Dell EMC Data Domain®

Version 6.2

Security Configuration Guide

302-005-263

REV 03

Published February 2019

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS-IS.“ DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Dell EMC
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.DellEMC.com

CONTENTS

Preface

As part of an effort to improve its products, Data Domain periodically releases software and hardware revisions. Therefore, some functions that are described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features, software updates, software compatibility guides, and information about Data Domain products, licensing, and service.

Contact a technical support professional if a product does not function correctly or does not function as described in this document.

Purpose

This document describes the key security features of Data Domain systems and provides the procedures that are required to ensure data protection and appropriate access control.

Audience

This document is primarily intended for Data Domain Field Engineers, contracted representatives, and business partners who are responsible for configuring, troubleshooting, and upgrading Data Domain systems at customer sites. System administrators or application integrators who are responsible for installing software, maintaining servers and clients on a network, and ensuring network security should also be aware of the contents of this document.

Related documentation

The following publications provide additional information:

- *Data Domain Operating System Release Notes*
- *Data Domain Operating System Administration Guide*
- *Data Domain Operating System Initial Configuration Guide*
- *Data Domain Operating System Command Reference Guide*
- *Data Domain Operating System MIB Quick Reference*
- *Data Domain Hardware Features and Specifications*
- Installation guide for the system, for example, *Data Domain DD6300 System Installation Guide*
- *Data Domain, System Controller Upgrade Guide*
- *Data Domain Expansion Shelf, Hardware Guide* (for shelf model ES30/FS15 or DS60)

If you have the optional RSA Data Protection (DPM) Key Manager, see the latest version of the *RSA Data Protection Manager Server Administrator's Guide*, available with the RSA Data Protection Manager product.

Special notice conventions used in this document

The following conventions are used for special notices:

⚠ DANGER

If not avoided, indicates a hazardous situation which results in death or serious injury.

⚠ WARNING

If not avoided, indicates a hazardous situation which could result in death or serious injury.

⚠ CAUTION

If not avoided, indicates a hazardous situation which could result in minor or moderate injury.

NOTICE

Addresses practices that are not related to personal injury.

Note

Presents information that is important, but not hazard-related.

Typographical conventions

Table 1 Style conventions

Bold	Used for names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what the user specifically selects or clicks)
Italic	Used for full titles of publications that are referenced in text
`Monospace`	Used for: - System code - System output, such as an error message or script - Pathnames, filenames, prompts, and syntax - Commands and options
`Monospace italic`	Used for variables
`Monospace bold`	Used for user input
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections - the bar means “or”
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate nonessential information that is omitted from the example

Where to get help

Support, product, and licensing information can be obtained as follows:

Product information

For documentation, release notes, software updates, or additional product information, go to the support site at https://support.emc.com.

Technical support

Go to the online support site and click Service Center. Several options are available for contacting Technical Support. Note that to open a service request, you must have a valid support agreement. Contact a sales representative for details about obtaining a valid support agreement or with account questions.

Comments

Suggestions help continue to improve the accuracy, organization, and overall quality of the user publications. Send opinions of this document to mailto:DPAD.Doc.feedback@emc.com.

Note

This document was accurate at publication time. Go to the online support site to ensure that you are using the latest version of this document.

Revision history

The following table presents the revision history of this document.

Table 2 Revisions

Revision	Date	Description
03	February 2019	Updated with the no spaces requirement for the system passphrase
02	February 2019	Updated information for "DD VE in Cloud"
01 (6.2)	December 2018	Updated for 6.2 to include information for DD3300 serial over LAN support, Alibaba Cloud, and Google Cloud recommendations.

CHAPTER 1

Overview

This chapter includes:

The Data Domain Operating System

A Data Domain system is an appliance that runs the Data Domain Operating System (DD OS). A web-based graphical user interface (GUI), Data Domain System Manager, is provided for configuration operations, management, and monitoring. In addition, a controlled command-line interface (CLI) environment is available, which provides a complete set of Data Domain administrative operations.

Because DD OS is an embedded operating system, additional software or agents cannot be installed or executed within a Data Domain system. This restriction ensures control and consistency of DD OS releases and provides additional security over the system.

Data Domain systems are purpose-built physical and virtual appliances with restricted access to their internal operation. Any tampering voids the warranty. Updated versions of embedded open source modules are included in DD OS updates as appropriate.

Data Domain system security

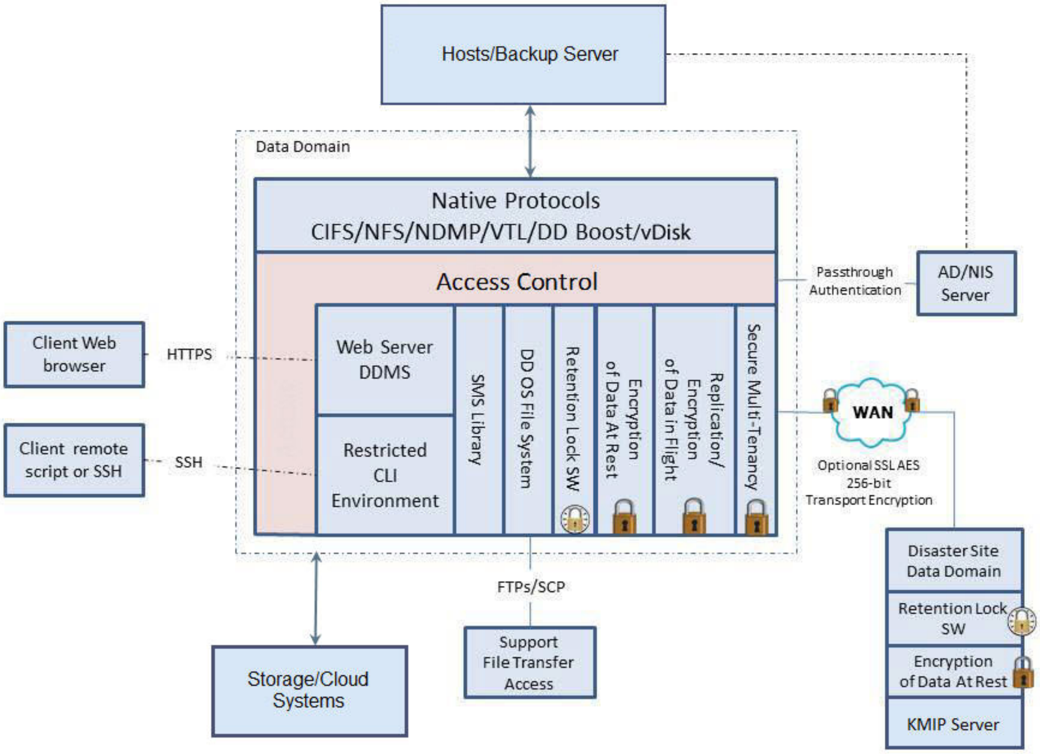
Data Domain systems, as central repositories for both structured and unstructured backup data, have many security capabilities and attributes to protect the data on the Data Domain systems. This document is a supplement to the *Data Domain Operating System Administration Guide* and provides an overview of key security features and procedures that are required to ensure data protection and appropriate access control.

System interfaces and access control

Hosts and backup applications interface with the Data Domain systems through one or more of the standard native server interface protocols: CIFS, NFS, NDMP, VTL, or Data Domain Boost.

Access control and user authentication to the Data Domain system is controlled by either local users, NIS environments, LDAP, or within a Microsoft Active Directory Domain environment. Other points that run the security attributes of the Data Domain system are listed in the simplified diagram.

Figure 1 System interfaces and access control


Hosts/Backup Server
Data Domain
Native Protocols
CIFS/NFS/NDMP/VTL/DD Boost/vDisk
Access Control
Passthrough Authentication
AD/NIS Server
Client Web browser
HTTPS
Client remote script or SSH
SSH
Web Server DDMS
Restricted CLI Environment
SMS Library
DD OS File System
Retention Lock SW
Encryption of Data At Rest
Replication/ Encryption of Data in Flight
Secure Multi-Tenancy
WAN
Optional SSL AES 256-bit Transport Encryption
Disaster Site Data Domain
Retention Lock SW
Encryption of Data At Rest
KMIP Server
FTPs/SCP
Storage/Cloud Systems
Support File Transfer Access

The following Data Domain native protocols and software options depend on or enable security attributes of the Data Domain system. See the current DD OS administration guide for more information.

Supported Native Ingest Protocols

Data Domain systems support simultaneous access through common network access protocols, enabling both backup servers and application servers to send data to the Data Domain system. Servers can attach and transfer files and backup images over one or more of these protocols:

- CIFS
- NFS
- Data Domain Boost over IP (encryption supported)
- Data Domain Boost over Fibre Channel (encryption not supported)
- NDMP
- VTL over Fibre Channel
- vDisk over Fibre Channel

Data that is transmitted over CIFS, NDMP, Data Domain Boost over Fibre Channel, VTL over Fibre Channel, and vDisk over Fibre Channel is transported unencrypted.

The following software options are related to security and require separate licenses:

Data Domain Replicator Software

Automated, policy-based, network-efficient replication for disaster recovery, remote office data protection, and multi-site tape consolidation. Data Domain Replicator software asynchronously replicates only the compressed, deduplicated data over the

WAN or LAN during the backup process, making network-based replication fast, reliable, and cost-effective.

For environments that do not leverage a VPN for secure connections between sites, DD Replicator software can securely encapsulate its replication payload over SSL with AES 256-bit encryption for secure transmission over the wire. This process is also known as encrypting data in flight.

