

The DD OS CLI allows you to configure a remote system for SOL and view the remote console output. This feature is supported only in the CLI.

- ① **NOTICE** IPMI power removal is provided for emergency situations during which attempts to shut down power using DD OS commands fail. IPMI power removal simply removes power to the system, it does not perform an orderly shutdown of the DD OS file system. The proper way to remove and reapply power is to use the DD OS `system reboot` command. The proper way to remove system power is to use the DD OS `system poweroff` command and wait for the command to properly shut down the file system.

## IPMI and SOL limitations

IPMI and SOL is supported on all systems supported by this release.

IPMI user support is as follows.:

- Maximum user IDs = 10.
- Two default users (NULL, root).
- Maximum user IDs available = 8.

## Adding and deleting IPMI users with DD System Manager

Each system contains its own list of configured IPMI users, which is used to control access to local power management features. Another system operating as an IPMI initiator can manage remote system power only after providing a valid username and password.

### About this task

This functionality is not supported on DD6900, DD9400, and DD9900 systems with DD OS 7.0 and later.

To give an IPMI user the authority to manage power on multiple remote systems, you must add that user to each of the remote systems.

- ① **Note:** The IPMI user list for each remote system is separate from the DD System Manager lists for administrator access and local users. Administrators and local users do not inherit any authorization for IPMI power management.

### Procedure

1. Select **Maintenance > IPMI**.
2. To add a user, complete the following steps.
  - a. Above the IPMI Users table, click **Add**.
  - b. In the Add User dialog box, type the user name (16 or less characters) and password in the appropriate boxes (reenter the password in the **Verify Password** box).
  - c. Click **Create**.  
The user entry appears in the **IPMI Users** table.
3. To delete a user, complete the following steps.
  - a. In the IPMI Users list, select a user and click **Delete**.
  - b. In the Delete User dialog box, click **OK** to verify user deletion.

## Changing an IPMI user password

Change the IPMI user password to prevent use of the old password for power management.

### About this task

This functionality is not supported on DD6900, DD9400, and DD9900 systems with DD OS 7.0 and later.

### Procedure

1. Select **Maintenance > IPMI**.
2. In the IPMI Users table, select a user, and click **Change Password**.
3. In the Change Password dialog box, type the password in the appropriate text box and reenter the password in the **Verify Password** box.
4. Click **Update**.

## Configuring an IPMI port

When you configure an IPMI port for a system, you select the port from a network ports list and specify the IP configuration parameters for that port. The selection of IPMI ports displayed is determined by the protection system model.

### About this task

Some systems support one or more dedicated ports, which can be used only for IPMI traffic. Other systems support ports that can be used for both IPMI traffic and all IP traffic supported by the physical interfaces in the **Hardware > Ethernet > Interfaces** view. Shared ports are not provided on systems that provide dedicated IPMI ports.

The port names in the IPMI Network Ports list use the prefix `bmc`, which represents baseboard management controller. To determine if a port is a dedicated port or shared port, compare the rest of the port name with the ports in the network interface list. If the rest of the IPMI port name matches an interface in the network interface list, the port is a shared port. If the rest of the IPMI port name is different from the names in the network interface list, the port is a dedicated IPMI port.

**Note:** DD4200, DD4500, and DD7200 systems are an exception to the naming rule described earlier. On these systems, IPMI port `bmc0a` corresponds to shared port `ethMa` in the network interface list. If possible, reserve the shared port `ethMa` for IPMI traffic and system management traffic (using protocols such as HTTP, Telnet, and SSH). Backup data traffic should be directed to other ports.

When IPMI and nonIPMI IP traffic share an Ethernet port, if possible, do not use the link aggregation feature on the shared interface because link state changes can interfere with IPMI connectivity.

### Procedure

1. Select **Maintenance > IPMI**.


The IPMI Configuration area shows the IPMI configuration for the managed system. The Network Ports table lists the ports on which IPMI can be enabled and configured. The IPMI Users table lists the IPMI users who can access the managed system.

**Table 45** Network Ports list column descriptions

Item	Description
Port	The logical name for a port that supports IPMI communications.
Enabled	Whether the port is enabled for IPMI (Yes or No).
DHCP	Whether the port uses DHCP to set its IP address (Yes or No).
MAC Address	The hardware MAC address for the port.
IP Address	The port IP address.
Netmask	The subnet mask for the port.
Gateway	The gateway IP address for the port.

**Table 46** IPMI Users list column descriptions

Item	Description
User Name	The name of a user with authority to power manage the remote system.

- In the **Network Ports** table, select a port to configure.
  -  Note: If the IPMI port also supports IP traffic (for administrator access or backup traffic), the interface port must be enabled before you configure IPMI.
- Above the **Network Ports** table, click **Configure**.  
The Configure Port dialog box appears.
- Choose how network address information is assigned.
  - To collect the IP address, netmask, and gateway configuration from a DHCP server, select **Dynamic (DHCP)**.
  - To manually define the network configuration, select **Static (Manual)** and enter the IP address, netmask, and gateway address.
- Enable a disabled IPMI network port by selecting the network port in the **Network Ports** table, and clicking **Enable**.
- Disable a disabled IPMI network port by selecting the network port in the **Network Ports** table, and clicking **Disable**.
- Click **Apply**.

## Preparing for remote power management and console monitoring with the CLI

Remote console monitoring uses the Serial Over Lan (SOL) feature to enable viewing of text-based console output without a serial server. You must use the CLI to set up a system for remote power management and console monitoring.

### About this task

Remote console monitoring is typically used in combination with the `ipmi remote power cycle` command to view the remote system's boot sequence. This procedure should be used on every system for which you might want to remotely view the console during the boot sequence.

**Procedure**

1. Connect the console to the system directly or remotely.
  - Use the following connectors for a direct connection.
    - DIN-type connectors for a PS/2 keyboard
    - USB-A receptacle port for a USB keyboard
    - DB15 female connector for a VGA monitor
  - ① **Note:** Systems DD4200, DD4500, and DD7200 do not support direct connection, including KVM.
  - For a serial connection, use a standard DB9 male or micro-DB9 female connector. Systems DD4200, DD4500, and DD7200 provide a female micro-DB9 connector. A null modem cable with male micro-DB9 and standard female DB9 connectors is included for a typical laptop connection.
  - For a remote IPMI/SOL connection, use the appropriate RJ45 receptacle as follows.
    - For DD990 systems, use default port eth0d.
    - For other systems, use the maintenance or service port. For port locations, refer to the system documentation, such as a hardware overview or installation and setup guide.
2. To support remote console monitoring, use the default BIOS settings.
3. To display the IPMI port name, enter `ipmi show config`.
4. To enable IPMI, enter `ipmi enable {port | all}`.
5. To configure the IPMI port, enter `ipmi config port { dhcp | ipaddress ipaddr netmask mask gateway ipaddr }`.
  - ① **Note:** If the IPMI port also supports IP traffic (for administrator access or backup traffic), the interface port must be enabled with the `net enable` command before you configure IPMI.
6. If this is the first time using IPMI, run `ipmi user reset` to clear IPMI users that may be out of synch between two ports, and to disable default users.
7. To add a new IPMI user, enter `ipmi user add user`.
8. To set up SOL, do the following:
  - a. Enter `system option set console lan`.
  - b. When prompted, enter `y` to reboot the system.

**Managing power with DD System Manager**

After IPMI is properly set up on a remote system, you can use DD System Manager as an IPMI initiator to log into the remote system, view the power status, and change the power status.

**Procedure**

1. Select **Maintenance > IPMI**.
2. Click **Login to Remote System**.  
The IPMI Power Management dialog box appears.
3. Enter the remote system IPMI IP address or hostname and the IPMI username and password, then click **Connect**.



4. View the IPMI status.

The IPMI Power Management dialog box appears and shows the target system identification and the current power status. The Status area always shows the current status.

**Note:** The Refresh icon (the blue arrows) next to the status can be used to refresh the configuration status (for example, if the IPMI IP address or user configuration were changed within the last 15 minutes using the CLI commands).

5. To change the IPMI power status, click the appropriate button.

- **Power Up**—Appears when the remote system is powered off. Click this button to power up the remote system.
- **Power Down**—Appears when the remote system is powered on. Click this button to power down the remote system.
- **Power Cycle**—Appears when the remote system is powered on. Click this button to power cycle the remote system.
- **Manage Another System**—Click this button to log into another remote system for IPMI power management.
- **Done**—Click to close the IPMI Power Management dialog box.

**NOTICE** The IPMI Power Down feature does not perform an orderly shutdown of the DD OS. This option can be used if the DD OS hangs and cannot be used to gracefully shutdown a system.

## Managing power with the CLI

You can manage power on a remote system and start remote console monitoring using the CLI.

### About this task

**Note:** The remote system must be properly set up before you can manage power or monitor the system.

### Procedure

1. Establish a CLI session on the system from which you want to monitor a remote system.
2. To manage power on the remote system, enter `ipmi remote power {on | off | cycle | status} ipmi-target <ipaddr | hostname> user user`.
3. To begin remote console monitoring, enter `ipmi remote console ipmi-target <ipaddr | hostname> user user`.

**Note:** The user name is an IPMI user name defined for IPMI on the remote system. DD OS user names are not automatically supported by IPMI.

4. To disconnect from a remote console monitoring session and return to the command line, enter the at symbol (@).
5. To terminate remote console monitoring, enter the tilde symbol (~).

## System access management

System access management features allow you to control system access to users in a local database or in a network directory. Additional controls define different access levels and control which protocols can access the system.

## Role-based access control

Role-based access control (RBAC) is an authentication policy that controls which DD System Manager controls and CLI commands a user can access on a system.

For example, users who are assigned the *admin* role can configure and monitor an entire system, while users who are assigned the *user* role are limited to monitoring a system. When logged into DD System Manager, users see only the program features that they are permitted to use based on the role assigned to the user. The following roles are available for administering and managing the DD OS.

### **admin**

An *admin* role user can configure and monitor the entire 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 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, and perform all tasks supported for user-role users.

The *security* role is provided to comply with the Write Once Read-Many (WORM) regulation. This regulation requires electronically stored corporate data be kept in an unaltered, original state for purposes such as eDiscovery, auditing, and logging. As a result of compliance regulations, most command options for administering sensitive operations, such as DD Encryption, DD Retention Lock Compliance, and archiving now require security officer approval.

In a typical scenario, an *admin* role user issues a command and, if security officer approval is required, the system displays a prompt for approval. To proceed with the original task, the security officer must enter his or her username and password on the same console at which the command was run. If the system recognizes the security officer credentials, the procedure is authorized. If not, a security alert is generated.

The following are some guidelines that apply to security-role users:

- Only the *sysadmin* user (the default user created during the DD OS installation) can create the first security officer, after which the privilege to create security officers is removed from the *sysadmin* user.
- After the first security officer is created, only security officers can create other security officers.
- Creating a security officer does not enable the authorization policy. To enable the authorization policy, a security officer must log in and enable the authorization policy.
- Separation of privilege and duty apply. *admin* role users cannot perform security officer tasks, and security officers cannot perform system configuration tasks.
- During an upgrade, if the system configuration contains security officers, a sec-off-defaults permission is created that includes a list of all current security officers.

**backup-operator**

A *backup-operator* role user can perform all tasks permitted for *user* role users, create snapshots for MTrees, import, export, and move tapes between elements in a virtual tape library, and copy tapes across pools.

A *backup-operator* role user can also add and delete SSH public keys for non-password-required log ins. (This function is used mostly for automated scripting.) He or she 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 protection system and can change his or her 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 can be appended to the other (non-tenant) roles when the Secure Multi-Tenancy (SMT) feature is enabled. A *tenant-admin* user can configure and monitor a specific tenant unit.

**tenant-user**

A *tenant-user* role can be appended to the other (non-tenant) roles when the SMT feature is enabled. The *tenant-user* role enables a user to monitor a specific tenant unit and change the user password. Users who are assigned the *tenant-user* management role can view tenant unit status, but they cannot change the tenant unit configuration.

## Access management for IP protocols

This feature manages system access for the FTP, FTPS, HTTP, HTTPS, SSH, SCP, and Telnet protocols.

### Viewing the IP services configuration

The Administrator Access tab displays the configuration status for the IP protocols that can be used to access the system. FTP and FTPS are the only protocols that are restricted to administrators.

**Procedure**

1. Select **Administration > Access > Administrator Access**.

**Results**

The Access Management page displays the Administrator Access, Local Users, Authentication, and Active Users tabs.

**Table 47** Administrator Access tab information

Item	Description
Passphrase	If no passphrase is set, the <b>Set Passphrase</b> button appears. If a passphrase is set, the <b>Change Passphrase</b> button appears.
Services	The name of a service/protocol that can access the system.

**Table 47** Administrator Access tab information (continued)

Item	Description
Enabled (Yes/No)	The status of the service. If the service is disabled, enable it by selecting it in the list and clicking <b>Configure</b> . Fill out the General tab of the dialog box. If the service is enabled, modify its settings by selecting it in the list and clicking <b>Configure</b> . Edit the settings in the General tab of the dialog box.
Allowed Hosts	The host or hosts that can access the service.
Service Options	The port or session timeout value for the service selected in the list.
FTP/FTPS	Only the session timeout can be set.
HTTP port	The port number opened for the HTTP protocol (port 80, by default).
HTTPS port	The port number opened for the HTTPS protocol (port 443, by default).
SSH/SCP port	The port number opened for the SSH/SCP protocol (port 22, by default).
Telnet	No port number can be set.
Session Timeout	The amount of inactive time allowed before a connection closes. The default is infinite, that is, the connection does not close. If possible, set a session timeout maximum of five minutes. Use the <b>Advanced</b> tab of the dialog box to set a timeout in seconds.

## Managing FTP access

The File Transfer Protocol (FTP) allows administrators to access files on the protection system.

### About this task

You can enable either FTP or FTPS access to users who are assigned the admin management role. FTP access allows admin user names and passwords to cross the network in clear text, making FTP an insecure access method. FTPS is recommended as a secure access method. When you enable either FTP or FTPS access, the other access method is disabled.

- ① **Note:** Only users who are assigned the admin management role are permitted to access the system using FTP
- ① **Note:** LFTP clients that connect to a protection system via FTPS or FTP are disconnected after reaching a set timeout limit. However the LFTP client uses its cached username and password to reconnect after the timeout while you are running any command.

### Procedure

1. Select **Administration > Access > Administrator Access**.
2. Select **FTP** and click **Configure**.
3. To manage FTP access and which hosts can connect, select the General tab and do the following:
  - a. To enable FTP access, select **Allow FTP Access**.
  - b. To enable all hosts to connect, select **Allow all hosts to connect**.

- c. To restrict access to select hosts, select **Limit Access to the following systems**, and modify the Allowed Hosts list.

① Note: You can identify a host using a fully qualified hostname, an IPv4 address, or an IPv6 address.

- To add a host, click Add (+). Enter the host identification and click OK.
- To modify a host ID, select the host in the **Hosts** list and click Edit (pencil). Change the host ID and click OK.
- To remove a host ID, select the host in the **Hosts** list and click Delete (X).

4. To set a session timeout, select the **Advanced** tab, and enter the timeout value in seconds.

① Note: The session timeout default is infinite, that is, the connection does not close.

5. Click OK.

If FTPS is enabled, a warning message appears with a prompt to click OK to proceed.

## Managing FTPS access

The FTP Secure (FTPS) protocol allows administrators to access files on the protection system.

### About this task

FTPS provides additional security over using FTP, such as support for the Transport Layer Security (TLS) and for the Secure Sockets Layer (SSL) cryptographic protocols. Consider the following guidelines when using FTPS.

- Only users who are assigned the admin management role are permitted to access the system using FTPS.
- When you enable FTPS access, FTP access is disabled.
- FTPS does not show up as a service for DD systems that run DD OS 5.2, managed from a DD system running DD OS 5.3 or later.
- When you issue the `get` command, the fatal error message `SSL_read: wrong version number lftp` appears if matching versions of SSL are not installed on the protection system and compiled on the LFTP client. As a workaround, attempt to re-issue the `get` command on the same file.

### Procedure

1. Select **Administration > Access > Administrator Access**.
2. Select **FTPS** and click **Configure**.
3. To manage FTPS access and which hosts can connect, select the **General** tab and do the following:
  - a. To enable FTPS access, select **Allow FTPS Access**.
  - b. To enable all hosts to connect, select **Allow all hosts to connect**.
  - c. To restrict access to select hosts, select **Limit Access to the following systems**, and modify the hosts list.

① Note: You can identify a host using a fully qualified hostname, an IPv4 address, or an IPv6 address.

- To add a host, click Add (+). Enter the host identification and click OK.
- To modify a host ID, select the host in the **Hosts** list and click Edit (pencil). Change the host ID and click OK.

- To remove a host ID, select the host in the **Hosts** list and click **Delete (X)**.
4. To set a session timeout, select the **Advanced** tab and enter the timeout value in seconds.  
**Note:** The session timeout default is Infinite, that is, the connection does not close.
  5. Click **OK**. If FTP is enabled, a warning message appears and prompts you to click **OK** to proceed.

## Managing HTTP and HTTPS access

HTTP or HTTPS access is required to support browser access to DD System Manager.

### Procedure

1. Select **Administration > Access > Administrator Access**.
2. Select **HTTP** or **HTTPS** and click **Configure**.  
The Configure HTTP/HTTPS Access dialog appears and displays tabs for general configuration, advanced configuration, and certificate management.
3. To manage the access method and which hosts can connect, select the **General** tab and do the following:
  - a. Select the checkboxes for the access methods you want to allow.
  - b. To enable all hosts to connect, select **Allow all hosts to connect**.
  - c. To restrict access to select hosts, select **Limit Access to the following systems**, and modify the host list.  
**Note:** You can identify a host using a fully qualified hostname, an IPv4 address, or an IPv6 address.
    - To add a host, click **Add (+)**. Enter the host identification and click **OK**.
    - To modify a host ID, select the host in the **Hosts** list and click **Edit (pencil)**. Change the host ID and click **OK**.
    - To remove a host ID, select the host in the **Hosts** list and click **Delete (X)**.
4. To configure system ports and session timeout values, select the **Advanced** tab, and complete the form.
  - In the **HTTP Port** box, enter the port number. Port 80 is assigned by default.
  - In the **HTTPS Port** box, enter the number. Port 443 is assigned by default.
  - In the **Session Timeout** box, enter the interval in seconds that must elapse before a connection closes. The minimum is 60 seconds and the maximum is 31536000 seconds (one year).  
**Note:** The session timeout default is 10,800 seconds.
5. Click **OK**.

## Managing host certificates for HTTP and HTTPS

A host certificate allows browsers to verify the identity of the system when establishing management sessions.



## Requesting a host certificate for HTTP and HTTPS

You can use DD System Manager to generate a host certificate request, which you can then forward to a Certificate Authority (CA).

### About this task

- ① **Note:** You must configure a system passphrase (`system passphrase set`) before you can generate a CSR.

### Procedure

1. Select **Administration > Access > Administrator Access**.
2. In the Services area, select **HTTP** or **HTTPS** and click **Configure**.
3. Select the **Certificate** tab.
4. Click **Add**.

A dialog appears for the protocol you selected earlier in this procedure.

5. Click **Generate the CSR for this Data Domain system**.

The dialog expands to display a CSR form.

- ① **Note:** DD OS supports one active CSR at a time. After a CSR is generated, the **Generate the CSR for this Data Domain system** link is replaced with the **Download the CSR for this Data Domain system** link. To delete a CSR, use the `adminaccess certificate cert-signing-request delete` CLI command.

6. Complete the CSR form and click **Generate and download a CSR**.

The CSR file is saved at the following path: `/ddvar/certificates/CertificateSigningRequest.csr`. Use SCP, FTP or FTPS to transfer the CSR file from the system to a computer from which you can send the CSR to a CA.

## Adding a host certificate for HTTP and HTTPS

You can use DD System Manager to add a host certificate to the system.

### Procedure

1. If you did not request a host certificate, request a host certificate from a certificate authority.
2. When you receive a host certificate, copy or move it to the computer from which you run DD Service Manager.
3. Select **Administration > Access > Administrator Access**.
4. In the Services area, select **HTTP** or **HTTPS** and click **Configure**.
5. Select the **Certificate** tab.
6. Click **Add**.

A dialog appears for the protocol you selected earlier in this procedure.

7. To add a host certificate enclosed in a .p12 file, do the following:
  - a. Select **I want to upload the certificate as a .p12 file**.
  - b. Type the password in the **Password** box.
  - c. Click **Browse** and select the host certificate file to upload to the system.
  - d. Click **Add**.

8. To add a host certificate enclosed in a .pem file, do the following:
  - a. Select **I want to upload the public key as a .pem file and use a generated private key.**
  - b. Click **Browse** and select the host certificate file to upload to the system.
  - c. Click **Add**.

### Deleting a host certificate for HTTP and HTTPS

DD OS supports one host certificate for HTTP and HTTPS. If the system is currently using a host certificate and you want to use a different host certificate, you must delete the current certificate before adding the new certificate.

#### Procedure

1. Select **Administration > Access > Administrator Access**.
2. In the Services area, select **HTTP** or **HTTPS** and click **Configure**.
3. Select the **Certificate** tab.
4. Select the certificate you want to delete.
5. Click **Delete**, and click **OK**.

### Managing SSH and SCP access

SSH is a secure protocol that enables network access to the system CLI, with or without SCP (secure copy). You can use DD System Manager to enable system access using the SSH protocol. SCP requires SSH, so when SSH is disabled, SCP is automatically disabled.

#### Procedure

1. Select **Administration > Access > Administrator Access**.
2. Select **SSH** or **SCP** and click **Configure**.
3. To manage the access method and which hosts can connect, select the **General** tab.
  - a. Select the checkboxes for the access methods you want to allow.
  - b. To enable all hosts to connect, select **Allow all hosts to connect**.
  - c. To restrict access to select hosts, select **Limit Access to the following systems**, and modify the host list.
    - ① **Note:** You can identify a host using a fully qualified hostname, an IPv4 address, or an IPv6 address.
    - To add a host, click **Add (+)**. Enter the host identification and click **OK**.
    - To modify a host ID, select the host in the **Hosts** list and click **Edit (pencil)**. Change the host ID and click **OK**.
    - To remove a host ID, select the host in the **Hosts** list and click **Delete (X)**.
4. To configure system ports and session timeout values, click the **Advanced** tab.
  - In the **SSH/SCP Port** text entry box, enter the port number. Port 22 is assigned by default.
  - In the **Session Timeout** box, enter the interval in seconds that must elapse before connection closes.

