3 - Canada (Toronto)
- DE1 - Germany (Frankfurt)
- GB1 - Great Britain (Portsmouth)
- GB3 - Great Britain (Slough)
- IL1 - US Central (Chicago)
- NY1 - US East (New York)**
 - Archive
 - Default Group
 - NY1SOFTSOFTNA01**
 - NY1SOFTSOFTNA02
 - Templates
- SG1 - APAC (Singapore)
- UC1 - US West (Santa Clara)
- UT1 - US Central (Salt Lake City)
- VA1 - US East (Sterling)
- WA1 - US West (Seattle)

NY1SOFTSOFTNA01

MONTH ESTIMATE: \$150.87 CURRENT HOUR: \$0.21 MONTH TO DATE: \$113.88

shut-down pause reboot **power off** reset action

STATUS: POWERED ON 12 Hours

CPU: 77% (8 Cores)

MEMORY: 4% (8 GB)

PARTITIONS

PATH	SIZE (GB)	USAGE

Now you are ready to configure SoftNAS. Simply log into your instance by using the IP address found in Server Info.

Dashboard \ NY1 - US East (New York) \ Default Group \ NY1SOFTSOFTNA01

EXPAND | COLLAPSE | FILTER

- CA1 - Canada (Vancouver)
- CA2 - Canada (Toronto)
- CA3 - Canada (Toronto)
- DE1 - Germany (Frankfurt)
- GB1 - Great Britain (Portsmouth)
- GB3 - Great Britain (Slough)
- IL1 - US Central (Chicago)
- NY1 - US East (New York)**
 - Archive
 - Default Group
 - NY1SOFTSOFTNA01**
 - NY1SOFTSOFTNA02
 - Templates
- SG1 - APAC (Singapore)
- UC1 - US West (Santa Clara)
- UT1 - US Central (Salt Lake City)
- VA1 - US East (Sterling)
- WA1 - US West (Seattle)

NY1SOFTSOFTNA01

MONTH ESTIMATE: \$150.87 CURRENT HOUR: \$0.21 MONTH TO DATE: \$113.88

shut-down pause reboot power off reset action settings

STATUS: POWERED ON 12 Hours SERVER INFO

CPU: 77% (8 Cores)

MEMORY: 4% (8 GB)

PARTITIONS

PATH	SIZE (GB)	USAGE

ADMIN CREDENTIALS

show credentials

Unknown

standard

standard

ny1softsoftna01

IP ADDRESS(ES)

74.201.135.153

10.72.71.12

add public ip

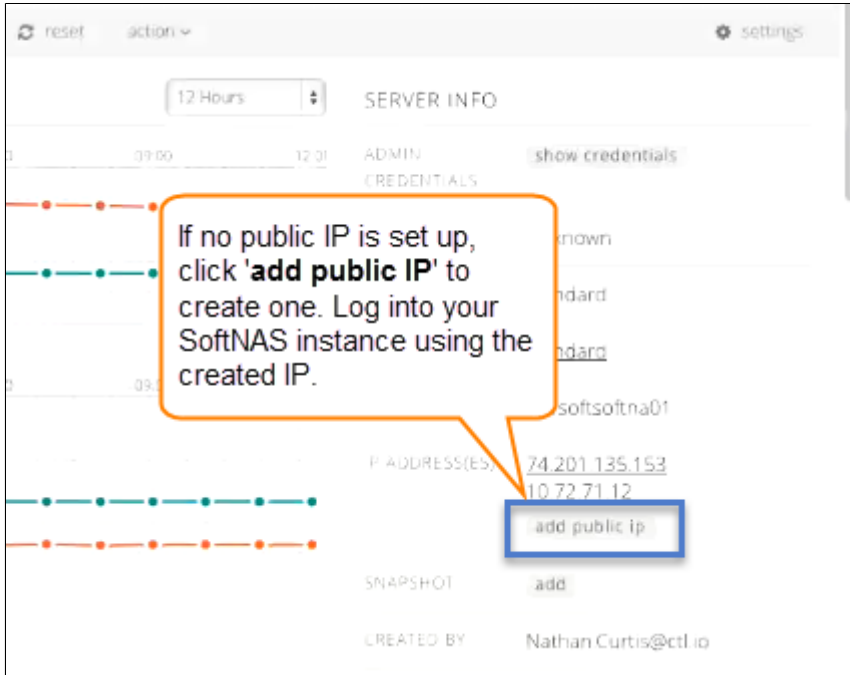
SNAPSHOT

add

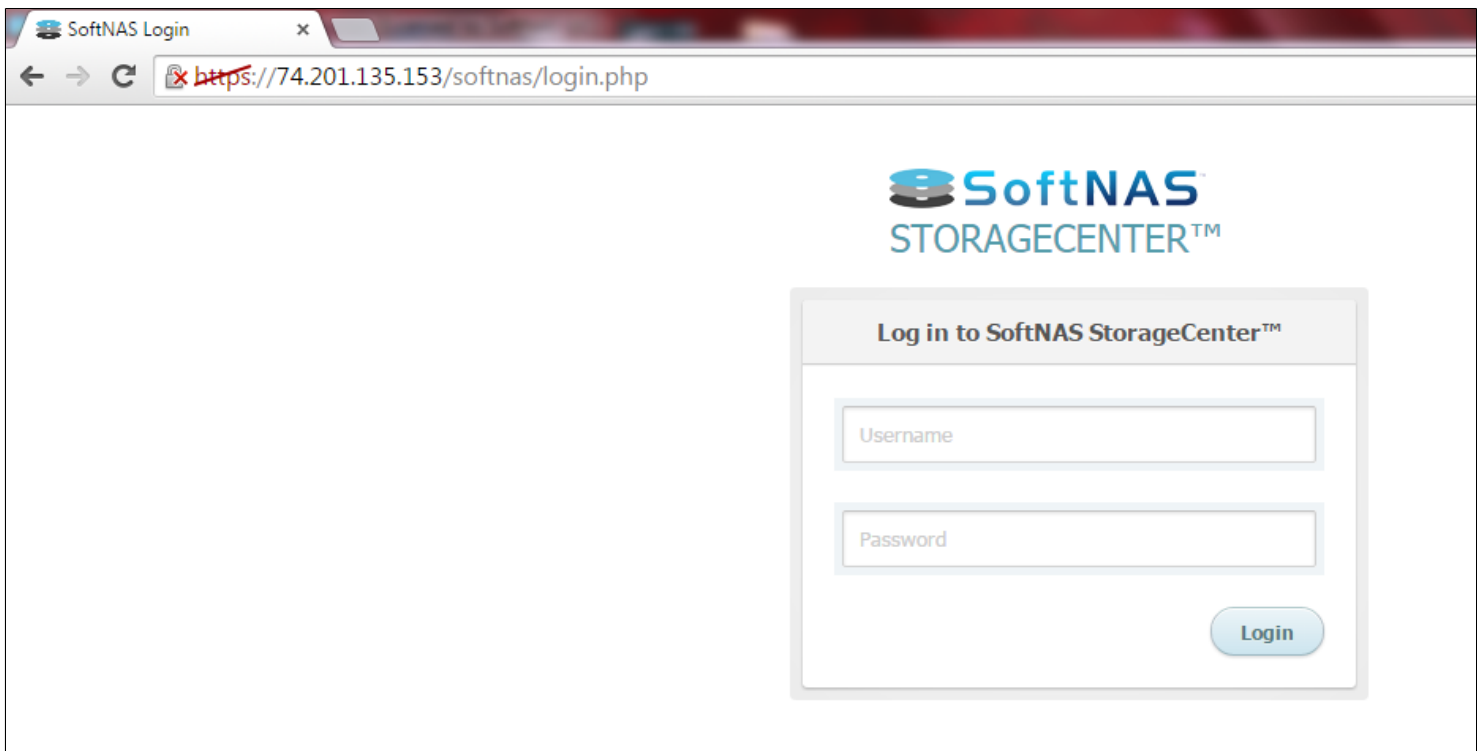
CREATED BY

Nathan Curtis@ctl.io

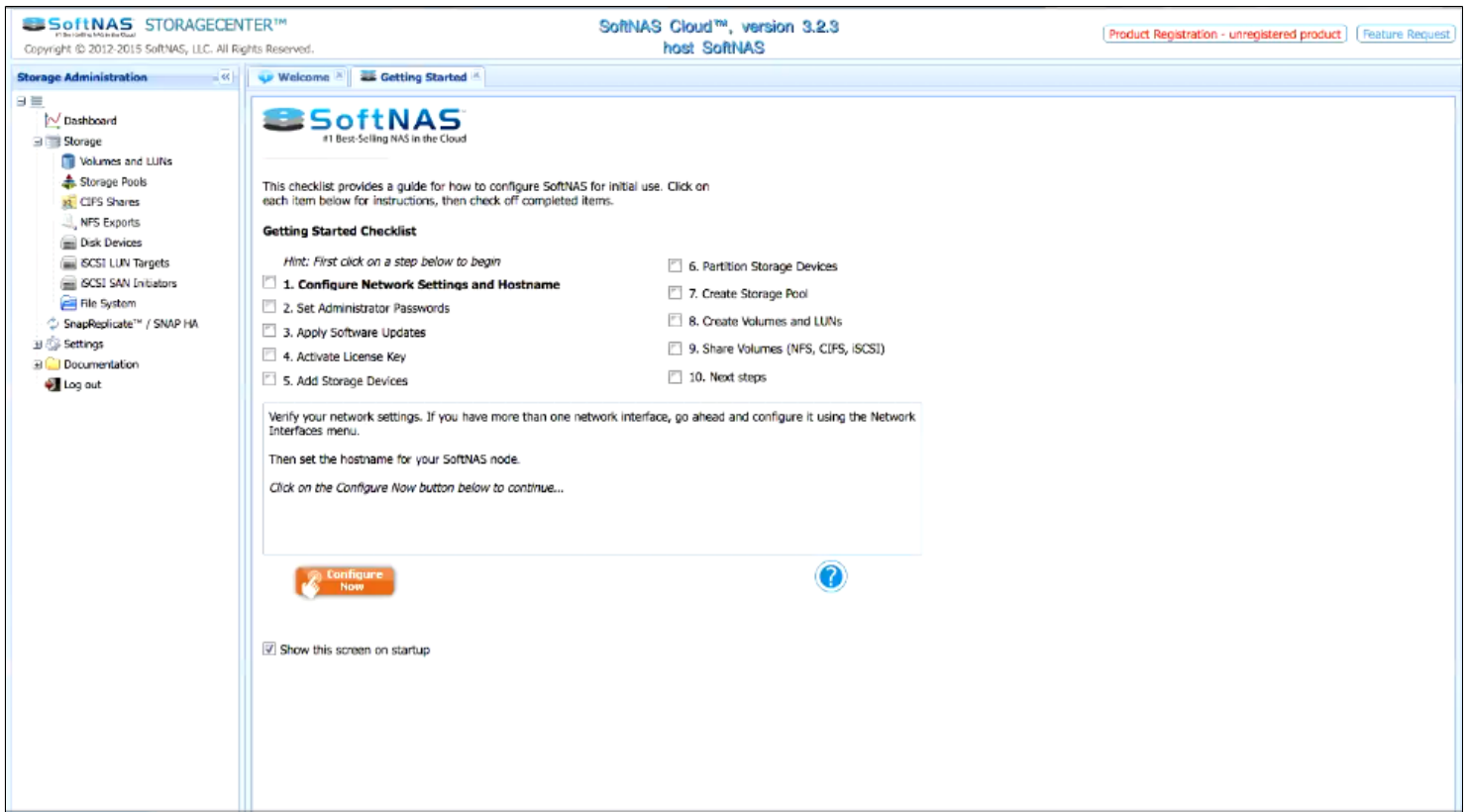
If a public IP is not yet set up, create one by clicking the button 'add public IP'. Fill in the required information.



Once a public IP is set up, click it, and open your softNAS instance by entering the IP address into your web browser.



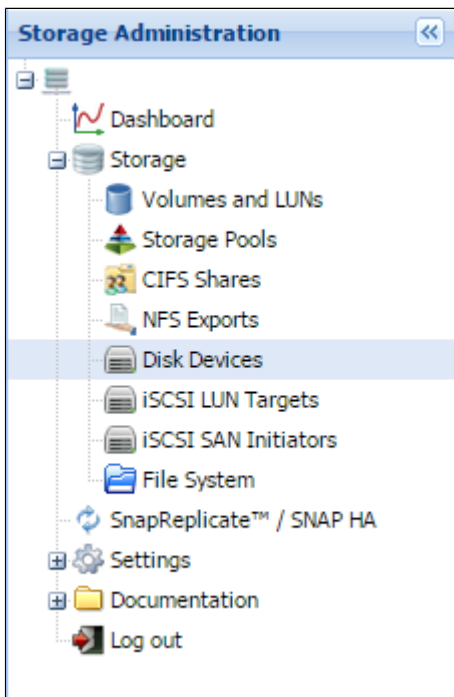
Once you have logged in, you will be presented with the option to register, as well as to provide user information, such as your email address. Provide the information, or skip till later. You will then find yourself within the SoftNAS control panel, with a checklist to help you set up your instance.



Best practices and setup information for set up of SoftNAS are covered in detail within [Getting Started Helper](#), and the other categories falling under **SoftNAS Cloud® Configuration**. Follow the instructions presented in the checklist until step 5, **Add Storage Devices**.

Adding Storage Devices through Century Link

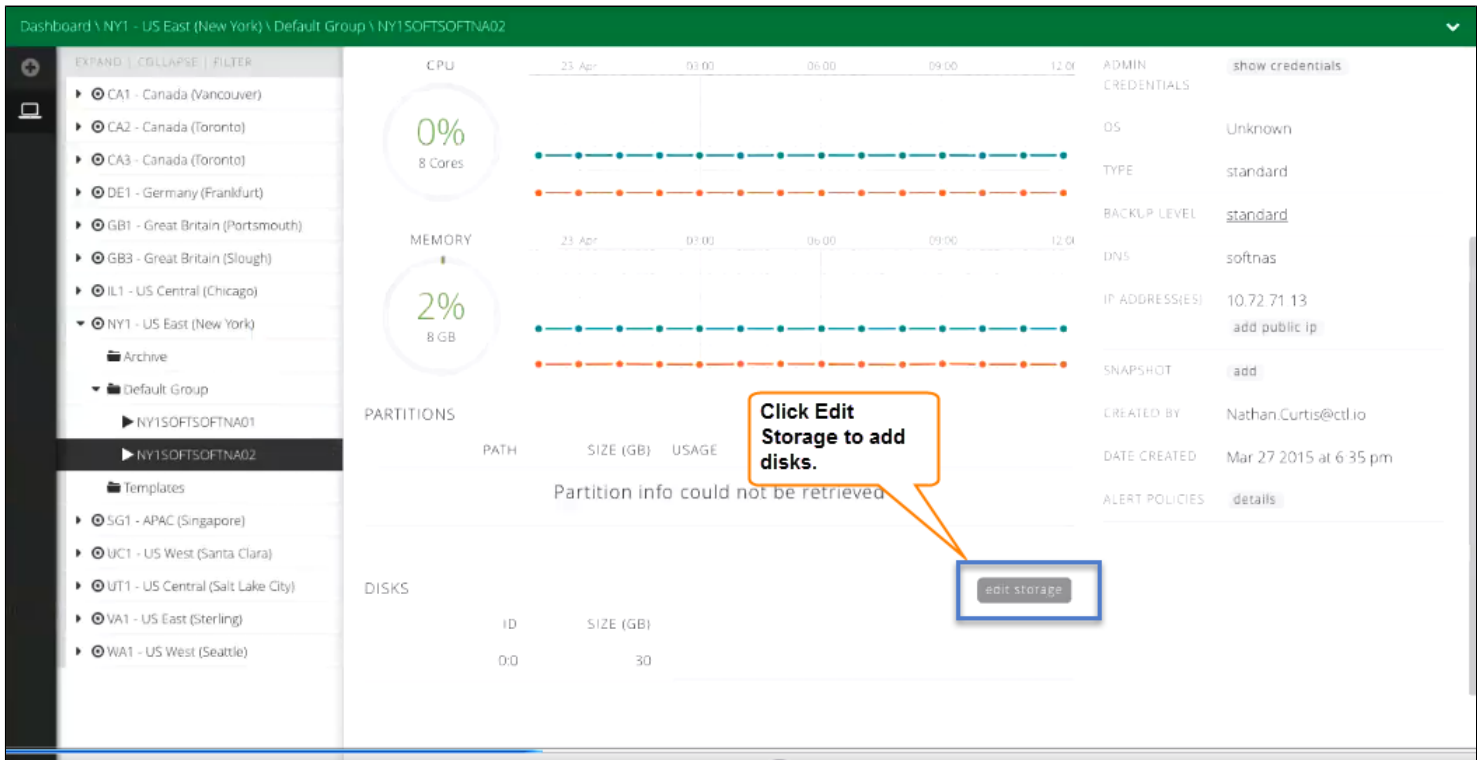
Typically, to add storage in SoftNAS, one would simply click on **Disk Devices** within the **Storage Administration Panel** on the left.



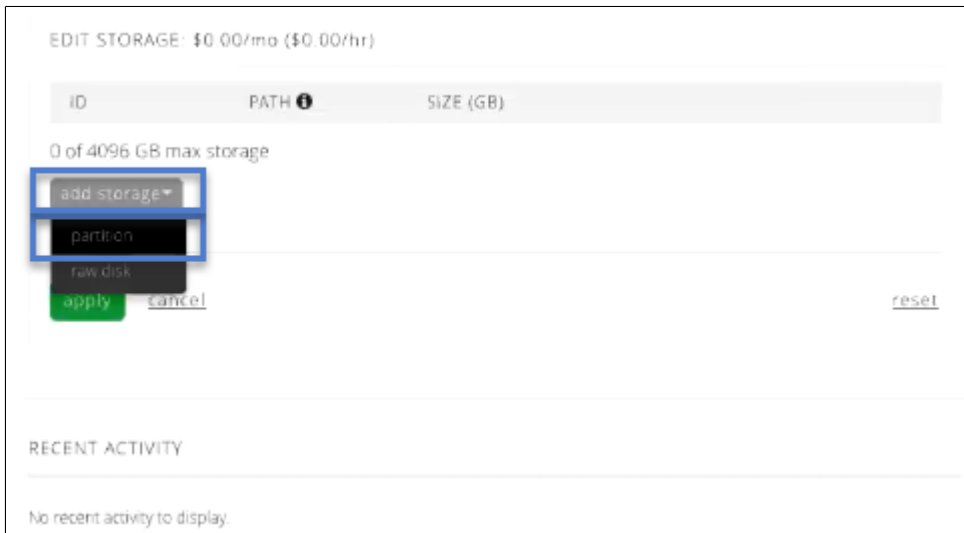
Then one would click **"Add Device"** and follow the steps presented in the wizard that appears. Unfortunately, for the moment, there are no APIs hooking directly to CenturyLink, in order to add storage. As you can see below, the only option available from within SoftNAS is to add S3 storage. As this is **not** what we want, click **Cancel**.



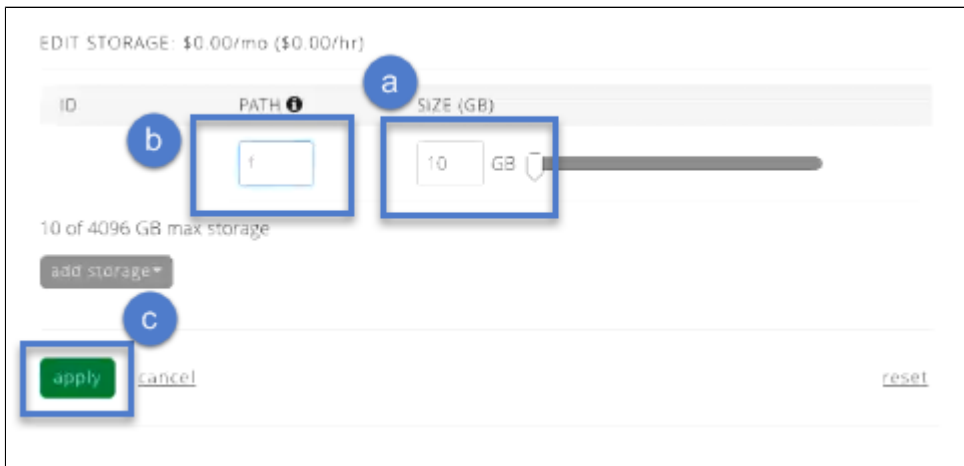
Instead, return to the CenturyLink Portal. Within the CenturyLink instance, click **Edit Storage**.



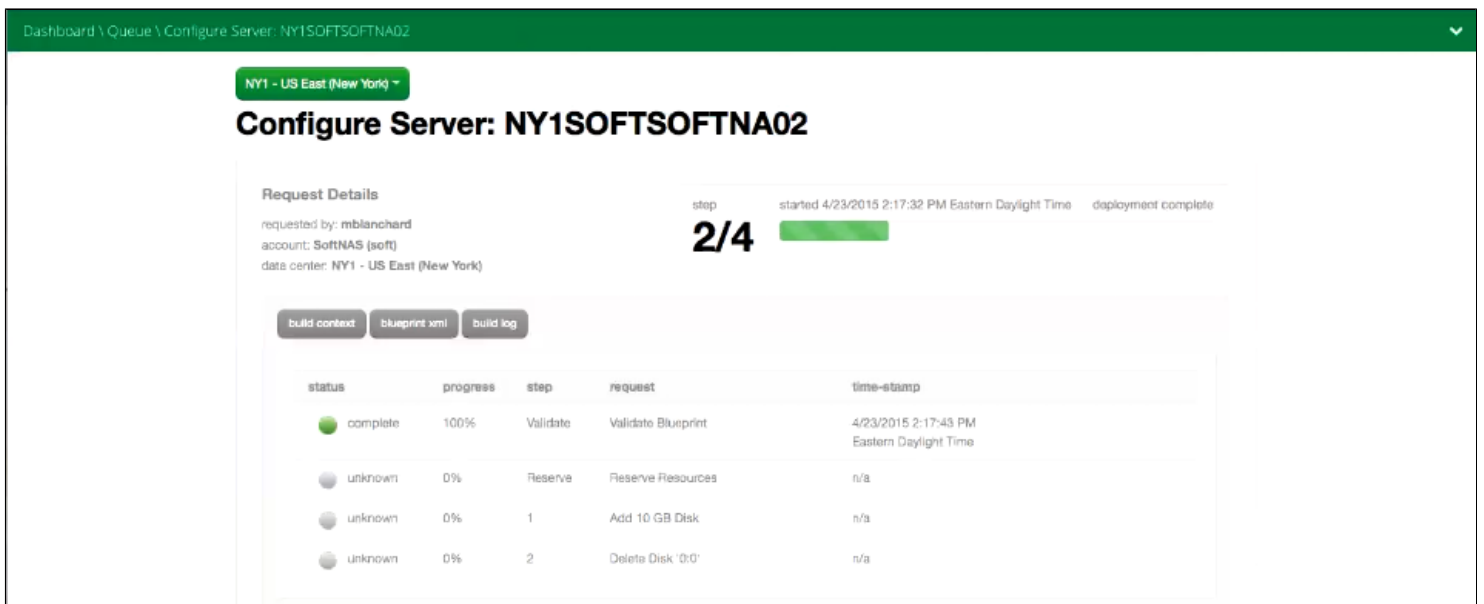
In **Edit Storage**, click **Add Storage**, then **Partition**.



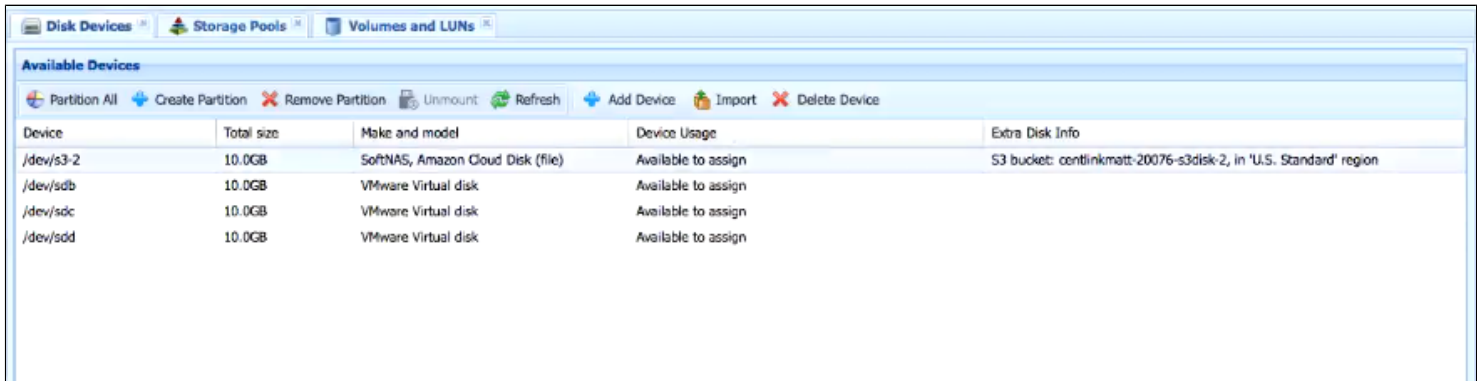
Enter a) the amount of space (in GB) for the storage, b) a drive letter, and c) click **apply**.



This will set up a build process within CenturyLink. If you refresh the screen, you can watch the progress of the build and see when it completes.



Once complete, return to SoftNAS via the public IP set up earlier. Click Disk Devices once more, and the new devices will be presented, and available to assign into pools.