Data Domain Encryption Software
Protects backup and archive data that is stored on Data Domain systems with data encryption that is performed inline before the data is written to disk. The Encryption at Rest feature satisfies internal governance rules, compliance regulations, and protects against the reading of customer data on individual disks or disk shelves that are removed from the system due to theft.

Data Domain Retention Lock Software
Prevents specified files from being overwritten, modified, or deleted for a user-defined retention period of up to 70 years.

Data Domain Secure Multi-Tenancy Software
Provides secure storage consolidation in multi-tenant backup environments. With SMT, multiple tenants can reside on a single Data Domain system simultaneously and the data of one tenant cannot be detected or accessed by another.

CHAPTER 2

Security Configuration Settings

This chapter includes:

Introduction

This chapter provides an overview of the settings available to ensure the secure operation of the product.

System passphrase

The passphrase is used to encrypt the encryption keys, cloud access, secure keys, imported host certificate private keys, and DD Boost token keys. It enables a Data Domain system to be transported with encryption keys on the system but without the passphrase being stored on it. The system uses the passphrase to encrypt imported host private keys and DD Boost token keys. If the system is stolen in transit, an attacker cannot easily recover the data, and at most, they can recover the encrypted user data and the encrypted keys.

Data at rest encryption keys are dependent on this passphrase, and therefore, the use of a stronger passphrase is mandatory. A valid passphrase must contain:

- A minimum of nine characters
- A minimum of one lowercase character
- A minimum of one uppercase character
- A minimum of one numeral
- A minimum of one special character
- No spaces

Data Domain supports passphrase up to 1024 characters.

For more information, see the *Data Domain Operating System Administration Guide*.

Passphrase security

The passphrase is encrypted and stored in a file on the head unit of the Data Domain system. The encryption key that is used to encrypt the passphrase is hardcoded.

Users can choose to not store the passphrase on disk. There is a hidden sysadmin command to accomplish this task: `system passphrase option set store-on-disk no`. With DD OS 6.1, there is no need to restart the system after running this command.

NOTICE

Customers must have a good process to keep the passphrase. If the Data Domain system is configured to not store the passphrase, there is no way to recover it if it is lost.

Change the passphrase after running the command to not store the passphrase on disk. A side-effect of not storing the passphrase is that the file system has to be unlocked every time the Data Domain system is rebooted. Until the file system is unlocked, all backup jobs/replication are impacted.

Note

If there is no concern that an attacker can gain physical access to the appliance in the environment, then choose to store the passphrase on disk.

For more information, see the *Data Domain Operating System Administration Guide* and *Data Domain Command Reference Guide*.

Access control settings

Access control settings enable the protection of resources against unauthorized access.

System access

The Data Domain operating environment provides secure administration through either the Data Domain System Manager via HTTPS or Secure Shell (SSH) for CLI. Either method allows locally defined users, Network Information Service (NIS) users, and Microsoft Active Directory (AD) domain users.

DD System Manager via HTTPS

The Data Domain system can use an imported certificate to establish a trusted connection to manage the Data Domain system over SSL. If a certificate is not provided, the Data Domain system can use its self-signed identity certificate. Data Domain enables both HTTP and HTTPS by default. The recommendation is to disable HTTP by running CLI command `adminaccess disable http`.

When connecting to DD System Manager from a web browser, all HTTP connections will automatically redirect to HTTPS.

Secure Shell for CLI

The administrator enters a controlled shell environment, where individual CLI commands are executed to manage the Data Domain system.

Note

When connecting to the HA system via the floating hostname/IP using an SSH client, the public key that is stored in the known-hosts list of the local shell may fail verification. Each node in the HA pair generates a unique SSH key pair, and the active node presents the key that it owns. Resolution for this issue is to physically verify that the correct system is connecting, and remove the offending key in the known-host list and revalidate the key on the next connection try. Knowledge Base article #212538 explains this issue in more detail.

Administrative system access can be either *local* or *remote*.

Local access

Authorized administrators with valid login credentials have access to CLI via serial console or IP in same subnet. User is prompted for username and password, and after authentication and authorization, they are granted login access.

Remote access

CLI and Web-based System Manager remote access are available for authorized administrators with proper login credentials (username and password). Remote users with network access and authorization can remotely administer the Data Domain systems over the network. Policies outside the Data Domain system should be put in place for users to log out after the session is over for both local and remote access.

Password-less login is supported for SSH using SSH keys and for Data Domain System Manager and REST API connections through the use of client certificates.

Note

SSH and secure browsing (HTTPS) are enabled on the Data Domain system by default. The recommendation is to use an imported certificate and to configure session timeout values to ensure that users are automatically logged out of the system after the session is over. A session timeout of 5 minutes maximum is recommended.

Host-based access lists

Data is not readily viewable from anywhere except a host that has been granted access. Administrator access is required to configure the Data Domain system and adjust which physical hosts can view an exported mount point. Users with administrative access can update the access list with a server's hostname or IP address. A Data Domain system can use DNS for name resolution.

For greater protection, administrators can use the Data Domain CLI `net hosts add <ipaddr> <host-list>` to add entries in the hosts file to control host resolution. Refer to the *Data Domain Command Reference Guide* for more information.

File permissions

Files that are created on the Data Domain system are "owned" by the creator. For example, backup software typically writes files as a particular user, so that user would own all files that the backup software that is created on the system. Explicit permissions (ACLs) must be set, however, to prevent users from viewing files that are created by others.

Microsoft CIFS

For every file or folder that is created through CIFS, the following attributes are created:

- Owner SID
- Group SID
- DACL (Discretionary ACL – Permissions)
- SACL (System ACL – Auditing Information)
- DOS Attributes such as READONLY, HIDDEN, SYSTEM & ARCHIVE

In addition, folders and files map UNIX UID/GID/MODE from Windows Owner-SID/Group-SID/DACL. The DACL is inherited from its parent. If the parent directory does not have DACL (created though NFS/non-CIFS), then a default ACL is assigned. The default gives the owner full control and gives others read permission. Access control is managed through the standard Microsoft Management Control (MMC) on any client with permissions to do so.

Linux NFS

Files and folders that are created through the remaining ingest protocols use the POSIX.1e ACL standard or NFSv4 native ACLs through the `nfs4_setacl` command. Every object is associated with three sets of permissions that define access for the owner, the owning group, and for others. Each set may contain Read [r], Write [w], and Execute [x] permissions. This scheme is implemented using only 9 bits for each object. In addition to these 9 bits, the Set User Id, Set

Group Id, and Sticky bits are used for a number of special cases. Access control is managed through a standard Linux client or Data Domain system CLI administration environment with permissions to do so.

DD Boost™

Files and directories that are created using DD Boost APIs are created with the mode (or permission) bits specified by the creator. Thus each object is associated with three sets of permissions that define access for the owner, the owning group, and for others. Each set may contain Read [r], Write [w], and Execute [x] permissions. The mode bits can be changed appropriately via a DD Boost change mode API.

Microsoft Active Directory (AD) Services

Data Domain systems can use Microsoft Active Directory pass-through authentication for the users/servers. Administrators can enable certain domains and groups of users to access files that are stored on the Data Domain system. It is recommended to have Kerberos configured. In addition, Data Domain systems support Microsoft Windows NT LAN Managers NTLMv1 and NTLMv2. However, NTLMv2 is more secure and is intended to replace NTLMv1.

NIS Directory Services

Data Domain systems can use NIS Directory Authentication for the users in UNIX/LINUX environments. Administrators can enable specific hosts and users to access files that are stored on the Data Domain system.

Kerberos Authentication

Data Domain systems can use Kerberos authentication for NFSv3 and NFSv4 clients. Kerberos performs in combination with NIS Directory or LDAP services to identify connecting clients. This authentication method allows the administrator to control which users and hosts have permissions to view data on a Data Domain system.

LDAP for NFS ID mapping

Data Domain systems can use LDAP for NFSv4 ID mapping, and NFSv3/NFSv4 Kerberos with LDAP. User can also configure Secure LDAP with either LDAPS or Start_TLS method. The LDAP client authentication can use Bind DN or Bind PW, but Data Domain systems do not support certificate based LDAP client authentication.

Note

Data Domain local user IDs start with the number 500. When setting up LDAP, a similar user ID range (500 through 1000) cannot be used or a user ID collision occurs. If there is user ID collision, files that are owned by a name LDAP service user become accessible by the other users due to configuration errors.

Separate NFS and CIFS shares

Administrators can easily create shares on the Data Domain file system. Using the native access control methods helps to define more granular share/directory/file-level access control over certain data on the Data Domain system. For example, when setting up a shared system for multiple customers, administrators can have an NFS or CIFS share that is created for each specific customer on the same Data Domain system and specify access controls for each customer/share.

User authentication

User authentication settings control the process of verifying an identity claimed by the user for accessing the product.

Default account

The default user account on the Data Domain system is *sysadmin*. The account cannot be deleted or modified.

For Data Domain systems, the factory default password is the Data Domain system's serial number. For its location, see the system's hardware overview manual.

For DD VE residing on ESXi, Hyper-V, and KVM, the default password is **`changeme`**. During the initial configuration, the administrator who logs in as sysadmin is prompted to change the password.

For AWS, the default password is the instance id, during the initial configuration, the administrator has to change the password during first login.

For Azure, if the user specified the password during deployment, the user is not forced to change the password.

For GCP, the default password is `changeme`. The administrator is required to change the password during the first login.