① **Note:** The session timeout default is infinite, that is, the connection does not close.

① **Note:** Click **Default** to revert to the default value.

5. Click **OK**.

## Managing Telnet access

Telnet is an insecure protocol that enables network access to the system CLI.

### About this task

① **Note:** Telnet access allows user names and passwords to cross the network in clear text, making Telnet an insecure access method.

### Procedure

1. Select **Administration > Access > Administrator Access**.
2. Select **Telnet** and click **Configure**.
3. To manage Telnet access and which hosts can connect, select the **General** tab.
  - a. To enable Telnet access, select **Allow Telnet Access**.
  - b. To enable all hosts to connect, select **Allow all hosts to connect**.
  - c. To restrict access to select hosts, select **Limit Access to the following systems**, and modify the host list.
 

① **Note:** You can identify a host using a fully qualified hostname, an IPv4 address, or an IPv6 address.

    - To add a host, click **Add (+)**. Enter the host identification and click **OK**.
    - To modify a host ID, select the host in the **Hosts** list and click **Edit** (pencil). Change the host ID and click **OK**.
    - To remove a host ID, select the host in the **Hosts** list and click **Delete (X)**.
4. To set a session timeout, select the **Advanced** tab and enter the timeout value in seconds.
 

① **Note:** The session timeout default is Infinite, that is, the connection does not close.
5. Click **OK**.

## Local user account management

A local user is a user account (user name and password) that is configured on the protection system instead of being defined in a Windows Active Directory, Windows Workgroup, or NIS directory.

After a trusted domain is configured, users who belong to that domain will be able to log into the protection system even if that trusted domain is offline.

### UID conflicts: local user and NIS user accounts

When you set up a protection system in an NIS environment, be aware of potential UID conflicts between local and NIS user accounts.

Local user accounts on a protection system start with a UID of 500. To avoid conflicts, consider the size of potential local accounts when you define allowable UID ranges for NIS users.

### Viewing local user information

Local users are user accounts that are defined on the system, rather than in Active Directory, a Workgroup, or UNIX. You can display the local user's username, management role, login status,

and target disable date. You can also display the user's password controls and the tenant units the user can access.

#### About this task

- ① **Note:** The user-authentication module uses Greenwich Mean Time (GMT). To ensure that user accounts and passwords expire correctly, configure settings to use the GMT that corresponds to the target local time.

#### Procedure

1. Select **Administration > Access > Local Users**.

The Local Users view appears and shows the Local Users table and the Detailed Information area.

**Table 48** Local user list column label descriptions

Item	Description
Name	The user ID, as added to the system.
Management Role	The role displayed is admin, user, security, backup-operator, or none. In this table, Tenant user roles are displayed as <i>none</i> . To see an assigned tenant role, select the user and view the role in the Detailed Information area.
Status	<ul style="list-style-type: none"> <li>• Active—User access to the account is permitted.</li> <li>• Disabled—User access to the account is denied because the account is administratively disabled, the current date is beyond the account expiration date, or a locked account's password requires renewal.</li> <li>• Locked—User access is denied because the password expired.</li> </ul>
Disable Date	The date the account is set to be disabled.
Last Login From	The location where the user last logged in.
Last Login Time	The time the user last logged in.

- ① **Note:** User accounts configured with the admin or security officer roles can view all users. Users with other roles can view only their own user accounts.

2. Select the user you want to view from the list of users.

Information about the selected user displays in the Detailed Information area.

**Table 49** Detailed User Information, Row Label Descriptions

Item	Description
Password Last Changed	The date the password was last changed.
Minimum Days Between Change	The minimum number of days between password changes that you allow a user. Default is 0.
Maximum Days Between Change	The maximum number of days between password changes that you allow a user. Default is 90.
Warn Days Before Expire	The number of days to warn the users before their password expires. Default is 7.

Table 49 Detailed User Information, Row Label Descriptions (continued)

Item	Description
Disable Days After Expire	The number of days after a password expires to disable the user account. Default is Never.
①	Note: The default values are the initial default password policy values. A system administrator (admin role) can change them by selecting <b>More Tasks &gt; Change Login Options</b> .

## Creating local users

Create local users when you want to manage access on the local system instead of through an external directory. Protection systems support a maximum of 500 local user accounts.

### Procedure

1. Select **Administration > Access > Local Users**.  
The Local Users view appears.
2. Click **Create** to create a new user.  
The Create User dialog appears.
3. Enter user information in the General Tab.

Table 50 Create User dialog, general controls

Item	Description
User	The user ID or name.
Password	The user password. Set a default password, and the user can change it later.
Verify Password	The user password, again.
Management Role	The role assigned to the user, which can be admin, user, security, backup-operator, or none. ① Note: Only the sysadmin user (the default user created during the DD OS installation) can create the first security-role user. After the first security-role user is created, only security-role users can create other security-role users.
Force Password Change	Select this checkbox to require that the user change the password during the first login when logging in to DD System Manager or to the CLI with SSH or Telnet.

The default value for the minimum length of a password is 6 characters. The default value for the minimum number of character classes required for a user password is 1. Allowable character classes include:

- Lowercase letters (a-z)
- Uppercase letters (A-Z)
- Numbers (0-9)
- Special Characters (\$, %, #, +, and so on)

**Note:** Sysadmin is the default admin-role user and cannot be deleted or modified.

- To manage password and account expiration, select the **Advanced** tab and use the controls described in the following table.

**Table 51** Create User dialog, advanced controls

Item	Description
Minimum Days Between Change	The minimum number of days between password changes that you allow a user. Default is 0.
Maximum Days Between Change	The maximum number of days between password changes that you allow a user. Default is 90.
Warn Days Before Expire	The number of days to warn the users before their password expires. Default is 7.
Disable Days After Expire	The number of days after a password expires to disable the user account. Default is Never.
Disable account on the following date	Check this box and enter a date (mm/dd/yyyy) when you want to disable this account. Also, you can click the calendar to select a date.

- Click **OK**.

**Note:** Note: The default password policy can change if an admin-role user changes them (**More Tasks > Change Login Options**). The default values are the initial default password policy values.

## Modifying a local user profile

After you create a user, you can use DD System Manager to modify the user configuration.

### Procedure

- Select **Administration > Access > Local Users**.

The Local Users view appears.

- Click a user name from the list.
- Click **Modify** to make changes to a user account.

The Modify User dialog box appears.

- Update the information on the **General** tab.

**Note:** If SMT is enabled and a role change is requested from none to any other role, the change is accepted only if the user is not assigned to a tenant-unit as a management-user, is not a DD Boost user with its default-tenant-unit set, and is not the owner of a storage-unit that is assigned to a tenant-unit.

**Note:** To change the role for a DD Boost user that does not own any storage units, unassign it as a DD Boost user, change the user role, and re-assign it as a DD Boost user again.



Table 52 Modify User dialog, general controls

Item	Description
User	The user ID or name.
Role	Select the role from the list.

- Update the information on the Advanced tab.

Table 53 Modify User dialog, advanced controls

Item	Description
Minimum Days Between Change	The minimum number of days between password changes that you allow a user. Default is 0.
Maximum Days Between Change	The maximum number of days between password changes that you allow a user. Default is 90.
Warn Days Before Expire	The number of days to warn the users before their password expires. Default is 7.
Disable Days After Expire	The number of days after a password expires to disable the user account. Default is Never.

- Click OK.

## Deleting a local user

You can delete certain users based on your user role. If one of the selected users cannot be deleted, the Delete button is disabled.

### About this task

The `sysadmin` user cannot be deleted. Admin users cannot delete security officers. Only security officers can delete, enable, and disable other security officers.

### Procedure

- Select **Administration > Access > Local Users**.  
The Local Users view appears.
- Click one or more user names from the list.
- Click **Delete** to delete the user accounts.  
The Delete User dialog box appears.
- Click **OK** and **Close**.

## Enabling and disabling local users

Admin users can enable or disable all users except the `sysadmin` user and users with the security role. The `sysadmin` user cannot be disabled. Only Security officers can enable or disable other security officers.

### Procedure

- Select **Administration > Access > Local Users**.  
The Local Users view appears.

2. Click one or more user names from the list.
3. Click either **Enable** or **Disable** to enable or disable user accounts.  
The Enable or Disable User dialog box appears.
4. Click **OK** and **Close**.

## Enabling security authorization

You can use the CLI to enable and disable the security authorization policy.

### About this task

For information on the commands used in this procedure, see the *DD OS Command Reference Guide*.

- ① **Note:** The DD Retention Lock Compliance license must be installed. You are not permitted to disable the authorization policy on DD Retention Lock Compliance systems.

### Procedure

1. Log into the CLI using a security officer username and password.
2. To enable the security officer authorization policy, enter: `# authorization policy set security-officer enabled`

## Changing user passwords

After you create a user, you can use DD System Manager to change the user's password. Individual users can also change their own passwords.

### Procedure

1. Click **Administration > Access > Local Users**.  
The Local Users view is displayed.
2. Click a username from the list.
3. To change the user password, click **Change Password**.  
The Change Password dialog box is displayed.
4. Enter the old password into the **Old Password** box.
5. Enter the new password into the **New Password** box.
6. Enter the new password again into **Verify New Password** box.
7. Click **OK**.

Only users with an "admin" role may change the password of other users. The administrator can change the password of other users from the CLI by running the `user change password [<user>]` command.

- ① **Note:** For security reasons, users with an "admin" role cannot change other "admin" users' passwords. If an "admin" user password needs to be changed by logging in as another user, contact DELL-EMC Support by creating a Support Request or chat request for assistance.

## Modifying the password policy and login controls

The password policy and login controls define login requirements for all users. Administrators can specify how often a password must be changed, what is required to create a valid password, and how the system responds to invalid login attempts.

### Procedure

1. Select **Administration > Access**.
2. Select **More Tasks > Change Login Options**.

The Change Login Options dialog appears.

3. Specify the new configuration in the boxes for each option. To select the default value, click **Default** next to the appropriate option.
4. Click **OK** to save the password settings.


### Change Login Options dialog

Use this dialog to set the password policy and specify the maximum login attempts and lockout period.

**Table 54** Change Login Options dialog controls

Item	Description
Minimum Days Between Change	The minimum number of days between password changes that you allow a user. This value must be less than the <b>Maximum Days Between Change</b> value minus the <b>Warn Days Before Expire</b> value. The default setting is 0.
Maximum Days Between Change	The maximum number of days between password changes that you allow a user. The minimum value is 1. The default value is 99999.
Warn Days Before Expire	The number of days to warn the users before their password expires. This value must be less than the <b>Maximum Days Between Change</b> value minus the <b>Minimum Days Between Change</b> value. The default setting is 7.
Disable Days After Expire	The system disables a user account after password expiration according to the number of days specified with this option. Valid entries are <i>never</i> or number greater than or equal to 0. The default setting is <i>never</i> .
Minimum Length of Password	The minimum password length required. Default is 6.
Minimum Number of Character Classes	The minimum number of character classes required for a user password. Default is 1. Character classes include: <ul style="list-style-type: none"> <li>• Lowercase letters (a-z)</li> <li>• Uppercase letters (A-Z)</li> <li>• Numbers (0-9)</li> <li>• Special Characters (\$, %, #, +, and so on)</li> </ul>
Lowercase Character Requirement	Enable or disable the requirement for at least one lowercase character. The default setting is disabled.

**Table 54** Change Login Options dialog controls (continued)

Item	Description
Uppercase Character Requirement	Enable or disable the requirement for at least one uppercase character. The default setting is disabled.
One Digit Requirement	Enable or disable the requirement for at least one numerical character. The default setting is disabled.
Special Character Requirement	Enable or disable the requirement for at least one special character. The default setting is disabled.
Max Consecutive Character Requirement	Enable or disable the requirement for a maximum of three repeated characters. The default setting is disabled.
Number of Previous Passwords to Block	Specify the number of remembered passwords. The range is 0 to 24, and the default settings is 1.  Note: If this setting is reduced, the remembered password list remains unchanged until the next time the password is changed. For example, if this setting is changed from 4 to 3, the last four passwords are remembered until the next time the password is changed.
Maximum login attempts	Specifies the maximum number of login attempts before a mandatory lock is applied to a user account. This limit applies to all user accounts, including sysadmin. A locked user cannot log in while the account is locked. The range is 4 to 10, and the default value is 4.
Unlock timeout (seconds)	Specifies how long a user account is locked after the maximum number of login attempts. When the configured unlock timeout is reached, a user can attempt login. The range is 120 to 600 seconds, and the default period is 120 seconds.
Maximum active logins	Specifies the maximum number of active logins to allow. The default value is 100.

## Directory user and group management

You can use DD System Manager to manage access to the system for users and groups in Windows Active Directory, Windows Workgroup, and NIS. Kerberos authentication is an option for CIFS and NFS clients.

### Viewing Active Directory and Kerberos information

The Active Directory Kerberos configuration determines the methods CIFS and NFS clients use to authenticate. The Active Directory/Kerberos Authentication panel displays this configuration.

#### Procedure

1. Select **Administration > Access > Authentication**.
2. Expand the Active Directory/Kerberos Authentication panel.

**Table 55** Active Directory/ Kerberos Authentication label descriptions

Item	Description
Mode	The type of authentication mode. In Windows/Active Directory mode, CIFS clients use Active Directory and Kerberos authentication, and NFS clients use Kerberos authentication. In Unix mode, CIFS clients use Workgroup authentication (without Kerberos), and NFS clients use Kerberos authentication. In Disabled mode, Kerberos authentication is disabled and CIFS clients use Workgroup authentication.
Realm	The realm name of the Workgroup or Active Directory.
DDNS	Whether or not the Dynamic Domain Name System is enabled.
Domain Controllers	The name of the domain controller for the Workgroup or Active Directory.
Organizational Unit	The name of the organizations unit for the Workgroup or Active Directory.
CIFS Server Name	The name of the CIFS server in use (Windows mode only).
WINS Server	The name of the WINS server in use (Windows mode only).
Short Domain Name	An abbreviated name for the domain.
NTP	Enabled/Disabled (UNIX mode only)
NIS	Enabled/Disabled (UNIX mode only)
Key Distribution Centers	Hostname(s) or IP(s) of KDC in use (UNIX mode only)
Active Directory Administrative Access	Enabled/Disabled: Click to Enable or disable administrative access for Active Directory (Windows) groups.

**Table 56** Active Directory administrative groups and roles

Item	Description
Windows Group	The name of the Windows group.
Management Role	The role of the group (admin, user, and so on)

## Configuring Active Directory and Kerberos authentication

Configuring Active Directory authentication makes the protection system part of a Windows Active Directory realm. CIFS clients and NFS clients use Kerberos authentication.

### Procedure

1. Select **Administration > Access > Authentication**.  
The Authentication view appears.
2. Expand the Active Directory/Kerberos Authentication panel.
3. Click **Configure...** next to Mode to start the configuration wizard.  
The Active Directory/Kerberos Authentication dialog appears.
4. Select **Windows/Active Directory** and click **Next**.
5. Enter the full realm name for the system (for example: domain1.local), the user name, and password for the system. Then click **Next**.

① **Note:** Use the complete realm name. Ensure that the user is assigned sufficient privileges to join the system to the domain. The user name and password must be compatible with Microsoft requirements for the Active Directory domain. This user must also be assigned permission to create accounts in this domain.

6. Select the default CIFS server name, or select **Manual** and enter a CIFS server name.
7. To select domain controllers, select **Automatically assign**, or select **Manual** and enter up to three domain controller names.

You can enter fully qualified domain names, hostnames, or IP (IPv4 or IPv6) addresses.

8. To select an organizational unit, select **Use default Computers**, or select **Manual** and enter an organization unit name.

① **Note:** The account is moved to the new organizational unit.

9. Click **Next**.

The Summary page for the configuration appears.

10. Click **Finish**.

The system displays the configuration information in the Authentication view.

11. To enable administrative access, click **Enable** to the right of **Active Directory Administrative Access**.

### Authentication mode selections

The authentication mode selection determines how CIFS and NFS clients authenticate using supported combinations of Active Directory, Workgroup, and Kerberos authentication.

#### About this task

DD OS supports the following authentication options.

- **Disabled:** Kerberos authentication is disabled for CIFS and NFS clients. CIFS clients use Workgroup authentication.
- **Windows/Active Directory:** Kerberos authentication is enabled for CIFS and NFS clients. CIFS clients use Active Directory authentication.
- **Unix:** Kerberos authentication is enabled for only NFS clients. CIFS clients use Workgroup authentication.

## Managing administrative groups for Active Directory

You can use the Active Directory/Kerberos Authentication panel to create, modify, and delete Active Directory (Windows) groups and assign management roles (admin, backup-operator, and so on) to those groups.

To prepare for managing groups, select **Administration > Access > Authentication**, expand the Active Directory/Kerberos Authentication panel, and click the Active Directory Administrative Access **Enable** button.

### Creating administrative groups for Active Directory

Create an administrative group when you want to assign a management role to all the users configured in an Active Directory group.

#### Before you begin

Enable Active Directory Administrative Access on the Active Directory/Kerberos Authentication panel in the **Administration > Access > Authentication** page.



**Procedure**

1. Click **Create....**
2. Enter the domain and group name separated by a backslash. For example: domainname \groupname.
3. Select the management role for the group from the drop-down menu.
4. Click **OK**.

**Modifying administrative groups for Active Directory**

Modify an administrative group when you want to change the administrative domain name or group name configured for an Active Directory group.

**Before you begin**

Enable Active Directory Administrative Access on the Active Directory/Kerberos Authentication panel in the **Administration > Access > Authentication** page.

**Procedure**

1. Select a group to modify under the **Active Directory Administrative Access** heading.
2. Click **Modify....**
3. Modify the domain and group name. These names are separated by a backslash. For example: domainname\groupname.

**Deleting administrative groups for Active Directory**

Delete an administrative group when you want to terminate system access for all the users configured in an Active Directory group.

**Before you begin**

Enable Active Directory Administrative Access on the Active Directory/Kerberos Authentication panel in the **Administration > Access > Authentication** page.

**Procedure**

1. Select a group to delete under the **Active Directory Administrative Access** heading.
2. Click **Delete**.

**Configuring UNIX Kerberos authentication**

Configuring UNIX Kerberos authentication enables NFS clients to use Kerberos authentication. CIFS clients use Workgroup authentication.

**Before you begin**

NIS must be running for UNIX-mode Kerberos authentication to function. For instructions about enabling Kerberos, see the section regarding enabling NIS services.

**Procedure**

1. Select **Administration > Access > Authentication**.  
The Authentication view appears.
2. Expand the Active Directory/Kerberos Authentication panel.
3. Click **Configure...** next to Mode to start the configuration wizard.  
The Active Directory/Kerberos Authentication dialog appears.
4. Select **Unix** and click **Next**.

5. Enter the realm name (for example: domain1.local), and up to three host names or IP addresses (IPv4 or IPv6) for key distribution centers (KDCs).
6. Optionally, click **Browse** to upload a keytab file, and click **Next**.

The Summary page for the configuration appears.

① **Note:** Keytab files are generated on the authentication servers (KDCs) and contain a shared secret between the KDC server and the DDR.

① **NOTICE** A keytab file must be uploaded and imported for Kerberos authentication to operate correctly.

7. Click **Finish**.

The system displays the configuration information in the Active Directory/Kerberos Authentication panel.

### Disabling Kerberos authentication

Disabling Kerberos authentication prevents CIFS and NFS clients from using Kerberos authentication. CIFS clients use Workgroup authentication.

#### Procedure

1. Select **Administration > Access Management > Authentication**.

The Authentication view appears.

2. Expand the Active Directory/Kerberos Authentication panel.
3. Click **Configure...** next to Mode to start the configuration wizard.

The Active Directory/Kerberos Authentication dialog appears.

4. Select **Disabled** and click **Next**.

The system displays a summary page with changes appearing in bold text.

5. Click **Finish**.

The system displays Disabled next to Mode in the Active Directory/Kerberos Authentication panel.

### Viewing Workgroup authentication information

Use the Workgroup Authentication panel to view Workgroup configuration information.

#### Procedure

1. Select **Administration > Access > Authentication**.
2. Expand the Workgroup Authentication panel.

Table 57 Workgroup Authentication label descriptions

Item	Description
Mode	The type of authentication mode (Workgroup or Active Directory).
Workgroup name	The specified workgroup
CIFS Server Name	The name of the CIFS server in use.
WINS Server	The name of the WINS server in use.

## Configuring workgroup authentication parameters

Workgroup authentication parameters allow you to configure a Workgroup name and CIFS server name.

### Procedure

1. Select **Administration > Access > Authentication**.  
The Authentication view appears.
2. Expand the Workgroup Authentication panel.
3. Click **Configure**.  
The Workgroup Authentication dialog appears.
4. For Workgroup Name, select **Manual** and enter a workgroup name to join, or use the default.  
The Workgroup mode joins a protection system to a workgroup domain.
5. For CIFS Server Name, select **Manual** and enter a server name (the DDR), or use the default.
6. Click **OK**.

## Viewing LDAP authentication information

The LDAP Authentication panel displays the LDAP configuration parameters and whether LDAP authentication is enabled or disabled.

### About this task

Enabling LDAP allows you to use an existing OpenLDAP server or deployment with the protection system for system-level user authentication, NFSv4 ID mapping, NFSv3 Kerberos with LDAP, or NFSv4 Kerberos with LDAP.

### Procedure

1. Select **Administration > Access > Authentication**.  
The Authentication view appears.
2. Expand the LDAP Authentication panel.