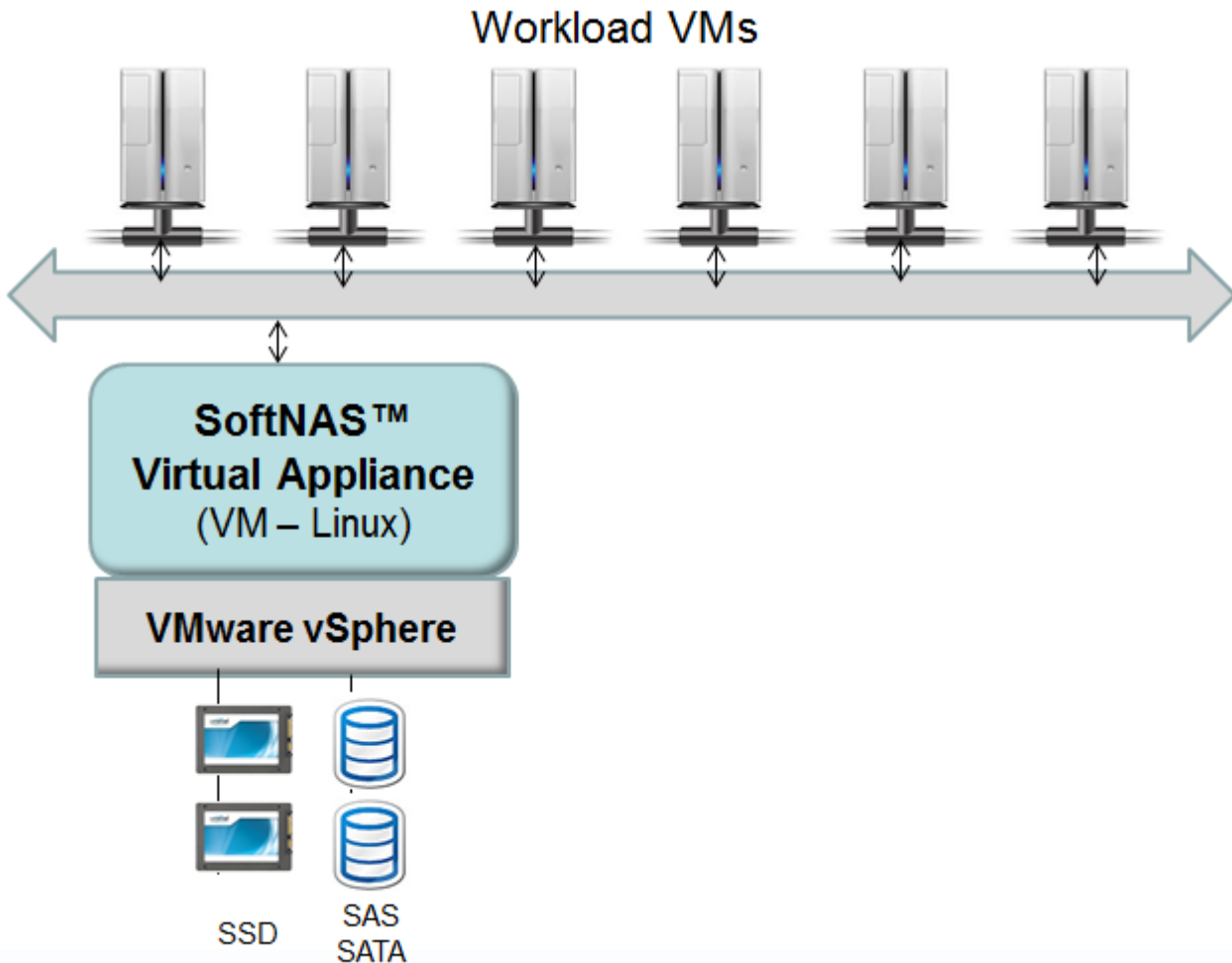


Set up of pools, volumes, high availability and more are covered in the **SoftNAS Cloud® Configuration** section of this Installation Guide. High Availability configurations are covered in more detail within our [High Availability Guide](#).

VMware vSphere

Overview

As shown below, **SoftNAS Cloud®** operates within the VMware virtualization environment, typically on a VMware host that is dedicated as a NAS storage server. VMware virtualization provides the broadest range of device and resources, resulting in superior management and administration. And because SoftNAS runs within VMware, it inherits all the features and support that comes from VMware, including vCenter and other administration tools.



VMware vSphere client is a familiar entity in on-premise storage environments. It is considered the principal administrative interface for **vCenter Server** and **ESXi** environments.

After downloading and installing **VMware vSphere**, ensure that the most recent version of this client has been installed.

Please review the [VMware vSphere System Requirements](#) for more details on recommended settings for the **SoftNAS Cloud® VM**.

Product and Installation Options

SoftNAS Cloud® provides the following applicable products:

- SoftNAS Cloud® **Express** (1TB of storage)
- SoftNAS Cloud® **Standard** (20TB of storage)
- SoftNAS Cloud® **Enterprise** (up to 16 PB of storage)

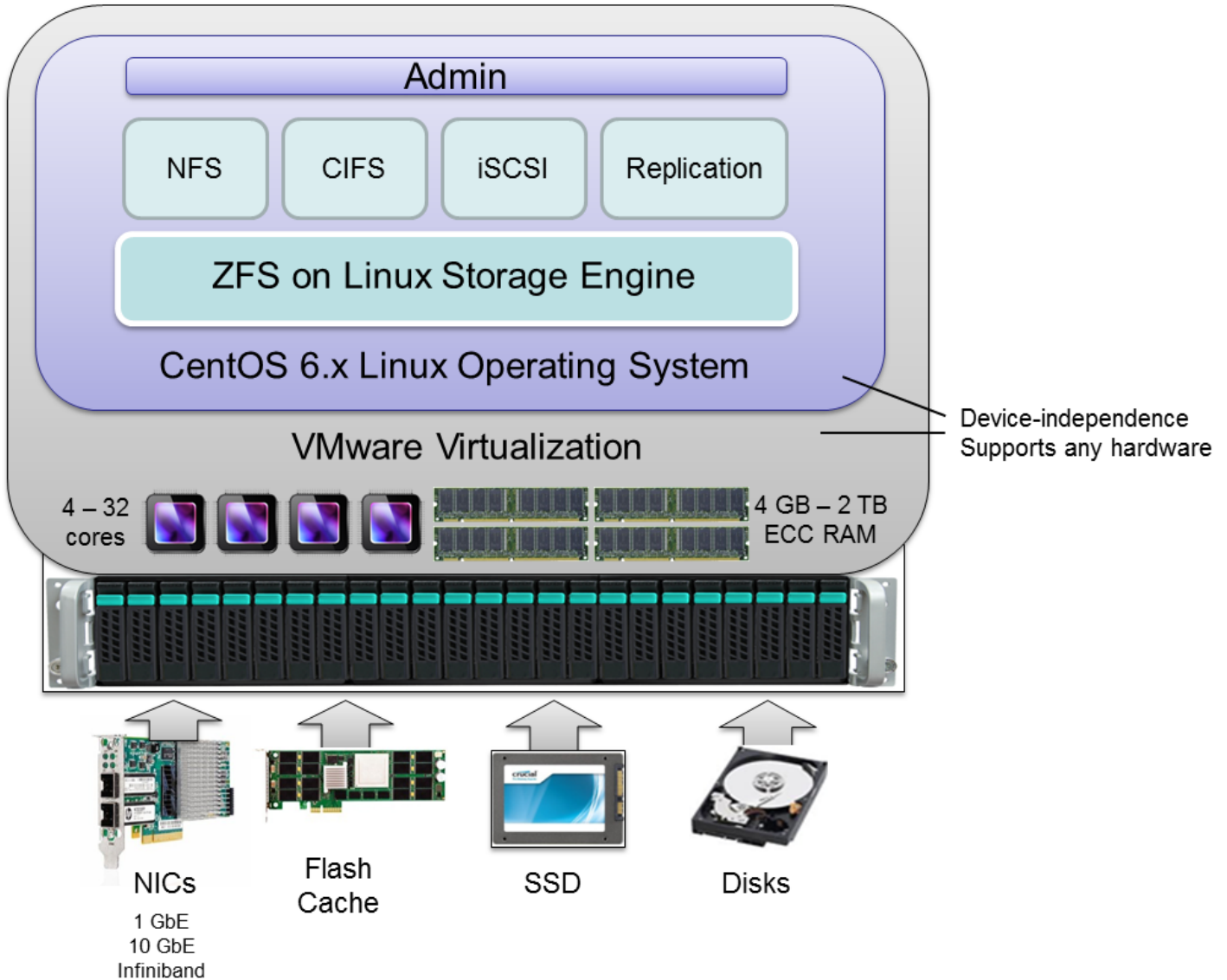
Product	Storage	Purchase	License
SoftNAS Cloud® Express	1 TB	Purchased from SoftNAS ,	Monthly & Annual license options
SoftNAS Cloud® Standard	20 TB	Purchased from SoftNAS ,	Monthly & Annual license options
SoftNAS Cloud® Enterprise	16 PB	Purchased from SoftNAS ,	Monthly & Annual license options

- **SoftNAS SNAP HA™** included with each product.

Preparing a VMWare Hardware Environment

VMware Considerations

As shown below, SoftNAS™ operates within the VMware virtualization environment, typically on a VMware host that is dedicated as a NAS storage server. VMware virtualization provides the broadest range of device and resources, resulting in superior management and administration. And because SoftNAS runs within VMware, it inherits all the features and support that comes from VMware, including vCenter and other administration tools.



On the VMware host for SoftNAS, one or more SoftNAS virtual machines are deployed using standard VMware best practices. As shown below, from 4 to 32 (or more) cores and hyperthreads are allocated to the SoftNAS VM(s) for storage management. Large amounts of ECC memory (from 4 GB up to 2 TB) are allocated to the SoftNAS VM, providing large amounts of RAM cache, which dramatically increases read performance.

Any desired network topology can be supported via the VMware physical and virtual network switching layers - from 1 GbE to 10 GbE and Infiniband for high throughput. It's common to deploy 1 GbE ports for administration of VMware and SoftNAS, plus 10 GbE or Infiniband bonded ports for high-speed storage access. And since all networking flows through VMware, all vSwitch functionality, including load-balancing, VLANs, throttling and more are all available.

For extremely high-IOPS deployments (e.g., VDI, databases, etc.), a combination of RAM, Flash Cache PCIe memory cards and/or SSD's can be deployed for maximum performance.

The SoftNAS VM runs as an x64 version of the robust, secure and stable CentOS 6.x Linux operating system. Linux provides a broad range of standard services, including NFS, CIFS (Samba) and iSCSI for NAS client connectivity.

Virtualization adds a minor amount of overhead (less than 5%) versus bare metal operation. The additional CPU and memory available more than compensates for this nominal virtualization overhead. Of course, virtualization provides SoftNAS storage many of the same benefits that workload VM's enjoy by being virtualized (e.g., ease of administration and management, and unparalleled flexibility and device compatibility).

Note: A minimum of 4 vCPUs is required for proper operation. ZFS includes 256-bit block checksums, which consume some CPU. If you choose to use data compression and/or deduplication, additional CPU power may be required.

The ZFS storage engine makes very effective use of RAM for caching. As RAM is relatively inexpensive, it is recommended to provide the SoftNAS VM with as much RAM as you can make available for optimal performance. Always use ECC RAM with SoftNAS, as you want to ensure there are no errors accidentally introduced into your data by memory read/write cycles (and ECC will detect and correct any such errors immediately).

Please review the [VMware vSphere System Requirements](#) for more details on recommended settings for the SoftNAS VM.

VMware vSphere Networking Considerations

A minimum of 1 gigabit networking is required and will provide throughput up to 120 MB/sec (line speed of 1Gb/E). 10Gb/E offers 750+ MB/sec throughput. To reduce the overhead for intensive storage I/O workloads, it is highly-recommended to configure the VMware hosts running **SoftNAS** and the heavy I/O workloads with "jumbo frames", MTU 9000. It's usually best to allocate a separate vSwitch for storage with dual physical NICs with their VMkernels configured for MTU 9000 (be sure to configure the physical switch ports for MTU 9000, as well). If possible, isolating storage onto its own VLAN is also a best practice.

If you are using dual switches for redundancy (usually a good idea and best practice for HA configurations), be sure to configure your VMware host vSwitch for Active-Active operation and test switch port failover prior to placing **SoftNAS** into production (like you would with any other production VMware host).

You should choose static IPv4 addresses for **SoftNAS**. If you plan to assign storage to a separate VLAN (usually a good idea), ensure the vSwitch and physical switches are properly configured and available for use. For VMware-based storage systems, **SoftNAS** is typically deployed on an internal, private network. Access to the Internet from **SoftNAS** is required for certain features to work; e.g., Software Updates (which download updates from softnas.com site), NTP time synchronization (which can be used to keep the system clock accurate), etc.

From an administration perspective, you will probably want browser-based access from the internal network only. Optionally, you may wish to use SSH for remote shell access (optional). If you prefer to completely isolate access to **SoftNAS** from both internal and external users, then access will be restricted to the VMware console only (you can launch a local web browser on the graphical console's desktop). Note that you can add as many network interfaces to the SoftNAS VM as permitted by the VMware environment.

Prior to installation, allocate a static IP address for **SoftNAS** and be prepared to enter the usual network mask, default gateway and DNS details during network configuration. By default, **SoftNAS** is configured to initially boot in DHCP mode (but it is recommended to use a fixed, static IP address for production use).

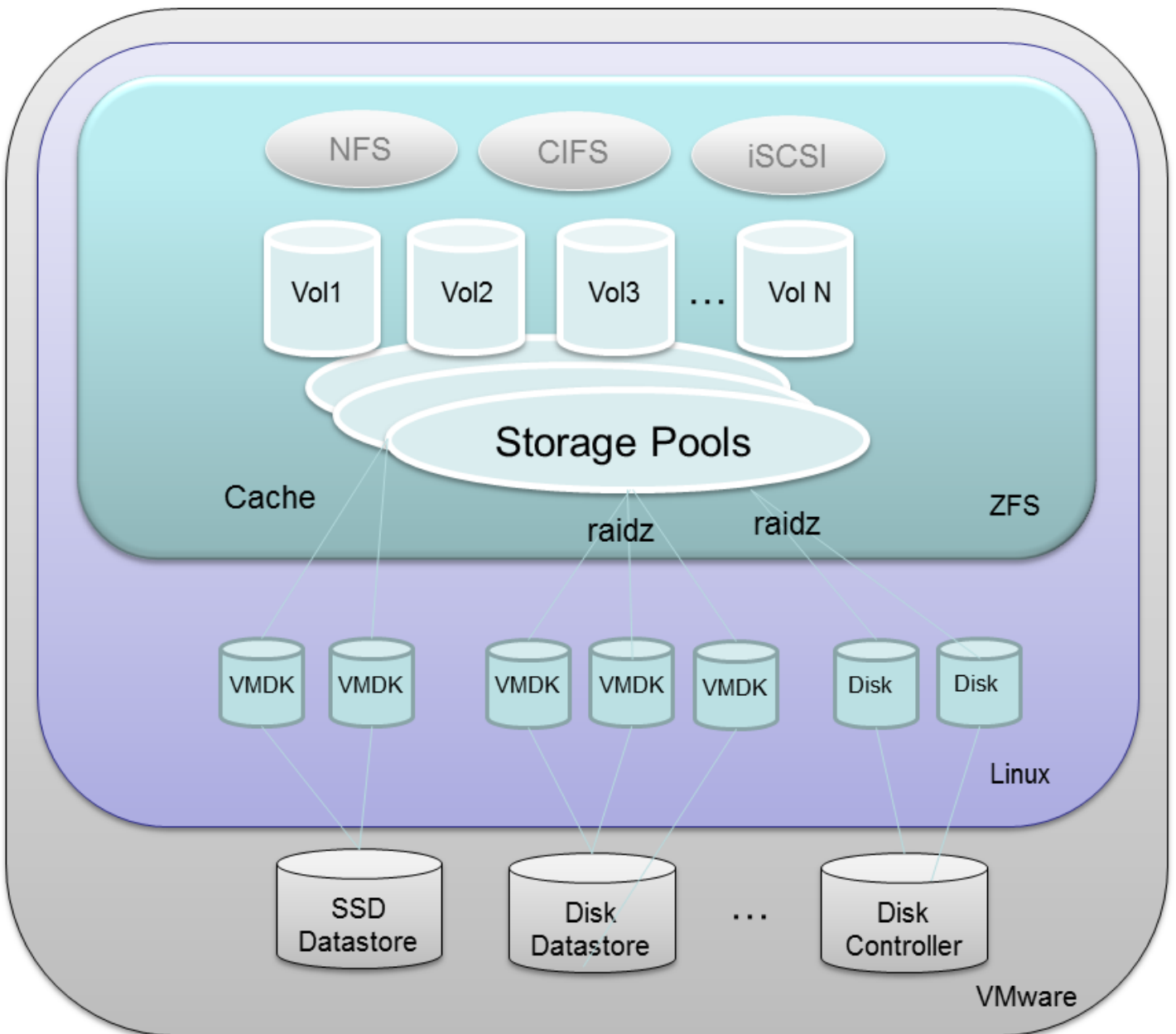
At a minimum, **SoftNAS** must have at least one NIC assigned for management and storage. It is best practice to provide a separate NICs for management/administration, storage I/O and replication I/O.

VMware vSphere Disk Device Considerations

The SoftNAS VM runs the Linux operating system, which boots from its own virtual hard disk (VMDK) on the local disk drive (host datastore).

SoftNAS manages a collection of locally-attached storage devices, as shown below. Physical storage devices are typically managed by VMware and presented as VMware datastore (it is also possible to pass disk controller through VMware directly to Linux for direct-attached raw disks, although that configuration is more complex and less common).

VMDKs are used to attach disk storage to the SoftNAS Linux VM. SSD read and write cache devices are attached in a similar way. Note that a single SoftNAS VM can be deployed for dedicated applications or multiple SoftNAS VM's can be deployed for service provider configurations, where different customers receive their own separate SoftNAS virtual storage server.



VMDK's can be arranged into raid configurations within SoftNAS to form RAID-1/10 mirrors or RAIDZ-1 to RAIDZ-3 configurations, which provide additional data protection features.

One or more VMDK's can be combined to create a "Storage Pool". Each storage pool provides an expandable aggregate of storage that can be shared by one or more Volumes. Volumes are then exported as NFS, shared as Windows CIFS shares or made available as iSCSI target LUNs.

Finally, when configuring the SoftNAS VM, for highest throughput it is recommended to change the SCSI disk type from "LSI Logic" to "Paravirtual", which provides the best disk I/O performance characteristics.

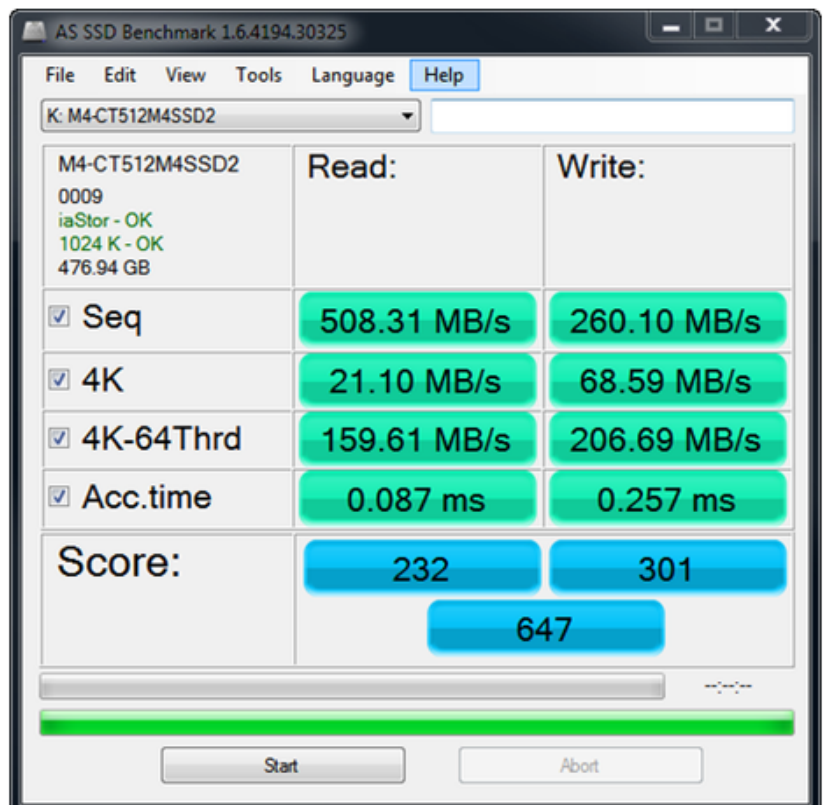
SSD (solid state disks) drives

SoftNAS supports the use of high-speed SSD drives, including the latest, affordable MLC drives comprised of flash NAND memory, which typically provide access times 100 times faster than physical disk drives (e.g., access times in the 0.1 millisecond range are common, with 300 MB/sec to 450 MB/sec transfer rate per drive). This equates to 40,000 to 50,000 or more IOPS (I/O per second).

SSD are excellent for use as both Read Cache and Write Log purposes, augmenting main memory with additional high-performance caching and logging storage. Note that write log devices can be configured as RAID 1 mirrors, so you have double protection against drive failures and data loss.

Some recommended drives include Crucial M4 series SSD, which are widely available and very affordable. The Crucial M4 512 GB drive shown below costs a few hundred dollars and provides very impressive throughput and extremely fast read access, and respectable write speed as well. These drives are now less than \$1 per GB and are as much as 100 times faster than SAS drives. However, there is a short life expectancy for these drives - est. 3 to 5 years, depending upon how much write activity your workloads exhibit. If you have high-write workloads, SAS drives may be a better choice for long term high-performance storage. If you have read-intensive workloads, it's hard to beat SSD for high-performance and durability, especially at the price. Of course, SSD are an excellent choice for read cache - a use case for which they're hard to beat.

Lastly, SSD consume about 1/10th the power of spindle drives like SAS and SATA disks, so if low-power operation is an objective, SSD are a great solution.



10K and 15K SAS Drives

SAS drives have long provided a solid foundation for storage systems. Assuming budgets permit, it is recommended to use 15K SAS drives for high-performance workloads, such as SQL Server databases, virtual desktop systems like RDS, VMware View, Citrix XenDesktop, Exchange Server and other performance-sensitive applications. As always, use of RAID 10 provides best read and write performance, while RAID 5/6/7 provide excellent read performance with some write performance penalty. Adding SSD as read cache and write log can greatly improve the performance of small writes and brief I/O bursts.

The Seagate Cheetah 15K SAS drive shown below, for example, provides high-performance with proven reliability for long-term reliability.



SATA drives

Modern SATA drives provide access to high capacity storage at relatively low performance levels. SATA storage is typically adequate for file servers and user data, backup data storage and many common applications that do not require high levels of performance. For best results, do not use SATA drives for high-performance workloads. High-capacity SATA drives like the Seagate Barracuda7200 3 TB drive shown below provide an enormous amount of storage when aggregated into a RAID array, and are very affordable at a hundred to two hundred dollars apiece.

VMware vSphere Guidance for Storage Enclosures

There are many options for storage enclosures, including chassis with redundant power supplies, redundant cabling in both 3.5" and 2.5" form factors.

12 Hot-swap drives: 36 TB (3TB drives)



24 Hot-swap drives: 72 TB (3TB drives)



You may also leverage JBOD arrays with SoftNAS.

After you have chosen which of the above methods of connecting JBOD (just a bunch of disks) to VMware, then you are ready to install and configure SoftNAS. If you are just giving SoftNAS a try on a smaller-scale basis, then almost any VMware-compatible disk storage will suffice as a starting point. Just remember, you don't need to spend a lot to get high-performance, high-quality NAS capabilities with SoftNAS, as there is enormous flexibility and choice available due to the broad compatibility provided by VMware and Linux.

Please review RAID Considerations for additional information on available and recommended data disk configurations.

Note: After the installation of SoftNAS, we recommend [updating the VMware Tools](#) that ship with SoftNAS to ensure you have the latest version of VMware Tools installed for your VMware system. This will ensure you can gracefully shut down and reboot SoftNAS from the VMware vSphere or vCenter console (as with any other VM) and that you have the latest vmxnet3 drivers (required for optimal 10 GbE throughput).

VMware vSphere System Requirements

SoftNAS Cloud® System Requirements

Listed below is a table to assist with the setup decisions during the configuration required to accomplish various tasks and goals.

Specifying Memory and CPU Reservations

Always specify the CPU and Memory reservations for the **SoftNAS Cloud® VMs** to prevent over-commitment of **vSphere Server** resources.

Note: Overcommitting **vSphere Server** resources without specifying CPU and Memory reservations will cause unwanted HA failovers.