Local users

After logging in as sysadmin, you can create additional accounts for the roles that are described in Table 3 on page 22. As an admin-role or limited-admin user, you can change a user's role for an account, password, and account expiration parameters. For more information and instructions, or to change just the password for individual users, see the *Data Domain Operating System Administration Guide*.

For uniform password management across the enterprise, the default password policy can be changed and applied to all newly created passwords with the default policy set. Parameters include the following:

- Minimum Days Between Change
- Maximum Days Between Change
- Warn Days Before Expire
- Disable Days After Expire
- Minimum Length of Password
- Minimum number of Character Classes
- Lowercase Character Requirement
- Uppercase Character Requirement
- One Digit Requirement
- Special Character Requirement
- Max Consecutive Character Requirement
- Number of Previous Passwords to Block
- Maximum login attempts
- Unlock timeout (seconds)

For more information and instructions, see the *Data Domain Operating System Administration Guide*.

Note

DD Boost users and passwords are created using the procedure that is described in the DD Boost chapter in the *Data Domain Operating System Administration Guide*.

Enabling, disabling, or deleting user accounts

Local user accounts are enabled, disabled, or deleted by the system administrator. For more information and instructions, see the *Data Domain Operating System Administration Guide*.

Active Directory
Data Domain systems can use Microsoft Active Directory pass-through authentication for the users. Refer to *Data Domain Operating System Administration Guide* for active directory configuration.

NIS
Data Domain systems can use NIS Directory Authentication for the users in UNIX/ LINUX environments for configuration management. Refer to *Data Domain Operating System Administration Guide* for NIS configuration.

LDAP
Data Domain systems can use LDAP for user authentication. Users can also configure Secure LDAP with either LDAPS or Start_TLS method.

Note

Data Domain local user IDs start with the number 500. When setting up LDAP, a similar user ID range (500 through 1000) cannot be used or a user ID collision occurs. If there is user ID collision, files that owned by a name LDAP service user become accessible by the other users due to configuration errors.

Refer to *Data Domain Operating System Administration Guide* for LDAP and Secure LDAP configuration.

Login using certificates

User certificate consisting of username is authenticated and authorized based on pre-existing role mapping to login to Data Domain System Manager from GUI and REST, see *Data Domain Operating System Administration Guide* for more information.

Two factor authentication (CAC/PIV card)

CAC/PIV cards offer two factor authentication, where a browser plugin interacts with the CAC card to extract the user certificate into the browser by providing the password to access the CAC card. Once the user certificate is loaded into the browser, a customer can login to Data Domain System Manager using the certificates.

User authorization

User authorization settings control rights or permissions that are granted to a user for accessing a resource that is managed by the product.

Specific authorization levels are defined for each user account created using the Role-Base Access Control scheme that is listed below. To change the authorization for an account, you must change the role that is specified for the account. For instructions, see the *Data Domain Operating System Administration Guide*.

Table 3 Role-based accounts

Role/Account Type	Description
admin	An *admin* role user can configure and monitor the entire Data Domain system. Most configuration features and commands are available only to admin role users. However, some features and commands require the approval of a security role user before a task is completed.
limited-admin	The *limited-admin* role can configure and monitor the Data Domain system with some limitations. Users who are assigned this role cannot perform data deletion operations, edit the registry, or enter bash or SE mode.
user	The *user* role enables users to monitor systems and change their own password. Users who are assigned the user management role can view system status, but they cannot change the system configuration.
security (security officer)	• A *security* role user, who may be referred to as a security officer, can manage other security officers, authorize procedures that require security officer approval, provide data destruction oversight, and perform all tasks that are supported for security role users. • The security role is provided to comply with the Write-Once-Read-Many (WORM) regulation. Most command options for administering sensitive operations, such as Encryption, Retention Lock Compliance, and Retention Lock Archiving now require security officer approval.
backup-operator	• A *backup-operator* role user has all user role permissions, can create snapshots for MTrees, and can import, export, and move tapes between elements in a virtual tape library. • A backup-operator role user can also add and delete SSH public keys for password-less logins. This function is used mostly for automated scripting. The backup-operator can add, delete, reset and view CLI command aliases, synchronize modified files, and wait for replication to complete on the destination system.
none	The *none* role is for DD Boost authentication and tenant-unit users only. A none role user can log in to a Data Domain system and can change their password, but cannot monitor, manage, or configure the primary system. When the primary system is partitioned into tenant units, either the tenant-admin or the tenant-user role is used to define a user's role with respect to a specific tenant unit. The tenant user is first assigned the none role to minimize access to the primary system, and then either the tenant-admin or the tenant-user role is appended to that user.
tenant-admin	A *tenant-admin* role user can configure and monitor a specific tenant unit.
tenant-user	The *tenant-user* role enables a user to monitor a specific tenant unit and change the user password. Users who are assigned the tenant-

Table 3 Role-based accounts (continued)

Role/Account Type	Description
	user management role can view tenant unit status, but they cannot change the tenant unit configuration.

After additional user accounts are created, those user accounts can change their own configuration, but cannot perform configuration changes on other user accounts of the same level.

For more information about user roles and instructions for creating users and viewing user configuration information, see the *Data Domain Operating System Administration Guide*.

Note

For Data Domain Management Center (DD MC) only admin, limited-admin and user roles are supported. Refer to the *Data Domain Management Center Installation and Administration Guide* for information on the differences between Data Domain Management Center and Data Domain System Manager and the RBAC settings for launching the system manager from DD MC.

Certificate management

Data Domain systems can use certificates to securely communicate with following applications and protocols: HTTPS, external Key Manager (KMIP, RSA DPM), DD Boost, LDAP server, Cloud tier (AWS, Azure, Alibaba Cloud, Google Cloud, ECS, Virtustream, AWS federal), and certificate based user authentication and two factor authentication with a Common Access Card (CAC).

Data Domain systems use self-signed certificates to build mutual trust between another Data Domain system for secure data replication. It supports two different secure configurations using certificate that is one-way and two-way authentication.

Managing a Data Domain system with DD MC

In order to manage a Data Domain system, a trust needs to be established between DD MC and the system. A self-signed certificate is used to establish the trust. For more information, refer to the *Data Domain Management Center Installation and Administration Guide*.

Externally signed certificates

Certificate authority (CA) is in PEM (public certificate) format to establish a trusted connection between the external entity and each Data Domain system.

The host certificate is in PKCS12 (public plus a private key) and in PEM formats. The certificate signing requires PKCS10 format. The PEM format is used only with the CSR (Certificate Signing Request) feature.

If there is a CSR on the system, you can import the host certificate in PEM format after the CSR is signed by a CA.

Note

The system passphrase is required to import the certificate.

Refer to the *Data Domain Operating System Administration Guide* for certificate management configuration.

Certificate revocation list

Certificate revocation list (CRL) is PEM formatted file which is issued by a CA lists the revoked user certificate. Once this CRL file is imported to Data Domain System Manager, the revoked certificates are not allowed to login. Online Certificate Status Protocol (OCSP) is not supported.

Cloud certificates

To verify the identity of a cloud provider before backing up data from a Data Domain system, the cloud providers have a host certificate that is issued by a CA. Import the CA certificate and any applicable CRLs before backing up any data to the cloud. See details in section Certificates for cloud providers.

DD Boost certificates

DD Boost protocol can be used with or without externally signed certificates for encryption of data and authentication and was introduced to offer a more secure data transport capability.

In-flight encryption allows applications to encrypt in-flight backup or restore data over LAN from the Data Domain system. When configured, the client can use TLS to encrypt the session between the client and the Data Domain system. If TLS with certificates is used, then the specific suites that are used are DHE-RSA-AES128-SHA and DHE-RSA-AES256-SHA for medium and high encryption, respectively.

HTTPS certificates

The Data Domain system can use an imported certificate to establish a trusted connection to manage the Data Domain system over SSL. If a certificate is not provided, Data Domain system can use its self-signed identity certificate.

Data encryption certificates

External CA and host certificates are required to set up RSA DPM Key Manager or SafeNet KeySecure Key Manager (KMIP). If encryption is enabled on Cloud Tier, only EKM is supported.

For information about encryption certificates and key managers, see the Encryption chapter in the *Data Domain Operating System Administration Guide*.

LDAP certificates

LDAP for NFS ID mapping for folder and file permissions support secure LDAP using certificates.

Data Domain High Availability

In a Data Domain High Availability (HA) configuration, there are two controllers, where only one at a time is active, and are logically considered as a single file system.

- Both systems have the same Root Certificate Authority.
- To establish mutual trust with the HA system, trust is required to be established with the active node ONLY.
- Mutual trust, certificate signing request, and all the imported certificates on the active node are mirrored to the standby node.
- Host certificate is generated per Active and Standby node and is used for HTTPS application. CA for secure support bundle upload is also kept per node.

Externally signed certificates

If the Data Domain system or Cloud Tier use the RSA Data Protection Manager (DPM) external encryption key manager, it requires a PKCS12 host certificate and CA certificate in PEM (public key) format to establish a trusted connection between the RSA Data Protection Manager Server and each Data Domain system that it manages.

The certificate signing requires PKCS10 format. The public certificate key can have either PKCS12 (public plus a private key) or PEM format. The host certificate PEM format is used only with the CSR (Certificate Signing Request) feature.

Individual host certificates can be imported for HTTPS and communication with RSA DPM Key Manager or SafeNet KeySecure Key Manager (KMIP).

Importing the host certificate in PKCS12 format is supported. If there is a CSR on the system, you can import the host certificate in PEM format after the CSR is signed by a Certificate Authority.