### Results


**Table 58** LDAP Authentication panel items

Item	Description
LDAP Status	Enabled or Disabled.
Base Suffix	LDAP base suffix.
Bind DN	Account name associated with the LDAP server.
SSL	Enabled or Disabled.
Server	Authentication server(s).
LDAP Group	The name of the LDAP group.
Management Role	The role of the group (admin, user, and so on).

## Enabling and disabling LDAP authentication

Use the LDAP authentication panel to enable, disable, or reset LDAP authentication.

### Procedure

1. Select **Administration > Access > Authentication**.  
The Authentication view appears.
2. Expand the LDAP authentication panel.
3. Click **Enable** next to LDAP Status to enable or **Disable** to disable LDAP Authentication.  
The Enable or Disable LDAP authentication dialog box appears.  
 **Note:** An LDAP server must exist before enabling LDAP authentication.
4. Click **OK**.

### Resetting LDAP authentication.

The **Reset** button disables LDAP authentication and clears the LDAP configuration information.

## Configuring LDAP authentication

Use the LDAP authentication panel to configure LDAP authentication.

### Procedure

1. Select **Administration > Access > Authentication**.  
The Authentication view appears.
2. Expand the LDAP Authentication panel.
3. Click **Configure**.  
The Configure LDAP Authentication dialog box appears.
4. Specify the base suffix in the **Base Suffix** field.
5. Specify the account name to associate with the LDAP server in the **Bind DN** field.
6. Specify the password for the Bind DN account in the **Bind Password** field.
7. Optionally select **Enable SSL**.
8. Optionally select **Demand server certificate** to require the protection system to import a CA certificate from the LDAP server.
9. Click **OK**.
10. If necessary at a later time, click **Reset** to return the LDAP configuration to its default values.

## Specifying LDAP authentication servers

Use the LDAP authentication panel to specify LDAP authentication servers.

### Before you begin

LDAP authentication must be disabled before configuring an LDAP server.

**About this task**

- Note:** DD SM performance when logging in with LDAP will decrease as the number of hops between the system and the LDAP server increases.

**Procedure**

1. Select **Administration > Access > Authentication**.  
The Authentication view appears.
2. Expand the LDAP authentication panel.
3. Click the + button to add a server.
4. Specify the LDAP server in one of the following formats:
  - IPv4 address—10.26.16.250
  - IPv6 address—[::ffff:9.53.96.21]
  - Hostname—myldapserver
5. Click **OK**.

**Configuring LDAP groups**

Use the LDAP authentication panel to configure LDAP groups.

**About this task**

LDAP group configuration only applies when using LDAP for user authentication on the protection system.

**Procedure**

1. Select **Administration > Access > Authentication**.  
The Authentication view appears.
2. Expand the LDAP authentication panel.
3. Configure the LDAP groups in the LDAP Group table.
  - To add an LDAP group, click **Add (+)**, enter the LDAP group name and role, and click **OK**.
  - To modify an LDAP group, select the checkbox of the group name in the LDAP group list and click **Edit (pencil)**. Change the LDAP group name and click **OK**.
  - To remove an LDAP group, select the LDAP group in the list and click **Delete (X)**.

**Using the CLI to configure LDAP authentication**

You can use the CLI to configure an existing OpenLDAP server or deployment with a protection system for system-level user authentication, NFSv4 ID mapping, NFSv3 Kerberos with LDAP, or NFSv4 Kerberos with LDAP.

**Configure LDAP servers**

You can configure one or more LDAP servers at the same time.

**About this task**

- Note:** LDAP must be disabled when making any changes to the configuration.

Specify the LDAP server in one of the following formats:

- IPv4 address—10.<A>.<B>.<C>
- IPv4 address with port number—10.<A>.<B>.<C>:400
- IPv6 address—[::ffff:9.53.96.21]
- IPv6 address with port number—[::ffff:9.53.96.21]:400
- Hostname—myldapserver
- Hostname with port number—myldapserver:400

When configuring multiple servers:

- Separate each server with a space.
- The first server listed when using the `authentication ldap servers add` command becomes the primary server.
- If any of the servers cannot be configured, the command fails for all servers listed.

#### Procedure

1. Add one or more LDAP servers by using the `authentication ldap servers add` command:

```
# authentication ldap servers add 10.A.B.C 10.X.Y.Z:400
LDAP server(s) added
LDAP Server(s):      2
#      IP Address/Hostname
-----
1.    10.A.B.C (primary)
2.    10.X.Y.Z:400
-----
```

2. Remove one or more LDAP servers by using the `authentication ldap servers del` command:

```
# authentication ldap servers del 10.X.Y.Z:400
LDAP server(s) deleted.
LDAP Servers: 1
#      Server
-----
1     10.A.B.C      (primary)
-----
```

3. Remove all LDAP servers by using the `authentication ldap servers reset` command:

```
# authentication ldap servers reset
LDAP server list reset to empty.
```

## Configure the LDAP base suffix

The base suffix is the base DN for search and is where the LDAP directory begins searching.

#### Procedure

1. Set the LDAP base suffix by using the `authentication ldap base set` command:

```
# authentication ldap base set "dc=anvil,dc=team"
LDAP base-suffix set to "dc=anvil,dc=team".
```

2. Reset the LDAP base suffix by using the `authentication ldap base reset` command:

```
# authentication ldap base reset
LDAP base-suffix reset to empty.
```



## Configure LDAP client authentication

Configure the account (Bind DN) and password (Bind PW) that is used to authenticate with the LDAP server and make queries.

### About this task

You should always configure the Bind DN and password. Normally, LDAP servers require authenticated bind by default. If `client-auth` is not set, anonymous access is requested, providing no name or password. The output of `authentication ldap show` is as follows:

```
# authentication ldap show
LDAP configuration
  Enabled:          yes (*)
  Base-suffix:     dc=u2,dc=team
  Binddn:          (anonymous)
  Server(s):       1
#   Server
-----
1  10.207.86.160  (primary)
-----

Secure LDAP configuration
  SSL Enabled:     no
  SSL Method:     off
  tls_reqcert:    demand
```

(\*) Requires a filesystem restart for the configuration to take effect.

If `binddn` is set using `client-auth` CLI, but `bindpw` is not provided, unauthenticated access is requested.

```
# authentication ldap client-auth set binddn "cn=Manager,dc=u2,dc=team"
Enter bindpw:
** Bindpw is not provided. Unauthenticated access would be requested.
LDAP client authentication binddn set to "cn=Manager,dc=u2,dc=team".
```

### Procedure

1. Set the Bind DN and password by using the `authentication ldap client-auth set binddn` command:

```
# authentication ldap client-auth set binddn
"cn=Administrator,cn=Users,dc=anvil,dc=team"
Enter bindpw:
LDAP client authentication binddn set to
"cn=Administrator,cn=Users,dc=anvil,dc=team".
```

2. Reset the Bind DN and password by using the `authentication ldap client-auth reset` command:

```
# authentication ldap client-auth reset
LDAP client authentication configuration reset to empty.
```

## Enable LDAP

### Before you begin

An LDAP configuration must exist before enabling LDAP. Additionally, you must disable NIS, ensure that the LDAP server is reachable, and be able to query the root DSE of the LDAP server.

### Procedure

1. Enable LDAP by using the `authentication ldap enable` command:

```
# authentication ldap enable
```

The details of the LDAP configuration are displayed for you to confirm before continuing. To continue, type `yes` and restart the file system for LDAP configuration to take effect.

- View the current LDAP configuration by using the `authentication ldap show` command:

```
# authentication ldap show
LDAP configuration
  Enabled:          no
  Base-suffix:     dc=anvil,dc=team
  Binddn:          cn=Administrator,cn=Users,dc=anvil,dc=team
  Server(s):       2
#   Server
-   -----
1   10.26.16.250   (primary)
2   10.26.16.251:400
-   -----

Secure LDAP configuration
  SSL Enabled:     no
  SSL Method:      off
  tls_reqcert:    demand
```

Basic LDAP and secure LDAP configuration details are displayed.

- View the current LDAP status by using the `authentication ldap status` command:

```
# authentication ldap status
```

The LDAP status is displayed. If the LDAP status is not `good`, the problem is identified in the output. For example:

```
# authentication ldap status
Status: invalid credentials
```

or

```
# authentication ldap status
Status: invalid DN syntax
```

- Disable LDAP by using the `authentication ldap disable` command:

```
# authentication ldap disable
LDAP is disabled.
```

## Enable secure LDAP

You can configure DDR to use secure LDAP by enabling SSL.

### Before you begin

If there is no LDAP CA certificate and `tls_reqcert` is set to `demand`, the operation fails. Import an LDAP CA certificate and try again.

If `tls_reqcert` is set to `never`, an LDAP CA certificate is not required. For more information, see [Configure LDAP server certificate verification with imported CA certificates](#) on page 153.

### Procedure

- Enable SSL by using the `authentication ldap ssl enable` command:

```
# authentication ldap ssl enable
Secure LDAP is enabled with 'ldaps' method.
```

The default method is secure LDAP, or `ldaps`. You can specify other methods, such as TLS:

```
# authentication ldap ssl enable method start_tls
Secure LDAP is enabled with 'start_tls' method.
```

2. Disable SSL by using the `authentication ldap ssl disable` command:

```
# authentication ldap ssl disable
Secure LDAP is disabled.
```

## Configure LDAP server certificate verification with imported CA certificates

You can change the TLS request certificate behavior.

### Procedure

1. Change the TLS request certificate behavior by using the `authentication ldap ssl set tls_reqcert` command.

Do not verify the certificate:

```
# authentication ldap ssl set tls_reqcert never
"tls_reqcert" set to "never". LDAP server certificate will not be
verified.
```

Verify the certificate:

```
# authentication ldap ssl set tls_reqcert demand
"tls_reqcert" set to "demand". LDAP server certificate will be verified.
```

2. Reset the TLS request certificate behavior by using the `authentication ldap ssl reset tls_reqcert` command. The default behavior is demand:

```
# authentication ldap ssl reset tls_reqcert
tls_reqcert has been set to "demand". LDAP Server certificate will be
verified with imported CA certificate. Use "adminaccess" CLI to import the
CA certificate.
```

## Manage CA certificates for LDAP

You can import or delete certificates and show current certificate information.

### Procedure

1. Import a CA certificate for LDAP server certificate verification by using the `adminaccess certificate import` command.

Specify ldap for ca application:

```
# adminaccess certificate import {host application {all | aws-federal | ddbboost | https |
keysecure | <application-list>} | ca application {all | cloud | ddbboost | ldap | login-
auth | keysecure | <application-list>}} [file <file-name>]
```

2. Delete a CA certificate for LDAP server certificate verification by using the `adminaccess certificate delete` command.

Specify ldap for application:

```
# adminaccess certificate delete {subject <subject-name> | fingerprint <fingerprint>}
[application {all | aws-federal | cloud | ddbboost | ldap | login-auth | https | keysecure
| support | <application-list>}]
```

3. Show current CA certificate information for LDAP server certificate verification by using the `adminaccess certificate show` command:

```
# adminaccess certificate show imported-ca application ldap
```

## Viewing NIS authentication information

The NIS Authentication panel displays the NIS configuration parameters and whether NIS authentication is enabled or disabled.

### Procedure

1. Select **Administration > Access > Authentication**.

The Authentication view appears.

2. Expand the NIS Authentication panel.

### Results

**Table 59** NIS Authentication panel items

Item	Description
NIS Status	Enabled or Disabled.
Domain Name	The name of the domain for this service.
Server	Authentication server(s).
NIS Group	The name of the NIS group.
Management Role	The role of the group (admin, user, and so on).

## Enabling and disabling NIS authentication

Use the NIS Authentication panel to enable and disable NIS authentication.

### Procedure

1. Select **Administration > Access > Authentication**.

The Authentication view appears.

2. Expand the NIS Authentication panel.

3. Click **Enable** next to NIS Status to enable or **Disable** to disable NIS Authentication.

The Enable or Disable NIS dialog box appears.

4. Click **OK**.

## Configuring the NIS domain name

Use the NIS Authentication panel to configure the NIS domain name.

### Procedure

1. Select **Administration > Access > Authentication**.

The Authentication view appears.

2. Expand the NIS Authentication panel.

3. Click **Edit** next to Domain Name to edit the NIS domain name.

The Configure NIS Domain Name dialog box appears.

4. Enter the domain name in the **Domain Name** box.

5. Click **OK**.

## Specifying NIS authentication servers

Use the NIS Authentication panel to specify NIS authentication servers.

### Procedure

1. Select **Administration > Access > Authentication**.  
The Authentication view appears.
2. Expand the NIS Authentication panel.
3. Below Domain Name, select one of the following:
  - **Obtain NIS Servers from DHCP** The system automatically obtains NIS servers using DHCP
  - **Manually Configure** Use the following procedures to manually configure NIS servers.
    - To add an authentication server, click Add (+) in the server table, enter the server name, and click **OK**.
    - To modify an authentication server, select the authentication server name and click the edit icon (pencil). Change the server name, and click **OK**.
    - To remove an authentication server name, select a server, click the X icon, and click **OK**.
4. Click **OK**.

## Configuring NIS groups

Use the NIS Authentication panel to configure NIS groups.

### Procedure

1. Select **Administration > Access > Authentication**.  
The Authentication view appears.
2. Expand the NIS Authentication panel.
3. Configure the NIS groups in the NIS Group table.
  - To add a NIS group, click Add (+), enter the NIS group name and role, and click **Validate**. Click **OK** to exit the add NIS group dialog box. Click **OK** again to exit the **Configure Allowed NIS Groups** dialog box.
  - To modify an NIS group, select the checkbox of the NIS group name in the NIS group list and click Edit (pencil). Change the NIS group name, and click **OK**.
  - To remove an NIS group name, select the NIS group in the list and click Delete X.
4. Click **OK**.

## Configuring SSO authentication

The Single Sign-On (SSO) panel displays the SSO configuration parameters and whether SSO is enabled or disabled. Configuring SSO requires action on both the protection system and the SSO provider. SSO is supported on physical protection systems, and locally installed DD VE instances. Cloud-based DD VE instances are not supported.

### About this task

SSO allows you to register a protection system with a supported SSO provider to use the SSO provider credentials for system-level user authentication. Logging in using single sign-on (SSO) on page 31 describes how to log in using SSO after SSO is configured, an SSO user group is created, and SSO is enabled.

- ① Note: Data Protection Central (DPC) is the only supported SSO provider. DPC version 19.1 is required to use SSO.

#### Procedure

1. Select **Administration > Access > Authentication**.  
The Authentication view appears.
2. Expand the Single Sign-On (SSO) panel.

#### Results

Table 60 Single Sign-On (SSO) panel items

Item	Description
Single Sign-On Status	Enabled or Disabled.
Provider	The name of the SSO provider.
Provider Status	Online or Offline.
Client Name	The IP address of the SSO client.
Host Name	The hostname of the SSO client.
User Group	The name of a user group configured to allow SSO provider users to access the protection system. ① Note: At least one user group is required to use SSO.
Domain Name	The domain name associated with a user group
Management Role	The level of management privileges associated with a user group.

## Registering the protection system in Data Protection Central (DPC)

### About this task

Complete the following steps to register the protection system in DPC.

#### Procedure

1. Log in to the DPC and navigate to the **System Management**.
2. Add the system to DPC.  
① Note: DPC requires sysadmin credentials for the system.
3. Refresh the Single Sign-On (SSO) panel in DD SM to confirm that the system is registered with DPC.

## Enabling and disabling SSO

Use the Single Sign-On (SSO) panel to enable or disable SSO.

#### Procedure

1. Select **Administration > Access > Authentication**.  
The Authentication view appears.
2. Expand the Single Sign-On (SSO) panel.
3. Click **Enable** next to Single Sign-On Status to enable or **Disable** to disable SSO.  
The Enable or Disable SSO dialog box appears.



4. Click **OK**.

## Configuring Single Sign-On (SSO) groups

Use the Single Sign-On (SSO) panel to configure SSO user groups.

### About this task

At least one SSO user group is required to use SSO functionality.

### Procedure

1. Select **Administration > Access > Authentication**.  
The Authentication view appears.
2. Expand the Single Sign-On (SSO) panel.
3. Configure the SSO user groups in the table.
  - To add an SSO user group, click Add (+), enter the SSO user group name and domain name, select the management role, and click **OK**.
    - ① Note: Admin users can set a group management role to user, admin, backup-operator, or limited-admin. Limited-admin users can set a group management role to user or backup operator.
    - ① Note: If a group name belongs to multiple domains, set up the same group name with all domain names on the protection system with the desired role, or make sure the domain name the user will log in with is configured on system with the desired role. This is important for Active Directory configurations with child or sub domains.
  - To modify an SSO user group, select the checkbox of the group name in the SSO group list and click Edit (pencil). Change the management role and click **OK**.
  - To remove an SSO user group, select the group in the list and click Delete (X).

## Diagnosing authentication issues

DD OS provides the ability to diagnose authentication issues for Active Directory from within the DD System Manager interface.

### Procedure

1. Select **Administration > Access > Authentication**
2. Expand the Active Directory/Kerberos Authentication panel.
3. Click **Diagnose**.
4. Select an issue to investigate, and click **Diagnose**.
5. Provide the requested information.

To diagnose issues logging in as an Active Directory user, provide:

- Active Directory server IP address
- Active Directory server FQDN
- Active Directory service username
- ① Note: The Active Directory user account specified here requires the following privileges:
  - Read-only access to the base DN identified by the domain name.
  - Read-only access to query attributes of all users in the base DN.

- Read-only access to query attributes of the machine account for the protection system.
- Active Directory service password
- Username experiencing login failure

To diagnose issues joining the system to an Active Directory Domain, provide:

- Active Directory server IP address
  - Active Directory server FQDN
  - Active Directory service username
  - Active Directory service password
6. Click **Diagnose**.
  7. View the report.
    - Click **View Report** to view the report online. Each item in the Action Items table can be clicked for additional details.
    - Click **Download** to download a copy of the report.
  8. Review and implement the suggested fixes for the issue, and retry the operation.

## Change system authentication method

The protection system supports password-based authentication, or certificate-based authentication. Password-based authentication is the default method.

### Before you begin

Certificate-based authentication requires SSH keys and CA certificates are imported to allow users to authenticate with the system when password-based authentication is disabled.

### About this task

Complete the following steps to change the system authentication method from password-based authentication to certificate-based authentication.

### Procedure

1. Select **Administration > Access**.

The Access Management view appears.
2. Click **Manage CA Certificates**.
3. Click **Add** to create a new certificate.
4. Add the certificate.
  - Select **I want to upload the certificate as a .pem file** and click **Choose File** to select the certificate file and upload it to the system.
  - Select **I want to copy and paste the certificate text** to copy and paste the certificate text into the text field.
5. Click **Add**.
6. Select **More Tasks > Change Login Options**.
7. In the **Password Based Login** drop-down menu, select **Disable**.

 Note: The drop-down menu is disabled if the required SSH keys and CA certificates are not configured on the system

8. Click **OK**.

If a security policy is configured, the system prompts for security officer credentials. Provide the credentials and click **OK**.

## Reset the system authentication method to password-based authentication.

### About this task

Complete the following steps to change the system authentication method from certificate-based authentication to password-based authentication.

### Procedure

1. Select **Administration > Access**.  
The Access Management view appears.
2. Select **More Tasks > Change Login Options**.
3. In the **Password Based Login** drop-down menu, select **Enable**.
4. Click **OK**.


If a security policy is configured, the system prompts for security officer credentials. Provide the credentials and click **OK**.

## Reset the iDRAC password

If the iDRAC password for DD3300, DD6900, DD9400, and DD9900 systems is lost or forgotten, it is possible to reset the password to the factory default setting.

### About this task

The Data Domain system requires that the Integrated Dell Remote Access Controller (iDRAC) is configured for system upgrade and maintenance operations. Additionally, the system supports the use of iDRAC to change security settings, and remotely power the system on and off.

 **CAUTION** Do not use iDRAC to change the storage configuration, system settings, or BIOS settings, as making changes will impact system functionality. Contact Support if changes are required in any of these areas.

### Procedure

1. Connect to the system serial console or connect KVM to the system.
2. Reboot the system.
3. During the system boot process, press #2 to access the BIOS menu.
4. Select **iDRAC Settings**.
5. Select **Reset iDRAC configurations to defaults all**.
6. Select **Yes** to confirm the reset.
7. Select **Continue**.
8. Exit the BIOS and reboot.

### Results

The iDRAC configuration resets to the following username and password:

- Username: root
- Password: calvin



# CHAPTER 4

## Monitoring Protection Systems

This chapter includes:

• Viewing individual system status and identity information.....	162
• Health Alerts panel.....	165
• Viewing and clearing current alerts.....	165
• Viewing the alerts history.....	166
• Viewing hardware component status.....	167
• Viewing system statistics.....	171
• Viewing active users.....	172
• History report management.....	173
• Viewing the Task Log.....	177
• Viewing the system High Availability status.....	178

## Viewing individual system status and identity information

The **Dashboard** area displays summary information and status for alerts, the file system, licensed services, and hardware enclosures. The **Maintenance** area displays additional system information, including the system uptime and system and chassis serial numbers.

### About this task

The system name, software version, and user information appear in the footer at all times.

### Procedure

1. To view system dashboard, select **Home > Dashboard**.

Figure 5 System dashboard



2. To view the system uptime and identity information, select **Maintenance > System**.

The system uptime and identification information appears in the System area.

## Dashboard Alerts area

The Dashboard Alerts area shows the count, type, and the text of the most recent alerts in the system for each subsystem (hardware, replication, file system, and others). Click anywhere in the alerts area to display more information on the current alerts.

Table 61 Dashboard Alerts column descriptions

Column	Description
Count	A count of the current alerts for the subsystem type specified in the adjacent column. The background color indicates the severity of the alert.
Type	The subsystem that generated the alert.



**Table 61** Dashboard Alerts column descriptions (continued)

Column	Description
Most recent alerts	The text of the most recent alert for the subsystem type specified in the adjacent column

## Troubleshooting alerts

Find the information you need to troubleshoot issues.