	Recommended	Configuration Note
Compute	• Set a compute reservation for all of the CPU assigned to the SoftNAS Cloud® VM.	
Light Use	2 vCPU	minimum
General Use	4+ vCPU	recommended, based on use of compression
Heavy Use	8+ vCPU	large-scale use with compression and deduplication
Memory	• Set a memory reservation for all of the memory assigned for the SoftNAS Cloud® VM.	
Base RAM - General	2 GB	minimum
System RAM - Medium	8 GB	medium-scale use
System RAM - Heavy	32+ GB	large-scale use with increased caching
Additional RAM	1 GB per 1 TB of deduplicated storage.	required for best performance
	e.g.: 50 TB deduplicated storage = 50 additional GB for deduplication tables.	
Storage		
Boot Disk	64-bit Linux CentOS 4/5/6 (64-bit)	30GB, Thin-provisioned
Data Disks	Virtual Hard Disks (VMDK) for data storage will support any VMware-supported datastore.	
Hardware RAID	If the local disk controller supports hardware RAID, hardware RAID can be used to create VMware host datastores.	
Software RAID	If SoftNAS Cloud® is preferred to handle RAID, add VMDKs to the SoftNAS Cloud® VM and configure RAID in the SoftNAS Cloud® product.	
iSCSI SAN	SoftNAS Cloud® can mount and support all VMware-supported disk configurations, including iSCSI SAN via software or hardware HBA.	
Networking		
Up to 120 MB/sec	1 GbE	minimum
Up to 750 MB/sec	10 GbE	Other VMware-supported networks, such as Infiniband, are also available.
HA Networking	Active/Active or Active/Passive vSwitch	Required setting for VMware vSphere to tolerate a NIC or switch failure.

	Use of "full mesh" HA switch configurations are also recommended to prevent switch failures from interrupting storage access.
HA Host Failover	Ensure that, for each host operating with SoftNAS Cloud®, the Data Disks are accessible. Preferred method: dual-path disks or iSCSI or fiber-attached disks with VMware drivers.

SoftNAS Cloud® System Capacities

Listed below is a table representing the capabilities of the **SoftNAS Cloud®** for **VMware vSphere**.

	SoftNAS Cloud® Capacity	Configuration Note
Editions		
SoftNAS Cloud® Express	1 TB	
SoftNAS Cloud® Standard	20 TB	
SoftNAS Cloud® Enterprise	16 PB	
Free Tier	Small-scale use case & evaluation	micro instance limits performance; not recommended for production use cases.
Memory		
RAM Cache	1 GB to 100 GB	Defaults to 50% total RAM for read cache
SSD Cache	low-speed level 2 cache	Optional
Ephemeral Cache	low-speed level 2 cache	Optional for read cache
Storage		
Maximum Storage	16 PB	Maximum usable storage capacity with SoftNAS Cloud® , contingent on license.
# of Storage Pools	Unlimited	
# of Volumes	Unlimited	
# of Snapshots	Unlimited	
# of Snapshot Clones	Unlimited	
SnapReplicate	Unlimited Pools & Volumes	
SnapReplicate Throttle	56Kb/sec to Unlimited bandwidth	
Active Directory	Kerberos Integration	
Files and Directories	Unlimited	
Network		
Schedules	Unlimited	
NFS Exports:	Linux Default	
iSCSI Targets	Linux Default	
CIFS Shares	Linux Default	
Firewall Ports:	22 (ssh), 443 (https)	Plus NFS, iSCSI, and CIFS as required by network
IP Tables Firewall	Off by default	May be configured, but is not required. Use an alternative method to set Security Groups unless added firewall protection on a SoftNAS Cloud® instance is required.

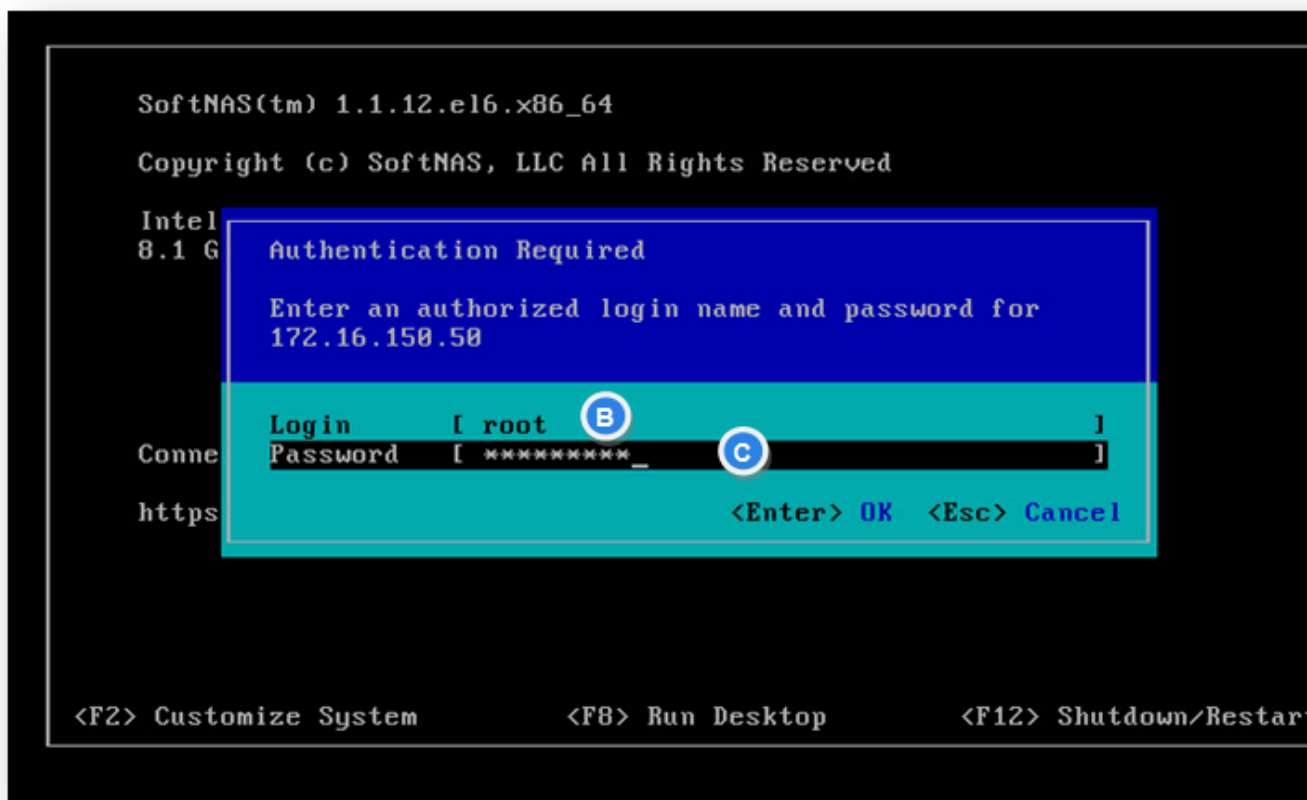
Update VMware Tools

As with any VM, it is important to ensure VMware Tools are current and operating correctly. SoftNAS ships with the latest version of VMware Tools already installed, but it is a recommended best practice to ensure the VMware Tools are installed and compatible.

SoftNAS makes use of the vmxnet 3 network driver to support 10 GbE virtual NICs, support which is provided by drivers that come with VMware Tools. These drivers are compatible across all ESXI 5.x versions.

To update VMware Tools on Linux, follow VMware's instructions [here](#). Log in as **root** (use the default password "Pass4W0rd" if the administrator has not yet changed the root password). To log in, open up a console window on VMware and press F8 in the SoftNAS Console, log in with the root password, then log into the SoftNAS Desktop and launch a command shell, then follow the VMware Tools installation and update instructions.

As shown below, after pressing F8, enter the root password.

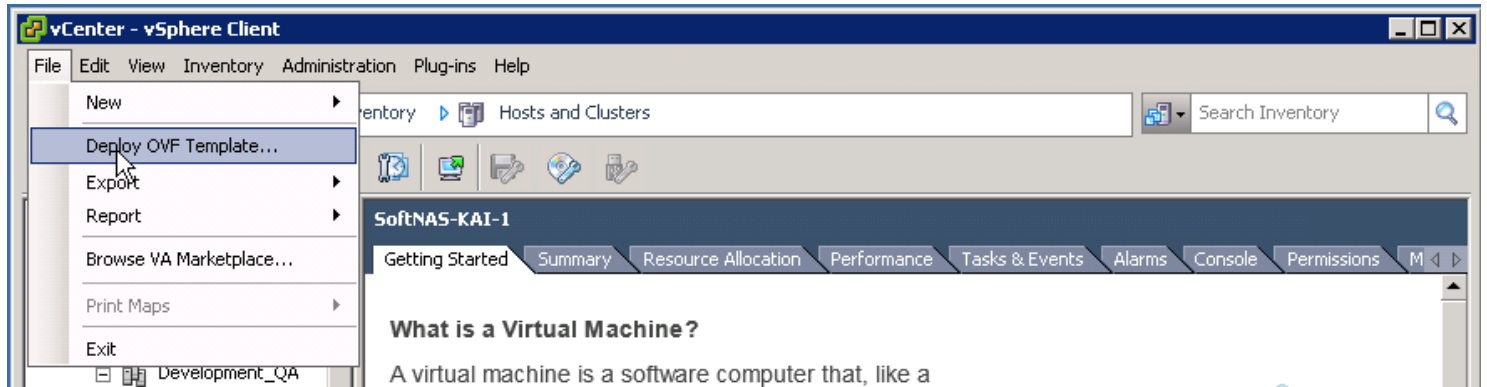


We recommend **automatic kernel rebuilds** (the last question during VMware Tools installs), so that VMware Tools remains compatible with future kernel updates.

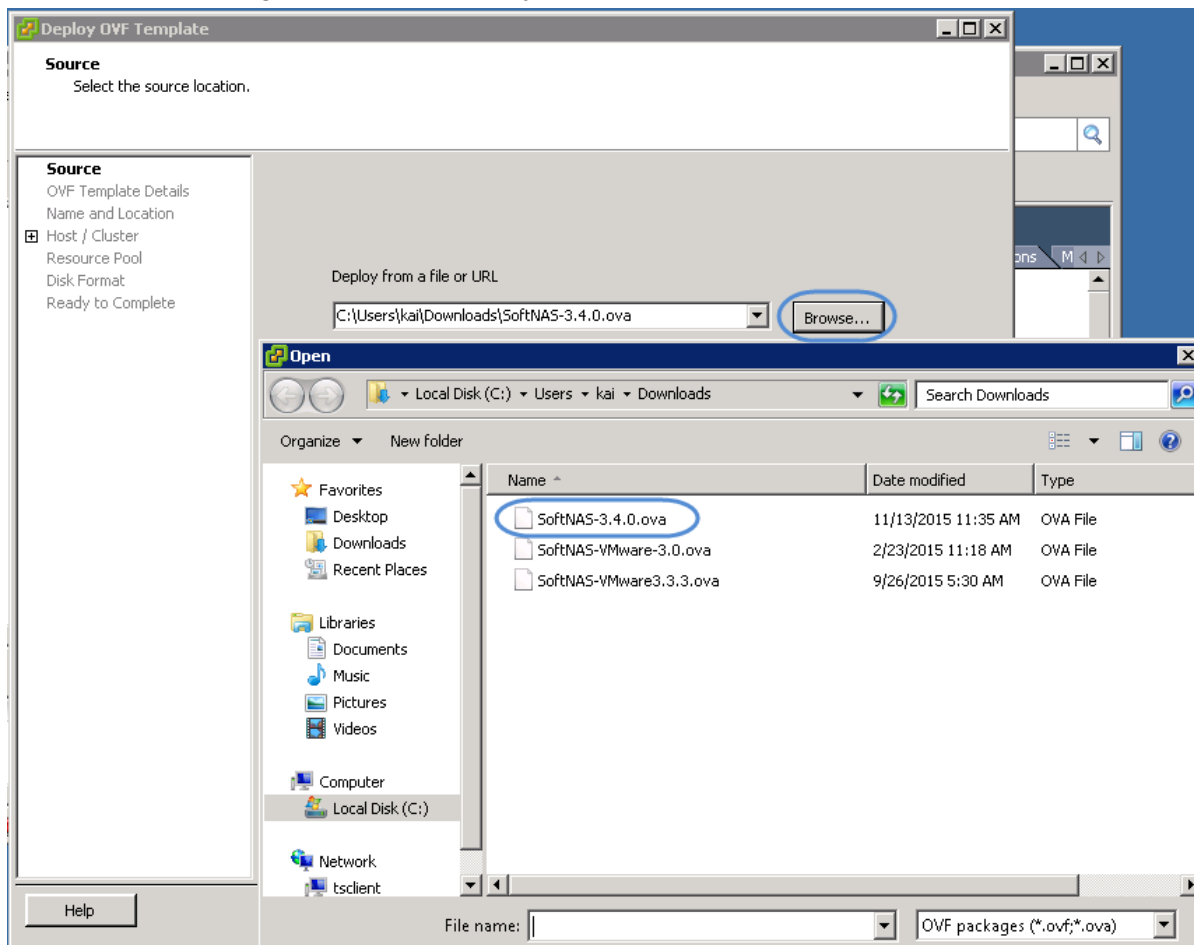
Deploying your SoftNAS Instance in VMware vSphere

Deploying your SoftNAS instance through VMware is a simple process. After obtaining the SoftNAS OVF file from our site (via purchase or trial, see [Launching SoftNAS Cloud® Platforms](#)), note the storage location, and make sure it is accessible from the machine hosting your vSphere Client.

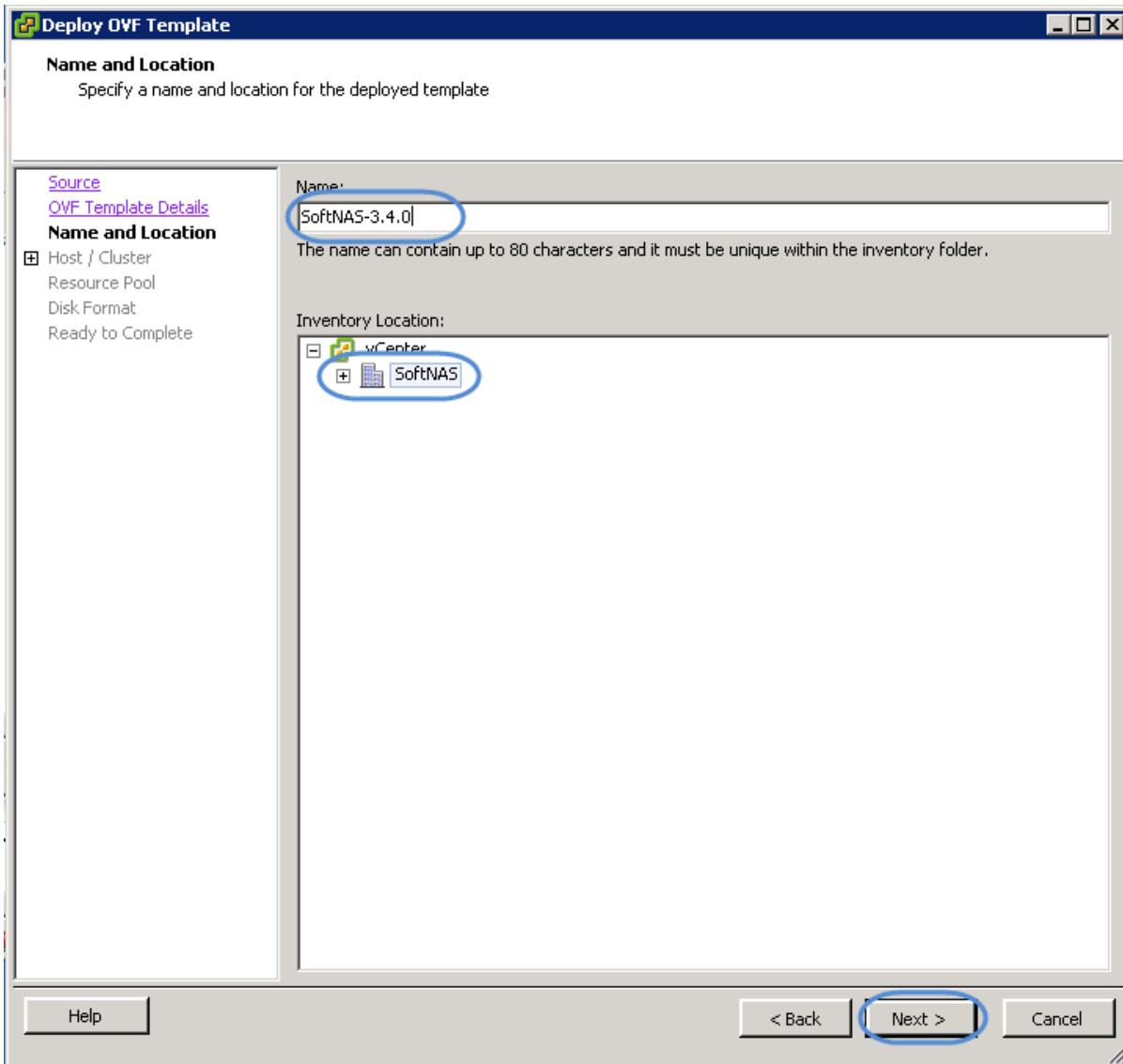
1. Log into your vSphere client with the appropriate credentials.
2. Click **File**, and **Deploy OVF Template**.



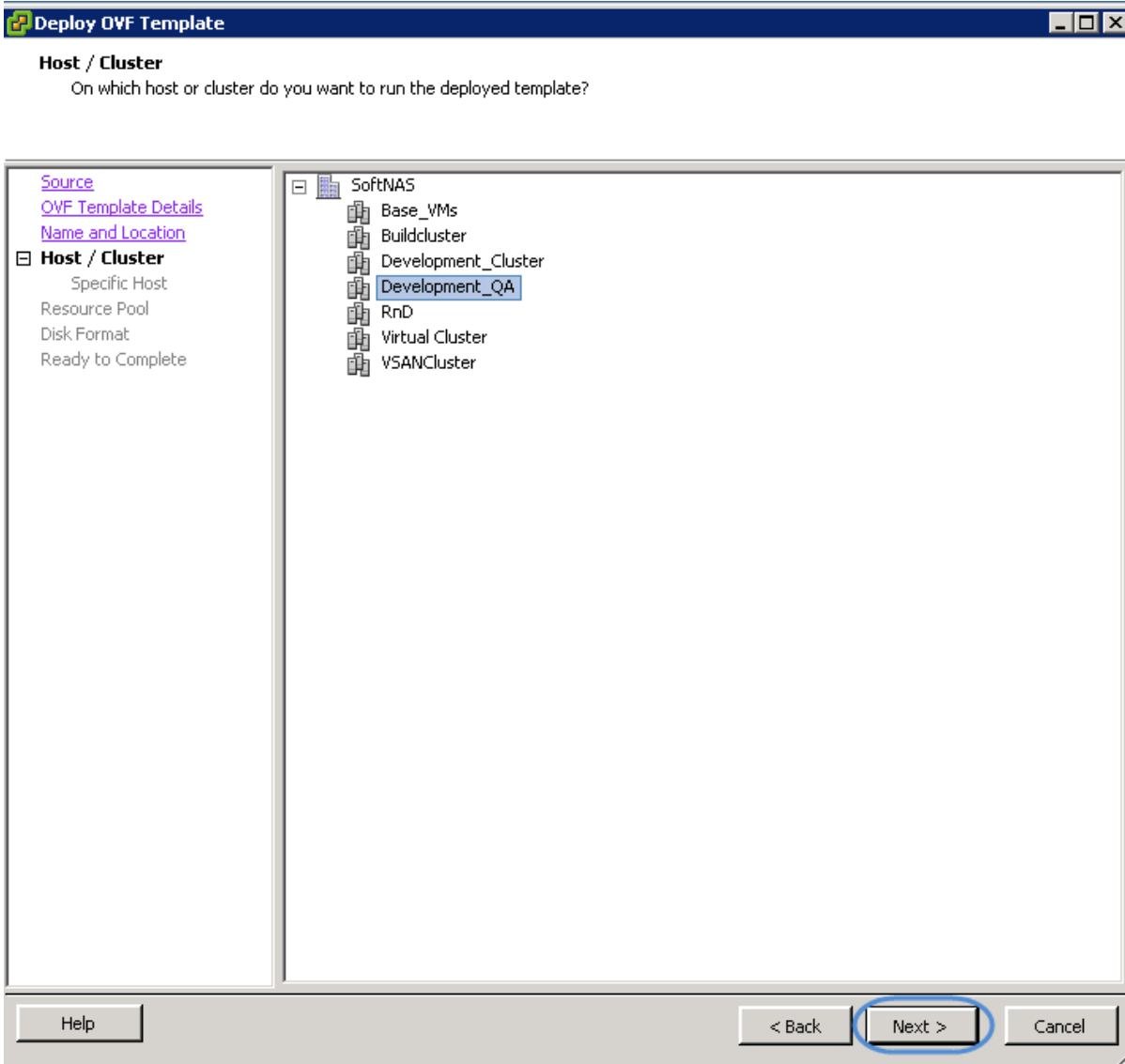
3. Click **Browse** to go to the location of your OVF file, and select it.



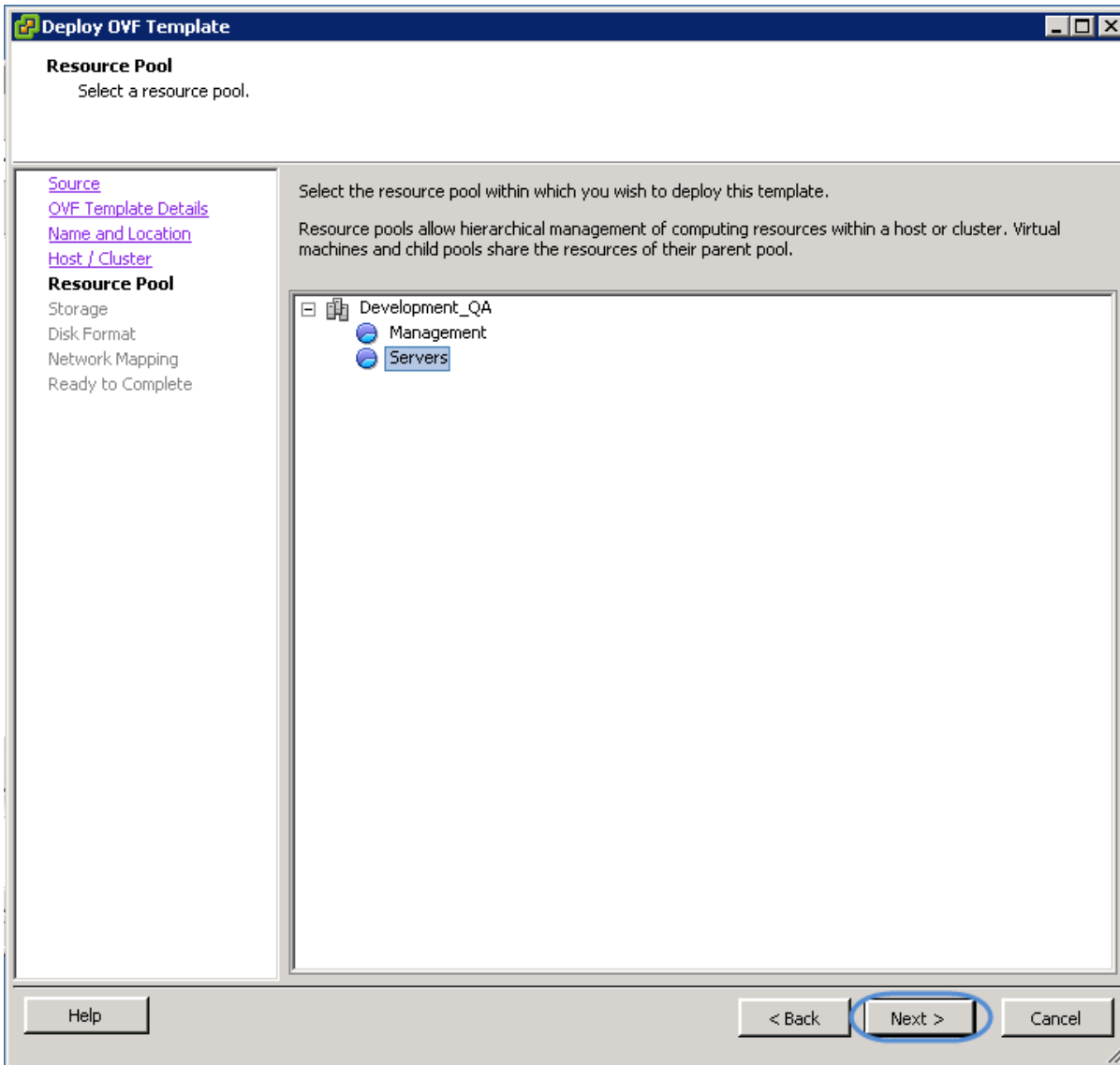
4. Click **Next**, then **Next** again on **OVF Template Details**.
5. Type a name, select a location, and click **Next**.