Note

The system passphrase is required to import the certificate.

Log settings

A log is a chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event from inception to final results.

All Data Domain system logs (system, space, errors, access related) are stored on the root file system partition, and not accessible directly except through these services:

- Logs can be configured to send to a remote syslog server.
- Authorized service personnel can copy logs to another system via FTP or SCP.
- Some logs can be accessed via successful login via the CLI or the System Manager.

The Data Domain system log file entries contain messages from the alerts feature, autosupport reports, and general system messages. The log directory is `/ddvar/log`.

For more information, see the *Data Domain Operating System Administration Guide*.

Log descriptions

Log files can be bundled and sent to Data Domain Support to provide the detailed system information that aids in troubleshooting any system issues that may arise. The Data Domain system log file entries contain information from the alerts feature, autosupport reports, bash scripts, and general system messages.

Audit and secure logs are searchable by multiple parameters, such as username, string, authentication failure/successes, including tenant-units. Users who are assigned the "tenant-admin" role on tenant-units can only see the logs for the tenant-units which belong to them. Any configuration changes that were done on the tenant-units that are owned by the tenant-admins are shown.

This table lists logs that are important to system security.

Table 4 Log files

Log name	Location and description
messages	`/ddvar/log/messages` The system log, generated from Data Domain system actions and general system operations.
audit.log	`/ddvar/log/debug/audit.log` Lists all the CLI commands that are run via DDSH, by user and associated user role. Access to this log is controlled by user roles. Data Domain admin users can see all audit logs in the system. Tenant-admin users can see the audit logs for all tenant-units they own.
access_log	`/ddvar/log/debug/sm/access_log` Tracks users of the Data Domain System Manager graphical user interface (GUI).
secure.log	`/ddvar/log/debug/secure.log` Messages from successful and unsuccessful logins and logouts, including authentication failures by known and unknown users, as well as changes to user accounts, and any other PAM messages.
cifs.log	`/ddvar/log/debug/cifs/cifs.log` Messages about CIFS-related activity from CIFS clients attempting to connect to the Data Domain system. Messages from the CIFS subsystem are logged only in `cifs.log`.
ddsh.info	`/ddvar/log/debug/sm/ddsh.info` Tracks all commands that are issued by CLI users on the Data Domain system.
bash_audit.log	`/ddr/log/bash_audit.log` All bash operations are logged for access with the console, Telnet, or SSH. The information that is captured includes the command run, username, timestamp, client IP address, and the PID of the client that invoked the bash shell.
kmip.log	`/ddr/var/log/debug/kmip.log` All KMIP initialization and transactions logs are listed here.

For more information about logs, see the *Data Domain Operating System Administration Guide*.

Log management and retrieval

See the *Data Domain Operating System Administration Guide* for the following topics:

- Log roll-over
- Viewing log files from the DD System Manager
- Displaying log files using the CLI
- Understanding and saving log messages
- Sending log messages to another system (configuration of an external Syslog server) - It is recommended to forward system logs to an external server. Logs can still be evaluated if the local Data Domain system is down or unresponsive.

Additional log management topics are covered in the *Data Domain Operating System Administration Guide*, as follows:

- To configure CIFS logging levels, see "Setting CIFS Options."

- To configure log alert mechanisms, see "Managing Alert Reporting and Configuration of Alert Mechanisms."

Communication security settings

Communication security settings enable the establishment of secure communication channels between the product components as well as between product components and external systems or components.

Data Domain TCP and UDP ports

The tables below show Data Domain's input and output ports for TCP and UDP.

Table 5 Data Domain system inbound communication ports

Service	Protocol	Port	Port Configurable	Default	Description
FTP	TCP	21	No	Disabled	Port is used only if FTP is enabled. Run `adminaccess show` on the Data Domain system to determine if it is enabled.
SSH and SCP	TCP	22	Yes	Enabled	Port is used only if SSH is enabled. Run `adminaccess show` on the Data Domain system to determine if it is enabled. SCP is enabled as default.
Telnet	TCP	23	No	Disabled	Port is used only if Telnet is enabled. Run `adminaccess show` on the Data Domain system to determine if it is enabled.
HTTP	TCP	80	Yes	Enabled [a]	Port is used only if HTTP is enabled. Run `adminaccess show` on the Data Domain system to determine if it is enabled.
DD Boost/NFS (portmapper)	TCP	111	No	Enabled	Used to assign a random port for the mountd service that is used by DD Boost and NFS. Mountd service port can be statically assigned and can be executed with the `nfs option set mountd-port` command.
NTP	UDP	123	No	Disabled	1. Port is used only if NTP is enabled on the Data Domain system. Run `ntp status` to determine if it is enabled. 2. Used by the Data Domain system to synchronize to a time server.
SNMP	TCP/UDP	161	No	Disabled	Port is used only if SNMP is enabled. Run `snmp status` to determine if it is enabled.

Table 5 Data Domain system inbound communication ports (continued)

Service	Protocol	Port	Port Configurable	Default	Description
HTTPS	TCP	443	Yes	Enabled	Port is used only if HTTPS is enabled. Run `adminaccess show` on the Data Domain system to determine if it is enabled.
CIFS (Microsoft-DS)	TCP	445	No	Enabled	Main port that is used by CIFS for data transfer.
DD Boost/NFS	TCP	2049	Yes	Enabled	Main port that is used by NFS. Run the `nfs option show` command on the Data Domain system to determine the current NFS server port.
NFS v3/NFS v4	TCP	2049	Yes	Enabled	Main port that is used by NFS service. Run `nfs status` to determine if NFS v3 or NFS v4 service is enabled. Run `nfs option show nfs3-port` or `nfs option show nfs4-port` on Data Domain system to determine the current port that is listening.
Replication	TCP	2051	Yes	Enabled	Port is used only if replication is configured on the Data Domain system. Run `replication show config` to determine if it is configured. This port can be modified via the `replication modify` command.
NFS (mountd)	TCP/UDP	2052	Yes	Enabled	Can be hardcoded via the `nfs option set mountd-port` command. (This command is SE mode, which means that it is issued only by a Service Engineer.) Run `nfs option show mountd-port` on the Data Domain system to determine the current port that mountd is listening on.
Data Domain Management Center Port	TCP	3009	No	Enabled	This port is used only if the Data Domain system is managed by the Data Domain Management Center. It is not configurable.

[a] HTTP is enabled by default, but automatically redirects to HTTPS.

Table 6 Data Domain system outbound communication ports

Service	Protocol	Port	Port Configurable	Default	Description
SMTP	TCP	25	No	Disabled	Used by the Data Domain system to send email autosupports and alerts.
SNMP	UDP	162	Yes	Disabled	Used by the Data Domain system to send SNMP traps to SNMP host. Use `snmp show trap-hosts` to see destination hosts and `snmp status` to display service status.
Syslog	UDP	514	No	Disabled	Used by the Data Domain system to send syslog messages, if enabled. Use `log host show` to display destination hosts and service status.
RMCP	UDP	623	Open	Enabled	Remotely access BMC through IPMI

To reach a Data Domain system behind a firewall, you may need to enable these ports defined above.

Use the net filter functionality to disable all ports that are not used.

Network routing management

Routes determine the path taken to transfer data to and from the local host (the Data Domain system) to another network or host.

Data Domain Operating System does not generate or respond to RIP, EGRP/EIGRP, or BGP network routing management protocols in any form or fashion – DD OS cannot perform any IP packet routing or forwarding tasks. The only routing implemented on Data Domain systems is based upon the internal route table, where the administrator may define which physical interface [interface group] to use to address a specific network or subnet. In addition, when multiple interfaces have the same subnet which will normally allow multiple interfaces to be used for packets going to the specific subnet, the appliance uses source-based routing. This defines that outbound network packets which matches the subnet of multiple interfaces will only be routed over the physical interface from which they originated from.

Time synchronization with external source

To configure time synchronization with an external source, see "Working with Time and Date Settings," "Data Domain System Clock," "Synchronizing from a Windows Domain Controller," and "Synchronize from an NTP Server" in the *Data Domain Operating System Administration Guide*.

Cloud tier network security recommendations

To verify the identity of a cloud provider before backing up data from a Data Domain system, the cloud providers have a host certificate issued by a certificate authority (CA). Import the CA certificate and any applicable certificate revocation lists (CRLs) before backing up any data to the cloud.

The following table shows the recommended settings for securely connecting to cloud tier storage.