### Data collection space usage is high

When space usage for data collection exceeds 90 percent, refer to KB article 500681:Data Domain: Space usage in Data Collection has exceeded 90% threshold on Dell EMC Online Support to troubleshoot the issue.

## Dashboard File System area

The Dashboard File System area displays statistics for the entire file system. Click anywhere in the File System area to display more information.

**Table 62** File System area label descriptions

Column	Description
Status	The current status of the file system.
Used	The total file system space being used.
Logical Written	The data quantity received by the system prior to compression.
Physical Written	The data quantity stored on the system after compression.
Compression Factor	The average compression reduction factor for the file system.

## Dashboard Services area

The Dashboard Services area displays the status of the replication, DD VTL, CIFS, NFS, DD Boost, and vDisk services. Click on a service to display detailed information about that service.

**Table 63** Services area column descriptions

Column	Description
Left column	The left column lists the services that may be used on the system. These service can include Replication, DD VTL, CIFS, NFS, DD Boost, vDisk.
Right column	The right column shows the operational status of the service. For most services, the status is enabled, disabled, or not licensed. The replication service row displays the number of

Table 63 Services area column descriptions (continued)

Column	Description
	replication contexts that are in normal, warning, and error states. A color coded box displays green for normal operation, yellow for warning situations, or red when errors are present).

## Dashboard HA Readiness area

In high-availability (HA) systems, the HA panel indicates whether the system can fail over from the active node to the standby node if necessary.

You can click on the **HA panel** to navigate to the **High Availability** section under **HEALTH**.

## Dashboard Hardware area

The Dashboard Hardware area displays the status of the system enclosures and drives. Click anywhere in the Hardware area to display more information on these components.

Table 64 Hardware area label descriptions

Label	Description
Enclosures	The enclosure icons display the number of enclosures operating in the normal (green checkmark) and degraded (red X) states.
Storage	The storage icons display the number of disk drives operating in the normal (green checkmark), spare (green +), or failed (red X) state.

## Maintenance System area

The Maintenance System area displays the system model number, DD OS version, system uptime, and system and chassis serial numbers.

Table 65 System area label descriptions

Label	Description
Model Number	The model number is the number assigned to the protection system.
Version	The version is the DD OS version and build number of the software running on the system.
System Uptime	The system uptime displays how long the system has been running since the last system start. The time in parenthesis indicates when the system uptime was last updated.

Table 65 System area label descriptions (continued)

Label	Description
System Serial No.	The system serial number is the serial number assigned to the system. The system serial number is independent of the chassis serial number and remains the same during many types of maintenance events, including chassis replacements.
Chassis Serial No.	The chassis serial number is the serial number on the current system chassis.

## Health Alerts panel

Alerts are messages from system services and subsystems that report system events. The Health > Alerts panel displays tabs that allow you to view current and non-current alerts, the configured alert notification groups, and the configuration for those who want to receive daily alert summary reports.

Alerts are also sent as SNMP traps. See the *MIB Quick Reference Guide* or the SNMP MIB for the full list of traps.

## Viewing and clearing current alerts

The Current Alerts tab displays a list of all the current alerts and can display detailed information for a selected alert. An alert is automatically removed from the Current Alerts list when the underlying situation is corrected or when manually cleared.

### Procedure

- To view all of the current alerts, select **Health > Alerts > Current Alerts**.
- To limit the number of entries in the current alert list, do the following.
  - In the Filter By area, select a **Severity** and **Class** to expose only alerts that pertain to those choices.
  - Click **Update**.  
All alerts not matching the Severity and Class are removed from the list.
- To display additional information for a specific alert in the **Details** area, click the alert in the list.
- To clear an alert, select the alert checkbox in the list and click **Clear**.  
A cleared alert no longer appears in the current alerts list, but it can be found in the alerts history list.
- To remove filtering and return to the full listing of current alerts, click **Reset**.

## Current Alerts tab

The Current Alerts tab displays a list of alerts and detailed information about a selected alert.

**Table 66** Alerts list, column label descriptions

Item	Description
Message	The alert message text.
Severity	The level of seriousness of the alert. For example, warning, critical, info, or emergency.
Date	The time and date the alert occurred.
Class	The subsystem where the alert occurred.
Object	The physical component where the alert is occurring.

**Table 67** Details area, row label descriptions

Item	Description
Name	A textual identifier for the alert.
Message	The alert message text.
Severity	The level of seriousness of the alert. For example, warning, critical, info, emergency.
Class	The subsystem and device where the alert occurred.
Date	The time and date the alert occurred.
Object ID	The physical component where the alert is occurring.
Event ID	An event identifier.
Tenant Units	Lists affected tenant units.
Description	More descriptive information about the alert.
Action	A suggestion to remedy the alert.
Object Info	Additional information about the affected object.
SNMP OID	SNMP object ID.

## Viewing the alerts history

The Alerts History tab displays a list of all the cleared alerts and can display detailed information for a selected alert.

### Procedure

1. To view all of the alerts history, select **Health > Alerts > Alerts History**.
2. To limit the number of entries in the current alert list, do the following.
  - a. In the Filter By area, select a **Severity** and **Class** to expose only alerts that pertain to those choices.
  - b. Click **Update**.  
All alerts not matching the Severity and Class are removed from the list.

3. To display additional information for a specific alert in the **Details** area, click the alert in the list.
4. To remove filtering and return to the full listing of cleared alerts, click **Reset**.

## Alerts History tab

The Alerts History tab displays a list of cleared alerts and details about a selected alert.

**Table 68** Alerts list, column label descriptions

Item	Description
Message	The alert message text.
Severity	The level of seriousness of the alert. For example, warning, critical, info, or emergency.
Date	The time and date the alert occurred.
Class	The subsystem where the alert occurred.
Object	The physical component where the alert is occurring.
Status	Whether the status is posted or cleared. A posted alert is not cleared.

**Table 69** Details area, row label descriptions

Item	Description
Name	A textual identifier for the alert.
Message	The alert message text.
Severity	The level of seriousness of the alert. For example, warning, critical, info, emergency.
Class	The subsystem and device where the alert occurred.
Date	The time and date the alert occurred.
Object ID	The physical component where the alert is occurring.
Event ID	An event identifier.
Tenant Units	Lists affected tenant units.
Additional Information	More descriptive information about the alert.
Status	Whether the status is posted or cleared. A posted alert is not cleared.
Description	More descriptive information about the alert.
Action	A suggestion to remedy the alert.

## Viewing hardware component status

The Hardware Chassis panel displays a block drawing of each enclosure in a system, including the chassis serial number and the enclosure status. Within each block drawing are the enclosure

components, such as disks, fans, power supplies, NVRAM, CPUs, and memory. The components that appear depend upon the system model.

#### About this task

DD SM also displays the system serial number. The system serial number is independent of the chassis serial number and remains the same during many types of maintenance events, including chassis replacements.

#### Procedure

1. Select **Hardware > Chassis**.

The Chassis view shows the system enclosures. Enclosure 1 is the system controller, and the rest of the enclosures appear below Enclosure 1.

Components with problems show yellow (warning) or red (error); otherwise, the component displays OK.

2. Click a component to see detailed status.

## Fan status

Fans are numbered and correspond to their location in the chassis. Hover over a system fan to display a tooltip for that device.

Table 70 Fan tooltip, column label descriptions

Item	Description
Description	The name of the fan.
Level	The current operating speed range (Low, Medium, High). The operating speed changes depending on the temperature inside the chassis.
Status	The health of the fan.

## Temperature status

Protection systems and some components are configured to operate within a specific temperature range, which is defined by a temperature profile that is not configurable. Hover over the Temperature box to display the temperature tooltip.

Table 71 Temperature tooltip, column label descriptions

Item	Description
Description	<p>The location within the chassis being measured. The components listed depend on the model and are often shown as abbreviations. Some examples are:</p> <ul style="list-style-type: none"> <li>• CPU 0 Temp (Central Processing Unit)</li> <li>• MLB Temp 1 (main logic board)</li> <li>• BP middle temp (backplane)</li> <li>• LP temp (low profile of I/O riser FRU)</li> <li>• FHFL temp (full height full length of I/O riser FRU)</li> <li>• FP temp (front panel)</li> </ul>



Table 71 Temperature tooltip, column label descriptions (continued)

Item	Description
C/F	The C/F column displays temperature in degrees Celsius and Fahrenheit. When the description for a CPU specifies <i>relative</i> (CPU <i>n</i> Relative), this column displays the number of degrees that each CPU is below the maximum allowable temperature and the actual temperature for the interior of the chassis (chassis ambient).
Status	Shows the temperature status: <ul style="list-style-type: none"> <li>• OK—The temperature is acceptable</li> <li>• Critical—The temperature is higher than the shutdown temperature.</li> <li>• Warning—The temperature is higher than the warning temperature (but lower than the shutdown temperature).</li> <li>• Dash (-) —No temperature thresholds are configured for this component, so there is no status to report.</li> </ul>

## Management panel status

DD6300, DD6800, and DD9300 systems have a fixed management panel with an Ethernet port for the management network on the rear of the chassis. Hover over the Ethernet port to display a tooltip.

Table 72 Management panel tooltip, column label descriptions

Item	Description
Description	The type of NIC installed in the management panel.
Vendor	The manufacturer of the management NIC.
Ports	The name of the management network (Ma).

## SSD status (DD6300 only)

The DD6300 supports up to two SSDs in slots on the rear of the chassis. The SSD slots are numbered and correspond to their location in the chassis. Hover over an SSD to display a tooltip for that device.

Table 73 SSD tooltip, column label descriptions

Item	Description
Description	The name of the SSD.
Status	The state of the SSD.
Life Used	The percentage of the rated operating life the SSD has used.

## Power supply status

The tooltip shows the status of the power supply (OK or DEGRADED if a power supply is absent or failed). You can also look at the back panel of the enclosure and check the LED for each power supply to identify those that need replacing.

## PCI slot status

The PCI slots shown in the chassis view indicate the number of PCI slots and the numbers of each slot. Tooltips provide component status for each card in a PCI slot. For example, the tooltip for one NVRAM card model displays the memory size, temperature data, and battery levels.

For DD6900, DD9400, and DD9900 systems, the included GAT card is viewable by clicking on the PCI slot where it resides.

## NVRAM status

Hover over NVRAM to display information about the Non-Volatile RAM, batteries, and other components.

**Table 74** NVRAM tooltip, column label descriptions

Item	Description
Component	<p>The items in the component list depend on the NVRAM installed in the system and can include the following items.</p> <ul style="list-style-type: none"> <li>• Firmware version</li> <li>• Memory size</li> <li>• Error counts</li> <li>• Flash controller error counts</li> <li>• Board temperature</li> <li>• CPU temperature</li> <li>• Battery number (The number of batteries depends on the system type.)</li> <li>• Current slot number for NVRAM</li> </ul>
C/F	Displays the temperature for select components in the Celsius/Fahrenheit format.
Value	<p>Values are provided for select components and describe the following.</p> <ul style="list-style-type: none"> <li>• Firmware version number</li> <li>• Memory size value in the displayed units</li> <li>• Error counts for memory, PCI, and controller</li> <li>• Flash controller error counts sorted in the following groups: configuration errors (Cfg Err), panic conditions (Panic), Bus Hang, bad block warnings (Bad Blk Warn), backup errors (Bkup Err), and restore errors (Rstr Err)</li> </ul>

Table 74 NVRAM tooltip, column label descriptions (continued)

Item	Description
	<ul style="list-style-type: none"> <li>Battery information, such percent charged and status (enabled or disabled)</li> </ul>

## Viewing system statistics

The Realtime Charts panel displays up to seven graphs that show real-time subsystem performance statistics, such as CPU usage and disk traffic.

### Procedure

1. Select **Home > Realtime Charts**.  
The Performance Graphs area displays the currently selected graphs.
2. To change the selection of graphs to display, select and clear the checkboxes for graphs in the list box.
3. To view specific data-point information, hover over a graph point.
4. When a graph contains multiple data, you can use the checkboxes in the upper-right corner of the graph to select what to display. For example, if Read is not selected in the upper right of the disk activity graph, only write data is graphed.

### Results

Each graph shows usage over the last 200 seconds. Click **Pause** to temporarily stop the display. Click **Resume** to restart it and show points missed during the pause.

## Performance statistics graphs

The performance statistics graphs display statistics for key system components and features.

### DD Boost Active Connections

The DD Boost Active Connections graph displays the number of active DD Boost connections for each of the past 200 seconds. Separate lines within the graph display counts for Read (recovery) connections and Write (backup) connections.

### DD Boost Data Throughput

The DD Boost Data Throughput graph displays the bytes/second transferred for each of the past 200 seconds. Separate lines within the graph display the rates for data read from the system by DD Boost clients and data written to the system by DD Boost clients.

### Disk

The Disk graph displays the amount of data in the appropriate unit of measurement based on the data received, such as KiB or MiB per second, going to and from all disks in the system.

### File System Operations

The File System Operations graph displays the number of operations per second that occurred for each of the past 200 seconds. Separate lines within the graph display the NFS and CIFS operations per second.

**Network**

The Network graph displays the amount of data in the appropriate unit of measurement based on the data received, such as KIB or MiB per second, that passes through each Ethernet connection. One line appears for each Ethernet port.

**Recent CPU Usage**

The Recent CPU Usage graph displays the percentage of CPU usage for each of the past 200 seconds.

**Replication (DD Replicator must be licensed)**

The Replication graph displays the amount of replication data traveling over the network for each of the last 200 seconds. Separate lines display the In and Out data as follows:

- **In:** The total number of units of measurement, such as kilobytes per second, received by this side from the other side of the DD Replicator pair. For the destination, the value includes backup data, replication overhead, and network overhead. For the source, the value includes replication overhead and network overhead.
- **Out:** The total number of units of measurement, such as kilobytes per second, sent by this side to the other side of the DD Replicator pair. For the source, the value includes backup data, replication overhead, and network overhead. For the destination, the value includes replication and network overhead.

## Viewing active users

The Active Users tab displays the names of users who are logged into the system and statistics about the current user sessions.

**Procedure**

1. Select **Administration > Access > Active Users**.

The Active Users list appears and displays information for each user.

**Table 75** Active Users list, column label descriptions

Item	Description
Name	User name of the logged-in user.
Idle	Time since last activity of user.
Last Login From	System from which the user logged in.
Last Login Time	Datestamp of when user logged in.
TTY	Terminal notation for login. GUI appears for DD System Manager users.

 **Note:** To manage local users, click **Go to Local Users**.

## History report management

DD System Manager enables you to generate reports to track space usage on a protection system for up to the previous two years. You can also generate reports to help understand replication progress, and view daily and cumulative reports on the file system.

The Reports view is divided into two sections. The upper section lets you create the various types of reports. The lower section lets you view and manage saved reports.

Reports display in a table format, and as charts, depending on the type of report. You can select a report for a specific system and provide a specific time period.

The reports display historical data, not real-time data. After the report is generated, the charts remain static and do not update. Examples of the types of information you can get from the reports include:

- The amount of data that was backed up to the system and the amount of de-duplication that was achieved
- Estimates of when the system will be full, based on weekly space usage trends
- Backup and compression utilization based on selected intervals
- Historical cleaning performance, including duration of cleaning cycle, amount of space that can be cleaned, and amount of space that was reclaimed
- Amount of WAN bandwidth used by replication, for source and destination, and if bandwidth is sufficient to meet replication requirements
- System performance and resource utilization

### Types of reports

The New Report area lists the types of reports you can generate on your system.

**Note:** Replication reports can only be created if the system contains a replication license and a valid replication context is configured.

### File System Cumulative Space Usage report

The File System Cumulative Space Usage Report displays 3 charts that detail space usage on the system during the specified duration. This report is used to analyze how much data is backed up, the amount of deduplication performed, and how much space is consumed.

Table 76 File System—Usage chart label descriptions

Item	Description
Date Written (GiB)	The amount of data written before compression. This is indicated by a purple shaded area on the report.
Time	The timeline for data that was written. The time displayed on this report changes based upon the Duration selection when the chart was created.
Total Compression Factor	The total compression factor reports the compression ratio.

**Table 77** File System—Consumption chart label descriptions

Item	Description
Used (GiB)	The amount of space used after compression.
Time	The date the data was written. The time displayed on this report changes based upon the Duration selection when the chart was created.
Used (Post Comp)	The amount of storage used after compression.
Usage Trend	The dotted black line shows the storage usage trend. When the line reaches the red line at the top, the storage is almost full.
Capacity	The total capacity on a protection system.
Cleaning	Cleaning is the Cleaning cycle (start and end time for each cleaning cycle). Administrators can use this information to choose the best time for space cleaning the best throttle setting.

**Table 78** File System Weekly Cumulative Capacity chart label descriptions

Item	Description
Date (or Time for 24 hour report)	The last day of each week, based on the criteria set for the report. In reports, a 24-hour period ranges from noon-to-noon.
Data Written (Pre-Comp)	The cumulative data written before compression for the specified time period.
Used (Post-Comp)	The cumulative data written after compression for the specified time period.
Compression Factor	The total compression factor. This is indicated by a black line on the report.

## File System Daily Space Usage report

The File System Daily Space Usage report displays five charts that detail space usage during the specified duration. This report is used to analyze daily activities.

**Table 79** File System Daily Space Usage chart label descriptions

Item	Description
Space Used (GiB)	The amount of space used. Post-comp is red shaded area. Pre-Comp is purple shaded area.
Time	The date the data was written.
Compression Factor	The total compression factor. This is indicated by a black square on the report.



**Table 80** File System Daily Capacity Utilization chart label descriptions

Item	Description
Date	The date the data was written.
Data Written (Pre-Comp)	The amount of data written pre-compression.
Used (Post-Comp)	The amount of storage used after compression.
Total Compression Factor	The total compression factor.

**Table 81** File System Weekly Capacity Utilization chart label descriptions

Item	Description
Start Date	The first day of the week for this summary.
End Date	The last day of the week for this summary.
Available	Total amount of storage available.
Consumed	Total amount of storage used.
Data (Post -Comp)	The cumulative data written before compression for the specified time period.
Replication (Post-Comp)	The cumulative data written after compression for the specified time period.
Overhead	Extra space used for non-data storage.
Reclaimed by Cleaning	The total space reclaimed after cleaning.

**Table 82** File System Compression Summary chart label descriptions

Item	Description
Time	The period of data collection for this report.
Data Written (Pre-Comp)	The amount of data written pre-compression.
Used (Post-Comp)	The amount of storage used after compression.
Total Compression Factor	The total compression factor.

**Table 83** File System Cleaning Activity chart label descriptions

Item	Description
Start Time	The time the cleaning activity started.
End Time	The time the cleaning activity finished.
Duration (Hours)	The total time required for cleaning in hours.
Space Reclaimed	The space reclaimed in Gibibytes (GiB).

## Replication Status report

The Replication Status report displays three charts that provide the status of the current replication job running on the system. This report is used to provide a snapshot of what is

happening for all replication contexts to help understand the overall replication status on a protection System.

**Table 84** Replication Context Summary chart label descriptions

Item	Description
ID	The Replication Context identification.
Source	Source system name.
Destination	Destination system name.
Type	Type of replication context: MTree, Directory, Collection, or Pool.
Status	Replication status types include: Error, Normal.
Sync as of Time	Time and date stamp of last sync.
Estimated Completion	The estimated time the replication should be complete.
Pre-Comp Remaining	The amount of pre-compressed data to be replicated. This only applies to Collection type.
Post-Comp Remaining	The amount of post-compressed data to be replicated. This only applies to Directory and Pool types.

**Table 85** Replication Context Error Status chart label descriptions

Item	Description
ID	The Replication Context identification.
Source	Source system name.
Destination	Destination system name.
Type	Replication context type: Directory or Pool.
Status	Replication status types include: Error, Normal, and Warning.
Description	Description of the error.

**Table 86** Replication Destination Space Availability chart label descriptions

Item	Description
Destination	Destination system name.
Space Availability (GiB)	Total amount of storage available.

## Replication Summary report

The Replication Summary report provides performance information about a system's overall network in-and-out usage for replication, as well as per context levels over a specified duration. You select the contexts to be analyzed from a list.

**Table 87** Replication Summary report label descriptions

Item	Description
Network In (MiB)	The amount of data entering the system. Network In is indicated by a thin green line.
Network Out (MiB)	The amount of data sent from the system. Network Out is indicated by a thick orange line.
Time	The date on which the data was written.
Pre-Comp Remaining (MiB)	The amount of pre-compressed data to be replicated. Pre-Comp Remaining is indicated by a blue line.

## Viewing the Task Log

The Task Log displays a list of currently running jobs, such as, replication or system upgrades. DD System Manager can manage multiple systems and can initiate tasks on those systems. If a task is initiated on a remote system, the progress of that task is tracked in the management station task log, not in the remote system task log.

### Procedure

1. Select **Health > Jobs**.  
The Tasks view appears.
2. Select a filter by which to display the Task Log from the Filter By list box. You can select **All**, **In Progress**, **Failed**, or **Completed**.  
The Tasks view displays the status of all tasks based on the filter you select and refreshes every 60 seconds.
3. To manually refresh the Tasks list, do either of the following.
  - Click **Update** to update the task log.
  - Click **Reset** to display all tasks and remove any filters that were set.
4. To display detailed information about a task, select the task in the task list.

**Table 88** Detailed Information, label descriptions

Item	Description
System	The system name.
Task Description	A description of the task.
Status	The status of the task (completed, failed, or in progress).
Start Time	The date and time the task started.

Table 88 Detailed information, label descriptions (continued)

Item	Description
End Time	The date and time the task ended.
Error Message	An applicable error message, if any.

## Viewing the system High Availability status

You can use the **High Availability** panel to see detailed information about the HA status of the system and whether the system can perform failover if necessary.

### Procedure

1. Select **Health > High Availability** on the DD System Manager.  
The **Health High Availability** screen appears.  
A green check mark indicates the system is operating normally and ready for failover.  
The screen shows the active node, which is typically Node 0.
2. Hover the cursor over a node to see its status.  
The node is highlighted in blue if it is active.
3. Click the drop-down menu in the banner if you want to change the view from the active node to the standby node, which is typically Node 1.