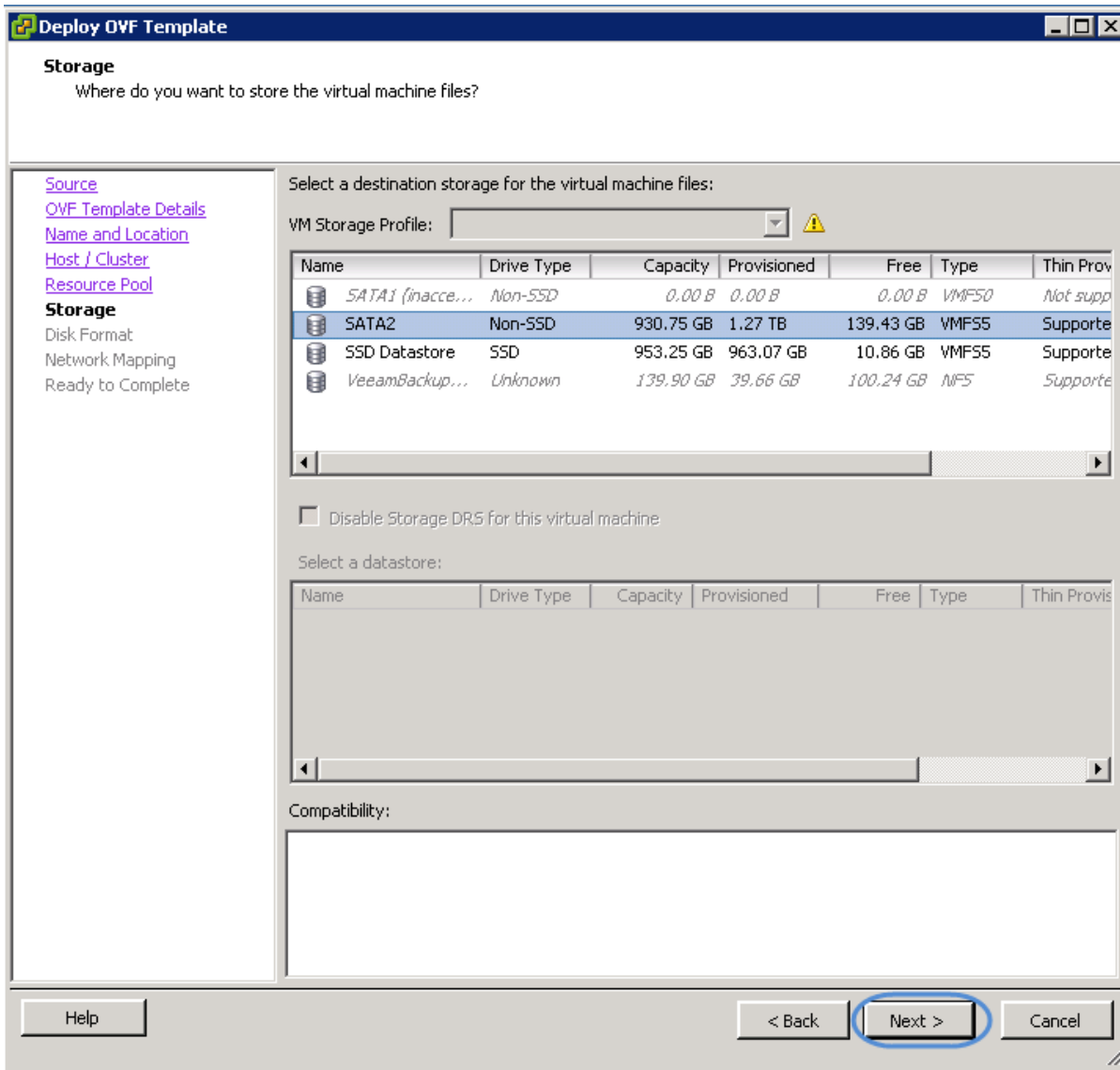
6. Select the Host or Cluster you wish to deploy on, and click **Next**.



7. Select a Resource Pool. Click **Next**.



8. Select your destination storage. Click **Next**.



9. Select a Disk Format, depending on your requirements. For example if running your VM in an environment with space constraints, select thin provisioning. Look to [VMware help](#) for more information. Click **Next**.

10. Select a network for your VM. If creating an HA environment, be sure to select the same network as other instances.

Note: If creating an HA environment, you will require at least three VMs, two to act as paired nodes, and one to act as HA Controller. Plan accordingly.

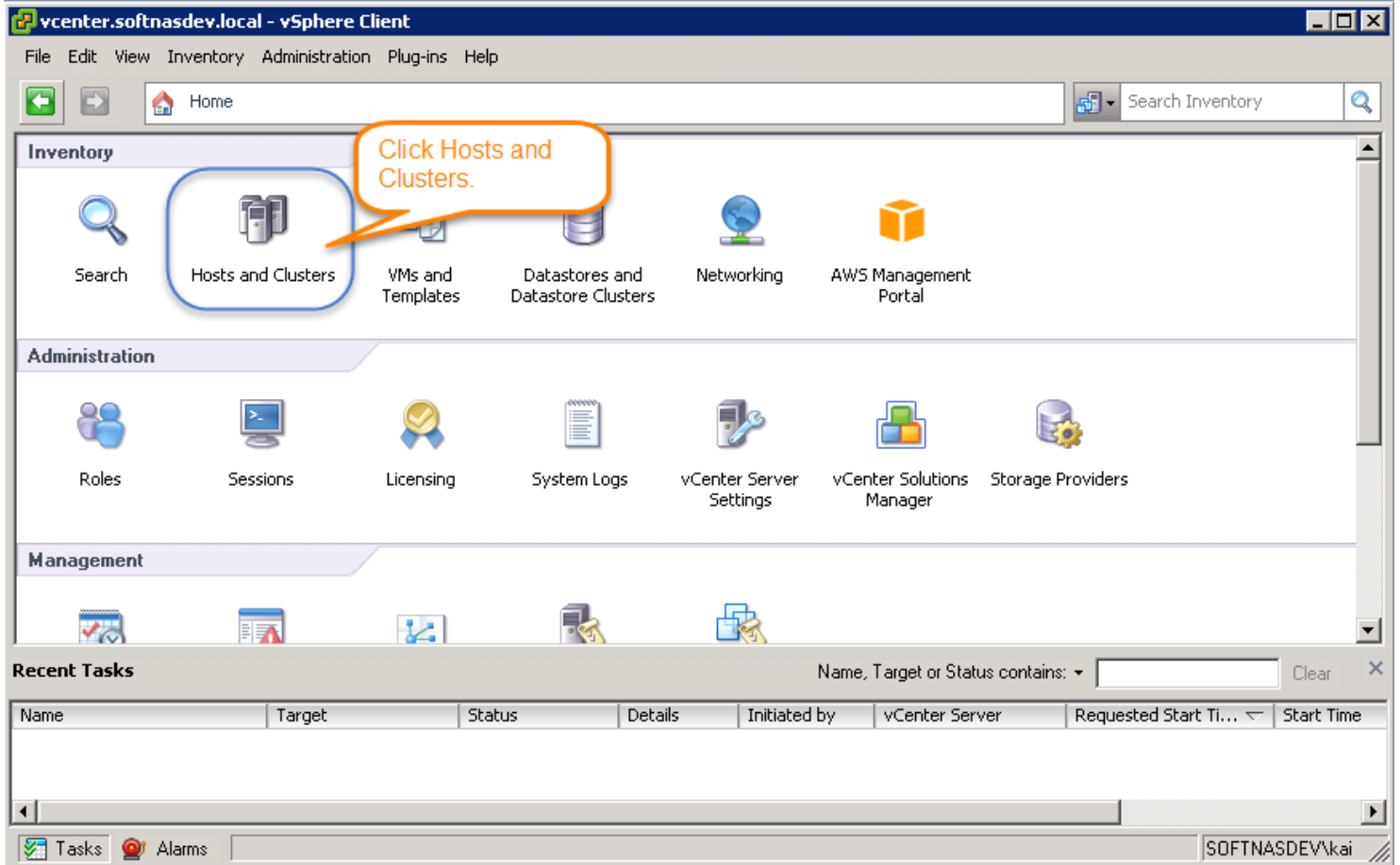
11. Click **Finish**.

Your SoftNAS instance will deploy after a short interval.

Configuring the Network Using SoftNAS Console

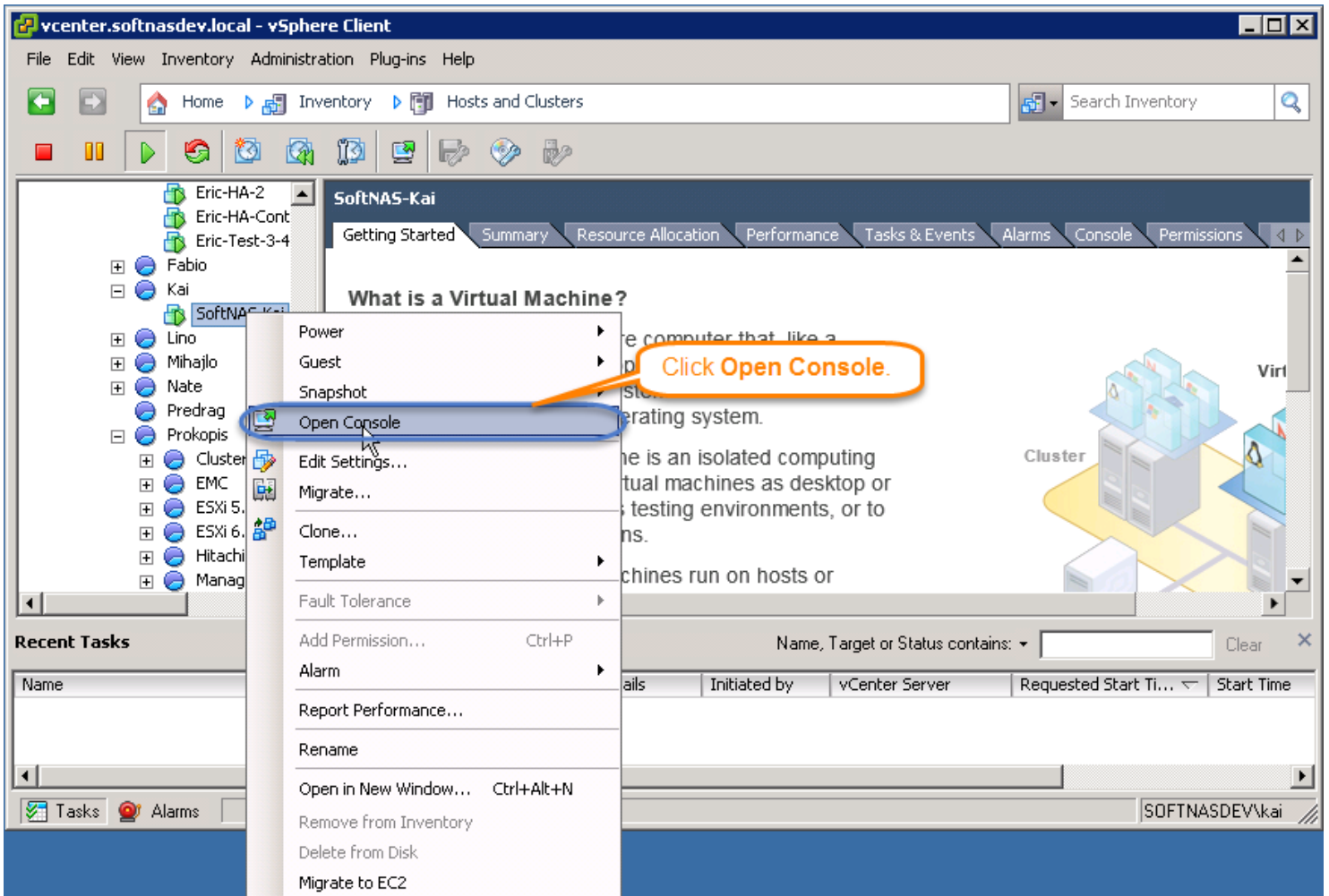
SoftNAS appliances have a **Console** for [VMware vSphere](#).

1. Log into **vSphere Client**.
2. On the **Home Page**, double click the **Host and Clusters** option under the **Inventory** section.



All **Hosts and Clusters** will be displayed.

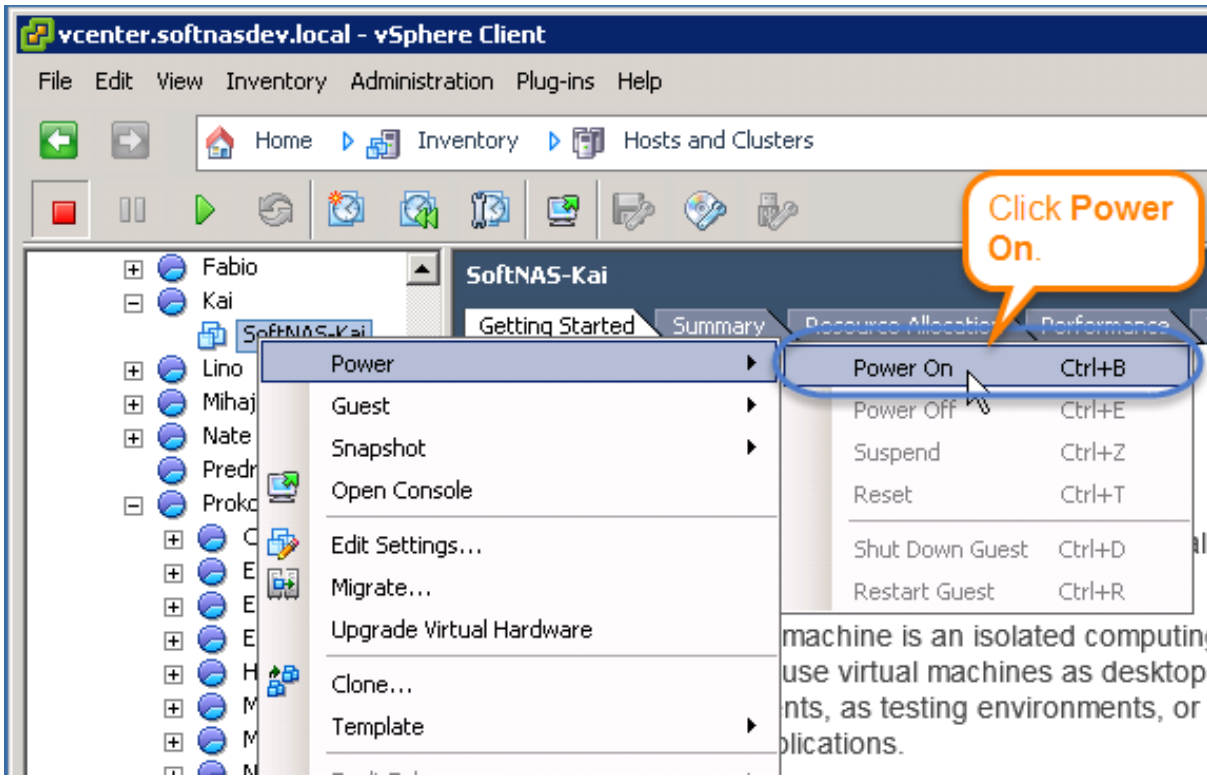
3. Right click on the **SoftNAS VM** and select **Open Console** option.



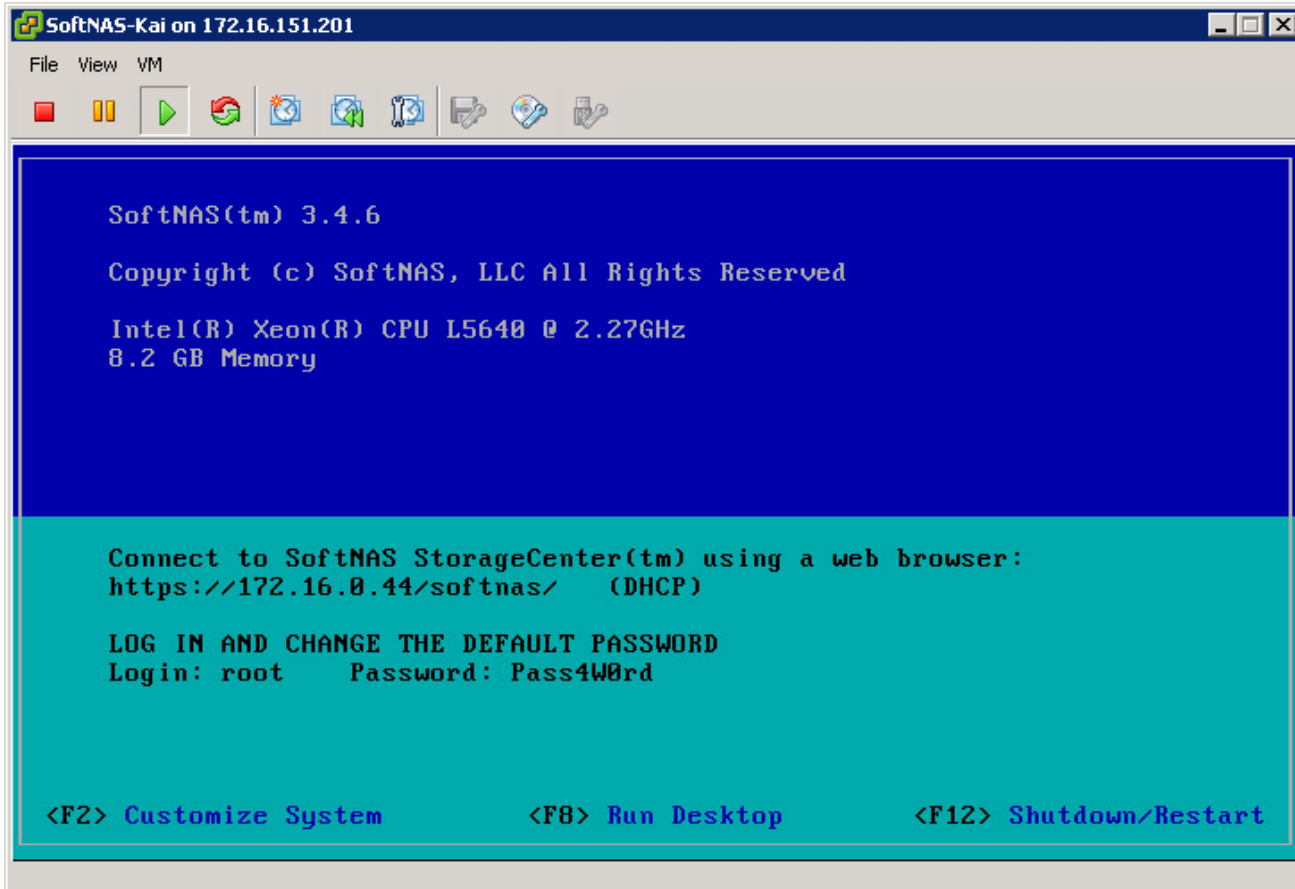
The console of the selected VM will be displayed.

Note: Check the status of VM on the console. If it is off, power it on.

Right click on the **SoftNAS VM** and select the **Power On** option.



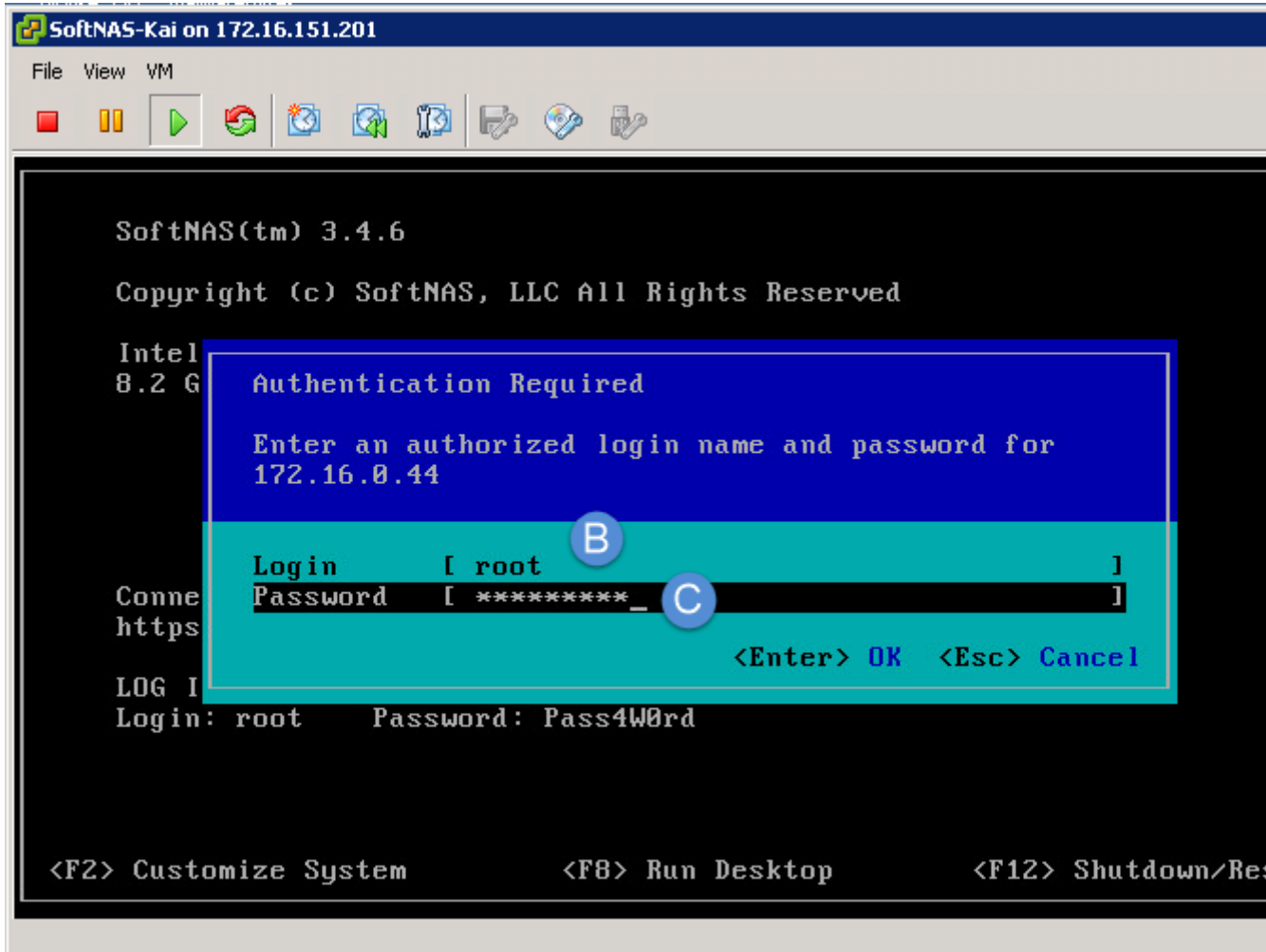
The **Console** with the new configuration screen will be displayed.



The Console has 3 options.

- **Customize System -**

A. To Customize the system, press the **F2** function key on the keyboard.



Enter an authorized login name and password for the logged in VM.

B. Use the login id as root in the **Login** text entry box.

C. Enter the root password as **Pass4W0rd** in the **Password** text entry box (change the root password using the console).

D. Press the **Enter** key on the keyboard to log in.

The [System Customization](#) screen will be displayed.

- **Run Desktop** - To run the desktop, press the **F8** function key on the keyboard.

- **Shutdown/Restart** - To shutdown or restart the system, press the **F12** key on the keyboard.

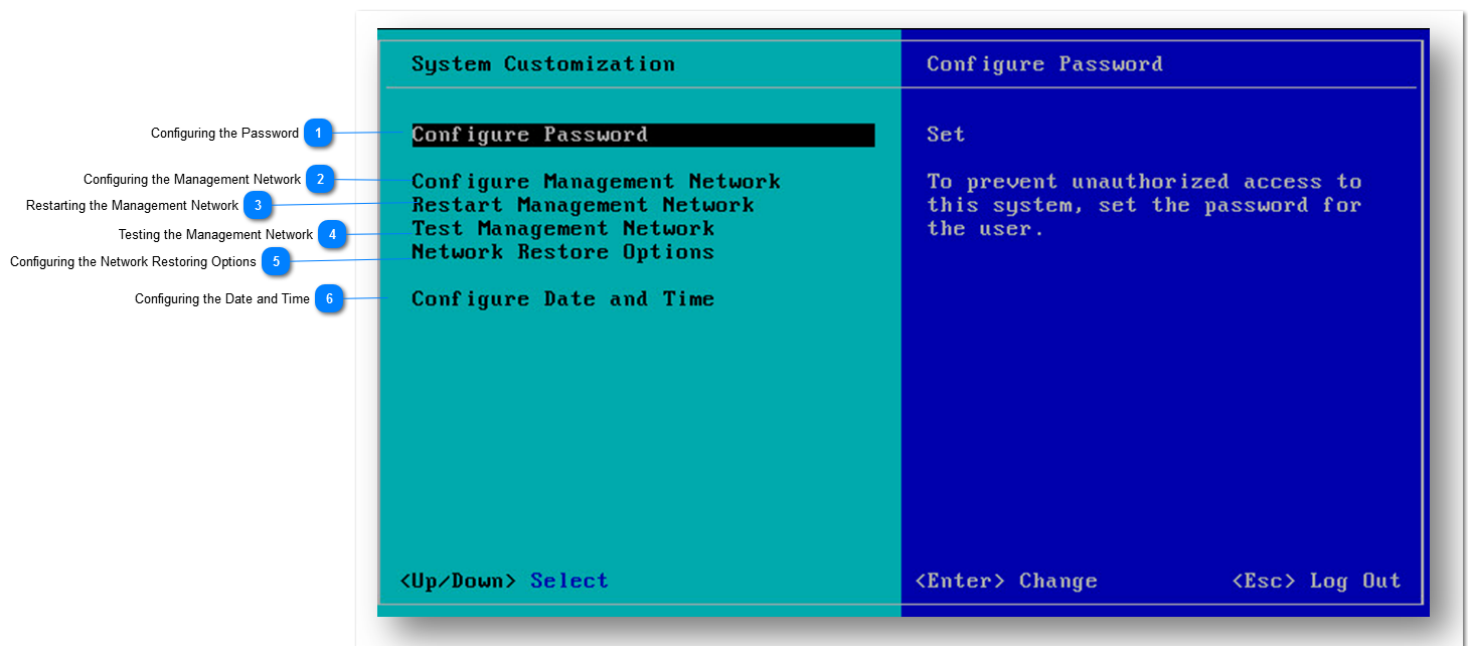
Customizing the System

The **System Customization** screen allows configuration of all the core components of the network (VMware vSphere platforms only).

The screen has the following options.

- Configure Password
- Configure Management Network
- Restart Management Network
- Test Management Network
- Network Restore Options
- Configure Date and Time

Use the Up/Down arrows on the Keyboard to navigate between the options.