Table 7 Cloud tier network security recommendations

Firewall port requirements[a]	• For ECS configuration, the system must be configured to allow traffic from ports 9020 and 9021. If a load balancer is configured on ECS, port rules have to be configured accordingly. • For Alibaba Cloud, AWS, Google Cloud, and Virtustream cloud providers, communication is on port 443 and 80.
OpenSSL cipher suites	• Ciphers - ECDHE-RSA-AES256-SHA384, AES256-GCM-SHA384 • TLS Version: 1.2
IP address range filtering	• Hostnames for Alibaba cloud provider to be resolved: ■ oss.aliyuncs.com ■ oss-us-west-1.aliyuncs.com ■ oss-us-east-1.aliyuncs.com ■ oss-ap-southeast-1.aliyuncs.com ■ oss-ap-southeast-2.aliyuncs.com ■ oss-ap-southeast-3.aliyuncs.com ■ oss-ap-southeast-5.aliyuncs.com ■ oss-ap-northeast-1.aliyuncs.com ■ oss-ap-south-1.aliyuncs.com ■ oss-eu-central-1.aliyuncs.com ■ oss-me-east-1.aliyuncs.com ■ oss-cn-hangzhou.aliyuncs.com ■ oss-cn-shanghai.aliyuncs.com ■ oss-cn-qingdao.aliyuncs.com ■ oss-cn-beijing.aliyuncs.com ■ oss-cn-zhangjiakou.aliyuncs.com ■ oss-cn-huhehaote.aliyuncs.com ■ oss-cn-shenzhen.aliyuncs.com ■ oss-cn-hongkong.aliyuncs.com • Hostnames for AWS cloud provider to be resolved: ■ s3.amazonaws.com ■ s3-us-west-1.amazonaws.com ■ s3-us-west-2.amazonaws.com ■ s3-eu-west-2.amazonaws.com ■ s3-eu-west-1.amazonaws.com ■ s3-ap-northeast-1.amazonaws.com ■ s3-ap-northeast-2.amazonaws.com

Table 7 Cloud tier network security recommendations (continued)

	■ s3-ap-south.amazonaws.com ■ s3-ap-southeast-1.amazonaws.com ■ s3-ap-southeast-2.amazonaws.com ■ s3-sa-east-1.amazonaws.com ■ s3-eu-central-1.amazonaws.com • Hostname for Google Cloud: ■ storage.googleapis.com • Hostnames for Virtustream cloud provider to be resolved: ■ s-us.objectstorage.io ■ s-eu.objectstorage.io ■ s-eu-west-1.objectstorage.io ■ s-eu-west-2.objectstorage.io ■ s-us-central-1.objectstorage.io
Proxy settings	• A self signed/CA-signed certificate of proxy has to be imported using `adminaccess certificate import ca application cloud`. • If there are any existing proxy settings that reject data above a certain size, those settings must be changed to allow object size up to 4.5 MB.
Supported protocols	• HTTP • HTTPS

a. By default, ports 9020 and 9021 are not able to receive incoming network traffic. They must be enabled to receive incoming network traffic to use DD Cloud Tier.

For enhanced security, the Cloud Tier feature uses:

- Signature Version 2 for Alibaba Cloud and Google Cloud requests.
- Signature Version 4 for all AWS requests. AWS V4 signing is enabled by default.

Certificates for cloud providers

Before you can add cloud units for Alibaba Cloud, Amazon Web Services S3 (AWS), Azure, Elastic Cloud Storage (ECS), Google Cloud Platform (GPC), and Virtustream Storage Cloud (VSC), you must import certificate authority (CA) certificates.

Note

The CLI to import the certificates for cloud providers is `adminaccess certificate import ca application cloud`.

Data Domain uses secure transport in all its communications with the public cloud providers and verifies the identity of the cloud provider. Each cloud provider has a host certificate that identifies the cloud provider and is issued by a CA.

As part of setting up Data Domain Cloud Tier, you must import the cloud provider's root CA certificate and any applicable certificate revocation lists (CRLs) on the Data

Domain system. This step must be performed before adding any cloud profiles for this cloud provider.

Note

Certificate auto-import is implemented if proxy is not involved. Refer to *Data Domain Operating System Administration Guide* for more information.

Alibaba Cloud

1. Download the GlobalSign Root R1 certificate from https://support.globalsign.com/customer/portal/articles/1426602-globalsign-root-certificates.
2. Convert the downloaded certificate to a PEM-encoded format. The OpenSSL command for this conversion is: `openssl x509 -inform der -in <root_cert.crt> -out <root_cert.pem>`.
3. Import the certificate to the Data Domain system.

AWS and Azure

1. Download root CA certificates from https://www.digicert.com/digicert-root-certificates.htm.
2. Convert the downloaded certificate to a PEM-encoded format. The OpenSSL command for this conversion is: `openssl x509 -inform der -in <root_cert.crt> -out <root_cert.pem>`.
3. Import the CA certificate to the Data Domain system.

Elastic Cloud Storage (ECS)

ECS is a private cloud provider and resides within the data center, and it gives you the choice of either configuring the transport over HTTP or HTTPS.

If using HTTPS (secure transport), on the Data Domain system, you must import the CA certificate from the load balancer front-ending the ECS nodes.

Google Cloud Platform (GCP)

1. Download the GlobalSign Root R1 certificate from https://support.globalsign.com/customer/portal/articles/1426602-globalsign-root-certificates.
2. Convert the downloaded certificate to a PEM-encoded format. The OpenSSL command for this conversion is: `openssl x509 -inform der -in <root_cert.crt> -out <root_cert.pem>`.
3. Import the certificate to the Data Domain system.

Virtustream Storage Cloud

1. Download the DigiCert High Assurance EV Root CA certificate from https://www.digicert.com/digicert-root-certificates.htm.
2. Convert the downloaded certificate to a PEM-encoded format. The OpenSSL command for this conversion is: `openssl x509 -inform der -in <root_cert.crt> -out <root_cert.pem>`.
3. Import the certificate on the Data Domain system.

The *Data Domain Operating System Administration Guide* provides more details.

Cloud user credential

Alibaba Cloud, AWS S3, and Google Cloud have minimum permission requirements.

Alibaba Cloud
The Alibaba Cloud user credentials must have permissions to create and delete buckets and to add, modify, and delete files within the buckets they create. AliyunOSSFullAccess is preferred, but the following are the minimum requirements:

- ListBuckets
- GetBucket
- PutBucket
- DeleteBucket
- GetObject
- PutObject
- DeleteObject

By default, the bucket access permission would be set as "private" so it can only be accessed with AK authentication. Alibaba Cloud provides 3 types of AK(AccessKeyId and an AccessKeySecret) for authentication:

- Cloud account AccessKeys
- RAM (Resource Access Management) account AccessKeys
- STS (Security Token Service) account AccessKeys

Note

Data Domain does not currently support STS account AccessKeys. Use Cloud account or RAM AK for authentication.

In accordance with the legal requirements of the People's Republic of China, account real-name registration must be completed in order to store data in OSS in the Mainland China region.

AWS S3
AWS S3 provides a way to restrict access rights to a specific bucket and IP address(es). It is recommended that the bucket policy restricts access rights to only that specific bucket. The read/write rights should only be allowed by the DD VE writing to the specific bucket.

Note

The AWS user credentials must have permissions to create and delete buckets and to add, modify, and delete files within the buckets they create. S3FullAccess is preferred, but the following are the minimum requirements:

- CreateBucket
- ListBucket
- DeleteBucket
- ListAllMyBuckets
- GetObject
- PutObject
- DeleteObject

Google Cloud

Google Cloud user credentials must have permissions to create and delete buckets and to add, modify, and delete files within the buckets they create. These are the minimum requirements:

- ListBucket
- PutBucket
- GetBucket
- DeleteBucket
- GetObject
- PutObject
- DeleteObject

DD VE in Cloud

The object store bucket (or "container" in Azure) that is created for a particular DD VE must not be shared with any other appliance or application. Sharing the bucket (or container) with other application or other DD VE could cause data loss and/or corruption.

For more information, see the applicable DD VE Installation and Administration Guide.

Network security

DD VE in cloud solution is a backend service. DD VE must be deployed in a private subnet and must not be exposed using public IP address. Note that most of the public IP address spaces are under continuous attacks by hackers.

Appropriate security groups network access lists shall be configured to enable only intended traffic to DD VE. Open only the required ports. A complete list of DD VE ports and their usage can be found in the applicable DD VE Installation and Administration Guide.

DD VE for kernel-based virtual machine considerations

Here are security recommendations for Data Domain Virtual Edition running on Kernel-based Virtual Machine (KVM).

- Do not provide access to non-admin users for the DD VE deployed and related files or storage on the host.
- The DD VE clock and the hypervisor host clocks must be in sync with each other to ensure that the time stamps match. To achieve this, configure the same NTP server on both the hypervisor and the DD VE. Alternatively, if NTP is not used on DD VE, then disable NTP on DD VE, and reboot so that it can sync its clock with the hypervisor host.

Secure multi-tenancy security

DD OS provides multiple security enhancements to enhance security for tenant administrators and tenant users.

Unique tenant-unit hostnames
A hostname that is configured for a tenant-unit cannot resolve to an IP address associated with another tenant-unit.

Data access isolation
Data access through the local IP addresses that are registered to a tenant-unit is restricted to the storage resources associated with that tenant unit.

The following constraints apply to data access isolation:

- The local IP address for data access must exist on the Data Domain system.
- Existing IP addresses cannot be shared by multiple tenant-units.
- IP ranges are not supported.
- DHCP-assigned IP addresses are not supported.

Network firewall
The Data Domain system can restrict access from specific remote IP addresses to provide those clients with access to specific tenant-unit IP addresses.

The following constraints apply to the network firewall:

- Remote data-access IP addresses cannot be shared between multiple tenants.
- Tenant exclusion checks are not performed for subnets or IP ranges.

Unique default gateways
The Data Domain system can route data from different tenants through different routers or gateways, with separate default gateways that are configured for each tenant-unit, and the tenant-unit IP addresses mapped to the gateways for their associated tenant-unit.

The following constraints apply to unique default gateways:

- Targeted default gateways, which are assigned to a specific interface, are supported with secure multi-tenancy (SMT).
- Static, added, or DHCP gateways are not supported with SMT.
- A single default gateway cannot be shared between multiple tenants.
- Unique gateways that are assigned to a tenant cannot be used by non-SMT entities on the Data Domain system.

There are no restrictions to the address used by the gateway.