## High Availability status

The **Health High Availability (HA)** view informs you about the system status using a diagram of the nodes and their connected storage. In addition, you can also see any current alerts as well as detailed information about the system.

You can determine if the active node and the storage are operational by hovering the cursor over them. Each is highlighted in blue when operating normally. The standby node should appear gray.

You can also filter the alerts table by clicking on a component. Only alerts related to the selected components will be displayed.

Figure 6 Health/High Availability indicators

Health: High Availability

**HA System Highly Available** The HA System is operating normally and is ready to failover. [Failover to Node 0](#) [Take Node 0 Offline](#)

**System Information**

Model: DD9600  
 Type: DD HA System  
 OS: 5.7.0.51-511967  
 License: Active-Standby

**HA Manager**

The diagram shows two nodes connected by a Networking line. Node 0 is in Standby mode and Node 1 is in Active mode. Both nodes are connected to a shared Storage unit. SAS 0 is connected to Node 0 and SAS 1 is connected to Node 1.

Severity	Component	Class	Post Time
No Alerts			

No Alert selected. Select one Alert to see Detailed Information.

Table 89 High Availability indicators

Item	Description
HA System bar	Displays a green check mark when the system is operating normally and ready for failover.
Failover to Node 0	Allows you to manually fail over to the standby node.
Take Node 1 Offline	Allows you to take the active node offline if necessary.
System Information	Lists the protection system model, the system type, the DD OS version in use, and the applied HA license.
HA Manager	Displays the nodes, their attached storage, the HA interconnect, and the cabling.
Severity	Indicates the severity of any alerts that could impact the system's HA status.
Component	Indicates which component is affected.
Class	Indicates the class of the alert received such as hardware, environment, and others.
Post Time	Indicates the time and date the alert was posted.

11/11/2011 10:11:11 AM

Device	IP Address	Port	Protocol	Status	Last Seen
192.168.1.1	192.168.1.1	80	TCP	Open	11/11/2011 10:11:11 AM
192.168.1.2	192.168.1.2	80	TCP	Open	11/11/2011 10:11:11 AM
192.168.1.3	192.168.1.3	80	TCP	Open	11/11/2011 10:11:11 AM
192.168.1.4	192.168.1.4	80	TCP	Open	11/11/2011 10:11:11 AM
192.168.1.5	192.168.1.5	80	TCP	Open	11/11/2011 10:11:11 AM
192.168.1.6	192.168.1.6	80	TCP	Open	11/11/2011 10:11:11 AM
192.168.1.7	192.168.1.7	80	TCP	Open	11/11/2011 10:11:11 AM
192.168.1.8	192.168.1.8	80	TCP	Open	11/11/2011 10:11:11 AM
192.168.1.9	192.168.1.9	80	TCP	Open	11/11/2011 10:11:11 AM
192.168.1.10	192.168.1.10	80	TCP	Open	11/11/2011 10:11:11 AM

# CHAPTER 5

## File System

This chapter includes:

- File system overview..... 182
- Monitoring file system usage..... 188
- Managing file system operations..... 195
- Fast copy operations..... 203



## File system overview

Learn how to use the file system.

### How the file system stores data

Storage capacity is best managed by keeping multiple backups and 20 percent empty space to accommodate backups until the next cleaning. Space use is primarily affected by the size and compressibility of data, and the retention period.

A protection system is designed as a very reliable online system for backups and archive data. As new backups are added to the system, old backups are aged out. Such removals are normally done under the control of backup or archive software based on the configured retention period.

When backup software expires or deletes an old backup from a system, the space on the system becomes available only after the cleans the data of the expired backups from disk. A good way to manage space is to retain as many online backups as possible with some empty space (about 20 percent of total space available) to comfortably accommodate backups until the next scheduled cleaning, which runs once a week by default.

Some storage capacity is used for internal indexes and other metadata. The amount of storage used over time for metadata depends on the type of data stored and the sizes of the stored files. With two otherwise identical systems, one system may, over time, reserve more space for metadata and have less space for actual backup data than the other if different data sets are sent to each system.

Space utilization is primarily affected by:

- The size and compressibility of the backup data.
- The retention period specified in the backup software.

High levels of compression result when backing up data sets with many duplicates and retaining them for long periods of time.

### How the file system reports space usage

All DD System Manager windows and system commands display storage capacity using base 2 calculations. For example, a command that displays 1 GiB of disk space as used reports  $2^{30}$  bytes = 1,073,741,824 bytes.

- 1 KiB =  $2^{10}$  = 1024 bytes
- 1 MiB =  $2^{20}$  = 1,048,576 bytes
- 1 GiB =  $2^{30}$  = 1,073,741,824 bytes
- 1 TiB =  $2^{40}$  = 1,099,511,627,776 bytes

### How the file system uses compression

The file system uses compression to optimize available disk space when storing data, so disk space is calculated two ways: physical and logical. (See the section regarding types of compression.) Physical space is the actual disk space used on the protection system. Logical space is the amount of uncompressed data written to the system.

The file system space reporting tools (DD System Manager graphs and `filesys show space` command, or the alias `df`) show both physical and logical space. These tools also report the size and amounts of used and available space.

When a system is mounted, the usual tools for displaying a file system's physical use of space can be used.

The system generates warning messages as the file system reaches 90%, 95%, and 100% of capacity. The following information about data compression gives guidelines for disk use over time.

The amount of disk space used over time depends on:

- The size of the initial full backup.
- The number of additional backups (incremental and full) retained over time.
- The rate of growth of the backup dataset.
- The change rate of data.

For data sets with typical rates of change and growth, data compression generally matches the following guidelines:

- For the first full backup to a protection system, the compression factor is generally 3:1.
- Each incremental backup to the initial full backup has a compression factor of approximately 6:1.
- The next full backup has a compression factor of about 60:1.

Over time, with a schedule of weekly full and daily incremental backups, the aggregate compression factor for all the data is about 20:1. The compression factor is lower for incremental-only data or for backups with less duplicate data. Compression is higher when all backups are full backups.

## Types of compression

DD OS compresses data at two levels: global and local. Global compression compares received data to data already stored on disks. Duplicate data does not need to be stored again, while data that is new is locally compressed before being written to disk.

### Local Compression

A protection system uses a local compression algorithm developed specifically to maximize throughput as data is written to disk. The lz algorithm allows shorter backup windows for backup jobs but uses more space. Two other types of local compression are available, gzfast and gz. Both provide increased compression over lz, but at the cost of additional CPU load. Local compression options provide a trade-off between slower performance and space usage. It is also possible to turn off local compression. To change compression, see *Changing local compression* on page 201.

After you change the compression, all new writes use the new compression type. Existing data is converted to the new compression type during cleaning. It takes several rounds of cleaning to recompress all of the data that existed before the compression change.

The initial cleaning after the compression change might take longer than usual. Whenever you change the compression type, carefully monitor the system for a week or two to verify that it is working properly.

All systems except the DD6900, DD9400, and DD9900 systems use the lz compression algorithm as the default local compression type. DD6900, DD9400, and DD9900 systems use the gzfast algorithm as the default local compression type.

PowerProtect DD6900, DD9400, and DD9900 systems come with a hardware accelerator card to support Intel Quick Assist Technology (QAT) in combination with gzfast compression. DD OS offloads compression and decompression work to the hardware accelerator to achieve a higher compression ratio and free up CPU resources to improve system performance. Gzfast is the default local compression type on all DD6900, DD9400, and DD9900 systems. No additional configuration is required.

## How the file system implements data integrity

Multiple layers of data verification are performed by the DD OS file system on data received from backup applications to ensure that data is written correctly to the system disks. This ensures 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

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.

### Fault avoidance and containment

DD OS uses a log-structured file system that never overwrites or updates existing data. New data is always written in new containers and appended to existing old containers. The old containers and references remain in place and are safe even in the face of software bugs or hardware faults that may occur when storing new backups.

### Continuous fault detection and healing

Continuous fault detection and healing protects against storage system faults. The system periodically rechecks the integrity of the RAID stripes, and uses the redundancy of the RAID system to heal any faults. During a read, data integrity is re-verified and any errors are healed on the fly.

### File system recoverability

Data is written in a self-describing format. The file system can be re-created, if necessary, by scanning the log and rebuilding it from the metadata stored with the data.

## How the file system reclaims storage space with file system cleaning

When the backup application (such as NetBackup or NetWorker) expires data, the data is marked for deletion. However, the data is not deleted immediately; it is removed during a cleaning operation.

- During the cleaning operation, the file system is available for all normal operations including backup (write) and restore (read).
- Although cleaning uses a significant amount of system resources, cleaning is self-throttling and gives up system resources in the presence of user traffic.
- Dell EMC recommends running a cleaning operation after the first full backup to a protection system. The initial local compression on a full backup is generally a factor of 1.5 to 2.5. An immediate cleaning operation gives additional compression by another factor of 1.15 to 1.2 and reclaims a corresponding amount of disk space.
- When the cleaning operation completes, a message is sent to the system log giving the percentage of storage space that was reclaimed.

A default schedule runs the cleaning operation every Tuesday at 6 a.m. (tue 0600). To change the schedule or run the operation manually, see the section regarding modifying a cleaning schedule.

Dell EMC recommends running the cleaning operation once a week.

Any operation that disables the file system, or shuts down a system during a cleaning operation (such as a system power-off or reboot) aborts the cleaning operation. The cleaning operation does not immediately restart when the system restarts. You can manually restart the cleaning operation or wait until the next scheduled cleaning operation.

With collection replication, data in a replication context on the source system that has not been replicated cannot be processed for file system cleaning. If file system cleaning is not able to complete because the source and destination systems are out of sync, the system reports the status of the cleaning operation as `partial`, and only limited system statistics are available for the cleaning operation. If collection replication is disabled, the amount of data that cannot be processed for file system cleaning increases because the replication source and destination systems remain out of sync. The KB article *Data Domain: An overview of Data Domain File System (DDFS) clean/garbage collection (GC) phases*, available from the Online Support site at <https://support.emc.com> provides additional information.

With MTree replication, if a file is created and deleted while a snapshot is being replicated, then the next snapshot will not have any information about this file, and the system will not replicate any content associated with this file. Directory replication will replicate both the create and delete, even though they happen close to each other.

With the replication log that directory replication uses, operations like deletions, renaming, and so on, execute as a single stream. This can reduce the replication throughput. The use of snapshots by MTree replication avoids this problem.

## Supported interfaces

Interfaces supported by the file system.

- NFS
- CIFS
- DD Boost
- DD VTL

## Supported backup software

Guidance for setting up backup software and backup servers to use with protection systems is available at [support.emc.com](https://support.emc.com).

## Data streams sent to a protection system

For optimal performance, Dell EMC recommends limits on simultaneous streams between Data Domain and PowerProtect systems, and your backup servers.

A data stream, in the context of the following table, refers to a large byte stream associated with sequential file access, such as a write stream to a backup file or a read stream from a restore image. A Replication source or destination stream refers to a directory replication operation or a DD Boost file replication stream associated with a file replication operation.

Table 90 Data streams sent to a protection system

Model	RAM / NVRAM	Backup write streams	Backup read streams	Repl <sup>®</sup> source streams	Repl <sup>®</sup> dest streams	Mixed
DD2200	8 GB	35	6	18	20	w<=35; r<=6; ReplSrc<=18; ReplDest<=20; ReplDest +w<=35; Total<=35

Table 90 Data streams sent to a protection system (continued)

Model	RAM / NVRAM	Backup write streams	Backup read streams	Repl <sup>®</sup> source streams	Repl <sup>®</sup> dest streams	Mixed
DD2200	16 GB	60	16	30	60	w<=60; r<=16; ReplSrc<=30; ReplDest<=60; ReplDest+w<=60; Total<=60
DD6300	48 or 96 GB / 8 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest+w<=270; Total<=270
DD6800	192 GB / 8 GB	400	110	220	400	w<=400; r<=110; ReplSrc<=220; ReplDest<=400; ReplDest+w<=400; Total<=400
DD6900	288 GB / 16 GB	400	110	220	400	w<=400; r<=110; ReplSrc<=220; ReplDest<=400; ReplDest+w<=400; Total<=400
DD9300	192 or 384 GB / 8 GB	800	220	440	800	w<=800; r<=220; ReplSrc<=440; ReplDest<=800; ReplDest+w<=800; Total<=800
DD9400	576 GB / 16 GB	800	220	440	800	w<=800; r<=220; ReplSrc<=440; ReplDest<=800; ReplDest+w<=800; Total<=800
DD9500	256 or 512 GB / 8 GB	1885	300	540	1080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest+w<=1080; Total<=1885
DD9800	256 or 768 GB / 8 GB	1885	300	540	1080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest+w<=1080; Total<=1885
DD9900	1152 GB / 16 GB	1885	300	540	1080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest+w<=1080; Total<=1885
DD VE 8 TB	8 GB / 512 MB	20	16	20	20	w<= 20 ; r<= 16 ReplSrc<=20; ReplDest<=20; ReplDest+w<=20; w+r+ReplSrc<=20; Total<=20
DD VE 16 TB	16 GB / 512 MB or 24 GB / 1 GB	45	30	45	45	w<= 45 ; r<= 30 ReplSrc<=45; ReplDest<=45; ReplDest+w<=45; w+r+ReplSrc<=45; Total<=45



Table 90 Data streams sent to a protection system (continued)

Model	RAM / NVRAM	Backup write streams	Backup read streams	Repl <sup>a</sup> source streams	Repl <sup>a</sup> dest streams	Mixed
DD VE 32 TB	24 GB / 1 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest +w<=90; w+r+ReplSrc <=90;Total<=90
DD VE 48 TB	36 GB / 1 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest +w<=90; w+r+ReplSrc <=90;Total<=90
DD VE 64 TB	48 GB / 1 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest +w<=90; w+r+ReplSrc <=90;Total<=90
DD VE 96 TB	64 GB / 2 GB	180	50	90	180	w<= 180 ; r<= 50 ReplSrc<=90; ReplDest<=180; ReplDest+w<=180; w+r +ReplSrc <=180;Total<=180
DD3300 4 TB	12 GB (virtual memory) / 512 MB	20	16	30	20	w<= 20 ; r<= 16 ReplSrc<=30; ReplDest<=20; ReplDest +w<=20; w+r+ReplSrc <=30;Total<=30
DD3300 8 TB	32 GB (virtual memory) / 1.536 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest +w<=90; w+r+ReplSrc <=90;Total<=90
DD3300 16 TB	32 GB (virtual memory) / 1.536 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest +w<=90; w+r+ReplSrc <=90;Total<=90
DD3300 32 TB	46 GB (virtual memory) / 1.536 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest +w<=90; w+r+ReplSrc <=90;Total<=140

a. DirRepl, OptDup, MTreeRepl streams

## File system limitations

File system limitations, including: limits on the number of files, the battery, and so on.

### Limits on number of files in a protection system

Consequences and considerations of storing more than 1 billion files.

Dell EMC recommends storing a total of no more than 1 billion files on a system. This limitation applies to the combined number of files stored in both the Active and Cloud storage tiers. Storing a larger number of files can adversely affect the performance and the length of cleaning, and some processes, such as file system cleaning, may run much longer with a very large number of files. For

example, the enumeration phase of cleaning may take from a few minutes to several hours depending upon the number of files in the system.

- i** Note: The overall system performance will fall to unacceptable levels if the system is required to support the maximum file amount and the workload from the client machines is not carefully controlled.

When the file system passes the billion file limit, several processes or operations might be adversely affected, for example:

- Cleaning may take a very long time to complete, perhaps several days.
- AutoSupport operations may take more time.
- Any process or command that needs to enumerate all the files.

If there are many small files, other considerations arise:

- The number of separate files that can be created per second, (even if the files are very small) may be more of a limitation than the number of MB/s that can be ingested. When files are large, the file creation rate is not significant, but when files are small, the file creation rate dominates and may become a factor. The file creation rate is about 100 to 200 files per second depending upon the number of MTrees and CIFS connections. This rate should be taken into account during system sizing when a bulk ingest of a large number of files is needed by a customer environment.
- File access latencies are affected by the number of files in a directory. To the extent possible, we recommend directory sizes of less than 250,000. Larger directory sizes might experience slower responses to metadata operations such as listing the files in the directory and opening or creating a file.

### Limits on the battery

For systems that use NVRAM, the operating system creates a low battery alert if the battery charge falls below 80% capacity, and the file system is disabled.

- i** NOTICE The DD2200 system does not use NVRAM so firmware calculations decide whether the battery charge is sufficient to save the data and disable the file system if there is a loss of AC power.

### Maximum number of supported inodes

An NFS or CIFS client request causes a protection system to report a capacity of about two billion inodes (files and directories). Systems can exceed that number, but the reporting on the client may be incorrect.

### Maximum path name length

The maximum length of a full path name (including the characters in `/data/coll/backup`) is 1023 characters. The maximum length of a symbolic link is also 1023 characters.

### Limited access during HA failover

Access to files may be interrupted for up to 10 minutes during failover on High Availability systems. (DD Boost and NFS require additional time.)

## Monitoring file system usage

View real-time data storage statistics.

The File System view has tabs and controls that provide access to real-time data storage statistics, cloud unit information, encryption information, and graphs of space usage amounts.



consumption factors, and data written trends. There are also controls for managing file system cleaning, expansion, copying, and destruction.

## Accessing the file system view

This section describes the file system functionality.

### Procedure

- Select **Data Management > File System**.

## About the File System Status panel

Display the status of file system services.

To access the File System Status panel, click **Data Management > File System > ^** in the lower-right corner of the screen.

### File System

The **File System** field contains an **Enable/Disable** link and shows the working state of the file system:

- Enabled and running—and the latest consecutive length of time the file system has been enabled and running.
- Disabled and shutdown.
- Enabling and disabling—in the process of becoming enabled or disabled.
- Destroyed—if the file system is deleted.
- Error—if there is an error condition, such as a problem initializing the file system.

### Cloud File Recall

The **Cloud File Recall** field contains a **Recall** link to initiate a file recall from the Cloud Tier. A **Details** link is available if any active recalls are underway. For more information, see the "Recalling a File from the Cloud Tier" topic.

### Physical Capacity Measurement

The **Physical Capacity Measurement** field contains an **Enable** button when physical capacity measurement status is disabled. When enabled, the system displays **Disable** and **View** buttons. Click **View** to see currently running physical capacity measurements: MTree, priority, submit time, start time, and duration.

### Data Movement

The **Data Movement** field contains **Start/Stop** buttons and shows the date the last data movement operation finished, the number of files copied, and the amount of data copied. The system displays a **Start** button when the data movement operation is available, and a **Stop** when a data movement operation is running.

### Active Tier Cleaning

The **Active Tier Cleaning** field contains a **Start/Stop** button and shows the date the last cleaning operation occurred, or the current cleaning status if the cleaning operation is currently running. For example:

Cleaning finished at 2009/01/13 06:00:43

or, if the file system is disabled, shows:

Unavailable

### Cloud Tier Cleaning

The **Cloud Tier Cleaning** field contains a **Start/Stop** button and shows the date the last cleaning operation occurred, or the current cleaning status if the cleaning operation is currently running. For example:

Cleaning finished at 2009/01/13 06:00:43

or, if the file system is disabled, shows:

Unavailable

### About the Summary tab

Click the **Summary** tab to show space usage statistics for the active and cloud tiers and to access controls for viewing file system status, configuring file system settings, performing a **Fast Copy** operation, expand capacity, and destroy the file system.

For each tier, space usage statistics include:

- **Size**—The amount of total physical disk space available for data.
- **Used**—The actual physical space used for compressed data. Warning messages go to the system log and an email alert is generated when the use reaches 90%, 95%, and 100%. At 100%, the system accepts no more data from backup servers. If the **Used** amount is always high, check the cleaning schedule to see how often the cleaning operation runs automatically. Then use the **modifying a cleaning schedule** procedure to run the operation more often. Also consider reducing the data retention period or splitting off a portion of the backup data to another system.
- **Available (GiB)**—The total amount of space available for data storage. This figure can change because an internal index may expand as the system fills with data. The index expansion takes space from the **Avail GiB** amount.
- **Pre-Compression (GiB)**—Data written before compression.
- **Total Compression Factor (Reduction %)**— $\text{Pre-Comp} / \text{Post-Comp}$ .
- **Cleanable (GiB)**—The amount of space that could be reclaimed if a cleaning were run.

For Cloud Tier, the **Cloud File Recall** field contains a **Recall** link to initiate a file recall from the Cloud Tier. A **Details** link is available if any active recalls are underway. For more information, see the "Recalling a File from the Cloud Tier" topic.

Separate panels provide the following statistics for the last 24 hours for each tier:

- **Pre-Compression (GiB)**—Data written before compression.
- **Post-Compression (GiB)**—Storage used after compression.
- **Global Compression Factor**— $(\text{Pre-Compression} / (\text{Size after global compression}))$ .
- **Local Compression Factor**— $(\text{Size after global compression} / \text{Post-Compression})$ .
- **Total Compression Factor (Reduction %)**— $[(\text{Pre-Comp} - \text{Post-Comp}) / \text{Pre-Comp}] * 100$ .

### About file system settings

Display and change system options as well as the current cleaning schedule.

To access the File System Settings dialog, click **Data Management > File System > Settings**.

Table 91 General settings

General settings	Description
Local Compression Type	The type of local compression in use. <ul style="list-style-type: none"> <li>See the section regarding types of compression for an overview.</li> <li>See the section regarding changing local compression</li> </ul>
Cloud Tier Local Comp	The type of compression in use for the cloud tier. <ul style="list-style-type: none"> <li>See the section regarding types of compression for an overview.</li> <li>See the section regarding changing local compression</li> </ul>
Report Replica as Writable	How applications see a replica. <ul style="list-style-type: none"> <li>See the section regarding changing read-only settings</li> </ul>
Staging Reserve	Manage disk staging. <ul style="list-style-type: none"> <li>See the section regarding working with disk staging</li> <li>See the section regarding configuring disk staging</li> </ul>
Marker Type	Backup software markers (tape markers, tag headers, or other names are used) in data streams. See the section regarding tape marker settings
Throttle	See the section regarding setting the physical capacity measurement throttle.
Cache	Physical Capacity Cache initialization cleans up the caches and enhances the measuring speed.