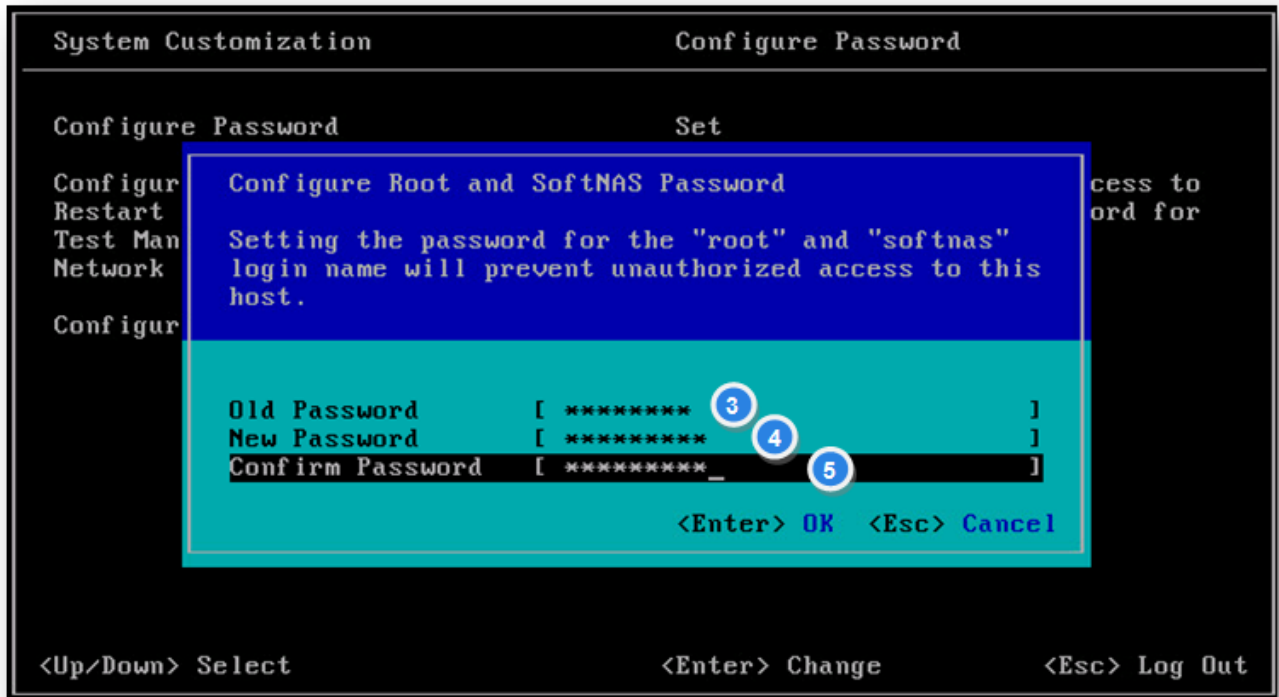


1 Configuring the Password

1. On the **System Configuration** Console, navigate to **Configure Password** option.
2. Press **Enter**.

The **Configure Root and SoftNAS Password** screen will be displayed.

Setting the password for the "root" and "softnas" login name will prevent unauthorized access to this host.



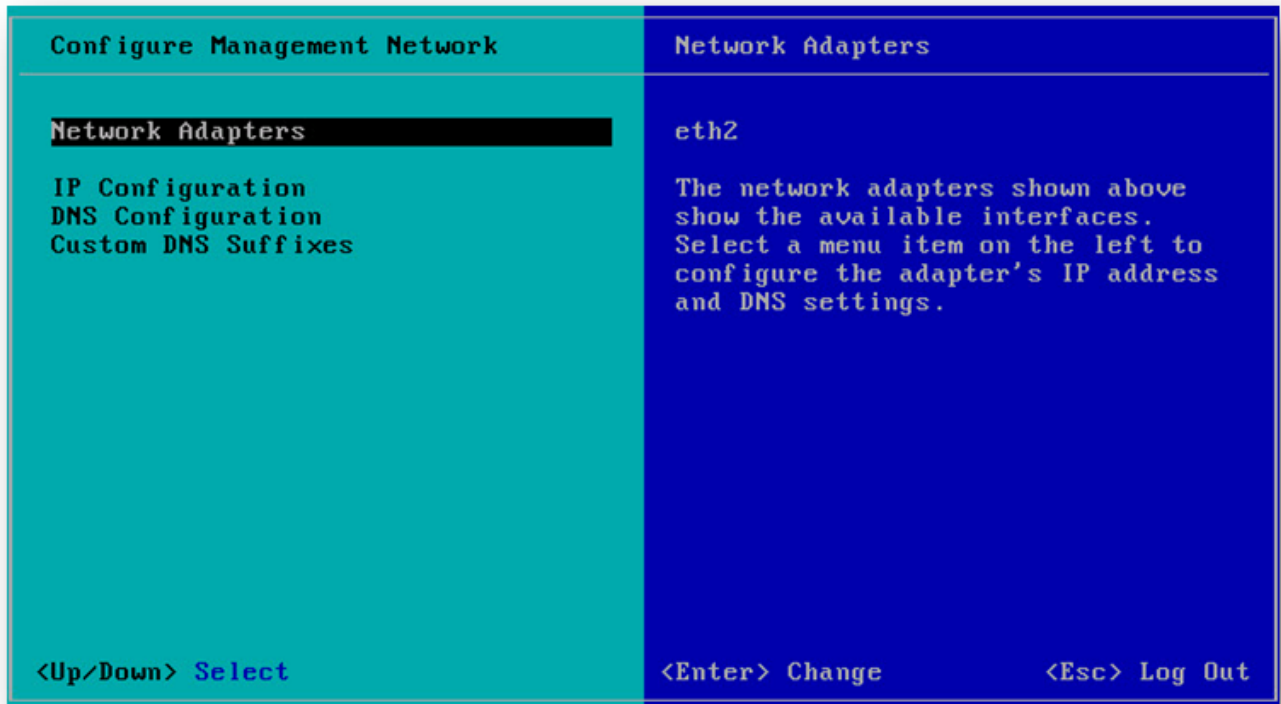
3. Enter the old password in the **Old Password** field.
4. Enter the new password in the **New Password** field.
5. Confirm the password by re-entering it in the **Confirm Password** field.
6. Press **Enter**.

The password will be reset.

2 Configuring the Management Network

1. On the **System Configuration Console**, navigate to **Configure Management Network** option.
2. Press **Enter**.

The **Configure Network Management** screen will be displayed.



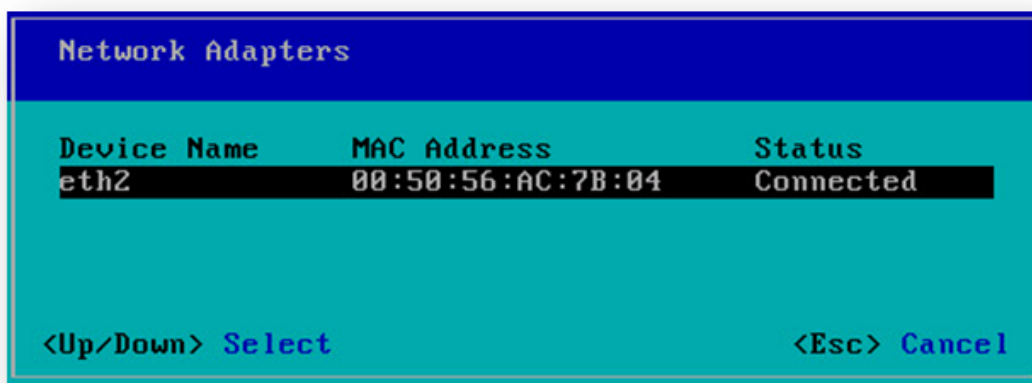
From here, configure the following options:

- Network Adapters
- IP Configuration
- DNS Configuration
- Custom DNS Suffixes

Note: To view or modify this host's management network settings in detail, select the required option and press the Enter key on the keyboard. Configure the selected adapter's IP Address and DNS settings.

3. On the **Network Adapters** option, press the **Enter** key on the keyboard.

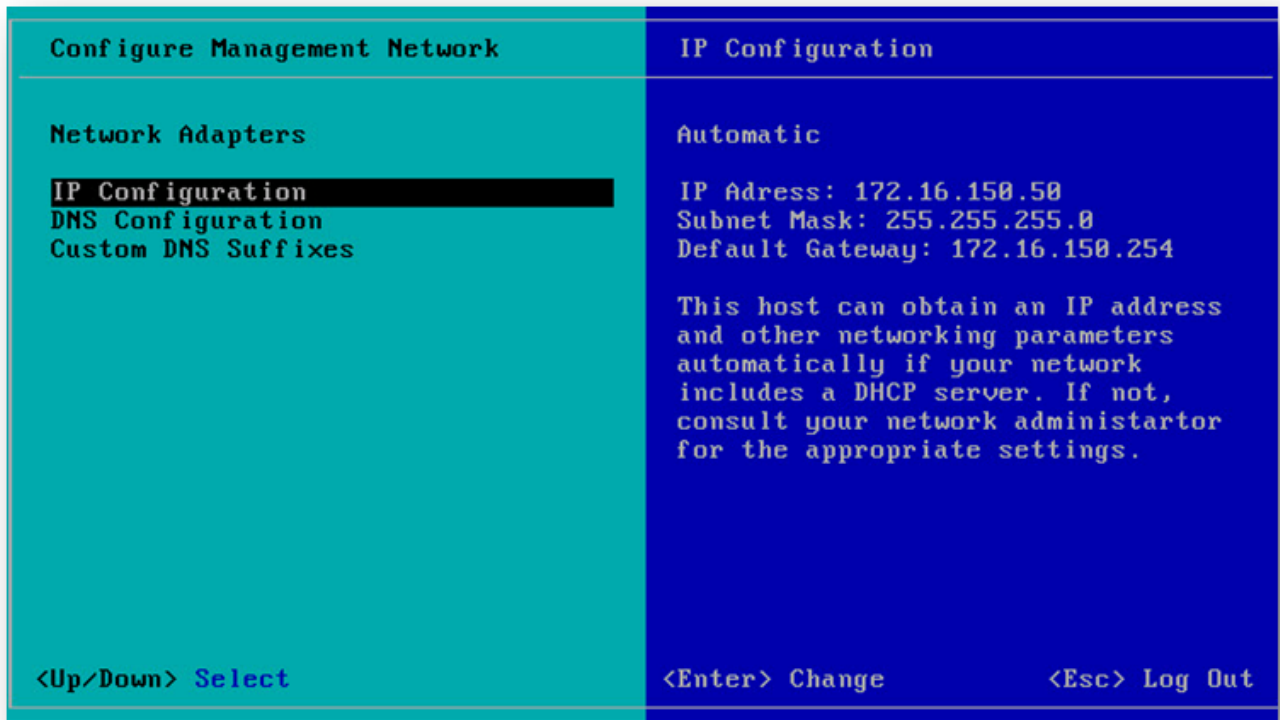
The network adapter screen will be displayed with the available interfaces.



4. Check the **Mac Address** and **Status** of the device.

5. Press **Esc** key on the keyboard.

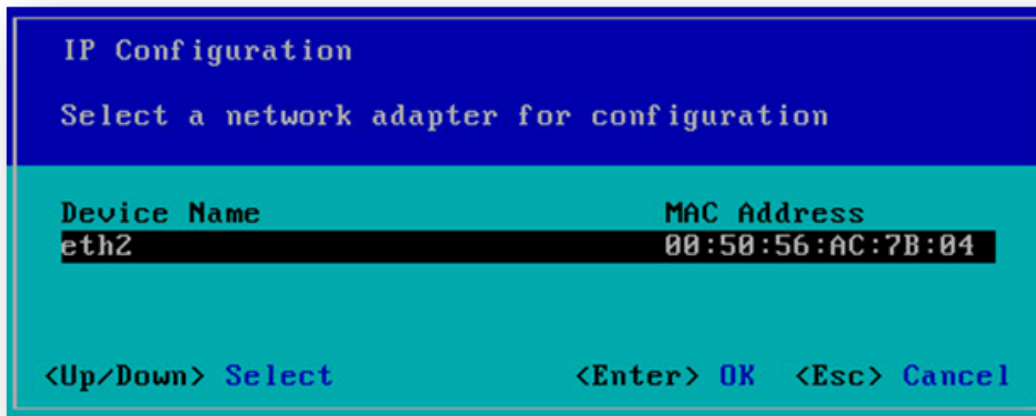
The **Configure Network Management** screen will be displayed.



6. Navigate to the **IP Configuration** option.

7. Press **Enter**.

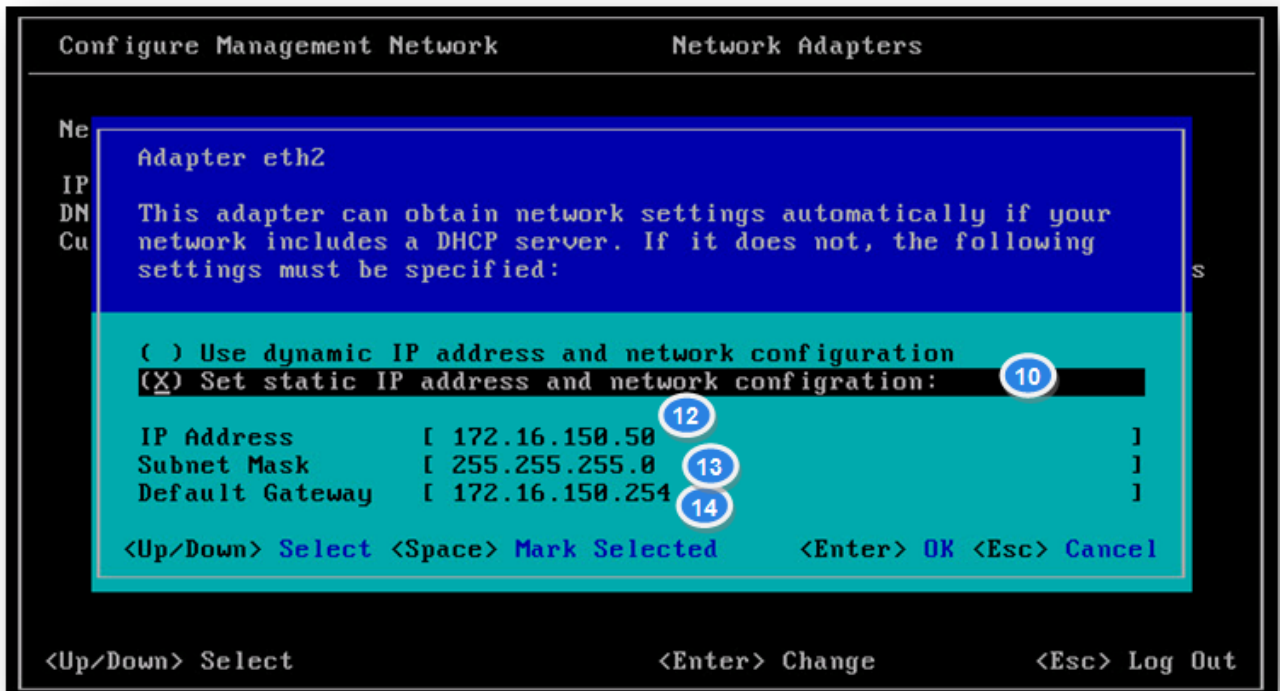
The **IP Configuration** dialog will be displayed.



8. Select the network adapter for configuration.

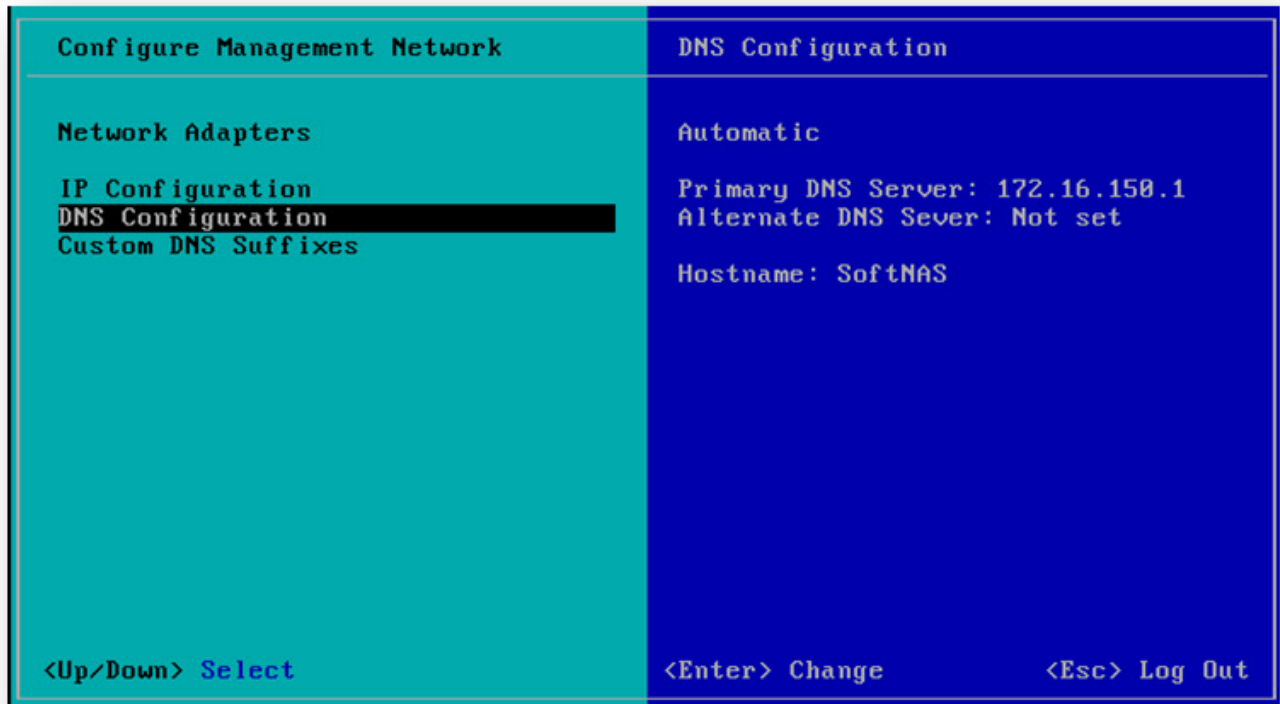
9. Press Enter key on the keyboard.

The configuration options for the selected adapter will be displayed.



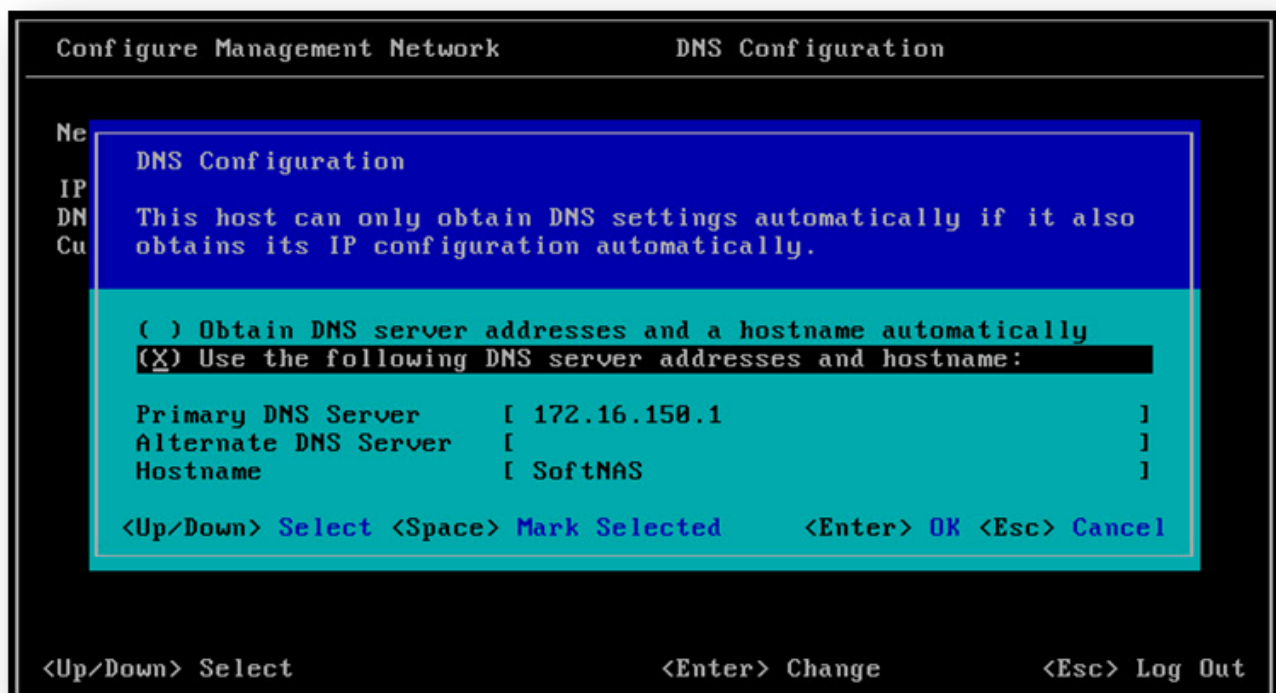
This adapter can obtain network settings automatically on a network including a DHCP server. If it does not, configure the right options.

10. Scroll down to static IP address and network configuration.
11. To select it, press the Space bar key on the keyboard.
12. Set the static IP address.
13. Configure the subnet mask address.
14. Enter the default gateway.
15. Press Enter key on the keyboard.
16. Back on the **Configure Management Network** screen, select the **DNS Configuration** option.
17. Press **Enter**.



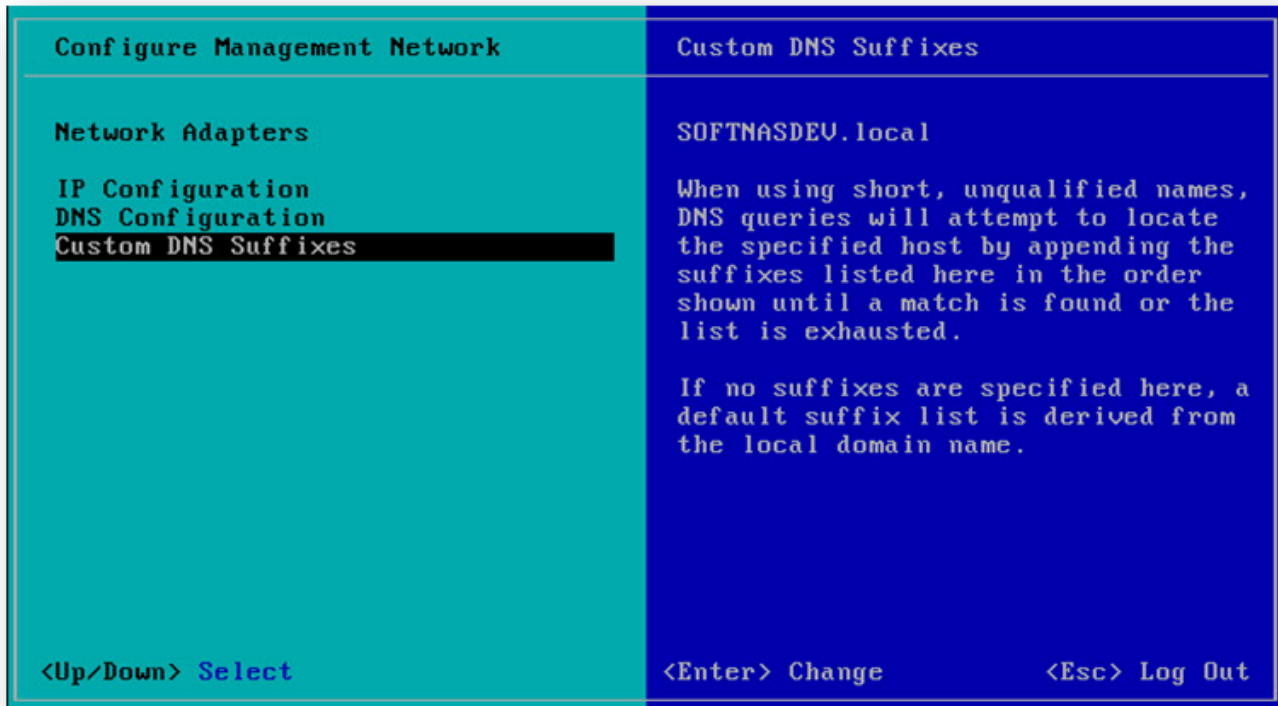
This host can only obtain DNS settings automatically if it also obtains its IP configuration automatically.