Data security settings

Data security settings (including data encryption) enable controls that prevent data permanently stored by the product from being disclosed in an unauthorized manner.

Note

For more information about data encryption, see the Data Encryption section in this guide and the *Data Domain Operating System Administration Guide*.

Dell EMC Data Domain Retention Lock software

Data Domain Retention Lock software provides immutable file locking and secure data retention capabilities for customers to meet both corporate governance and compliance standards, such as SEC 17a-4(f). DD Retention Lock provides the capability for administrators to apply retention policies at an individual file level. This software enables customers to leverage their existing Data Domain systems for backup and archive data. DD Retention Lock ensures that archive data is retained long-term with data integrity and secure data retention.

DD Retention Lock Governance edition and DD Retention Lock Compliance edition can coexist on the same Data Domain system to enable different retention periods for different classes of archive data. DD Retention Lock software is compatible with industry-standard, NAS-based (CIFS, NFS) Write-Once-Read-Many (WORM) protocols and is qualified with leading archive applications such as EMC SourceOne, EMC DiskXtender, and Veritas Enterprise Vault.

Note

The Data Domain Compliance mode is not supported for DD VE.

Dual sign-on requirement

When DD Retention Lock Compliance is enabled on a Data Domain system, additional administrative security is provided in the form of “dual” sign-on. This requirement involves a sign-on by the system administrator as well as a sign-on by a second authorized authority (the “Security Officer”). The dual sign-on mechanism of the DD Retention Lock Compliance edition acts as a safeguard against any actions that could potentially compromise the integrity of locked files before the expiration of the retention period.

Secure system clock

DD Retention Lock Compliance implements an internal security clock to prevent malicious tampering with the system clock. The security clock closely monitors and records the system clock. If there is an accumulated two-week skew within a year between the security clock and the system clock, the Data Domain file system (DDFS) is disabled and can be resumed only by a security officer.

Data integrity

- The DD OS Data Invulnerability Architecture™ protects against data loss from hardware and software failures.

- When writing to disk, the DD OS creates and stores checksums and self-describing metadata for all data received. After writing the data to disk, the DD OS then recomputes and verifies the checksums and metadata.
- An append-only write policy guards against overwriting valid data.
- After a backup completes, a validation process examines what was written to disk and verifies that all file segments are logically correct within the file system and that the data is identical before and after writing to disk.
- In the background, the online verification operation continuously checks that data on the disks is correct and unchanged since the earlier validation process.
- Storage in most Data Domain systems is set up in a double-parity RAID 6 configuration (two parity drives). Additionally, most configurations include a hot spare in each enclosure, except in certain low-end series systems, which have eight or fewer disks. Each parity stripe has block checksums to ensure that data is correct. Checksums are constantly used during the online verification operation and while data is read from the Data Domain system. With double parity, the system can fix simultaneous errors on as many as two disks.
- To keep data synchronized during a hardware or power failure, the Data Domain system uses NVRAM (non-volatile RAM) to track outstanding I/O operations. An NVRAM card with fully charged batteries (the typical state) can retain data for a period of hours, which is determined by the hardware in use.
- When reading data back on a restore operation, the DD OS uses multiple layers of consistency checks to verify that restored data is correct.

Data Domain systems support SNMP V2C and/or SNMP V3. SNMP V3 provides a greater degree of security than V2C by replacing cleartext community strings as a means of authentication with user-based authentication using either MD5 or SHA1. Also, SNMP V3 user authentication packets can be encrypted and their integrity that is verified with either DES or AES.

Multiple layers of data verification are performed by the DD OS file system on data that is received from backup applications to ensure that data is written correctly to the Data Domain system disks. This process ensures that the data can be retrieved without error. The DD OS is purpose-built for data protection and it is architecturally designed for data invulnerability. There are four critical areas of focus, described in the following sections: end-to-end verification, data erasure, system sanitization, and data encryption.

End-to-End verification

End-to-end checks protect all file system data and metadata.

As data comes into the system, a strong checksum is computed. The data is deduplicated and stored in the file system. After all data is flushed to disk, it is read back, and re-checksummed. The checksums are compared to verify that both the data and the file system metadata are stored correctly.

Data erasure

The `filesys destroy` command deletes all data in the Data Domain file system. You can also destroy the file system using the Data Domain System Manager. For more information on commands, see the *Data Domain Operating System Command Reference Guide*. See the *Data Domain Operating System Administration Guide* for information about using the System Manager.

Note

The Data Domain data erasure is not compliant with DoD requirements. For DoD compliance, service Model Number: PS- BAS-DDDE is available.

System sanitization

System sanitization was designed to remove all traces of deleted files and restore the system to the previous state.

The primary use of the `sanitize` command is to resolve Classified Message Incidents (CMIs) that occur when classified data is copied inadvertently onto a non-secure system. System sanitization is typically required in government installations. Sanitization is not supported with SSD cache tier. Use the `storage remove` and `storage add` commands to remove the logical to physical mapping. This action ensures that physical pages not to return previous written data. However, the previously written data may still be on SSD.

For more information, see the*Data Domain Operating System Administration Guide*.

Data encryption

There are three types of encryption offered with Data Domain systems.

They are:

- Encryption of data at rest via the Data Domain Encryption software option,
- Encryption of data in flight via DD Replicator software, which is used for replicating data between sites over the WAN, and
- Encryption of data in flight via DD Boost software, using TLS.

Encryption of data at rest

Encryption of data at rest protects user data in the situation where a Data Domain system is lost or stolen and eliminates accidental exposure if a failed drive requires replacement. When the file system is intentionally locked, an intruder who circumvents network security controls and gains access to the Data Domain system is unable to read the file system without the proper administrative control, passphrase, and cryptographic key. DD Encryption software is completely transparent to the backup or archive application.

DD Encryption provides inline encryption, which means as data is being ingested, the stream is deduplicated, compressed, and encrypted using an encryption key before being written to the RAID group. Data Domain Encryption software uses RSA BSAFE libraries, which are FIPS 140-2 validated.

By default, the Data Domain Embedded Key Manager (EKM) is in effect unless you configure the RSA Data Protection Manager (DPM) or SafeNet KeySecure Key Manager (Key Management Interoperability Protocol (KMIP)) key manager. External CA and Host certificates are required to set up RSA DPM Key Manager or SafeNet KeySecure Key Manager (KMIP). You can request these certificates from third-party certificate authorities, or create them using appropriate OpenSSL utility. If encryption is enabled on Cloud Tier, only EKM is supported.

One of two cipher modes, Cipher Block Chaining mode (CBC) or Galois/Counter mode (GCM), can be selected to best fit security and performance requirements. In addition, the system leverages a user-defined passphrase to encrypt that key before it is stored in multiple locations on disk. The system encryption key cannot be changed and is not, in any way, accessible to a user. Without the passphrase, the Data Domain file system cannot be unlocked, thus data is not accessible.

For the RSA DPM Key Manager, the Data Domain administrator can select a 128-bit or 256-bit Advanced Encryption Standard (AES) algorithm for encrypting all data within the system. SafeNet KeySecure Key Manager (KMIP) only supports AES-256.

For more information, see the *Data Domain Operating System Administration Guide*.

Export encryption keys
Encryption keys are exported by running the `filesys encryption keys export` command. This applies to keys in both the active, cloud tier, and the retention tiers when cloud tier storage or DD Extended Retention is enabled. All encryption keys in the file system are exported to a file that can recover encryption keys in the system if required. The key file is passphrase encrypted, and you are prompted for a passphrase. To protect the key file, you may type a new passphrase that differs from the Data Domain system passphrase. To perform this task, the *admin* or *limited-admin* role is required.

1. Run this command when a new key is created or when a change of state occurs to any of the existing keys.
2. Send the exported file via FTP for storage in a secure location, accessible to authorized users only.

Lost or forgotten passphrases cannot be recovered.

Working with KeySecure Key Manager
KeySecure Key Manager supports external key managers by using Key Management Interoperability Protocol (KMIP) and centrally manages encryption keys in a single, centralized platform.

- Keys will be pre-created on the Key Manager.
- KMIP Key Manager cannot be enabled on systems that have encryption enabled on one or more cloud units.

Encryption of data in flight

Encryption of data in flight encrypts data being transferred via DD Replicator software between two Data Domain systems. It uses OpenSSL AES 256-bit encryption to encapsulate the replicated data over the wire. The encryption encapsulation layer is immediately removed as soon as it lands on the destination Data Domain system. Data within the payload can also be encrypted via Data Domain encryption software.

Encryption of data in flight via NFS
NFSv3 and NFSv4 support krb5i and krb5p for integrity and privacy, respectively. However, there are performance penalties for encryption.

Encryption of data in flight through DD Boost

The DD Boost protocol can be used with or without certificates for authentication and encryption of data. The use of certificates was introduced to offer a more secure data transport capability.

In-flight encryption enables applications to encrypt in-flight backup or restore data over LAN from the Data Domain system. When configured, the client can use TLS to encrypt the session between the client and the Data Domain system. If TLS with certificates is used, then the specific suites that are used are DHE-RSA-AES128-SHA and DHE-RSA-AES256-SHA for medium and high encryption, respectively. If anonymous TLS is used to encrypt the session, then either ADH-AES256-SHA, for the

HIGH encryption option, or ADH-AES128-SHA, for the MEDIUM encryption option, is used.