Adjust the workload balance of the file system to increase performance based on your usage.

Table 92 Workload Balance settings

Workload Balance settings	Description
Random workloads (%)	Instant access and restores perform better using random workloads.
Sequential workloads (%)	Traditional backups and restores perform better with sequential workloads.

Table 93 Data Movement settings

Data movement policy settings	Description
File Age Threshold	When data movement starts, all files that have not been modified for the specified threshold number of days will be moved from the active to the retention tier.
Schedule	Days and times data is moved.
Throttle	The percentage of available resources the system uses for data movement. A throttle value of 100% is the default throttle and means that data movement will not be throttled.

Table 94 Cleaning settings

Cleaning schedule settings	Description
Time	The date time cleaning operations run. <ul style="list-style-type: none"> <li>• See the section regarding modifying a cleaning schedule</li> </ul>
Throttle	The system resources allocation. <ul style="list-style-type: none"> <li>• See the section regarding throttling the cleaning operation</li> </ul>

### About the Cloud Units tab

Display summary information for cloud units, add and modify cloud units, and manage certificates.

The Cloud Units tab on the File System page is shown only when the optional Cloud Tier license is enabled. This view lists summary information (status, network bandwidth, read access, local compression, data movement and data status) the name of the cloud provider, the used capacity, and the licensed capacity. Controls are provided for editing the cloud unit, managing certificates, and adding a new cloud unit.

### About the DD Encryption tab

Display encryption status, progress, algorithms, and so on.

Table 95 DD Encryption settings

Setting	Description
DD System	Status can be one of the following: <ul style="list-style-type: none"> <li>• Not licensed—No other information provided.</li> <li>• Not configured—Encryption is licensed but not configured.</li> <li>• Enabled—Encryption is enabled and running.</li> <li>• Disabled—Encryption is disabled.</li> </ul>
Active Tier	View encryption status for the active tier: <ul style="list-style-type: none"> <li>• Enabled—Encryption is enabled and running.</li> <li>• Disabled—Encryption is disabled.</li> </ul>
Cloud Unit	View encryption status per cloud unit: <ul style="list-style-type: none"> <li>• Enabled—Encryption is enabled and running.</li> <li>• Disabled—Encryption is disabled.</li> </ul>
Encryption Progress	View encryption status details for the active tier regarding the application of changes and re-encryption of data. Status can be one of the following: <ul style="list-style-type: none"> <li>• None</li> <li>• Pending</li> <li>• Running</li> <li>• Done</li> </ul>

Table 95 DD Encryption settings (continued)

Setting	Description
	<p>Click <b>View Details</b> to display the <b>Encryption Status Details</b> dialog that includes the following information for the <b>Active Tier</b>:</p> <ul style="list-style-type: none"> <li>Type (Example: <b>Apply Changes</b> when encryption has already been initiated, or <b>Re-encryption</b> when encryption is a result of compromised data—perhaps a previously destroyed key.)</li> <li>Status (Example: <b>Pending</b>)</li> <li>Details: (Example: <b>Requested on December xx/xx/xx and will take after the next system clean.</b>)</li> </ul>
Encryption Algorithm	<p>The algorithm used to encrypt the data:</p> <ul style="list-style-type: none"> <li>AES 256-bit (CBC) (default)</li> <li>AES 256-bit (GCM) (more secure but slower)</li> <li>AES 128-bit (CBC) (not as secure as 256-bit)</li> <li>AES 128-bit (GCM) (not as secure as 256-bit)</li> </ul> <p>See <b>Changing the Encryption Algorithm</b> for details.</p>
Encryption Passphrase	When configured, shows as "*****." To change the passphrase, see <b>Managing the System Passphrase</b> .
File System Lock	
Status	<p>The File System Lock status is either:</p> <ul style="list-style-type: none"> <li>Unlocked—The feature is not enabled.</li> <li>Locked—The feature is enabled.</li> </ul>
Key Management	
Key Manager	The internal Embedded Key Manager or the optional KeySecure Key Manager. Click <b>Configure</b> to modify Key Manager options.
FIPS mode	Whether or not the imported host certificate is FIPS compliant. The default mode is enabled.
Encryption Keys	<p>Lists keys by ID numbers. Shows when a key was created, how long it is valid, its type, its state, and the amount of the data encrypted with the key. The system displays the last updated time for key information above the right column. Selected keys in the list can be:</p> <ul style="list-style-type: none"> <li>Deleted.</li> <li>Destroyed.</li> </ul>

### About the space usage view (file system)

Display a visual (but static) representation of data use for the file system at certain points in time.

Click **Data Management > File System > Charts**. Select **Space Usage** from the Chart drop-down list.

Click a point on a graph line to display data at that point. The lines of the graph denote measurements for:

- **Pre-comp Written**—The total amount of data sent to the MTree by backup servers. Pre-compressed data on an MTree is what a backup server sees as the total uncompressed data held by an MTree-as-storage-unit, shown with the Space Used (left) vertical axis of the graph.
- **Post-comp Used**—The total amount of disk storage in use on the MTree, shown with the Space Used (left) vertical axis of the graph.
- **Comp Factor**—The amount of compression performed with the data received (compression ratio), shown with the Compression Factor (right) vertical axis of the graph.

#### Checking Historical Space Usage

On the Space Usage graph, clicking a Date Range (that is, 1w, 1m, 3m, 1y, or All) above the graph lets you change the number of days of data shown on the graph, from one week to all.

### About the consumption view

Display space used over time, in relation to total system capacity.

Click **Data Management > File System > Charts**. Select **Consumption** from the Chart drop-down list.

Click a point on a graph line to display data at that point. The lines of the graph denote measurements for:

- **Capacity**—The total amount of disk storage available for data on the system. The amount is shown with the Space Used (left) vertical axis of the graph. Clicking the Capacity checkbox toggles this line on and off.
- **Post-comp**—The total amount of disk storage in use on the system. Shown with the Space Used (left) vertical axis of the graph.
- **Comp Factor**—The amount of compression performed with the data received (compression ratio). Shown with the Compression Factor (right) vertical axis of the graph.
- **Cleaning**—A grey diamond is displayed on the chart each time a file system cleaning operation was started.
- **Data Movement**—The amount of disk space moved to the cloud storage area (if the Cloud Tier license is enabled).

#### Checking Historical Consumption Usage

On the Consumption graph, clicking a Date Range (that is, 1w, 1m, 3m, 1y, or All) above the graph lets you change the number of days of data shown on the graph, from one week to all.

### About the daily written view (file system)

Display the flow of data over time. The data amounts are shown over time for pre- and post-compression amounts.

Click **Data Management > File System > Charts**. Select **Daily Written** from the Chart drop-down list.

Click a point on a graph line to display a box with data at that point. The lines on the graph denote measurements for:

- **Pre-Comp Written**—The total amount of data written to the file system by backup servers. Pre-compressed data on the file system is what a backup server sees as the total uncompressed data held by the file system.
- **Post-Comp Written**—The total amount of data written to the file system after compression has been performed, as shown in GiBs.
- **Total Comp Factor**—The total amount of compression performed with the data received (compression ratio), shown with the Total Compression Factor (right) vertical axis of the graph.



### Checking Historical Written Data

On the Daily Written graph, clicking a Date Range (that is, 1w, 1m, 3m, 1y, or All) above the graph lets you change the number of days of data shown on the graph, from one week to all.

### When the file system is full or nearly full

Protection systems have three progressive levels of being full. As each level is reached, more operations are progressively disallowed. At each level, deleting data and then performing a file system cleaning operation makes disk space available.

- i Note: The process of deleting files and removing snapshots does not immediately reclaim disk space, the next cleaning operation reclaims the space.
- Level 1—At the first level of fullness, no more new data can be written to the file system. An informative out of space alert is generated.  
Remedy—Delete unneeded datasets, reduce the retention period, delete snapshots, and perform a file system cleaning operation.
- Level 2—At the second level of fullness, files cannot be deleted. This is because deleting files also require free space but the system has so little free space available that it cannot even delete files.  
Remedy—Expire snapshots and perform a file system cleaning operation.
- Level 3—At the third and final level of fullness, attempts to expire snapshots, delete files, or write new data fail.  
Remedy—Perform a file system cleaning operation to free enough space to at least delete some files or expire some snapshots and then rerun cleaning.

### Monitor the space usage with email alerts

Alerts are generated when the file system is at 90%, 95%, and 100% full. To send these alerts, add the user to the alert emailing list.

- i Note: To join the alert email list, see Viewing and Clearing Alerts.

## Managing file system operations

This section describes file system cleaning, sanitization, and performing basic operations.

### Performing basic operations

Basic file system operations include enabling and disabling the file system, and in the rare occasion, destroying a file system.

#### Creating the file system

Create a file system from the Data Management > File System page using the Summary tab.

##### About this task

There are three reasons to create a file system:

- For a new system.
- When a system is started after a clean installation.
- After a file system has been destroyed.

To create the file system:



**Procedure**

1. Verify that storage has been installed and configured (see the section on viewing system storage information for more information). If the system does not meet this prerequisite, a warning message is displayed. Install and configure the storage before attempting to create the file system.
2. Select **Data Management > File System > Summary > Create**.


The File System Create Wizard is launched. Follow the instructions provided.

**Enabling or disabling the file system**

The option to enable or disable the file system is dependent on the current state of the file system—if its enabled, you can disable it and vice versa.

**About this task**

- Enabling the file system allows system operations to begin. This ability is available to administrative users only.
- Disabling the file system halts all system operations, including cleaning. This ability is available to administrative users only.

 **CAUTION** Disabling the file system when a backup application is sending data to the system can cause the backup process to fail. Some backup software applications are able to recover by restarting where they left off when they are able to successfully resume copying files; others might fail, leaving the user with an incomplete backup.

**Procedure**

1. Select **Data Management > File System > Summary**.
2. For **File System**, click **Enable** or **Disable**.
3. On the confirmation dialog, click **Close**.

**Expanding the file system**

You might need to expand the size of a file system if the suggestions given in "When the File System Is Full or Nearly Full" do not clear enough space for normal operations.


**About this task**

A file system may not be expandable, however, for these reasons:

- The file system is not enabled.
- There are no unused disks or enclosures in the Active or Cloud tiers.
- An expanded storage license is not installed.
- There are not enough capacity licenses installed.

DD6300 systems support the option to use ES30 enclosures with 4 TB drives ( 43.6 TiB) at 50% utilization (21.8 TiB) in the active tier if the available licensed capacity is exactly 21.8 TiB. The following guidelines apply to using partial capacity shelves.

- No other enclosure types or drive sizes are supported for use at partial capacity.
- A partial shelf can only exist in the Active tier.
- Only one partial ES30 can exist in the Active tier.
- Once a partial shelf exists in a tier, no additional ES30s can be configured in that tier until the partial shelf is added at full capacity.

 **Note:** This requires licensing enough additional capacity to use the remaining 21.8 TiB of the partial shelf.

- If the available capacity exceeds 21.8 TB, a partial shelf cannot be added.
- Deleting a 21 TiB license will not automatically convert a fully-used shelf to a partial shelf. The shelf must be removed, and added back as a partial shelf.


For DD6900, DD9400, and DD9900 systems, storage capacity licenses are available in increments of 60 TB raw (48 TB usable) capacity. Therefore, systems with 8 TB drives may encounter situations where the licensed capacity does not the full capacity of the disks installed in the disk shelves. For example, if a system has a licensed capacity of 48 TB usable capacity, and has one pack of 8 TB disks for a total of 96 TB usable capacity, only half the system capacity is available for use.

To expand the file system:

#### Procedure

1. Select **Data Management > File System > Summary > Expand Capacity**.

The Expand File System Capacity wizard is launched. The **Storage Tier** drop-down list always contains Active Tier, and it may contain Cloud Tier as a secondary choice. The wizard displays the current capacity of the file system for each tier as well as how much additional storage space is available for expansion.

 Note: File system capacity can be expanded only if the physical disks are installed on the system and file system is enabled.


2. From the **Storage Tier** drop-down list, select a tier.
3. In the **Addable Storage** area, select the storage devices to use and click **Add to Tier**.
4. Follow the instructions in the wizard. When the confirmation page is displayed, click **Close**.


## Destroying the file system

Destroying the file system should be done only under the direction of Customer Support. This action deletes all data in the file system, including virtual tapes. Deleted data is not recoverable. This operation also removes Replication configuration settings.

#### About this task

This operation is used when it is necessary to clean out existing data, to create a new collection replication destination, or to replace a collection source, or for security reasons because the system is being removed from operation.

 **CAUTION** The optional **Write zeros to disk** operation writes zeros to all file system disks, effectively removing all traces of data. If the system contains a large amount of data, this operation can take many hours, or a day, to complete.

 Note: As this is a destructive procedure, this operation is available to administrative users only.

#### Procedure

1. Select **Data Management > File System > Summary > Destroy**.
2. In the Destroy File System dialog box, enter the sysadmin password (it is the only accepted password).
3. Optionally, click the checkbox for **Write zeros to disk** to completely remove data.
4. Click **OK**.

## Performing cleaning

This section provides information about cleaning and describes how to start, stop, and modify cleaning schedules.

DD OS attempts to maintain a counter called 'Cleanable GiB' for the active tier. This number is an estimation of how much physical (postcomp) space could potentially be reclaimed in the active tier

by running clean/garbage collection. This counter is shown using the `fileSYS show space and df` commands.

```
Active Tier:
Resource Size GiB Used GiB Avail GiB Use% Cleanable GiB*
-----
/data: pre-comp - 7259347.5 - - -
/data: post-comp 304690.8 251252.4 53438.5 82% 51616.1 <==== NOTE
/ddvar 29.5 12.5 15.6 44% -
-----
```

Run active tier clean if either:

- The value for 'Cleanable GiB' is large
- DDFS has become 100% full (and is therefore read-only)

Clean may not reclaim all potential space in a single run. On systems containing very large datasets, clean works against the portion of the file system containing the most superfluous data and may need to be run multiple times before all potential space is reclaimed.

## Starting cleaning

To immediately start a cleaning operation.

### Procedure

1. Select **Data Management > File System > Summary > Settings > Cleaning**.

The **Cleaning** tab of the **File System Setting** dialog displays the configurable settings for each tier.

2. For the active tier:
  - a. In the Throttle % text box, enter a system throttle amount. This is the percentage of CPU usage dedicated to cleaning. The default is 50 percent.
  - b. In the Frequency drop-down list, select one of these frequencies: Never, Daily, Weekly, Biweekly, and Monthly. The default is Weekly.
  - c. For At, configure a specific time.
  - d. For On, select a day of the week.
3. For the cloud tier:
  - a. In the Throttle % text box, enter a system throttle amount. This is the percentage of CPU usage dedicated to cleaning. The default is 50 percent.
  - b. In the Frequency drop-down list, select one of these frequencies: Never, After every 'N' Active Tier cleans.

**Note:** If a cloud unit is inaccessible when cloud tier cleaning runs, the cloud unit is skipped in that run. Cleaning on that cloud unit occurs in the next run if the cloud unit becomes available. The cleaning schedule determines the duration between two runs. If the cloud unit becomes available and you cannot wait for the next scheduled run, you can start cleaning manually.

4. Click **Save**.

**Note:**  
To start the cleaning operation using the CLI, use the `fileSYS clean start` command.

```
# fileSYS clean start
Cleaning started. Use 'fileSYS clean watch' to monitor progress.
```

To confirm that cleaning is in progress, use the `filesys status` command.

```
# filesys status
The filesystem is enabled and running.
Cleaning started at 2017/05/19 16:05:56: phase 1 of 12 (pre-merge)
50.6% complete, 64942 GiB free; time: phase 0:01:05, total 0:01:05
```

If cleaning is already running, the following message is displayed when it is attempted to be started.

```
**** Cleaning already in progress. Use 'filesys clean watch' to monitor
progress.
```

- ① **Note:** If `clean` is not able to start, contact the contracted support provider for further assistance. This issue may indicate that the system has encountered a `missing segment error`, causing `clean` to be disabled.

## Scheduling or stopping cleaning

To immediately stop or schedule a cleaning operation.

### Procedure

1. Select **Data Management > File System > Summary > Settings > Cleaning**.  
The Cleaning tab of the File System Setting dialog displays the configurable settings for each tier.
2. For the active tier:
  - a. In the Frequency drop-down list, select wanted frequency.
3. For the cloud tier:
  - a. In the Frequency drop-down list, select wanted frequency.
4. Click **Save**.

- ① **Note:** The CLI can be used to check that a clean schedule has been set.

```
# filesys clean show schedule
```

If necessary, set an active tier clean schedule. The following example sets cleaning to run every Tuesday at 6 AM:

```
# filesys clean set schedule Tue 0600
Filesystem cleaning is scheduled to run "Tue" at "0600".
```

## Performing sanitization

To comply with government guidelines, system sanitization, also called data shredding, must be performed when classified or sensitive data is written to any system that is not approved to store such data.

When an incident occurs, the system administrator must take immediate action to thoroughly eradicate the data that was accidentally written. The goal is to effectively restore the storage device to a state as if the event never occurred. If the data leakage is with sensitive data, the entire storage will need to be sanitized using Dell EMC Professional Services' Secure Data erasure practice.

The sanitization command exists to enable the administrator to delete files at the logical level, whether a backup set or individual files. Deleting a file in most file systems consists of just flagging the file or deleting references to the data on disk, freeing up the physical space to be consumed at a later time. However, this simple action introduces the problem of leaving behind a residual representation of underlying data physically on disks. Deduplicated storage environments are not immune to this problem.

Shredding data in a system implies eliminating the residual representation of that data and thus the possibility that the file may be accessible after it has been shredded. Dell EMC's sanitization

approach ensures is compliant with the 2007 versions of Department of Defense (DoD) 5220.22 of the following specifications:

- *US Department of Defense 5220.22-M Clearing and Sanitization Matrix*
- *National Institute of Systems and Technology (NIST) Special Publication 800-88 Guidelines for Media Sanitization*

## Sanitizing deduplicated data

Protection systems sanitize data in place, in its native deduplicated state.

Deduplication storage systems extract common data patterns from files sent to the system and store only unique copies of these patterns, referencing all the redundant instances. Because these data patterns or segments may potentially be shared among many files in the system, the sanitization process must first determine whether each of the segments of the contaminated file are shared with a clean file and then erase only those segments that are not shared, along with any contaminated metadata.

All storage tiers, caches, unused capacity, and free space are cleared so that every copy of every segment that belongs exclusively to the deleted files is eradicated. The system reclaims and overwrites all of the storage occupied by these segments to effectively restore the storage device to a state as if the contaminated files never existed in that system.

## Sanitization level 1: data clearing or shredding

If the data you need to remove is unclassified, as defined in the "US Department of Defense 5220.22-M Clearing and Sanitization Matrix," Level 1 sanitization can be used to overwrite the affected storage once. This provides the basis for handling most data shredding and system sanitization cases.

### About this task

The system sanitization feature ensures that every copy of every segment that belongs only to erased files is overwritten using a single-pass zeroization mechanism. Clean data in the system being sanitized is online and available to users.

### Procedure

1. Delete the contaminated files or backups through the backup software or corresponding client. In the case of backups, be sure to manage the backup software appropriately to ensure that related files on that image are reconciled, catalog records are managed as required, and so forth.
2. Run the `system sanitize start` command on the contaminated system to cause all previously used space in it to be overwritten once (see the figure below).
3. Wait for the affected system to be sanitized. Sanitization can be monitored by using the `system sanitize watch` command.

If the affected system has replication enabled, all the systems containing replicas need to be processed in a similar manner. Depending on how much data exists in the system and how it is distributed, the `system sanitize` command could take some time. However, during this time, all clean data in the system is available to users.



## Sanitization level 2: full system sanitization

If the data you need to remove is classified, as defined in the "US Department of Defense 5220.22-M Clearing and Sanitization Matrix," Level 2 sanitization, or full system sanitization, is now required.

### About this task

Dell EMC recommends Blancco for multi-pass overwrites with any overwrite pattern and a certificate. This provides the basis for handling universal Department of Defense requirements where complete system sanitization is required. For more information, go to:

[https://www.emc.com/auth/rcoll/servicekitdocument/cp\\_datadomaindataerase\\_psbasddde.pdf](https://www.emc.com/auth/rcoll/servicekitdocument/cp_datadomaindataerase_psbasddde.pdf)

## Modifying basic settings

Change the type of compression used, marker types, Replica write status, and Staging Reserve percentage, as described in this section.

### Changing local compression

Use the General tab of the File System Settings dialog to configure the local compression type.

#### About this task

① **Note:** Do not change the type of local compression unless it is necessary.

#### Procedure

1. Select **Data Management > File System > Summary > Settings > General**.
2. From the Local Compression Type drop-down list, select a compression type.

**Table 96** Compression type

Option	Description
NONE	Do not compress data.
LZ	The algorithm that gives the best throughput. Dell EMC recommends the lz option, which is the default setting, for the following systems: <ul style="list-style-type: none"> <li>• DD2200</li> <li>• DD3300</li> <li>• DD6300</li> <li>• DD6800</li> <li>• DD9300</li> <li>• DD9500</li> <li>• DD9800</li> </ul>
GZFAST	A zip-style compression that uses less space for compressed data, but more CPU cycles (twice as much as lz). Gzfast is the recommended alternative for sites that want more compression at the cost of lower performance. Dell EMC recommends the gzfast option, which is the default setting, for the following systems: <ul style="list-style-type: none"> <li>• DD6900</li> </ul>

Table 96 Compression type (continued)

Option	Description
	<ul style="list-style-type: none"> <li>• DD9400</li> <li>• DD9900</li> </ul>
GZ	A zip-style compression that uses the least amount of space for data storage (10% to 20% less than lz on average; however, some datasets get much higher compression). This also uses the most CPU cycles (up to five times as much as lz). The gz compression type is commonly used for nearline storage applications in which performance requirements are low.