18. Configure the required settings.



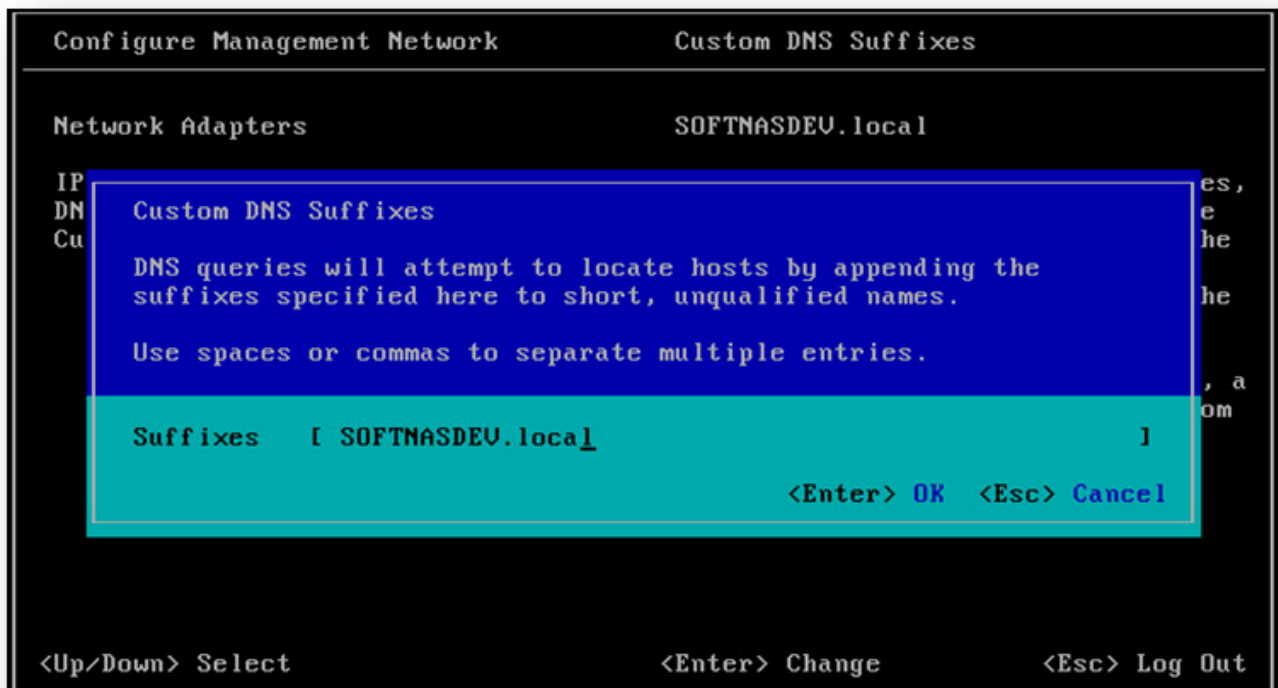
19. Back on the **Configure Management Network** screen, select the **Custom DNS Suffixes**.

20. Press **Enter**.



When using short, unqualified names, DNS queries will attempt to locate the specified host by appending the suffixes listed here in the order shown until a match is found or the list is exhausted.

If no suffixes are specified here, a default suffix list is derived from the local domain name.



DNS queries will attempt to locate hosts by appending the suffixes specified here to short, unqualified names.

21. Enter the proper suffix in the **Suffixes** field. Use spaces or commas to separate multiple entries.
22. Press **Enter**.

3 Restarting the Management Network

1. On the **System Configuration** screen, select the **Restart Management Network** option.
2. Press **Enter**.

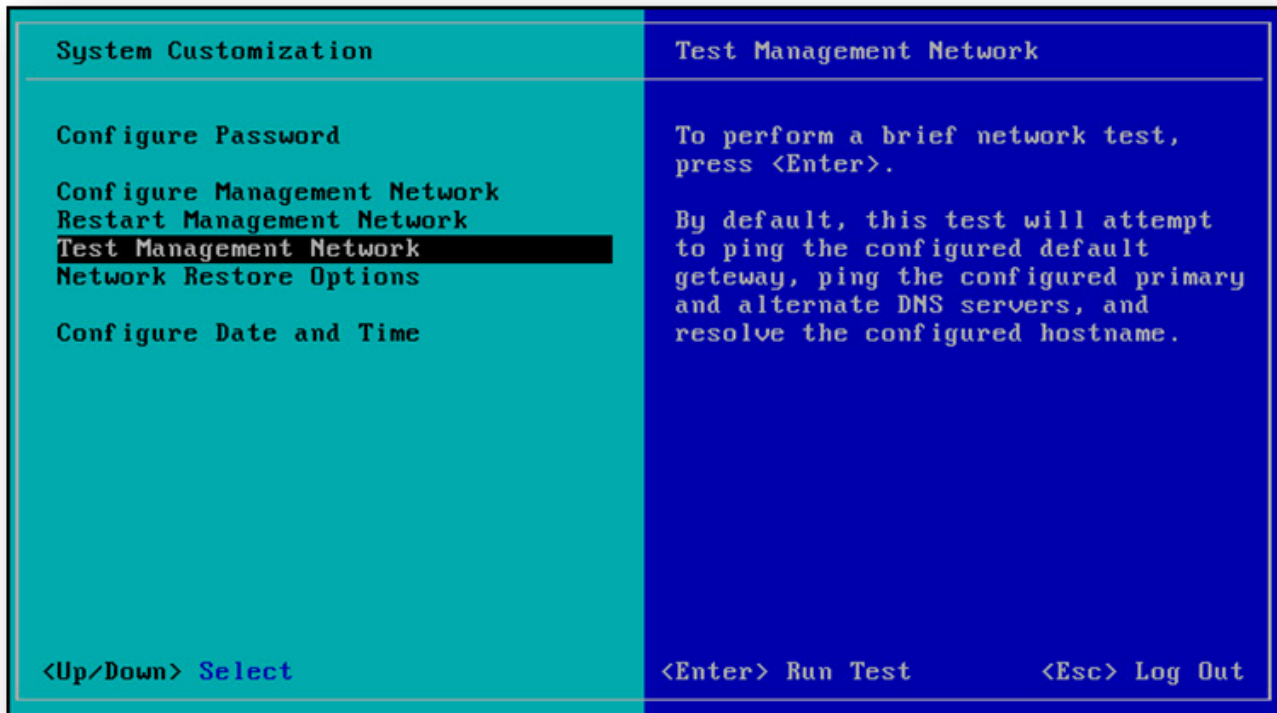


Restarting the management network interface may be required to restore networking or to renew a DHCP lease.

Note: Restarting the management network will result in a brief network outage that may temporarily affect running virtual machines.

4 Testing the Management Network

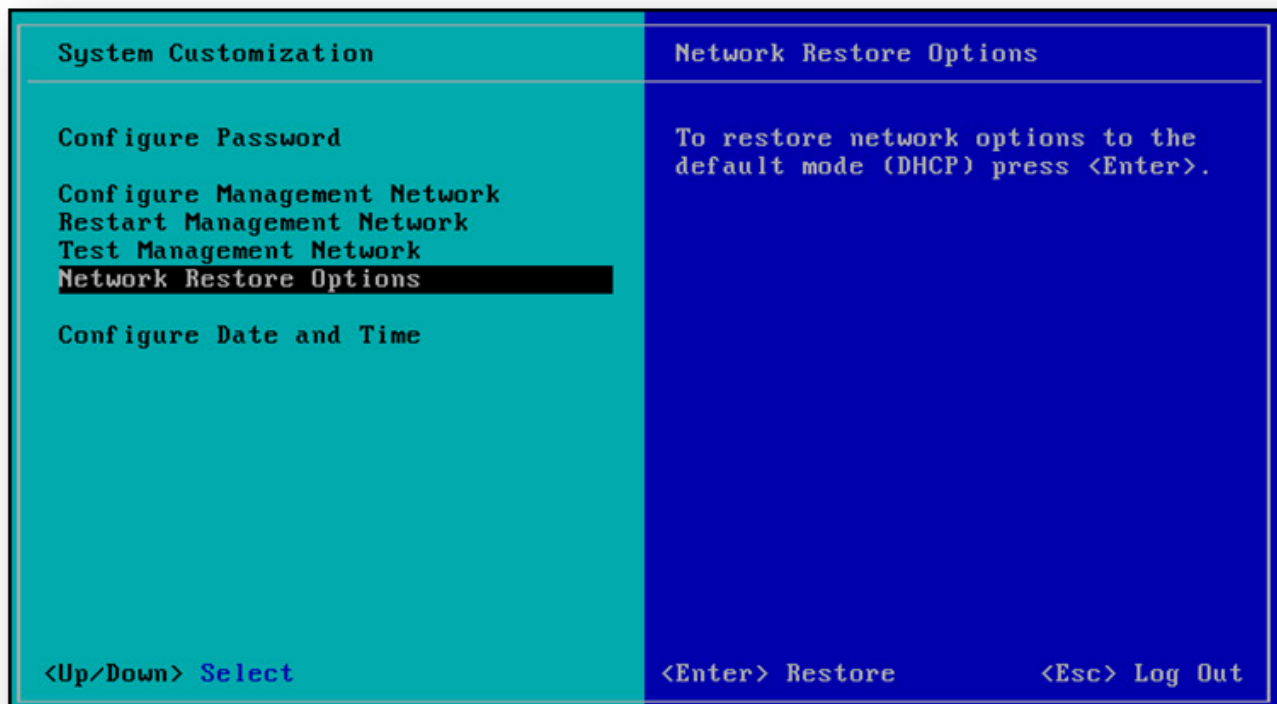
1. On the **System Configuration** screen, select the **Test Management Network** option.
2. To perform a brief network test, press the **Enter** key on the keyboard.



By default, this test will attempt to ping the configured default gateway, ping the configured primary and alternate DNS servers, and resolve the configured hostname.

5 Configuring the Network Restoring Options

1. On the **System Configuration** screen, select the **Network Restore Options**.
2. To restore network options to the default mode (DHCP), press the **Enter** key on the keyboard.

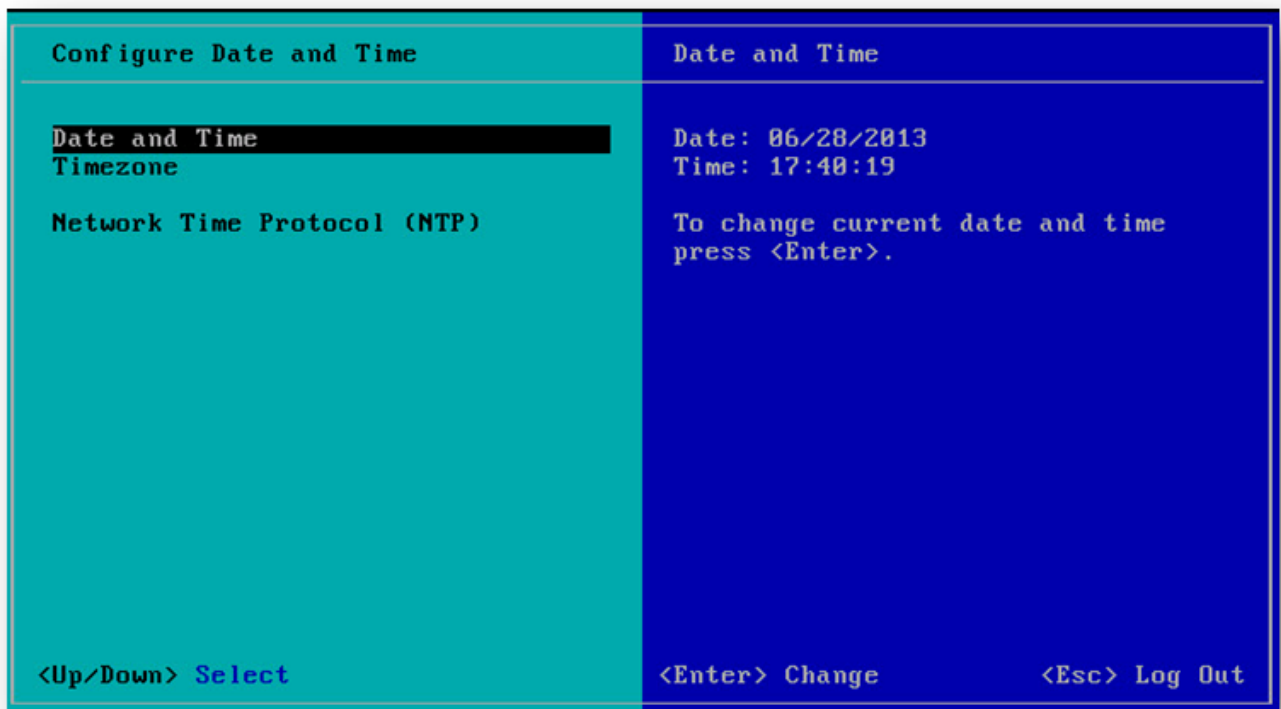


The default network options will be restored.

6 Configuring the Date and Time

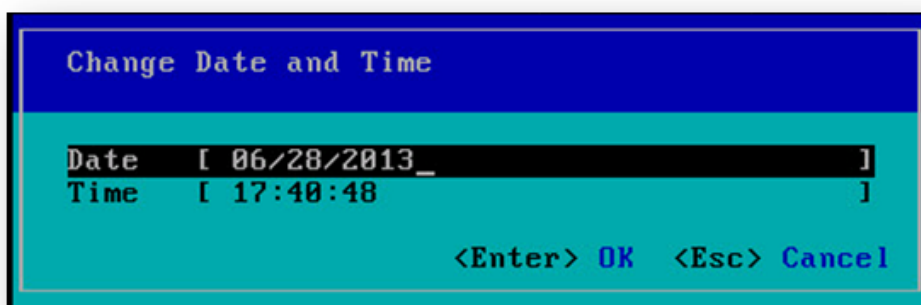
1. On the **System Configuration** screen, select the **Configure Date and Time** option.
2. To restore network options to the default mode (DHCP), press the **Enter** key on the keyboard.

The **Configure Date and Time** screen will be displayed.



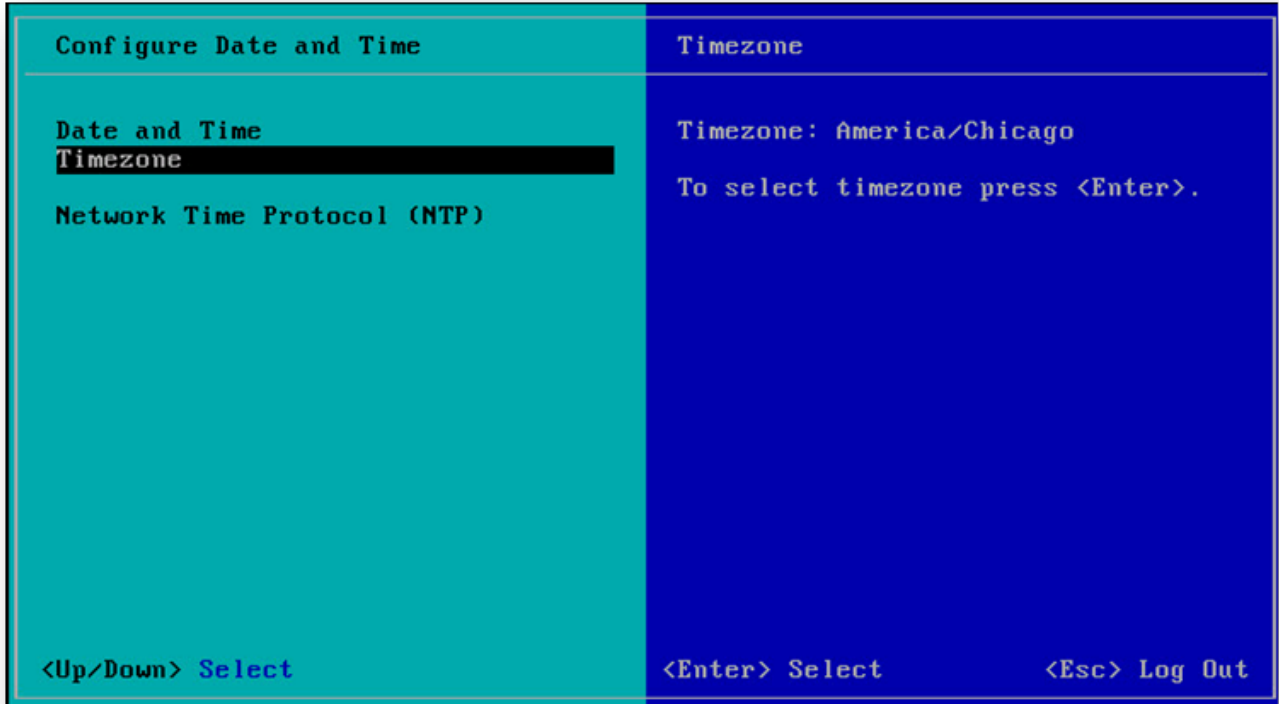
3. To set date and time, select the **Date and Time** option.
4. Press **Enter**.

The **Change Date and Time** dialog will be displayed.

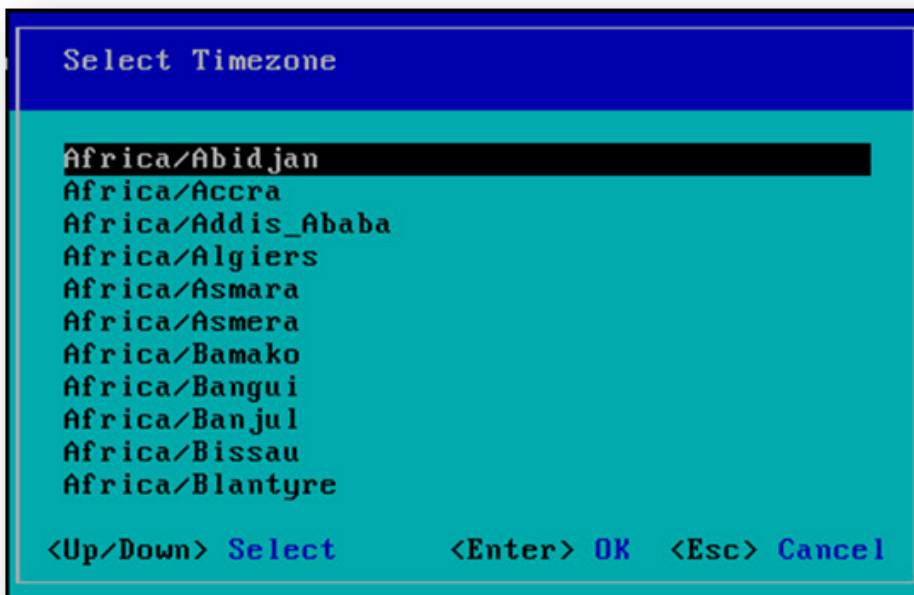


5. Enter the correct date in the **Date** field.
6. Enter the time in hours, minutes and seconds in the field.

7. Press **Enter**.
8. Back on the **Configure Date and Time** screen, select the **Timezone** option to set the required time zone.
9. Press **Enter**.



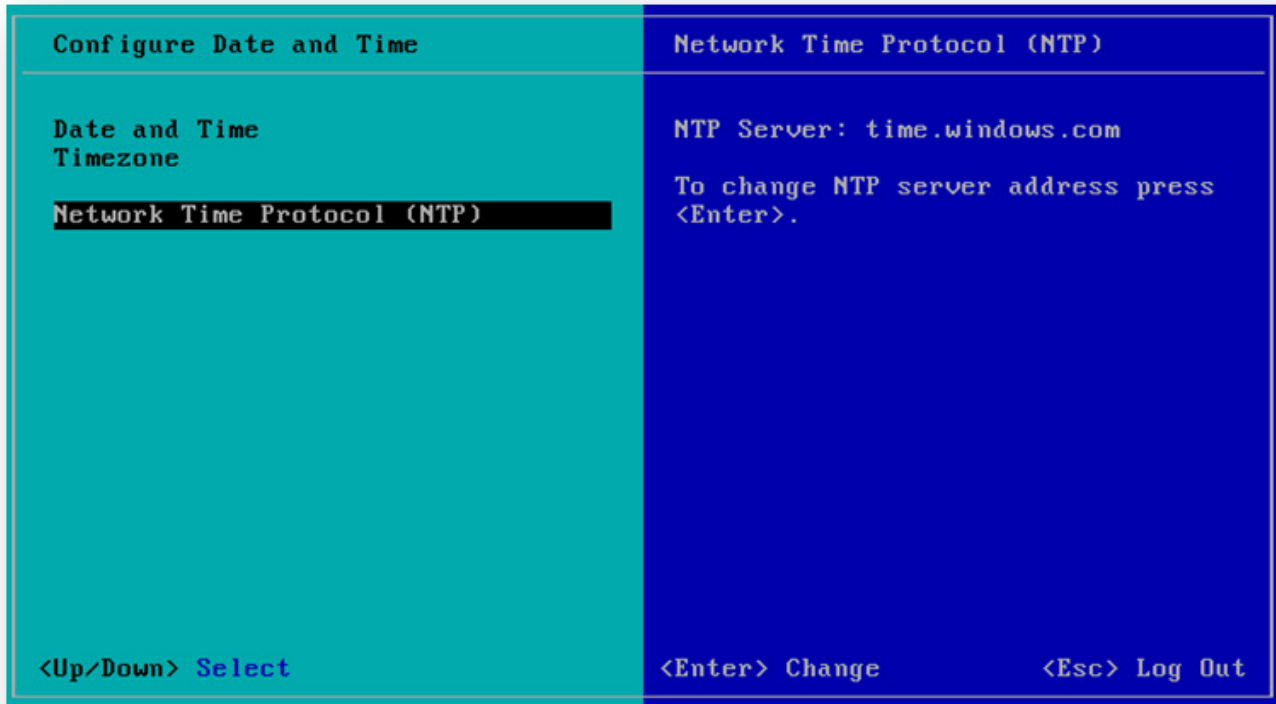
The **Select Timezone** screen will be displayed.



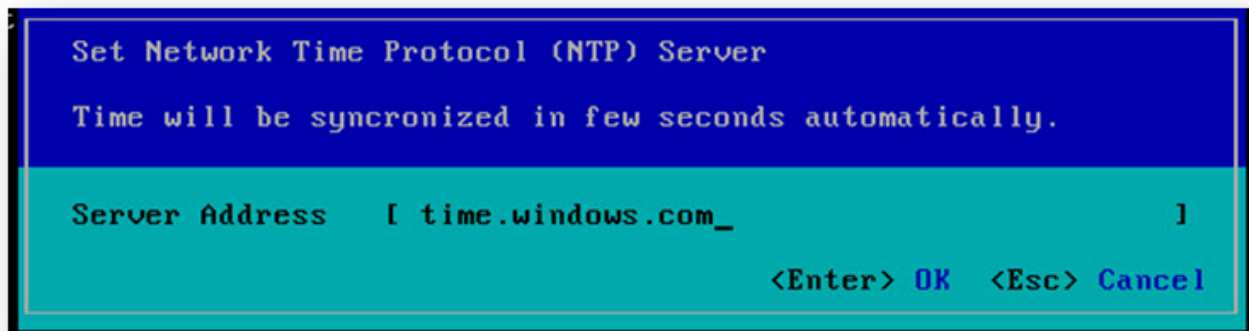
10. Move the up or down arrow to select the required time zone.
11. Press **Enter**.

The selected time zone will be set.

12. Back on the **Configure Date and Time** screen, select the **Network Time Protocol** option.
13. Press **Enter**.



The **Set Network Time Protocol (NTP) Server** screen will be displayed.



14. Enter the NTP server address in the **Server Address** field.
15. Press **Enter**.

The NTP server time will be synchronized.

Configuring VM Settings

Required Settings

After installing the OVF to create the **SoftNAS Virtual Storage Appliance VM**, configure the VM settings in accordance with best practices and network needs. The boot disk (Hard Disk 1) should be set to 30 GB, thin-provisioned.

For a quick benchmarking resource configuration, use 4 vCPUs and 4 to 8 GB of RAM. Configure storage and run benchmarking tools to observe resource utilization in the **SoftNAS StorageCenter Dashboard** charts and vSphere performance charts.

RAM Note: The operating system and **SoftNAS** consume up to 1 GB of RAM, using most of the remaining RAM for cache memory and metadata. The more RAM assigned to the VM, the better read cache performance will be, as SoftNAS will keep as much data in RAM cache as possible. Consider this resource allocation for deduplication: at least 1 GB of RAM per terabyte of deduplicated storage, to keep the deduplication tables in memory (or supplement the RAM cache with a read cache device).

Optional Settings

Paravirtual SCSI Disk Controller Support

For maximum throughput and IOPS on VMware, choose the **Paravirtual SCSI Controller for the SoftNAS VM** (instead of using the default LSI Logic Parallel SCSI controller).

VM Snapshot Mode

Before applying software updates to **SoftNAS** after it is in production, and to support online backups in popular backup programs, VM snapshots are useful as part of the backup and recovery process. Depending on the plan to manage backups of VM data, choose which mode snapshots will operate in.

- **Independent Mode** - to enable smaller VM snapshots, configure the boot disk, Hard Disk 1, in the "Independent" mode. This causes VM snapshots to apply only to this first hard disk by default (and not include all added data disks, which could be prohibitively large). The advantage of using Independent mode is VM snapshots will be faster and smaller.
- **Dependent Mode** - by default, VM snapshots include all hard disks attached to the VM. When used with SoftNAS and a VM backup process, this setting causes all SoftNAS VM disks to be backed up together as a set. This results in much larger backup sets, but may be preferable as a means of achieving additional protection and recoverability in the event of a disaster or need to restore the entire storage system to a different computer or location. If there are only a few terabytes to back up, this may be the prudent choice.

Network Adapter

On a typical 1 gigabit network, the default E1000 network adapter is sufficient; however, for a 10 gigabit or higher-performance network card, the VMXNET 3 network adapter should be used for best results and higher throughput. Note that installation of the VMXNET 3 requires installation of the proper VMware Tools in the guest operating system (in this case, CentOS 64-bit Linux).

Memory / CPU Hot Plug

It is recommended to **allow CPU Hot Plug** and **disable Memory Hot Add**, which will make it more convenient to add CPU later to use a lot of data compression or other features that consume additional CPU. Linux seems to do fine when additional CPU are added at run-time.

Note: Add memory with the system powered down and disable hot add of memory at run time.