Secure Remote Services

Secure Remote Services is an IP-based automated connect home and remote support solution and creates both a unified architecture and a common point of access for remote support activities that are performed on the product. The Secure Remote Services IP Solution does the following:

- Provides continuous monitoring, diagnosis, and repair of minor hardware issues.
- Uses the most advanced encryption, authentication, audit, and authorization for ultra-high security remote support.
- Addresses compliance with corporate and governmental regulations by providing logs of all access events.
- Provides easy integration and configuration with the storage management network and firewalls.
- Provides maximum information infrastructure protection. IP-based sessions enable fast information transfer and resolution.
- Consolidates remote support for the information with the Secure Remote Services Gateway Client.
- Provides remote access to the disaster recovery site and makes recovery from unplanned events seamless.
- Protects information in motion or at rest. AES 256 encryption during information transfer protects the information.
- Reduces costs and data center clutter and accelerates time to resolution. The elimination of modem/phone line costs translates to lower costs.

Note

Use of FTP or unsecure email while connecting to Secure Remote Services Gateway could be a security risk.

Secure Remote Services technical documentation is available on the online support site.

Security alert system settings

You can monitor Data Domain system operation with a variety of DD System Manager tools: reporting tools that automatically send emails containing status and alerts, log files that contain a record of important system events, and SNMP monitoring using third party SNMP managers.

Automatic logging and reporting tools that provide system status to Support and designated email recipients are important in monitoring system operation. Their setup and use are described in this chapter.

Alerts are also sent as SNMP traps. See the *Data Domain Operating System MIB Quick Reference* for the full list of traps.

For more information on handling alerts, see the *Data Domain Operating System Administration Guide*.

Other security considerations

The section below describes additional steps you can take to increase your system's security.

Securing data in flight

Data can be vulnerable to man-in-the-middle (MITM) attacks when the attacker can impersonate an endpoint.

Replication
Data Domain systems use self-signed certificates to build mutual trust between another Data Domain system for secure data replication. It supports two different secure configurations using certificate that is one-way and two-way authentication.

DD OS supports one-way and two-way authentication between the replication source and destination to provide additional security for replication operations.

DD Boost
To avoid MITM attacks when an application is accessing the Data Domain system, two way authentication which provides mutual verification must be done. Methods for doing two way authentication include certificates and Kerberos. With DD OS 6.1, Data Domain Boost also supports two way authentication using pre-shared keys (PSK), which does not require certificates. Various applications may support one or more methods of two way authentication depending on the application and the protocol (such as DD Boost). For example, Avamar supports two-way authentication using certificates.

System hardening

The hardening process is twofold. Traditionally, customers that are looking to harden a system are doing so because they are either under mandate, or are simply practicing secure computing practices. The latter group requires only the hardening procedures that are listed here, while the former requires a mitigation explanation for all perceived vulnerabilities as well as the hardening process. These paragraphs provide both the hardening procedures as well as the mitigation steps to comply with federal Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) on the Data Domain device product.

When a DISA STIG or SRR is run against a Data Domain device, the vulnerabilities here are reported. While some of these vulnerabilities are false positives, others require actions to be taken to mitigate or resolve the vulnerability. The following information and where applicable, mitigation procedures, must be used for customers that require the use of DISA STIGs or SRRs.

The following processes can be used to harden DD OS to comply with the DISA STIG standards:

Table 8 DISA STIG standards

GEN000020 - Single User Bootable Mode	The Data Domain device CMOS can be set with a Supervisor and User password. However, the maintenance of the passwords is handled by the customer unless specific agreement is maintained with Dell EMC to manage these passwords.

Table 8 DISA STIG standards (continued)

• GEN000400 - DoD Login Banner for Interactive Sessions • GEN000402	The customer can use the `system option set {login-banner <file>}` command to change the login banner to whatever is required to be compliant with regulations.
• GEN000540 - Password Change Policy • GEN000580 • GEN000600 • GEN000610 • GEN000620 • GEN000680 • GEN000700 • GEN000800	The customer can set/modify the account password policy characteristics and complexity to whatever is desired within the application code. This feature mitigates this finding.
GEN000700 - Password Aging	By default the password policy is relaxed to be backward compatible. The customer can use the CLIs to modify the password configuration so it is more restrictive and meets the aging requirements.
CVE-2000-1200 - Null Session Vulnerability in NetBIOS	Run the `cifs option set restrict-anonymous enabled` command to eliminate this vulnerability. Also, Data Domain has applied all security patches for NETBIOS available in Samba.
GEN005450 - Remote syslog servers	Run the `log host add <host>` command to forward logs to external log server.
GEN000240 - The system clock must be synchronized to an authoritative DoD time source.	Use the CLI to add NTP server.
GEN000242, NET0812, NET0817 - The system must use at least two time sources for clock synchronization	Use the CLI to add at least 2 NTP servers.
GEN000244 - The system must use time sources local to the enclave.	If using `ntpdate`, remove NTP servers external to the enclave.
GEN000460 - The system must disable accounts after three consecutive unsuccessful login attempts.	Use the CLI to change the login options.
Remote Access Policy V2R10 - SRC-NAC-160 - The policy assessment/ enforcement device is configured to use separate authentication server to perform user authentication.	Use the CLI to configure authentication server such as AD or other KDC, depending on the environment.
NET0240 - Network devices must not have any default manufacturer passwords. Remove any vendor default passwords from the network devices configuration	Use the CLI to change the default password, either do it with the `config seup` command or in user CLI.

Table 8 DISA STIG standards (continued)

NET0340 - Network devices must display the DoD-approved login banner warning.	Refer to GEN000400.
NET0386 - Alerts must be automatically generated to notify the administrator when log storage reaches 75% or more of its maximum capacity.	Use the CLI to configure this setting. 1. Refer to the *DD OS Administration Guide*. 2. Refer to the section "System Settings Administrator" page. 3. Configure administrator's email address. 4. Configure to **Send Alert Notification Emails to this address** box.

Use the following recommendations as precautions when hardening a Data Domain OS:

- When configuring a client list, do not use a wildcard character enabling access for any user. Type individual IP addresses or client names instead.
- The system must use a FIPS 140-2 approved cryptographic hashing algorithm for generating account password hashes. Systems must employ cryptographic hashes for passwords using the SHA-2 family of algorithms or FIPS 140-2 approved successors. The use of unapproved algorithms may result in weak password hashes more vulnerable to compromise.

  Note

  The *Data Domain Operating System Command Reference Guide* describes how to use the `adminaccess option set password-hash {md5 | sha512}` command to set the FIPS 140-2-approved cryptographic hashing on the Data Domain system.

- Enable HTTPS and disable HTTP.
- Do not enable Telnet.
- Use FTPS and SCP, but not FTP.
- Use Kerberos with NFS.
- Use strong passwords.
- If the customer’s SSH client does not comply with the ciphers DD supports by default, the customers can add the additional ciphers with from the CLI so that the SSH client can connect to DD.
- Change the default SSH port.

Note

Changing the SSH port may cause three concerns:

- The Admin interface allows only two ports: 22 and 443. If the ports change, there is no way to change the ports of the Admin interface and are left exposed. The safest way to handle this exposure is to assign the Admin interface to a temporary interface, and then bring that interface down so there are no processes listening to the old port numbers.
- The default filter function for SSH is 22 and it remains 22. The default function can be disabled. Going into SE mode a new port number can be used via the `se net filter add` operation. Specific addresses that are allowed to access it and a specific interface can be identified. Once the filter function is added, all the "normal" operations, such as enable, disable, destroy, and move, can apply.
- If the SSH port changes, it is blocked by the net filter unless `auto` is enabled. (While this option is enabled by default, it is recommended to turn off this option in a secure customer environment.) The only way to enable the new port without `auto` is via SE mode.

CHAPTER 3

Secure Maintenance

This chapter includes:

Security patch management

Your contracted service provider is responsible for installing the latest security patches. Contact Support for additional information.

CHAPTER 4

Physical Security Controls

This chapter includes:

Physical controls

Physical security controls enable the protection of resources against unauthorized physical access and physical tampering.

The ES20, DS60, and DD690 have a disk drive locking mechanism that prevents the removal of a disk drive without the appropriate tool, which is a T10 Torx screwdriver. The bezel on the ES30/FS15 has a lock and key that prevents access to the drives.

DD2200, DD2500, DD3300, DD4200, DD4500, DD7200, DD6300, DD6800, DD9300, and DD990 systems have ES30-style bezels, although there is no key lock on the DD990.

DD160, DD620, DD860, and DD880 systems have no physical access controls.

DD9500/DD9800 systems have a lock and a key, which prevents access to the drives.

For more information, see the related expansion shelf and hardware guide or disk FRU replacement documentation for the specific product.

Baseboard management controller and basic input/output system recommendations

This list contains the recommended baseboard management controller (BMC) and basic input/output system (BIOS) security practices.

- Always flash the latest BMC and BIOS images as they are released even if the release notes do not explicitly state a security fix.
- Use the Administrator Password in BIOS setup.
- Use strong passwords for IPMI user accounts and BIOS administrator password.
- Set up an isolated network for manageability and never expose that network to the internet.
- If using onboard NICs for manageability is required, configure VLANs to isolate it from the host network.

General USB security best practices

1. Prohibit booting from USB (or any device other than the hard disks) in BIOS.
2. Disable the USB ports completely in BIOS (if possible).
3. Setting a password in BIOS.

The following sections provide the general operations for disabling USB and password setup in BIOS.

Disabling USB in BIOS
For DD9500 and DD9800, the process is:

1. Browse to **IntelRCSetup** > **PCH Configuration** > **PCH Devices** > **USB Configuration**.
2. Set **USB Controller 0 Enable** to **Disabled**.