3. Click **Save**.

### Changing read-only settings

Change the replica to writable. Some backup applications must see the replica as writable to do a restore or vault operation from the replica.

#### Procedure

1. Select **Data Management > File System > Summary > Settings > General**.
2. In the Report Replica as Writable area, toggle between **Disabled** and **Enabled as appropriate**.
3. Click **Save**.

### Working with disk staging

Disk staging enables a protection system to serve as a staging device, where the system is viewed as a basic disk via a CIFS share or NFS mount point.

Disk staging can be used in conjunction with your backup software, such as NetWorker and Veritas NetBackup (NBU), it does not require a license, and is disabled by default.

**Note:** The DD VTL feature is not required or supported when the system is used as a Disk Staging device.

The reason that some backup applications use disk staging devices is to enable tape drives to stream continuously. After the data is copied to tape, it is retained on disk for as long as space is available. Should a restore be needed from a recent backup, more than likely the data is still on disk and can be restored from it more conveniently than from tape. When the disk fills up, old backups can be deleted to make space. This delete-on-demand policy maximizes the use of the disk.

In normal operation, the system does not reclaim space from deleted files until a cleaning operation is done. This is not compatible with backup software that operates in a staging mode, which expects space to be reclaimed when files are deleted. When you configure disk staging, you reserve a percentage of the total space—typically 20 to 30 percent—in order to allow the system to simulate the immediate freeing of space.

The amount of available space is reduced by the amount of the staging reserve. When the amount of data stored uses all of the available space, the system is full. However, whenever a file is deleted, the system estimates the amount of space that will be recovered by cleaning and borrows from the staging reserve to increase the available space by that amount. When a cleaning operation runs, the space is actually recovered and the reserve restored to its initial size. Since the amount of space made available by deleting files is only an estimate, the actual space reclaimed by cleaning may not match the estimate. The goal of disk staging is to configure enough reserve so that you do not run out before cleaning is scheduled to run.



## Configuring disk staging

Enable disk staging and specify the staging reserve percentage.

### Procedure

1. Select **Data Management > File System > Summary > Settings > General**.
2. In the Staging Reserve area, toggle between **Disabled** and **Enabled** as appropriate.
3. If Staging Reserve is enabled, enter a value in the % of Total Space box.

This value represents the percentage of the total disk space to be reserved for disk staging, typically 20 to 30%.

4. Click **Save**.

## Tape marker settings

Backup software from some vendors insert markers (tape markers, tag headers, or other names are used) in all data streams (both file system and DD VTL backups) sent to a protection system.

Markers can significantly degrade data compression. As such, the default marker type auto is set and cannot be changed by the user. If this setting is not compatible with your backup software, contact your contracted support provider.

- ① **Note:** For information about how applications work, see *How EMC Data Domain Systems Integrate into the Storage Environment*. You can use these matrices and integration guides to troubleshoot vendor-related issues.

## SSD Random workload share

The value for the threshold at which to cap random I/O on the protection system can be adjusted from the default value to accommodate changing requirements and I/O patterns.

By default, the SSD random workload share is set at 40%. This value can be adjusted up or down as needed. Select **Data Management > File System > Summary > Settings > Workload Balance**, and adjust the slider.

Click **Save**.

## Fast copy operations

A fast copy operation clones files and directory trees of a source directory to a target directory on a protection system.

The `force` option allows the destination directory to be overwritten if it exists. Executing the fast copy operation displays a progress status dialog box.

- ① **Note:** A fast copy operation makes the destination equal to the source, but not at a specific time. There are no guarantees that the two are or were ever equal if you change either folder during this operation.

## Performing a fast copy operation

Copy a file or directory tree from a protection system source directory to another destination on the same system.

### Procedure

1. Select **Data Management > File System > Summary > Fast Copy**.

The Fast Copy dialog is displayed.

2. In the Source text box, enter the pathname of the directory where the data to be copied resides. For example, `/data/col1/backup/.snapshot/snapshot-name/dir1`.

① | Note: col1 uses a lower case L followed by the number 1.

3. In the Destination text box, enter the pathname of the directory where the data will be copied to. For example, `/data/col1/backup/dir2`. This destination directory must be empty, or the operation fails.
  - If the Destination directory exists, click the checkbox **Overwrite existing destination if it exists**.
4. Click OK.
5. In the progress dialog box that appears, click **Close** to exit.

# CHAPTER 6

## MTrees

This chapter includes:

- MTrees overview .....206
- Monitoring MTree usage ..... 213
- Managing MTree operations..... 216

## MTrees overview

An MTree is a logical partition of the file system.

You can use MTrees in the following ways: for CIFS shares, DD Boost storage units, DD VTL pools, or NFS exports. MTrees allow granular management of snapshots, quotas, and DD Retention Lock.

- Note:**  
There can be up to the maximum configurable MTrees designated for MTree replication contexts.

Do not place user files in the top-level directory of an MTree. Create subdirectories within the MTree to store user data.

## MTree limits

MTree limits for DD systems

**Table 97** Number of supported MTrees

System	DD OS Version	Supported configurable MTrees	Supported concurrently active MTrees
DD9900	7.0 and later	256	256
DD6900, DD9400	7.0 and later	128	128
DD9800	6.0 and later	256	256
DD9500	5.7 and later	256	256
DD6800, DD9300	6.0 and later	128	128
DD6300	6.0 and later	100	32
DD2200	5.7 and later	100	32

## Quotas

MTree quotas apply only to the logical data written to the MTree.

An administrator can set the storage space restriction for an MTree, Storage Unit, or DD VTL pool to prevent it from consuming excess space. There are two kinds of quota limits: hard limits and soft limits. You can set either a soft or hard limit or both a soft and hard limit. Both values must be integers, and the soft value must be less than the hard value.

When a soft limit is set, an alert is sent when the MTree size exceeds the limit, but data can still be written to it. When a hard limit is set, data cannot be written to the MTree when the hard limit is reached. Therefore, all write operations fail until data is deleted from the MTree.

See [Configure MTree quotas](#) on page 218 for more information.

## Quota enforcement

Enable or disable quota enforcement.

## About the MTree panel

Lists all the active MTrees on the system and shows real-time data storage statistics. Information in the overview area is helpful in visualizing space usage trends.

Select **Data Management > MTree**.

- Select a checkbox of an MTree in the list to display details and perform configuration in the Summary view.
- Enter text (wildcards are supported) in the Filter By MTree Name field and click **Update** to list specific MTree names in the list.
- Delete filter text and click **Reset** to return to the default list.

**Table 98** MTree overview information

Item	Description
MTree Name	The pathname of the MTree.
Quota Hard Limit	Percentage of hard limit quota used.
Last 24 Hr Pre-Comp (pre-compression)	Amount of raw data from the backup application that has been written in the last 24 hours.
Last 24 Hr Post-Comp (post-compression)	Amount of storage used after compression in the last 24 hours.
Last 24 hr Comp Ratio	The compression ratio for the last 24 hours.
Weekly Avg Post-Comp	Average amount of compressed storage used in the last five weeks.
Last Week Post-Comp	Average amount of compressed storage used in the last seven days.
Weekly Avg Comp Ratio	The average compression ratio for the last five weeks.
Last Week Comp Ratio	The average compression ratio for the last seven days.

## About the summary view

View important file system statistics.

### View detail information

Select an MTree to view information.

**Table 99** MTree detail information for a selected MTree

Item	Description
Full Path	The pathname of the MTree.
Pre-Comp Used	The current amount of raw data from the backup application that has been written to the MTree.
Status	The status of the MTree (combinations are supported). Status can be: <ul style="list-style-type: none"> <li>• D: Deleted</li> </ul>

Table 99 MTree detail information for a selected MTree (continued)

Item	Description
	<ul style="list-style-type: none"> <li>• RO: Read-only</li> <li>• RW: Read/write</li> <li>• RD: Replication destination</li> <li>• RLCE: DD Retention Lock Compliance enabled</li> <li>• RLCD: DD Retention Lock Compliance disabled</li> <li>• RLGE: DD Retention Lock Governance enabled</li> <li>• RLGD: DD Retention Lock Governance disabled</li> </ul>
Quota	
Quota Enforcement	Enabled or Disabled.
Pre-Comp Soft Limit	Current value. Click Configure to revise the quota limits.
Pre-Comp Hard Limit	Current value. Click Configure to revise the quota limits.
Quota Summary	Percentage of Hard Limit used.
Protocols	
CIFS Shared	<p>The CIFS share status. Status can be:</p> <ul style="list-style-type: none"> <li>• Yes—The MTree or its parent directory is shared.</li> <li>• Partial—The subdirectory under this MTree is shared.</li> <li>• No—This MTree and its parent or subdirectory are not shared.</li> </ul> <p>Click the CIFS link to go to the CIFS view.</p>
NFS Exported	<p>The NFS export status. Status can be:</p> <ul style="list-style-type: none"> <li>• Yes—The MTree or its parent directory is exported.</li> <li>• Partial—The subdirectory under this MTree is exported.</li> <li>• No—This MTree and its parent or subdirectory are not exported.</li> </ul> <p>Click the NFS link to go to the NFS view.</p>
DD Boost Storage Unit	<p>The DD Boost export status. Status can be:</p> <ul style="list-style-type: none"> <li>• Yes—The MTree is exported.</li> <li>• No—This MTree is not exported.</li> <li>• Unknown—There is no information.</li> </ul> <p>Click the DD Boost link to go to the DD Boost view.</p>
DD VTL Pool	<p>VTL pool report status. Status can be:</p> <ul style="list-style-type: none"> <li>• Yes— The MTree is a DD VTL MTree pool.</li> <li>• No— The MTree is not a DD VTL MTree pool.</li> <li>• Unknown— There is no information.</li> </ul>
vDisk Pool	vDisk report status. Status can be:

Table 99 MTree detail information for a selected MTree (continued)

Item	Description
	<ul style="list-style-type: none"> <li>Unknown— vDisk service is not enabled.</li> <li>No— vDisk service is enabled but the MTree is not a vDisk pool.</li> <li>Yes— vDisk service is enabled and the MTree is a vDisk pool.</li> </ul>
Physical Capacity Measurements	
Used (Post-Comp)	MTree space that is used after compressed data has been ingested.
Compression	Global Comp-factor.
Last Measurement Time	Last time the system measured the MTree.
Schedules	<p>Number of schedules assigned.</p> <p>Click <b>Assign</b> to view and assign schedules to the MTree.</p> <ul style="list-style-type: none"> <li>Name: The schedule name.</li> <li>Status: Enabled or Disabled</li> <li>Priority: <ul style="list-style-type: none"> <li>Normal— Submits a measurement task to the processing queue.</li> <li>Urgent— Submits a measurement task to the front of the processing queue.</li> </ul> </li> <li>Schedule: Time the task runs.</li> <li>MTree Assignments: Number of MTrees the schedule is assigned to.</li> </ul>
Submitted Measurements	<p>Displays the post compression status for the MTree.</p> <p>Click <b>Measure Now</b> to submit a manual post compression job for the MTree and select a priority for the job.</p> <ul style="list-style-type: none"> <li>0— No measurement job submitted.</li> <li>1— 1 measurement job running.</li> <li>2— 2 measurement jobs running.</li> </ul>
Snapshots	<p>Displays these statistics:</p> <ul style="list-style-type: none"> <li>Total Snapshots</li> <li>Expired</li> <li>Unexpired</li> <li>Oldest Snapshot</li> <li>Newest Snapshot</li> <li>Next Scheduled</li> <li>Assigned Snapshot Schedules</li> </ul>



**Table 99** MTree detail information for a selected MTree (continued)

Item	Description
	Click <b>Total Snapshots</b> to go to the <b>Data Management &gt; Snapshots</b> view.
	Click <b>Assign Schedules</b> to configure snapshot schedules.

### View MTree replication information

Display MTree replication configuration.

If the selected MTree is configured for replication, summary information about the configuration displays in this area. Otherwise, this area displays `No Record Found`.

- Click the **Replication** link to go to the **Replication** page for configuration and to see additional details.

**Table 100** MTree replication information

Item	Description
Source	The source MTree pathname.
Destination	The destination MTree pathname.
Status	The status of the MTree replication pair. Status can be Normal, Error, or Warning.
Sync As Of	The last day and time the replication pair was synchronized.

### View MTree snapshot information

If the selected MTree is configured for snapshots, summary information about the snapshot configuration displays.

- Click the **Snapshots** link to go to the **Snapshots** page to perform configuration or to see additional details.
- Click **Assign Schedules** to assign a snapshot schedule to the selected MTree. Select the schedule's checkbox, and then click **OK** and **Close**. To create a snapshot schedule, click **Create Snapshot Schedule** (see the section about creating a snapshot schedule for instructions).

**Table 101** MTree snapshot information

Item	Description
Total Snapshots	The total number of snapshots created for this MTree. A total of 750 snapshots can be created for each MTree.
Expired	The number of snapshots in this MTree that have been marked for deletion, but have not been removed with the clean operation as yet.
Unexpired	The number of snapshots in this MTree that are marked for keeping.
Oldest Snapshot	The date of the oldest snapshot for this MTree.
Newest Snapshot	The date of the newest snapshot for this MTree.

Table 101 MTree snapshot information (continued)

Item	Description
Next Scheduled	The date of the next scheduled snapshot.
Assigned Snapshot Schedules	The name of the snapshot schedule assigned to this MTree.

### View MTree retention lock information

If the selected MTree is configured for one of the DD Retention Lock software options, summary information about the DD Retention Lock configuration displays.

① **Note:** For information on how to manage DD Retention Lock for an MTree, see the section about working with DD Retention Lock.

Table 102 DD Retention Lock information

Item	Description
Status	Indicates whether DD Retention Lock is enabled or disabled.
Mode	Indicates whether the MTree is configured for DD Retention Lock Compliance or DD Retention Lock Governance.
Use	Indicates the use of the MTree.
Retention period min	Indicates the minimum DD Retention Lock time period.
Retention period max	Indicates the maximum DD Retention Lock time period.

### Enabling and managing DD Retention Lock settings

Use the DD Retention Lock area of the GUI to modify retention lock periods.

#### Procedure

1. Select **Data Management > MTree > Summary**.
2. In the Retention Lock area, click **Edit**.
3. In the Modify Retention Lock dialog box, select **Enable** to enable DD Retention Lock.
4. Modify the retention lock values:
  - a. In the **Use** drop-down list, select **Manual** or **Automatic**.
    - For manual retention lock, to change the minimum or maximum retention period for the MTree:
      - a. Type a number for the interval in the text box (for example, 5 or 14).
      - b. From the drop-down list, select an interval (minutes, hours, days, years).
 

① **Note:** Specifying a minimum retention period of less than 12 hours, or a maximum retention period longer than 70 years, results in an error.
    - For automatic retention lock, to change the minimum, maximum, or automatic retention period, or the automatic lock delay for the MTree:
      - a. Type a number for the interval in the text box (for example, 5 or 14).
      - b. From the drop-down list, select an interval (minutes, hours, days, years).

- ① Note: Specifying a minimum retention period of less than 12 hours, a maximum retention period longer than 70 years, an automatic retention period that does not fall between the minimum and maximum values, or an automatic lock delay less than 5 minutes or more than 7 days results in an error.
- ① Note: If a file is modified before the automatic lock delay has elapsed, the lock delay time starts over when the file modification is complete. For example, if the lock delay is 120 minutes and the file is modified after 60 minutes, the lock delay will start again at 120 minutes after the file is modified.

b. Click OK to save the settings.

### Results

After you close the Modify Retention Lock dialog box, updated MTree information is displayed in the DD Retention Lock summary area.

## About the space usage view (MTrees)

Display a visual representation of data usage for an MTree at certain points in time.

Select **Data Management > MTree > Space Usage**.

- Click a point on a graph line to display a box with data at that point.
- Click **Print** (at the bottom on the graph) to open the standard Print dialog box.
- Click **Show in new window** to display the graph in a new browser window.

The lines of the graph denote measurement for:

- **Pre-comp Written**—The total amount of data sent to the MTree by backup servers. Pre-compressed data on an MTree is what a backup server sees as the total uncompressed data held by an MTree-as-storage-unit, shown with the Space Used (left) vertical axis of the graph.
- **Post-comp Used**—The total amount of storage space consumed on the MTree after compression, shown with the Space Used (left) vertical axis of the graph.
- **Comp Factor**—The compression ratio of the data stored on the MTree, shown with the Comp Factor (right) vertical axis of the graph.

- ① Note: For the MTrees Space Usage view, the system displays only pre-compressed information. Data can be shared between MTrees so compressed usage for a single MTree cannot be provided.

### Checking Historical Space Usage

On the Space Usage graph, clicking an interval (that is, 1w, 1m, 3m, or 1y) on the Duration line above the graph allows you to change the number of days of data shown on the graph, from 7 to 120 days.

To see space usage for intervals over 120 days, issue the following command:

```
# filesys show compression [summary | daily | daily-detailed] ([last n (hours | days | weeks | months)] | [start date [end date]])
```

## About the daily written view (MTrees)

Display the flow of data over the last 24 hours. Data amounts are shown over time for pre- and post-compression.

It also provides totals for global and local compression amounts, and pre-compression and post-compression amounts.

- Click a point on a graph line to display a box with data at that point.
- Click **Print** (at the bottom on the graph) to open the standard Print dialog box.
- Click **Show in new window** to display the graph in a new browser window.

The lines on the graph denote measurements for:

- **Pre-Comp Written**—The total amount of data written to the MTree by backup servers. Pre-compressed data on an MTree is what a backup server sees as the total uncompressed data held by an MTree -as-storage-unit.
- **Post-Comp Written**—The total amount of data written to the MTree after compression has been performed, as shown in GiBs.
- **Total Comp Factor**—The total amount of compression performed with the data received (compression ratio), shown with the Total Compression Factor (right) vertical axis of the graph.

#### Checking Historical Written Data

On the Daily Written graph, clicking an interval (that is, 7d, 30d, 60d, or 120d) on the Duration line above the graph allows you to change the number of days of data shown on the graph, from 7 to 120 days.

Below the Daily Written graph, the following totals display for the current duration value:

- Pre-Comp Written
- Post-Comp Written
- Global-Comp Factor
- Local-Comp Factor
- Total-Comp Factor

## Monitoring MTree usage

Display space usage and data written trends for an MTree.

#### Procedure

- Select **Data Management > MTree**.

The MTree view shows a list of configured MTrees, and when selected in the list, details of the MTree are shown in the Summary tab. The Space Usage and Daily Written tabs show graphs that visually display space usage amounts and data written trends for a selected MTree. The view also contains options that allow MTree configuration for CIFS, NFS, and DD Boost, as well as sections for managing snapshots and DD Retention Lock for an MTree.

The MTree view has an MTree overview panel and three tabs which are described in detail in these sections.

- About the MTree panel on page 207
- About the summary view on page 207
- About the space usage view (MTrees) on page 212
- About the daily written view (MTrees) on page 212

① **Note:** Physical capacity measurement (PCM) provides space usage information for MTrees. For more information about PCM, see the section regarding understanding physical capacity measurement.

## Understanding physical capacity measurement

Physical capacity measurement (PCM) provides space usage information for a sub-set of storage space. From the DD System Manager, PCM provides space usage information for MTrees, but from the command line interface you can view space usage information for MTrees, tenants, tenant units, and pathsets.

Once a path is selected for PCM, all paths underneath it are automatically included. Do not select a child path after its parent path is already selected. For example, if `/data/coll/mtree3` is selected, do not select any subdirectories under `mtree3`.

The *DD OS Command Reference Guide* provides more information about using PCM from the command line.

### Enabling, disabling, and viewing physical capacity measurement

Physical capacity measurement provides space usage information for an MTree.

#### Procedure

1. Select **Data Management > File System > Summary**.  
The system displays the Summary tab in the File System panel.
2. Click **^** in the bottom-right corner to view the status panel.
3. Click **Enable** to the right of **Physical Capacity Measurement Status** to enable PCM.
4. Click **Details** to the right of **Physical Capacity Measurement Status** to view currently running PCM jobs.
  - **MTree:** The MTree that PCM is measuring.
  - **Priority:** The priority (normal or urgent) for the task.
  - **Submit Time:** The time the task was requested.
  - **Duration:** The length of time PCM ran to accomplish of the task.
5. Click **Disable** to the right of **Physical Capacity Measurement Status** to disable PCM and cancel all currently running PCM jobs.

### Initializing physical capacity measurement

Physical capacity measurement (PCM) initialization is a one-time action that can take place only if PCM is enabled and the cache has not been initialized. It cleans the caches and enhances measuring speed. During the initialization process, you can still manage and run PCM jobs.

#### Procedure

1. Select **Data Management > File System > Configuration**.
2. Click **Initialize** under Physical Capacity Measurement to the right of Cache.
3. Click **Yes**.

### Managing physical capacity measurement schedules

Create, edit, delete, and view physical capacity measurement schedules. This dialog only displays schedules created for MTrees and schedules that currently have no assignments.

#### Procedure

1. Select **Data Management > MTree > Manage Schedules**.
  - Click **Add (+)** to create a schedule.
  - Select a schedule and click **Modify** (pencil) to edit the schedule.

- Select a schedule and click **Delete (X)** to delete a schedule.
2. Optionally, click the heading names to sort by schedule: **Name**, **Status** (Enabled or Disabled) **Priority** (Urgent or Normal), **Schedule** (schedule timing), and **MTree Assignments** (the number of MTrees the schedule is assigned to).

## Creating physical capacity measurement schedules

Create physical capacity measurement schedules and assign them to MTrees.

### Procedure

1. Select **Data Management > MTree > Manage Schedules**.
2. Click **Add (+)** to create a schedule.
3. Enter the name of the schedule.
4. Select the status:
  - **Normal**: Submits a measurement task to the processing queue.
  - **Urgent**: Submits a measurement task to the front of the processing queue.
5. Select how often the schedule triggers a measurement occurrence: every **Day**, **Week**, or **Month**.
  - For **Day**, select the time.
  - For **Week**, select the time and day of the week.
  - For **Month**, select the time, and days during the month.
6. Select MTree assignments for the schedule (the MTrees that the schedule will apply to):
7. Click **Create**.
8. Optionally, click on the heading names to sort by schedule: **Name**, **Status** (Enabled or Disabled) **Priority** (Urgent or Normal), **Schedule** (schedule timing), and **MTree Assignments** (the number of MTrees the schedule is assigned to).