Logging on to VM

Save the **SoftNAS Cloud® for VMware vSphere OVA** file to a computer from the email received after product registration. This version of **SoftNAS Cloud®** is delivered as an **OVA** virtual machine appliance file for **VMware vSphere** related virtual machine environments. This **OVA** has been tested and certified for use with **VMware vSphere**.

Connect to **ESXi** host via **VMware vSphere** Client, either directly to the host or using **vCenter**, as appropriate.

From vSphere Client

For virtual machine environment such as **VMware ESXi**, deploy the **SoftNAS™ Virtual Storage Appliance** on hosts that are running ESXi version 4.x or later. Then access the **OVF** files from **vSphere Client**.

1. Start **vSphere Client** installed on a computer within the virtual network.



2. Provide the host IP login credentials to access **SoftNAS Virtual Storage Appliance** installed on the local host server.

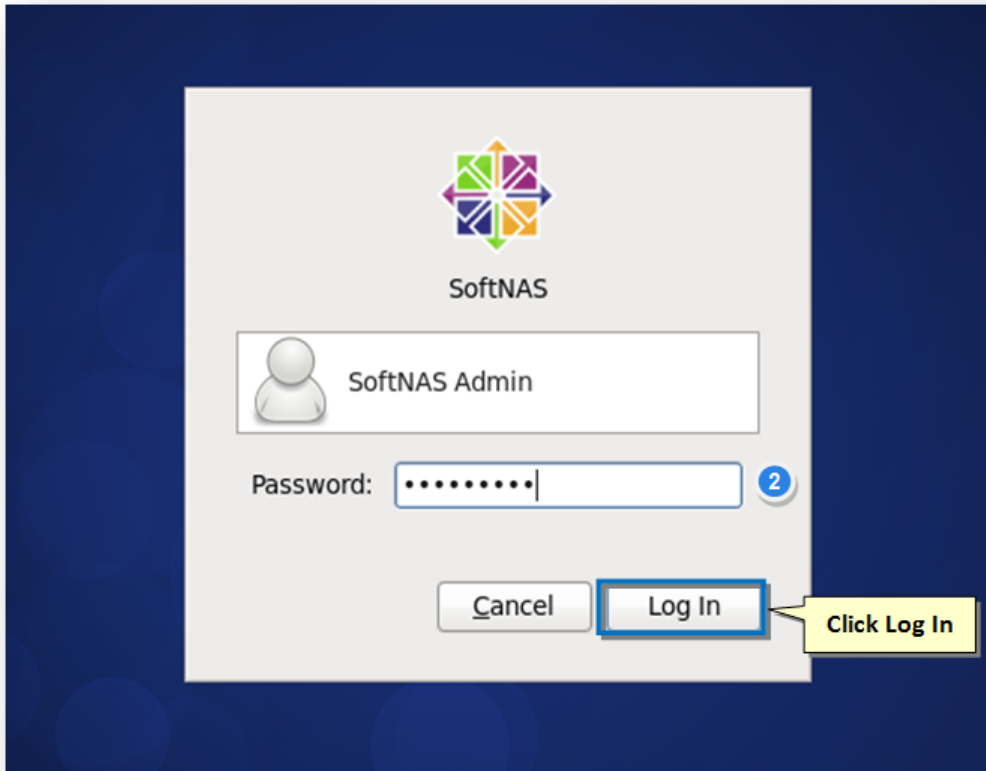
Select the **SoftNAS VM**.

3. Install the **OVA** software appliance using **VMware vSphere Client** and follow the on-screen instructions.
 - In the **VMware vSphere Client**, select **File > Deploy OVF Template** and enter the path or navigate to the **OVA** file on the local system.
 - Follow the prompts in the **Deploy OVF Template wizard** to create the **SoftNAS Cloud® Virtual Storage Appliance** as a VM on the local host.
 - If prompted to choose the operating system, select **64-bit Linux CentOS 4/5/6 (64-bit)** and **Thin Provisioned**. The VM will consume approximately 30GB of disk space.

4. **Power On** the VM and **Open Console**.

5. Click the **SoftNAS Admin** option to begin the login process.

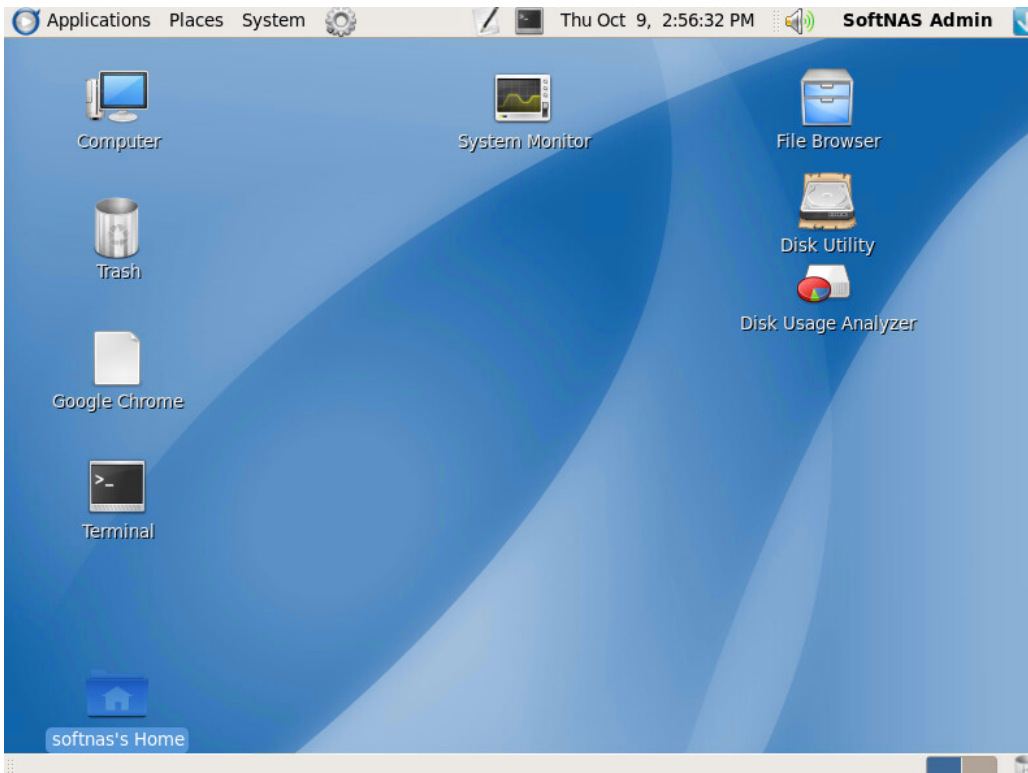
The **SoftNAS Cloud® Login** screen will be displayed,.



5. If the administrator password has not been changed yet, enter the default password **Pass4W0rd** (with a zero), in the Password text entry box.

6. Click **Log In**.

The **SoftNAS Cloud® VM's** desktop will be displayed.



Open **Terminal** from the **SoftNAS Cloud® VM** desktop to find or verify the IP address required for access to **SoftNAS StorageCenter**.

From the **SoftNAS Cloud® VM** desktop, either access the **SoftNAS Storage Administration** or **Terminal** to configure network settings.

Now that the VM has been verified, open [SoftNAS StorageCenter](#).

Performance Tuning for VMware vSphere

Achieving peak storage performance in the VMware environment involves tuning the VMware configuration beyond default values. The following are recommended best practices for tuning VMware for use with SoftNAS.

VMDirectPath

VMDirectPath provides a means of passing a disk controller device directly through to the guest operating system (i.e., CentOS Linux).

To enable VMDirectPath Configuration page in the vSphere Client

- 1) Select the ESX host from Inventory.
- 2) Select the Configuration tab.
- 3) Select Advanced Settings under Hardware.
- 4) Edit and select device(storage controller,physical nic)

Note that Intel VT-d (or equivalent) processor feature is required for support of VMDirectPath.

VM SCSI Controller - Set to Paravirtual

In VMware, change the SCSI controller type to "Paravirtual", which provides more efficient access to storage.

Physical NIC Settings

A host physical NIC can have settings, which can provide better utilization and performance improvement:

Most 1GbE or 10GbE NICs (Network Interface Cards) support a feature called interrupt moderation or interrupt throttling, which coalesces interrupts from the NIC to the host so that the host does not get overwhelmed and spend too many CPU cycles processing interrupts.

To disable physical NIC interrupt moderation on the ESXi host execute the following from ESXi SSH session.

Find the appropriate module parameter for the NIC by first finding the driver using the ESXi command:

```
# esxcli network nic list
```

Then find the list of module parameters for the driver used:

```
# esxcli system module parameters list -m <driver>
```

This example applies to the Intel 10GbE driver called ixgbe.

```
# esxcli system module parameters set -m ixgbe -p "InterruptThrottleRate=0"
```

Also, check the host for SR-IOV support, which provides additional performance and throughput in virtualized systems like VMware.

Adjust Network Heap Size for high network traffic

By default ESX server network stack allocates 64MB of buffers to handle network data.

Increase buffer allocation from 64MB to 128MB memory to handle more network data

To change Heap Size ESX Host:

Configuration tab for the ESX Server host- Advanced Settings-VMkernel - Boot-VMkernel.Boot.netPktHeapMaxSize

Virtual NIC Settings

VM's virtual adapter has many tuning options, which can also provide much better throughput:

Configure jumbo frames (MTU 9000) in vSwitch and virtual network adapter (be sure physical switch supports MTU 9000)

We recommend VMXNET 3 virtual NICs

Disable virtual interrupt coalescing for VMXNET 3 virtual NICs as follows:

Go to vSphere Client, go to VM Settings - Options tab - Advanced General - Configuration Parameters and add an entry for ethernetX.coalescingScheme with the value of disabled.

An alternative way to disable virtual interrupt coalescing for all virtual NICs on the host which affects all VMs, not just the latency-sensitive ones, is by setting the advanced networking performance option (Configuration - Advanced Settings - Net) CoalesceDefaultOn to 0 (disabled).

Disable LRO

Reload the vmxnet3 driver in the **SoftNAS CentOS** guest operating system. Log into the **SoftNAS Cloud® VM** using SSH (or the Desktop Console) and **su root**:

```
# modprobe -r vmxnet3
```

Add the following line in `/etc/modprobe.conf`:

```
(options vmxnet3 disable_lro=1)
```

Then reload the driver using:

```
# modprobe vmxnet3
```

Physical Host BIOS Settings

On most servers, these BIOS Settings can improve the overall performance of the host:

- Turn on Hyper-threading in BIOS
- Confirm that the BIOS is set to enable all populated sockets for all cores
- Enable "Turbo Mode" for processors that support it
- Confirm that hardware-assisted virtualization features are enabled in the BIOS
- Disable any other power-saving mode in the BIOS
- Disable any unneeded devices from the BIOS, such as serial and USB ports
- In order to allow ESXi to control CPU power-saving features, set power management in the BIOS to "OS Controlled Mode" or equivalent. Even without planning to use these power-saving features, ESXi provides a convenient way to manage them.
- C-states deeper than C1/C1E (i.e., C3, C6) allow further power savings, though with an increased chance of performance impacts. We recommend, however, enabling all C-states in BIOS, then use ESXi host power management to control their use.

NUMA Settings

NUMA systems are advanced server platforms with more than one system bus. They can harness large numbers of processors in a single system image with superior price to performance ratios. The high latency of accessing remote memory in NUMA (Non-Uniform Memory Access) architecture servers can add a non-trivial amount of latency to application performance.

For best performance of latency-sensitive applications in guest OSes, all vCPUs should be scheduled on the same NUMA node and all VM memory should fit and be allocated out of the local physical memory attached to that NUMA node.

Processor affinity for vCPUs to be scheduled on specific NUMA nodes, as well as memory affinity for all VM memory to be allocated from those NUMA nodes, can be set using the vSphere Client under VM Settings – Options tab – Advanced General – Configuration Parameters and adding entries for “numa.nodeAffinity=0, 1, …,” where 0, 1, etc. are the processor socket numbers.

Allocating Disk Storage Devices

Add Data Disks to SoftNAS Cloud® VM

Adding storage to **SoftNAS Cloud®** involves adding virtual hard disks (VMDKs on **VMware**) to the **SoftNAS Cloud® VM**. The first step is to decide how to connect the drives, then associate the disks' storage with the **SoftNAS Cloud® VM** as virtual disks.

For example, consider a network of ten 300 GB 15K SAS drives attached to a **VMware vSphere** host. There are several ways to incorporate these drives into the **SoftNAS Cloud®**.

Option 1 - Add Hardware RAID Datastore and Virtual Disks

In this case, treat the 15K SAS drives just like any other RAID array created for a **VMware vSphere** host:

Configure and establish a RAID array.

- Use the vendor-supplied software that came with the disk controller

For example, a configuration of ten disks as RAID 6 (dual parity), plus one hot spare. This leaves seven data drives in the array.

In **VMware vSphere**, the disk array will appear as a single datastore to **VMware**. Add this storage in the usual way, using **Add Storage** menu in **vCenter / vSphere** client to create a datastore from the array. Call this datastore **hwraid1**.

hwraid1 array	7 data disks
	2 parity disks
	1 spare disk
datastore 1	hwraid1 array

Then, in VM Settings for **SoftNAS Cloud®**, allocate one or more VMDKs to the **SoftNAS Cloud® VM** in this new datastore **hwraid1**. In environments with **ESXi 5.x** or later, allocate one large VMDK so the entire datastore is allocated to **SoftNAS** as a single virtual disk. In environments using **ESXi 4.x**, the datastores are limited to 2 TB maximum, so allocate as many virtual disks as needed to add this storage to the **SoftNAS Cloud® VM**.

Thin-provisioned VMDKs are faster to back up later (using a **VMware vSphere** backup tool), since the only thing being backed up is the storage that's actually used. Thick-provisioned VMDKs are slightly faster and may be preferred for higher-performance applications.

Hardware RAID generally provides the highest performance:

- The disk controller is optimized for managing the RAID operations
- And all RAID overhead is handled in hardware
- LED indicators and other hot-swap functionality is handled by the vendor software (including failure notification and remediation).
- When a disk fails, the hardware is optimized for rebuilding the array with the replaced disk (whether hot-swapped or manually swapped).

With a large number of disks (e.g., 48 or more), using hardware RAID with an optimal number of physical drives per RAID array provides significant performance advantages vs. very large single arrays (and hardware RAID rebuilds will be much faster this way).

After creating the RAID array, follow the usual steps in **VMware vSphere / vCenter** to add the array as a storage device and create a datastore. This datastore will then be used to create one or more VMDKs to be used as **SoftNAS Cloud®** data disks.

Option 2 - Add Disks Individually to VMware and use Software RAID

In this case, add each 15K SAS drive to the **VMware vSphere** host directly. The options in **VMware vSphere** are to either format each disk and create a corresponding datastore per disk device, or use the disks directly as raw disks. Whichever approach is chosen, the goal is to make the disks available to the **SoftNAS Cloud® VM** on a one-to-one basis; i.e., each disk's storage is mapped to the **SoftNAS Cloud® VM** as a separate VMDK.

Disks mapped to datastores:

```
disk 1 --- datastore1
disk 2 --- datastore2
. . .
disk 10 --- datastore10
```

2

Disks mapped as raw devices:

```
disk 1 --- rawdisk1
disk 2 --- rawdisk2
. . .
disk 10 --- rawdisk10
```

The key at this stage is to map the disk drives to VMDKs and attach to **SoftNAS Cloud®**.

SoftNAS Cloud® will map disks into one or more **storage pools**, and software RAID will be applied to each disk group. Software RAID provides may provide increased flexibility of administration, enabling the **SoftNAS Cloud®** administrator to more quickly and easily add, expand and manage RAID groups from the **SoftNAS StorageCenter** interface. Of course, software RAID is handled by the CPU, which adds overhead to the **VMware vSphere** system and **SoftNAS Cloud® VM**. In the event of a drive failure, the rebuild process also must take place in software, which is typically much slower than when handled by a hardware RAID controller.

Add VMDKs to SoftNAS Cloud® VM

Once an option has been chosen, proceed and connect the disk drives to the **SoftNAS Cloud® VM** as **data disk** VMDKs.

Inside of Linux (where **SoftNAS Cloud®** executes), each attached VMDK will appear as a block **disk device**. The devices will be named **/dev/sdb**, **/dev/sdc**, etc. - one Linux block device per data disk VMDK. These block devices appear as unpartitioned, raw disk devices inside of Linux, so the next step will be to partition the block devices with a GPT partition.

After adding the VMDKs to the **SoftNAS Cloud® VM** and partitioning the disks, they become available to assign to storage pools.

Note: Do not remove the virtual disks attached to the VM after they are placed into production. Should this happen, the next time the drives are rebooted they will be renumbered and require an **Import** of storage pools. (To remove VMDKs for any reason, be aware of the implications).

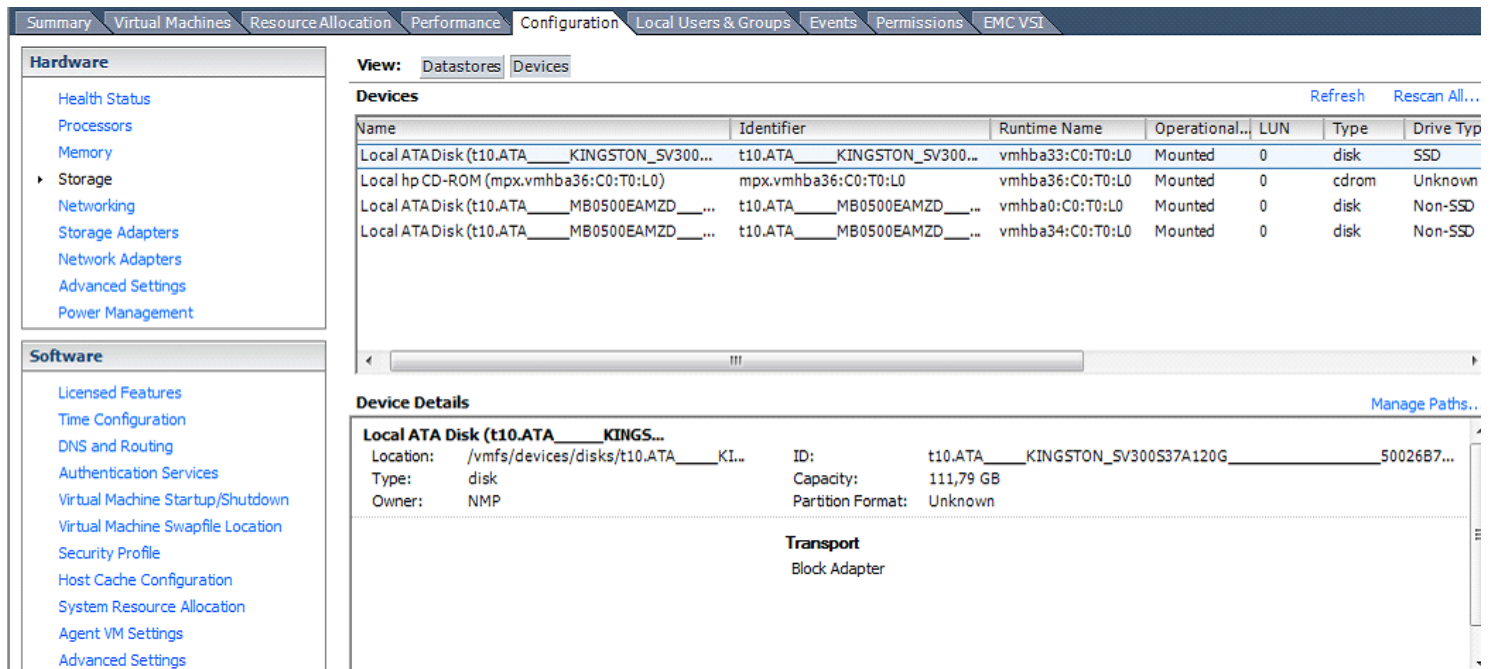
Add RAW Device Mapping in VMware

Raw Device Mapping (RDM) is one way to pass a raw disk device directly through from the disk controller to the **SoftNAS Cloud® VM** in VMware. Older VMware documentation indicates RDM is not supported by locally-attached devices, which is no longer the case; however, like many things in VMware administration, local RDM devices must be configured partially using command line tools.

Use an RDM for direct SSD access, especially for write logs, in order to improve synchronous write speeds (especially for small block synchronous writes like 4K blocks used by VMware and many databases). Normally VMFS works great for creating storage VMDKs for SoftNAS, but for small block sync writes, the VMFS 1 MB block size gets in the way. RDM provides the **SoftNAS Cloud® VM** with direct access to the raw SSD SCSI interface, providing the fastest possible write log.

Configuring Raw Device Mapping (RDM) in VMware

1. Open the vSphere client click on the VMware host on configuration tab under storage in the devices find the identifier of the SSD hard disk, as shown below.



Devices

Name	Identifier	Runtime Name	Operational...	LUN	Type	Drive Typ
Local ATADisk (t10.ATA_____KINGSTON_SV300...	t10.ATA_____KINGSTON_SV300...	vmhba33:C0:T0:L0	Mounted	0	disk	SSD
Local hp CD-ROM (mpx.vmhba36:C0:T0:L0)	mpx.vmhba36:C0:T0:L0	vmhba36:C0:T0:L0	Mounted	0	cdrom	Unknown
Local ATADisk (t10.ATA_____MB0500EAMZD_...	t10.ATA_____MB0500EAMZD_...	vmhba0:C0:T0:L0	Mounted	0	disk	Non-SSD
Local ATADisk (t10.ATA_____MB0500EAMZD_...	t10.ATA_____MB0500EAMZD_...	vmhba34:C0:T0:L0	Mounted	0	disk	Non-SSD

Device Details

Local ATA Disk (t10.ATA_____KINGS...

Location: /vmfs/devices/disks/t10.ATA_____KI... ID: t10.ATA_____KINGSTON_SV300S37A120G_____50026B7...

Type: disk Capacity: 111,79 GB

Owner: NMP Partition Format: Unknown

Transport
Block Adapter

2. Connect to the ESXi host with ssh and `cd /dev/disks`.

```
login as: root
Using keyboard-interactive authentication.
Password:
The time and date of this login have been sent to the system logs.

VMware offers supported, powerful system administration tools. Please
see www.vmware.com/go/sysadmintools for details.

The ESXi Shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.
~ # cd /dev/disks
/dev/disks # ls -l
```

3. Enter `ls -l` command to see all the devices and identify the SSD disk

```

/dev/disks # ls -l
total 2079443913
-rw-rw-rw- 1 root root 7946108928 Mar 4 00:18 mpk.vmhba32:CO:T0:L0
-rw-rw-rw- 1 root root 4161536 Mar 4 00:18 mpk.vmhba32:CO:T0:L0:1
-rw-rw-rw- 1 root root 262127616 Mar 4 00:18 mpk.vmhba32:CO:T0:L0:5
-rw-rw-rw- 1 root root 262127616 Mar 4 00:18 mpk.vmhba32:CO:T0:L0:6
-rw-rw-rw- 1 root root 115326976 Mar 4 00:18 mpk.vmhba32:CO:T0:L0:7
-rw-rw-rw- 1 root root 299876352 Mar 4 00:18 mpk.vmhba32:CO:T0:L0:8
-rw-rw-rw- 1 root root 120034123776 Mar 4 00:18 t10.ATA_KINGSTON_SV300S37A120G_50026B773C029FF0
-rw-rw-rw- 1 root root 500107842016 Mar 4 00:18 t10.ATA_MB0500EAMZD_9WJ145RE
-rw-rw-rw- 1 root root 500098400256 Mar 4 00:18 t10.ATA_MB0500EAMZD_9WJ145RE :1
-rw-rw-rw- 1 root root 8388608 Mar 4 00:18 t10.ATA_MB0500EAMZD_9WJ145RE :9
-rw-rw-rw- 1 root root 500107842016 Mar 4 00:18 t10.ATA_MB0500EAMZD_9WJ1461D
-rw-rw-rw- 1 root root 500104200704 Mar 4 00:18 t10.ATA_MB0500EAMZD_9WJ1461D :11
lrwxrwxrwx 1 root root 20 Mar 4 00:18 vml.000000000766d68626133323a30a30 -> mpk.vmhba32:CO:T0:L0
lrwxrwxrwx 1 root root 22 Mar 4 00:18 vml.000000000766d68626133323a30a30:1 -> mpk.vmhba32:CO:T0:L0:1
lrwxrwxrwx 1 root root 22 Mar 4 00:18 vml.000000000766d68626133323a30a30:5 -> mpk.vmhba32:CO:T0:L0:5
lrwxrwxrwx 1 root root 22 Mar 4 00:18 vml.000000000766d68626133323a30a30:6 -> mpk.vmhba32:CO:T0:L0:6
lrwxrwxrwx 1 root root 22 Mar 4 00:18 vml.000000000766d68626133323a30a30:7 -> mpk.vmhba32:CO:T0:L0:7
lrwxrwxrwx 1 root root 22 Mar 4 00:18 vml.000000000766d68626133323a30a30:8 -> mpk.vmhba32:CO:T0:L0:8
lrwxrwxrwx 1 root root 72 Mar 4 00:18 vml.01000000003530303236423737334330323946463020202046494e475354 -> t10.ATA_KINGSTON_SV300S37A120G_50026B773C029FF0
lrwxrwxrwx 1 root root 72 Mar 4 00:18 vml.010000000039574a313435524520202020202020202020202020204d4230353030 -> t10.ATA_MB0500EAMZD_9WJ145RE
lrwxrwxrwx 1 root root 74 Mar 4 00:18 vml.010000000039574a313435524520202020202020202020202020204d4230353030:1 -> t10.ATA_MB0500EAMZD_9WJ145RE :11
lrwxrwxrwx 1 root root 74 Mar 4 00:18 vml.010000000039574a313435524520202020202020202020202020204d4230353030:9 -> t10.ATA_MB0500EAMZD_9WJ145RE :9
lrwxrwxrwx 1 root root 72 Mar 4 00:18 vml.010000000039574a313436314620202020202020202020202020204d4230353030 -> t10.ATA_MB0500EAMZD_9WJ1461D
lrwxrwxrwx 1 root root 74 Mar 4 00:18 vml.010000000039574a313436314620202020202020202020202020204d4230353030:11 -> t10.ATA_MB0500EAMZD_9WJ1461D :11
/dev/disks #