Note

Another available option is to set **USB Ports Per-port Disable** to **Enabled**, and then disable each port respectively.

For DD4200, DD4500, DD6300, DD6800, DD7200, and DD9300, the process is:

1. Browse to **IntelRCSetup** > **PCH Configuration** > **USB Configuration** > **USB Ports**.
2. Set **Per-port** from**Disable** to **Enable**.
3. Disable each port as needed.

Setting BIOS password

1. Browse to **Security** > **Administrator Password**.
2. Type the password to be set in **Create New Password**.
3. **Confirm New Password** window.
4. After reset, system will ask you for password if you want to enter BIOS setup menu.

Clearing BIOS password

1. Browse to **Security** > **Administrator Password**.
2. Type the current password in **Enter Current Password** window.
3. Without any input in **Create New Password** window, press **Enter** from keyboard.

Securing Integrated Dell Remote Access Controller 9 for DD3300

Integrated Dell Remote Access Controller 9 (iDRAC) features
iDRAC provides user with the following features:

- Monitors server health
- Remotely power on/off/cycle system
- Provides view of system's inventory

Because iDRAC is independent from the Data Domain Operating System (DD OS), users still can access a powered on system even if DD OS is not running.

iDRAC physical connection
iDRAC can be accessed through the dedicated iDRAC port in the back of the DD3300 system. By default, this port is enabled with IP address 192.168.0.120. If this port is not used, users can choose to disable iDRAC port.

iDRAC services and ports
iDRAC supports many services that are separated from DD OS services. Configure these services appropriately to correctly secure the system.

The following table shows the available iDRAC services, ports, and their default setting.

Table 9 iDRAC services and ports

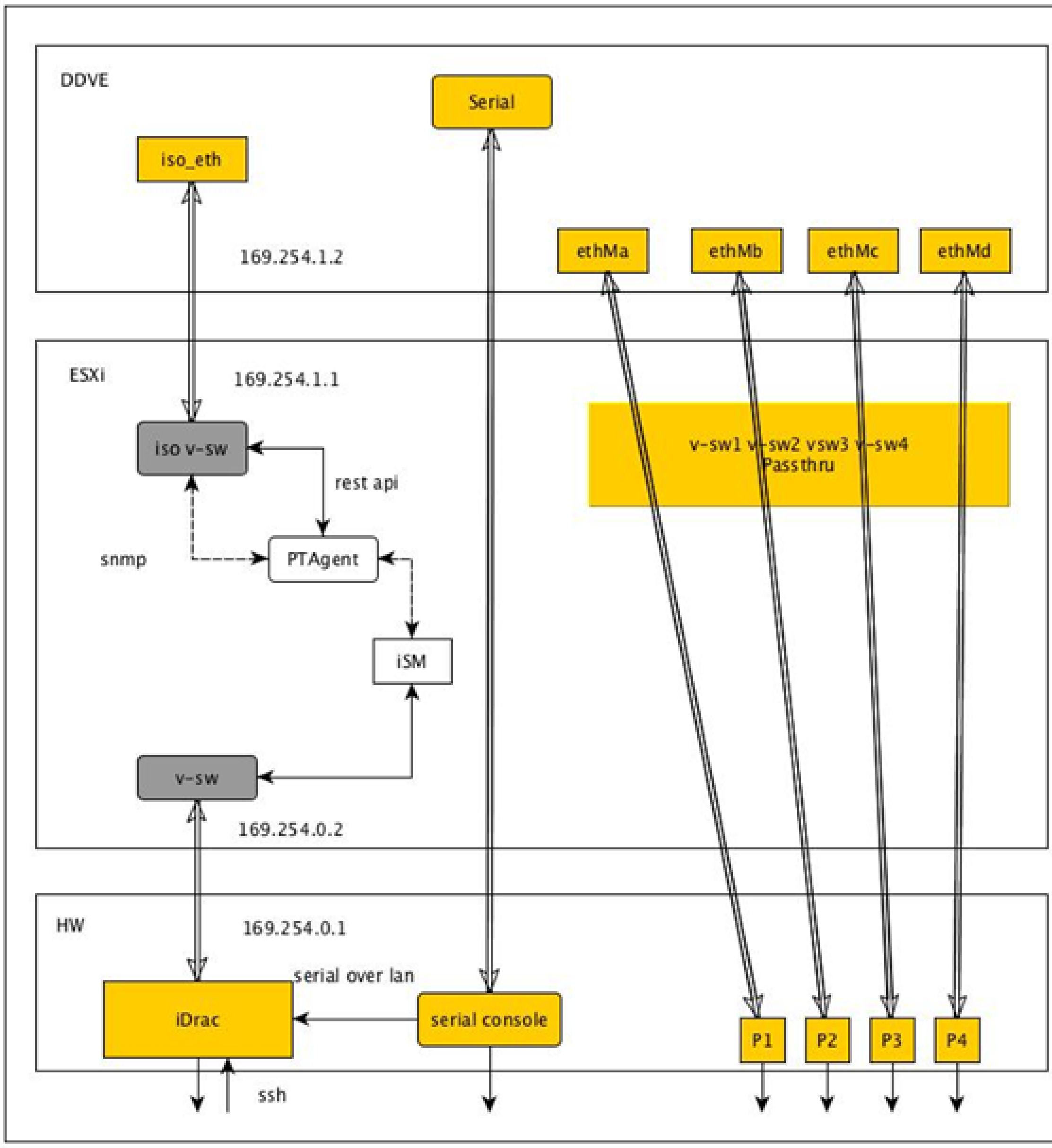
Services	Ports	Description	Default Setting
Local Configuration	Not applicable	Disable access to iDRAC configuration (from the host system) using local RACADM and iDRAC Setting utility	Disabled
Web Server ⁎	80 & 443	iDRAC web interface	Enabled
SSH ⁎	22	Access iDRAC through SSH	Enabled
Telnet	23	Access iDRAC through Telnet	Disabled
Remote RACADM ⁎	Not applicable	Remotely access iDRAC	Enabled
SNMP Agent	161	Enable support for SNMP queries in iDRAC	Disabled
Automated System Recovery Agent	Not applicable	Enable Last System Crash Screen	Disabled
Redfish ⁎	Not applicable	Redfish RESTful API	Enabled
VNC Server	5901	VNC Server on iDRAC	Disabled
Virtual Console	5900	Virtual Console of iDRAC	Disabled

⁎ These services must be enabled for system's functionality.

To configure iDRAC services, please see *Integrated Dell Remote Access Controller 9 User's Guide*.

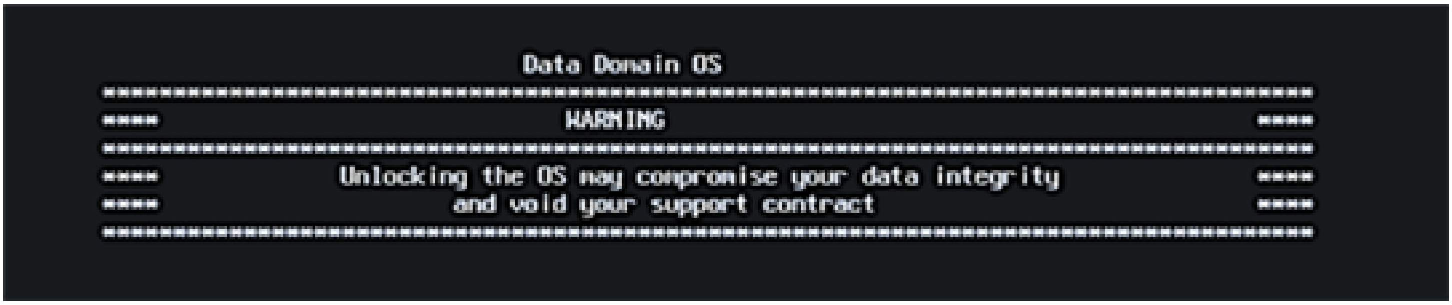
The following diagram shows the iDRAC NIC port, DD OS serial console port, and P1-P4 DD OS NIC ports.

Figure 2 DD3300 iDRAC ports



If an attempt is made through iDRAC access to unlock the virtual console, the following warning is displayed.

Figure 3 DD3300 DD OS iDRAC banner



```
                              Data Domain OS
*****************************************************************************
****                             WARNING                                 ****
*****************************************************************************
****          Unlocking the OS may compromise your data integrity        ****
****                 and void your support contract                      ****
*****************************************************************************
```

See the Knowledge Base article "Security Considerations and Best Practices for iDRAC et SNMP monitoring" for more information.

iDRAC accounts

iDRAC has the following password-protected default accounts:

- Root: The default password is the system serial number. User can use this account to monitor system's hardware. User is recommended to change the default password.
- Reserved: The account is disabled by default. It is reserved for system internal functionality. User must not use, edit, or remove this account.
- PTAdmin: The account is enabled by default. It is reserved for system internal functionality. User must not use, edit, or remove this account.

For detailed instruction how to configure account, please see *Integrated Dell Remote Access Controller 9 User's Guide*.

DD3300 Serial over LAN best practices

- Access the Data Domain console through the iDRAC dedicated port.
- Create an iDRAC "operator" account with only **Login** and **Access Virtual Console** boxes checked.
- Limit the time the console is open. It is recommended to not change the default setting for Serial Console Idle Timeout (300 seconds).
- Restrict which remote client/IP can SSH to iDRAC. The recommendation is to limit access from core switch such as ACL or VLAN tagging.