```

4. To configure the device as an RDM and output the RDM pointer file to a chosen destination, run the command:

```
# vmkfstools -z /vmfs/devices/disks/<diskname> /vmfs/volumes/<datastorename>/<vmfolder>/<vmname>.vmdk
```

In this case, we have the following:

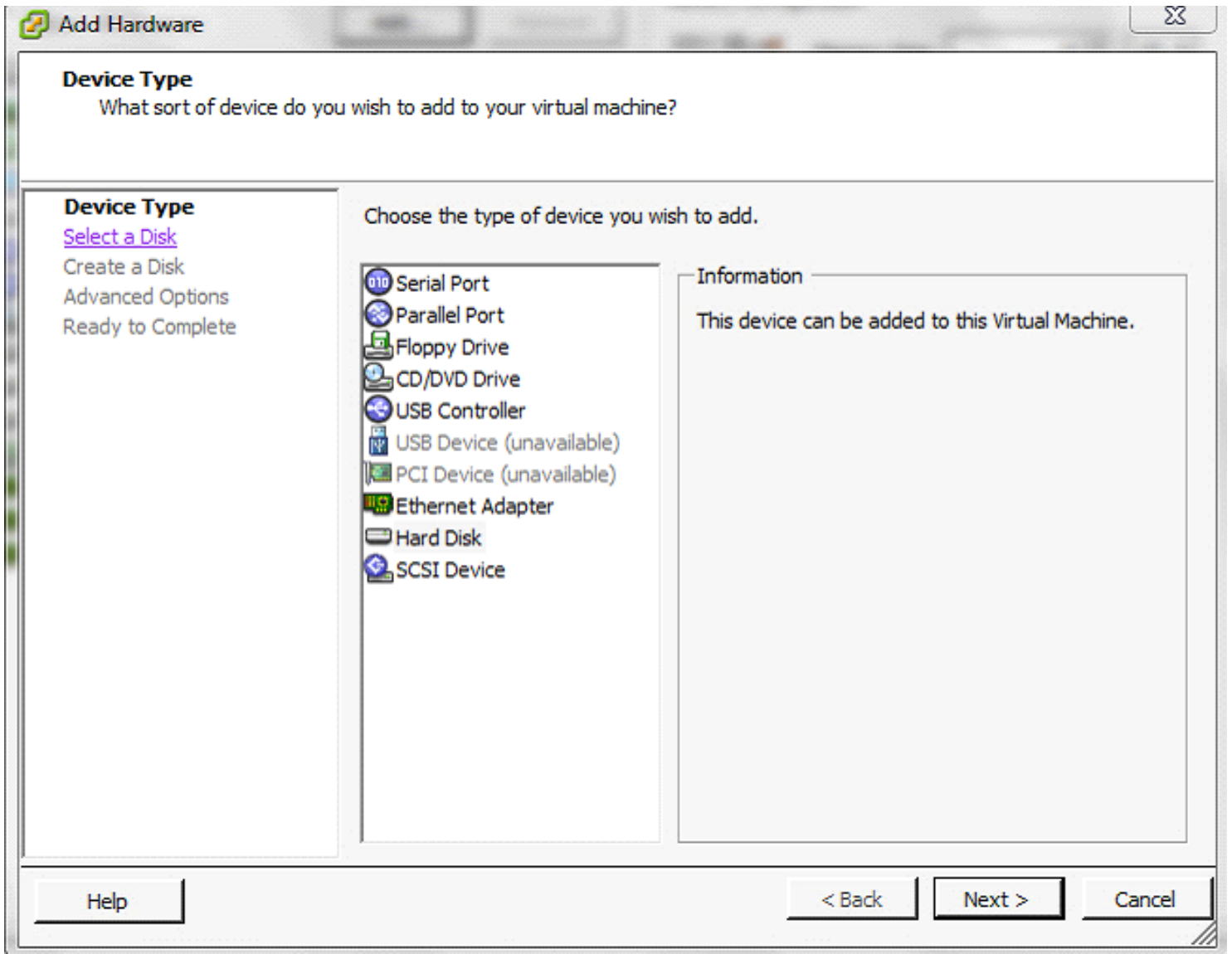
```

/dev/disks # vmkfstools -z /vmfs/devices/disks/t10.ATA_KINGSTON_SV300S37A120G_50026B773C029FF0 /vmfs/volumes/datastore01/RDM/ssdrdm.vmdk
/dev/disks #

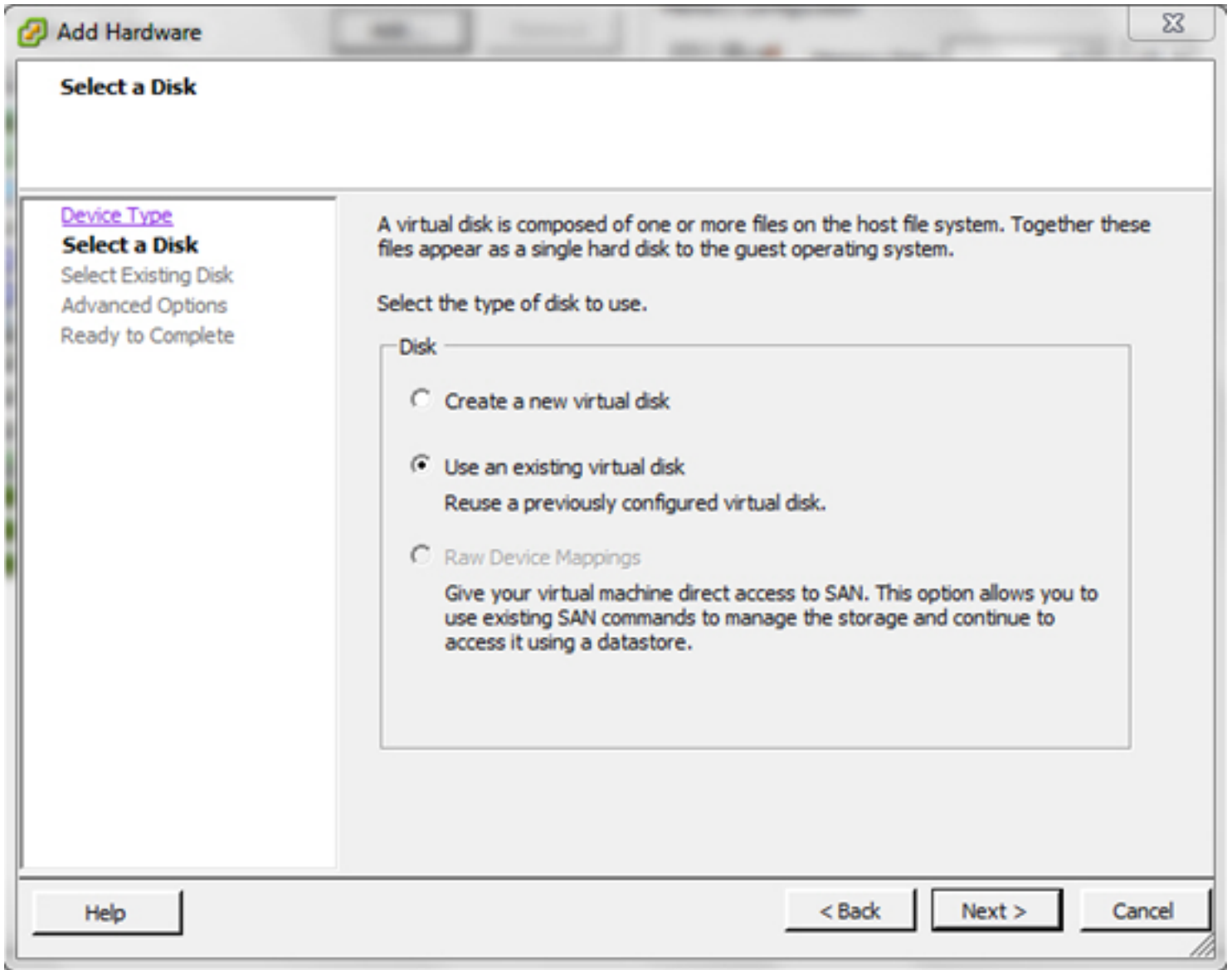
```

5. Now that we have created an RDM, we must assign it to our VM.

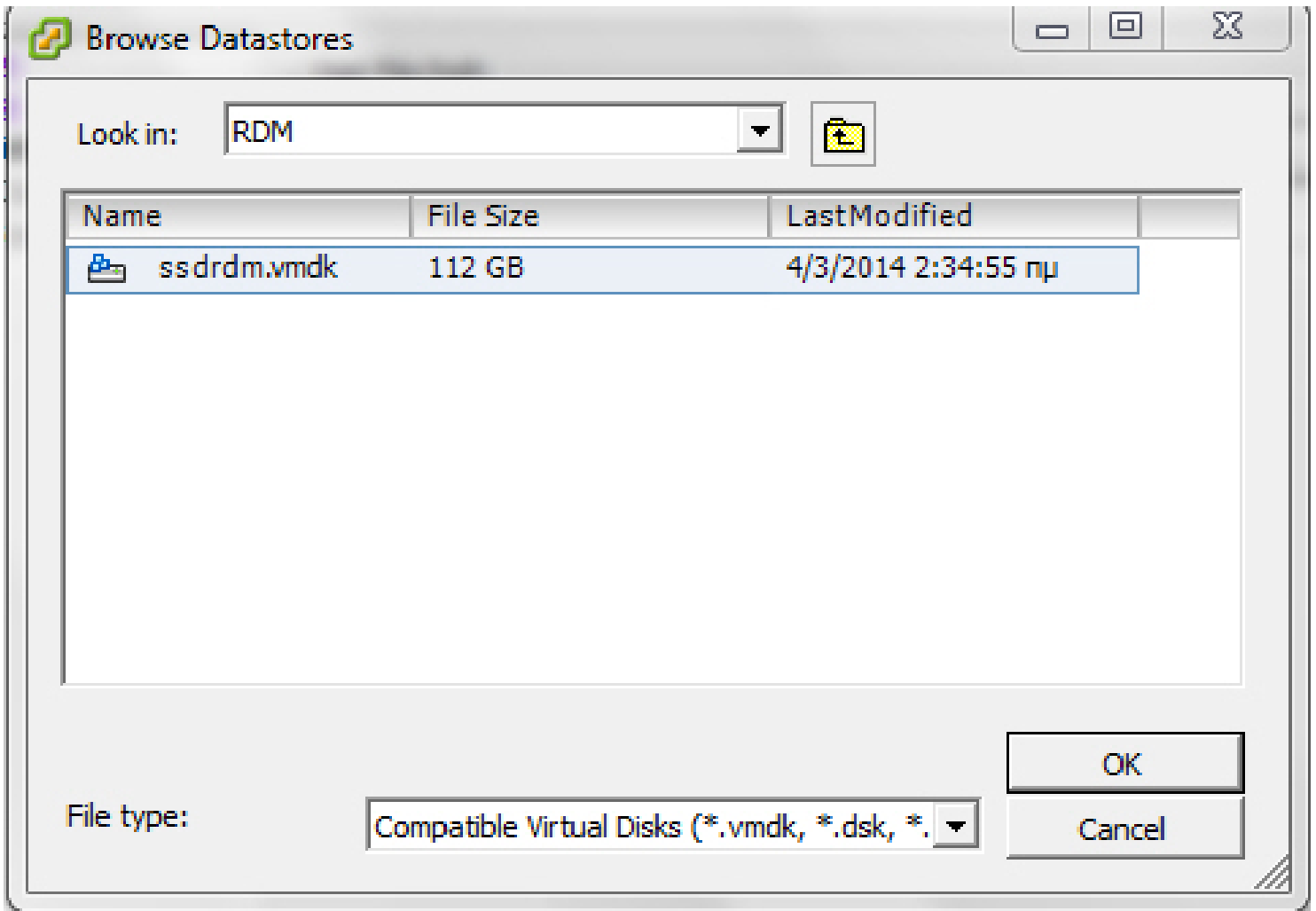
Right click on the **SoftNAS Cloud® VM** edit settings ADD tab, Select Hard disk and press Next.



6. Next, choose the existing virtual disk option and press Next.



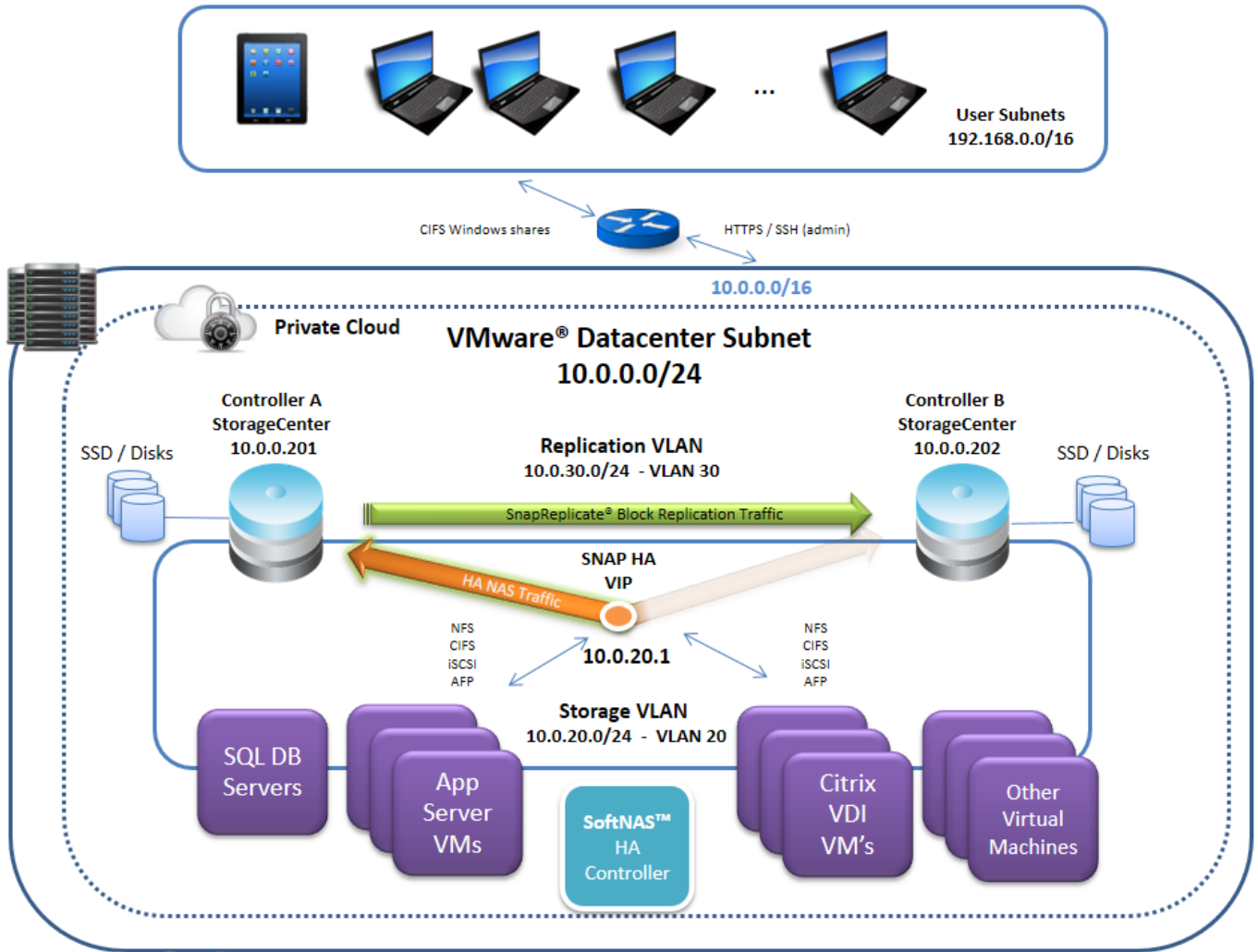
7. Browse to the location where the RDM pointer is stored. Choose the pointer, then press **OK**.



Confirm the settings for new hard disk in the virtual machine inventory as **Mapped Raw LUN**

At this point, the **SoftNAS Cloud® VM** has been mapped to the raw SSD device.

VMWare HA Considerations



VMware has a few requirements specific to setting up high availability through SoftNAS. SnapReplicate can be performed as described in [SnapReplicate](#), and requires only two nodes. Setting up **SNAP HA™** in any VMWare virtualized environment requires the following:

- Two **SoftNAS Cloud®** controller nodes for replication and their corresponding IP addresses (DNS names) and networking credentials.
- A virtual IP within the storage VLAN subnet (see [HA Design Principles](#) for more information).
- An additional **SoftNAS** controller node is **required**, to act as an HA Controller. This **SoftNAS SNAP HA™ Controller** node is necessary, as it acts as a 3rd party witness and controller to all **SNAP HA™** failover and takeover operations.
- Replication must be set up between the two **SoftNAS Cloud®** controller nodes.

For more information see our [SoftNAS High Availability Guide](#).

Advanced Configuration Notes for SoftNAS Cloud®

Occasionally, administrators will need to configure at a deeper level of the storage network. Here are some common notes. If the information here is not sufficient, we encourage contacting our [Support Team](#).

[SnapReplicate iSCSI Volume Sync](#)

[Changing Email Report Frequency](#)

[Networking Tips](#)

[Applying CHAP Authentication to iSCSI ACLs](#)

SnapReplicate iSCSI Volume Sync

Topic:

When using an HA cluster with iSCSI Targets, **SnapReplicate** can fail due to an issue with file locking on the iSCSI Volumes. This issue only occurs when re-adding replication to an existing target node.

Procedure:

Delete the target node's iSCSI LUN, then re-add replication.

Changing Monitoring Notification Frequency

Topic:

Increase, decrease, or completely cease email reports sent by established VMs and monitored network relationships.

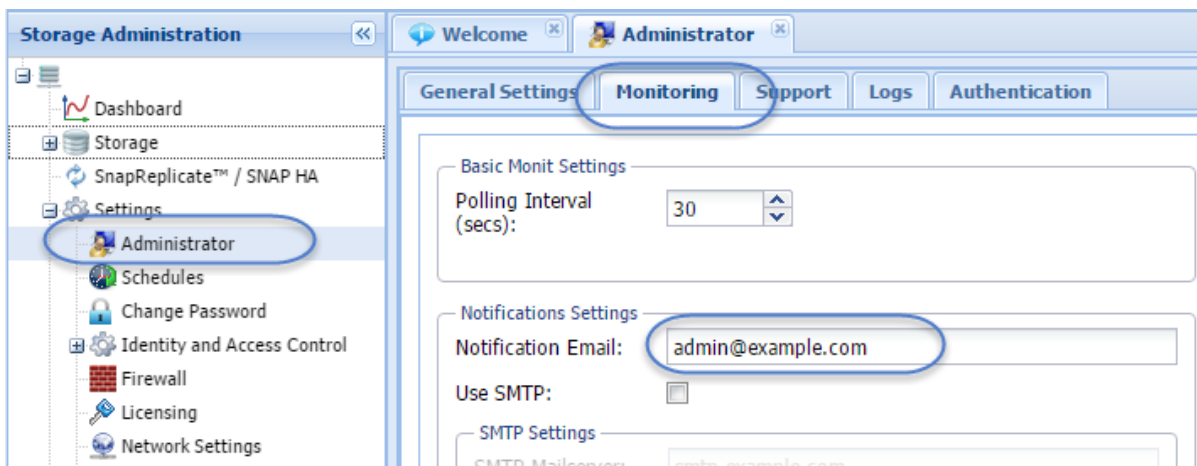
Procedure:

SoftNAS Cloud® is installed with a Monitoring Notification setting turned on. This setting sends notifications to whatever email address is initially registered with the account. To change the frequency or completely discontinue these notifications, sign in to **SoftNAS StorageCenter**.

If this issue persists, first try updating the **SoftNAS StorageCenter** from the **Getting Started** tab.

On the left menu pane, expand **Settings** and click **Administrator**. On the **Monitoring tab**, there are options available to either increase the Polling Interval or completely remove the contact email address altogether.

Note: Complete removal of the email address will immediately cease any monitoring emails from this setup. This is NOT recommended as it may result in the client being unaware of important alerts and potentially avoidable failures.



Note: If the SoftNAS instance is running in a proxy environment, it may have difficulty sending the desired email reports to its intended target. In order to ensure delivery of monitoring emails, a local SMTP server must be added in the Monitoring tab.

The screenshot shows the 'Administrator' interface with tabs for 'General Settings', 'Monitoring', 'Support', 'Logs', and 'Authentication'. The 'Monitoring' tab is active, displaying 'Basic Monit Settings' and 'Notifications Settings'. Under 'Basic Monit Settings', the 'Polling Interval (secs)' is set to 30. Under 'Notifications Settings', the 'Notification Email' is 'admin@example.com' and the 'Use SMTP' checkbox is checked. A blue circle highlights the 'Use SMTP' checkbox, and a blue rounded rectangle highlights the 'SMTP Settings' section, which includes fields for 'SMTP Mailserver' (smtp.example.com), 'SMTP Port' (25 (SMTP), 587 (Submission), 465 (SMTPS)), 'SMTP Username' (username), 'SMTP Password' (password), and 'SMTP Encryption' (dropdown menu).

These settings must be saved from this point.

Networking Tips

10 Gigabit Network Configurations on VMware vSphere

By default, the **SoftNAS Cloud® VM** (on **VMware vSphere**) ships with the default E1000 virtual NIC adapter and VMware defaults to MTU 1500.

For best performance results above 1 gigabit, follow the steps outlined below.

1. Replace the **E1000** virtual NIC adapter with a **vmxnet3** on the **SoftNAS Cloud® VM**.
2. Use **MTU 9000** instead of **MTU 1500** for **vSwitch**, **vmKernel** and physical switch configurations. Be sure to configure the **network interface** in **SoftNAS for MTU 9000** also.

Refer to the [MTU 9000](#) section for more information.

A dedicated VLAN for storage traffic is recommended. For VMware, refer to the [Performance Tuning for VMware vSphere](#) section for details.

iSCSI Multi-pathing

To increase performance throughput and resiliency, use of **iSCSI** multipathing is recommended by VMware and other vendors.

Since **SoftNAS** operates in a hypervisor environment, it is possible to configure multi-path operation as follows:

1. On the **VMware** host where the **SoftNAS Cloud® VM** runs, install and use multiple physical NIC adapters
2. Assign a dedicated **vSwitch** for each incoming **iSCSI** target path (one per physical NIC)
3. Assign the **SoftNAS Cloud® VM** a dedicated virtual NIC adapter for each incoming iSCSI target path (per **vSwitch**/ physical NIC)
4. Assign a unique IP address to each corresponding Linux network interface (for each virtual NIC attached to the **SoftNAS Cloud® VM**)
5. Restart the **SoftNAS iSCSI** service and verify connectivity from the iSCSI initiator client(s) to each iSCSI target path.

A dedicated VLAN for storage traffic is recommended.

Applying CHAP Authentication to iSCSI ACLs

About CHAP Authentication

In computing, the Challenge-Handshake Authentication Protocol (CHAP) authenticates a user or network host to an authenticating entity.

CHAP provides protection against replay attacks by the peer through the use of an incrementally changing identifier and of a variable challenge-value. CHAP requires that both the client and server know the plaintext of the secret, although it is never sent over the network. Thus, CHAP provides better security as compared to Password Authentication Protocol (PAP) which is vulnerable for both these reasons.

The below steps allow you to apply CHAP Authentication to iSCSI ACLs, improving the security of your SoftNAS volumes.

Setting up ACLs

1. Set up iSCSI as per the documentation for SoftNAS v3.2.3 and higher.
2. Use SSH to access the system, login as root. Perform the following commands:

- a. targetcli
- b. cd /
- c. cd iscsi
- d. cd <iQN for iSCSI needing ACL's>
- e. ls
- f. cd tpg1/acls
- g. create <iQN for iSCSI Initiator, windows iSCSI Initiator Configure Tab>
- h. cd ../../
- i. ls
- j. cd /
- k. saveconfig
- l. exit

3. You should now be able to see the ACL listed for iQN.
4. Repeat the process as required for any other iQN's.

Note: Determine whether the portal needs to be reconfigured prior to moving beyond the above steps.

CHAP Authentication Setup

1. Set up iSCSI as described in the documentation for SoftNAS v3.2.3 and higher.
2. Use SSH to access the system, logging in as root. Perform the following commands:

- a. targetcli
- b. cd /
- c. cd iscsi
- d. cd <iQN for iSCSI Target>
- e. ls
- f. cd tpg1
- g. get attribute authentication

3. At this point, authentication should be 0(zero) by default.

- a. set attribute authentication=1
- b. get attribute authentication

4. Confirm CHAP Authentication via the following commands.

- a. cd acls
- b. ls
- c. cd <ACL created earlier(iQN)>
- d. set userid=<for windows use iQN of initiator>
- e. set password=<Secret Target Password>
- f. set mutual_userid=<for Mutual CHAP, trget iQN>
- g. set mutual_password=<Secret CHAP Password>
- h. cd /
- i. saveconfig
- j. exit
- k. service fcoe-target restart