## Editing physical capacity measurement schedules

Edit a physical capacity measurement schedule.

### Procedure

1. Select **Data Management > MTree > Manage Schedules**.
2. Select a schedule and click **Modify** (pencil).
3. Modify the schedule and click **Save**.  
Schedule options are described in the [Creating physical capacity measurement schedules](#) topic.
4. Optionally, click the heading names to sort by schedule: **Name**, **Status** (Enabled or Disabled) **Priority** (Urgent or Normal), **Schedule** (schedule timing), and **MTree Assignments** (the number of MTrees the schedule is assigned to).

## Assigning physical capacity measurement schedules to an MTree


Attach schedules to an MTree.

### Before you begin

Physical capacity measurement (PCM) schedules must be created.



**About this task**

 Note: Administrators can assign up to three PCM schedules to an MTree.

**Procedure**

1. Select **Data Management > MTree > Summary**.
2. Select MTrees to assign schedules to.
3. Scroll down to the Physical Capacity Measurements area and click **Assign** to the right of Schedules.
4. Select schedules to assign to the MTree and click **Assign**.

**Starting physical capacity measurement immediately**

Start the measurement process as soon as possible.

**Procedure**

1. Select **Data Management > MTree > Summary**.
2. Scroll down to the Physical Capacity Measurements area and click **Measure Now** to the right of Submitted Measurements.
3. Select **Normal** (Submits a measurement task to the processing queue), or **Urgent** (Submits a measurement task to the front of the processing queue).
4. Click **Submit**.

**Setting the physical capacity measurement throttle**

Set the percentage of system resources that are dedicated to physical capacity measurement.

**Procedure**

1. Select **Data Management > File System > Settings**.
2. In the Physical Capacity Measurement area, click **Edit** to the left of Throttle.
- 3.

Option	Description
Click Default	Enters the 20% system default.
Type throttle percent	The percentage of system resources that are dedicated to physical capacity measurement.

4. Click **Save**.

## Managing MTree operations

This section describes MTree creation, configuration, how to enable and disable MTree quotas, and so on.

### Creating an MTree

An MTree is a logical partition of the file system. Use MTrees CIFS shares, DD Boost storage units, DD VTL pools, or NFS exports.

**About this task**

MTrees are created in the area `/data/col1/mtree_name`.



### Procedure

1. Select **Data Management > MTree**.
2. In the MTree overview area, click **Create**.
3. Enter the name of the MTree in the MTree Name text box. MTree names can be up to 50 characters. The following characters are acceptable:
  - Upper- and lower-case alphabetical characters: A-Z, a-z
  - Numbers: 0-9
  - Embedded space
  - comma (,)
  - period (.), as long as it does not precede the name.
  - explanation mark (!)
  - number sign (#)
  - dollar sign (\$)
  - per cent sign (%)
  - plus sign (+)
  - at sign (@)
  - equal sign (=)
  - ampersand (&)
  - semi-colon (;)
  - parenthesis [(and)]
  - square brackets ([and])
  - curly brackets ({and})
  - caret (^)
  - tilde (~)
  - apostrophe (unslanted single quotation mark)
  - single slanted quotation mark (')
4. Set storage space restrictions for the MTree to prevent it from consuming excessive space. Enter a soft or hard limit quota setting, or both. With a soft limit, an alert is sent when the MTree size exceeds the limit, but data can still be written to the MTree. Data cannot be written to the MTree when the hard limit is reached.
  - ① Note: The quota limits are pre-compressed values.  
To set quota limits for the MTree, select **Set to Specific value** and enter the value. Select the unit of measurement: MiB, GiB, TiB, or PiB.
  - ① Note: When setting both soft and hard limits, a quota's soft limit cannot exceed the quota's hard limit.
5. Click **OK**.  
The new MTree displays in the MTree table.
  - ① Note: You may need to expand the width of the MTree Name column to see the entire pathname.

## Configure and enable/disable MTree quotas

Set the storage space restriction for an MTree, Storage Unit, or DD VTL pool.

The **Data Management > Quota** page shows the administrator how many MTrees have no soft or hard quotas set. For MTrees with quotas set, the page shows the percentage of pre-compressed soft and hard limits used.

Consider the following information when managing quotas.

- MTree quotas apply to ingest operations. These quotas can be applied to DD VTL, DD Boost, CIFS, and NFS.
- Snapshots are not counted.
- Quotas cannot be set on the `/data/coll/backup` directory.
- The maximum quota value allowed is 4096 PiB.


### Configure MTree quotas

Use the MTree tab or the Quota tab to configure MTree quotas.

#### About this task

#### Procedure

1. Select one of the following menu paths:
  - Select **Data Management > MTree**.
  - Select **Data Management > Quota**.
2. Select only one MTree in the MTree tab, or one or more MTrees in the Quota tab.
 

 **Note:** Quotas cannot be set on the `/data/coll/backup` directory.
3. In the MTree tab, click the **Summary** tab, and then click the **Configure** button in the Quota area.
4. In the Quota tab, click the **Configure Quota** button.

### Configuring MTree quotas

Enter values for hard and soft quotas and select the unit of measurement.


#### Procedure

1. In the Configure Quota for MTrees dialog box, enter values for hard and soft quotas and select the unit of measurement: MiB, GiB, TiB, or PiB.
2. Click **OK**.

## Deleting an MTree

Removes the MTree from the MTree table. The MTree data is deleted at the next cleaning.

#### About this task

-  **Note:** Because the MTree and its associated data are not removed until file cleaning is run, you cannot create a new MTree with the same name as a deleted MTree until the deleted MTree is completely removed from the file system by the cleaning operation.

#### Procedure

1. Select **Data Management > MTree**.

2. Select an MTree.
3. In the MTree overview area, click **Delete**.
4. Click **OK** at the Warning dialog box.
5. Click **Close** in the Delete MTree Status dialog box after viewing the progress.

## Undeleting an MTree

Undelete retrieves a deleted MTree and its data and places it back in the MTree table.

### About this task

An undelete of an MTree retrieves a deleted MTree and its data and places it back in the MTree table.

An undelete is possible only if file cleaning has not been run after the MTree was marked for deletion.

① **Note:** You can also use this procedure to undelete a storage unit.

### Procedure

1. Select **Data Management > MTree > More Tasks > Undelete**.
2. Select the checkboxes of the MTrees you wish to bring back and click **OK**.
3. Click **Close** in the Undelete MTree Status dialog box after viewing the progress.

The recovered MTree displays in the MTree table.

## Renaming an MTree

Use the Data Management MTree GUI to rename MTrees.

### Procedure

1. Select **Data Management > MTree**.
2. Select an MTree in the MTree table.
3. Select the Summary tab.
4. In the Detailed Information overview area, click **Rename**.
5. Enter the name of the MTree in the New MTree Name text box.  
See the section about creating an MTree for a list of allowed characters.
6. Click **OK**.

The renamed MTree displays in the MTree table.

MTrees	MTrees	MTrees	MTrees	MTrees	MTrees
1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30
31	32	33	34	35	36
37	38	39	40	41	42
43	44	45	46	47	48
49	50	51	52	53	54
55	56	57	58	59	60
61	62	63	64	65	66
67	68	69	70	71	72
73	74	75	76	77	78
79	80	81	82	83	84
85	86	87	88	89	90
91	92	93	94	95	96
97	98	99	100	101	102
103	104	105	106	107	108
109	110	111	112	113	114
115	116	117	118	119	120
121	122	123	124	125	126
127	128	129	130	131	132
133	134	135	136	137	138
139	140	141	142	143	144
145	146	147	148	149	150
151	152	153	154	155	156
157	158	159	160	161	162
163	164	165	166	167	168
169	170	171	172	173	174
175	176	177	178	179	180
181	182	183	184	185	186
187	188	189	190	191	192
193	194	195	196	197	198
199	200	201	202	203	204
205	206	207	208	209	210
211	212	213	214	215	216
217	218	219	220	221	222
223	224	225	226	227	228
229	230	231	232	233	234
235	236	237	238	239	240
241	242	243	244	245	246
247	248	249	250	251	252
253	254	255	256	257	258
259	260	261	262	263	264
265	266	267	268	269	270
271	272	273	274	275	276
277	278	279	280	281	282
283	284	285	286	287	288
289	290	291	292	293	294
295	296	297	298	299	300

# CHAPTER 7

## Snapshots

This chapter includes:

- Snapshots overview..... 222
- Monitoring snapshots and their schedules.....222
- Managing snapshots.....224
- Managing snapshot schedules.....225
- Recover data from a snapshot.....227

## Snapshots overview

This chapter describes how to use the snapshot feature with MTree.

A snapshot saves a read-only copy (called a *snapshot*) of a designated MTree at a specific time. You can use a snapshot as a restore point, and you can manage MTree snapshots and schedules and display information about the status of existing snapshots.

- ① **Note:** Snapshots created on the source protection system are replicated to the destination with collection and MTree replication. It is not possible to create snapshots on a system that is a replica for collection replication. It is also not possible to create a snapshot on the destination MTree of MTree replication. Directory replication does not replicate the snapshots, and it requires you to create snapshots separately on the destination system.

Snapshots for the MTree named `backup` are created in the system directory `/data/coll/backup/.snapshot`. Each directory under `/data/coll/backup` also has a `.snapshot` directory with the name of each snapshot that includes the directory. Each MTree has the same type of structure, so an MTree named `SantaClara` would have a system directory `/data/coll/SantaClara/.snapshot`, and each subdirectory in `/data/coll/SantaClara` would have a `.snapshot` directory as well.

- ① **Note:** The `.snapshot` directory is not visible if only `/data` is mounted. When the MTree itself is mounted, the `.snapshot` directory is visible.

An expired snapshot remains available until the next file system cleaning operation.

The maximum number of snapshots allowed per MTree is 750. Warnings are sent when the number of snapshots per MTree reaches 90% of the maximum allowed number (from 675 to 749 snapshots), and an alert is generated when the maximum number is reached. To clear the warning, expire snapshots and then run the file system cleaning operation.

- ① **Note:** To identify an MTree that is nearing the maximum number of snapshots, check the Snapshots panel of the MTree page regarding viewing MTree snapshot information.

Snapshot retention for an MTree does not take any extra space, but if a snapshot exists and the original file is no longer there, the space cannot be reclaimed.

- ① **Note:** Snapshots and CIFS Protocol: As of DD OS 5.0, the `.snapshot` directory is no longer visible in the directory listing in Windows Explorer or DOS CMD shell. You can access the `.snapshot` directory by entering its name in the Windows Explorer address bar or the DOS CMD shell. For example, `\\dd\backup\.snapshot` or `Z:\.snapshot` when `Z:` is mapped as `\\dd\backup`).

## Monitoring snapshots and their schedules

This section provides detailed and summary information about the status of snapshots and snapshot schedules.

### About the snapshots view

The topics in this section describe the Snapshot view.

## Snapshots overview panel

View the total number of snapshots, the number of expired snapshots, unexpired snapshots, and the time of the next cleaning.

Select **Data Management > Snapshots**.

**Table 103** Snapshot overview panel information

Field	Description
Total Snapshots (Across all MTrees)	The total number of snapshots, active and expired, on all MTrees in the system.
Expired	The number of snapshots that have been marked for deletion, but have not been removed with the cleaning operation as yet.
Unexpired	The number of snapshots that are marked for keeping.
Next file system clean scheduled	The date the next scheduled file system cleaning operation will be performed.

## Snapshots view

View snapshot information by name, by MTree, creation time, whether it is active, and when it expires.

The Snapshots tab displays a list of snapshots and lists the following information.

**Table 104** Snapshot information

Field	Description
Selected Mtree	A drop-down list that selects the MTree the snapshot operates on.
Filter By	Items to search for in the list of snapshots that display. Options are: <ul style="list-style-type: none"> <li>• <b>Name</b>—Name of the snapshot (wildcards are accepted).</li> <li>• <b>Year</b>—Drop-down list to select the year.</li> </ul>
Name	The name of the snapshot image.
Creation Time	The date the snapshot was created.
Expires On	The date the snapshot expires.
Status	The status of the snapshot, which can be Expired or blank if the snapshot is active.

## Schedules view

View the days snapshots will be taken, the times, the time they will be retained, and the naming convention.

**Table 105** Snapshot schedule information

Field	Description
Name	The name of the snapshot schedule.



Table 105 Snapshot schedule information (continued)

Field	Description
Days	The days the snapshots will be taken.
Times	The time of day the snapshots will be taken.
Retention Period	The amount of time the snapshot will be retained.
Snapshot Name Pattern	A string of characters and variables that translate into a snapshot name (for example, <code>scheduled=%Y-%m-%d-%H-%M</code> , which translates to "scheduled-2010-04-12-17-33").

1. Select a schedule in the Schedules tab. The Detailed Information area appears listing the MTrees that share the same schedule with the selected MTree.
2. Click the **Add/Remove** button to add or remove MTrees from schedule list.

## Managing snapshots

This section describes how to manage snapshots.

### Creating a snapshot

Create a snapshot when an unscheduled snapshot is required.

#### About this task

#### Procedure

1. Select **Data Management > Snapshots** to open the Snapshots view.
2. In the Snapshots view, click **Create**.
3. In the Name text field, enter the name of the snapshot.
4. In the MTree(s) area, select a checkbox of one or more MTrees in the Available MTrees panel and click **Add**.
5. In the Expiration area, select one of these expiration options:
  - a. **Never Expire**.
  - b. Enter a number for the In text field, and select **Days**, **Weeks**, **Month**, or **Years** from the drop-down list. The snapshot will be retained until the same time of day as when it is created.
  - c. Enter a date (using the format `mm/dd/yyyy`) in the On text field, or click **Calendar** and click a date. The snapshot will be retained until midnight (00:00, the first minute of the day) of the given date.
6. Click **OK** and **Close**.

### Modifying a snapshot expiration date

Modify snapshot expiration dates to remove them or extend their life for auditing or compliance.

#### Procedure

1. Select **Data ManagementSnapshots** to open the Snapshots view.
2. Click the checkbox of the snapshot entry in the list and click **Modify Expiration Date**.

- ① Note: More than one snapshot can be selected by clicking additional checkboxes.
3. In the Expiration area, select one of the following for the expiration date:
    - a. **Never Expire.**
    - b. In the **In** text field, enter a number and select **Days, Weeks, Month,** or **Years** from the drop-down list. The snapshot will be retained until the same time of day as when it is created.
    - c. In the **On** text field, enter a date (using the format *mm/dd/yyyy*) or click **Calendar** and click a date. The snapshot will be retained until midnight (00:00, the first minute of the day) of the given date.
  4. Click **OK**.

## Renaming a snapshot

Use the Snapshot tab to rename a snapshot.

### Procedure

1. Select **Data Management > Snapshots** to open the Snapshots view.
2. Select the checkbox of the snapshot entry in the list and click **Rename**.
3. In the Name text field, enter a new name.
4. Click **OK**.

## Expiring a snapshot

Snapshots cannot be deleted. To release disk space, expire snapshots and they will be deleted in the next cleaning cycle after the expiry date.

### Procedure

1. Select **Data Management > Snapshots** to open the Snapshots view.
2. Click the checkbox next to snapshot entry in the list and click **Expire**.

- ① Note: More than one snapshot can be selected by selecting additional checkboxes. The snapshot is marked as Expired in the Status column and will be deleted at the next cleaning operation.

## Managing snapshot schedules

Set up and manage a series of snapshots that will be automatically taken at regular intervals (a snapshot schedule).

Multiple snapshot schedules can be active at the same time.

- ① Note: If multiple snapshots with the same name are scheduled to occur at the same time, only one is retained. Which one is retained is indeterminate, thus only one of the snapshots with that name should be scheduled for a given time.

## Creating a snapshot schedule

Create a weekly or monthly snapshot schedule using the Data Management GUI.

### Procedure

1. Select **Data Management > Snapshots > Schedules** to open the Schedules view.
2. Click **Create**.
3. In the **Name** text field, enter the name of the schedule.
4. In the **Snapshot Name Pattern** text box, enter a name pattern.  
 Enter a string of characters and variables that translates to a snapshot name (for example, `scheduled-%Y-%m-%d-%H-%m`, translates to "scheduled-2012-04-12-17-33"). Use alphabetic characters, numbers, `_`, `-`, and variables that translate into current values.
5. Click **Validate Pattern & Update Sample**.
6. Click **Next**.
7. Select the date when the schedule will be executed:
  - a. **Weekly**—Click checkboxes next to the days of the week or select **Every Day**.
  - b. **Monthly**—Click the **Selected Days** option and click the dates on the calendar, or select the **Last Day of the Month** option.
  - c. Click **Next**.
8. Select the time of day when the schedule will be executed:
  - a. **At Specific Times**—Click **Add** and in the Time dialog that appears, enter the time in the format `hh:mm`, and click **OK**.
  - b. **In Intervals**—Click the drop-down arrows to select the start and end time `hh:mm` and AM or PM. Click the **Interval** drop-down arrows to select a number and then the hours or minutes of the interval.
  - c. Click **Next**.
9. In the **Retention Period** text entry field, enter a number and click the drop-down arrow to select days, months, or years, and click **Next**.  
 Schedules must explicitly specify a retention time.
10. Review the parameters in the schedule summary and click **Finish** to complete the schedule or **Back** to change any entries.
11. If an MTree is not associated with the schedule, a warning dialog box asks if you would like to add an MTree to the schedule. Click **OK** to continue (or **Cancel** to exit).
12. To assign an MTree to the schedule, in the MTree area, click the checkbox of one or more MTrees in the Available MTrees panel, then click **Add** and **OK**.

### Naming conventions for snapshots created by a schedule

The naming convention for scheduled snapshots is the word `scheduled` followed by the date when the snapshot is to occur, in the format `scheduled-yyyy-mm-dd-hh-mm`. For example, `scheduled-2009-04-27-13-30`.

The name `mon_thurs` is the name of a snapshot schedule. Snapshots generated by that schedule might have the names `scheduled-2008-03-24-20-00`, `scheduled-2008-03-25-20-00`, etc.

## Modifying a snapshot schedule

Change the snapshot schedule name, date, and retention period.

### Procedure

1. In the schedule list, select the schedule and click **Modify**.
2. In the Name text field, enter the name of the schedule and click **Next**.  
Use alphanumeric characters, and the \_ and -.
3. Select the date when the schedule is to be executed:
  - a. **Weekly**—Click checkboxes next to the days of the week or select **Every Day**.
  - b. **Monthly**—Click the **Selected Days** option and click the dates on the calendar, or select the **Last Day of the Month** option.
  - c. Click **Next**.
4. Select the time of day when the schedule is to be executed:
  - a. **At Specific Times**—Click the checkbox of the scheduled time in the Times list and click **Edit**. In the Times dialog that appears, enter a new time in the format *hh:mm*, and click **OK**. Or click **Delete** to remove the scheduled time.
  - b. **In Intervals**—Click the drop-down arrows to select the start and end time *hh:mm* and AM or PM. Click the Interval drop-down arrows to select a number and then the hours or minutes of the interval.
  - c. Click **Next**.
5. In the Retention Period text entry field, enter a number and click the drop-down arrow to select days, months, or years, and click **Next**.
6. Review the parameters in the schedule summary and click **Finish** to complete the schedule or **Back** to change any entries.

## Deleting a snapshot schedule

Delete a snapshot schedule from the schedule list.

### Procedure

1. In the schedule list, click the checkbox to select the schedule and click **Delete**.
2. In the verification dialog box, click **OK** and then **Close**.

## Recover data from a snapshot

Use the fastcopy operation to retrieve data stored in a snapshot. See the section regarding fast copy operations.



# CHAPTER 8

## CIFS

### CIFS overview

#### This chapter includes:

- CIFS overview..... 230
- Performing CIFS setup..... 230
- Working with shares..... 232
- Configuring SMB signing..... 237
- Managing access control..... 238
- Monitoring CIFS operation..... 242
- Performing CIFS troubleshooting..... 245

### Performing CIFS setup

### HA systems and CIFS

## CIFS overview

Common Internet File System (CIFS) clients can have access to the system directories on the protection system.

- The `/data/coll/backup` directory is the destination directory for compressed backup server data.
- The `/ddvar/core` directory contains system core and log files (remove old logs and core files to free space in this area).

① **Note:** You can also delete core files from the `/ddvar` or the `/ddvar/ext` directory if it exists.

Clients, such as backup servers that perform backup and restore operations need access to the `/data/coll/backup` directory, at a minimum. Clients that have administrative access need to be able to access the `/ddvar/core` directory to retrieve core and log files.

As part of the initial protection system configuration, CIFS clients were configured to access these directories. This chapter describes how to modify these settings and how to manage data access using the DD System Manager and the `cifs` command.

① **Note:**

- The DD System Manager **Protocols > CIFS** page allows you to perform major CIFS operations such as enabling and disabling CIFS, setting authentication, managing shares, and viewing configuration and share information.
- The `cifs` command contains all the options to manage CIFS backup and restores between Windows clients and protection systems, and to display CIFS statistics and status. For complete information about the `cifs` command, see the *DD OS Command Reference Guide*.
- For information about setting up clients to use the protection system as a server, see the related tuning guide, such as the *CIFS Tuning Guide*, which is available from the [support.emc.com](http://support.emc.com) web site. Search for the complete name of the document using the Search field.

## Performing CIFS setup

This section contains instructions about enabling CIFS services, naming the CIFS server, and so on.

### HA systems and CIFS

HA systems are compatible with CIFS; however, if a CIFS job is in progress during a failover, the job will need to be restarted.

`/ddvar` is an ext3 file system, and cannot be shared like a normal MTree-based share. The information in `/ddvar` will become stale when the active node fails over to the standby node because the filehandles are different on the two nodes. If `/ddvar` is mounted to access log files or upgrade the system, unmount and remount `/ddvar` if a failover has occurred since the last time `/ddvar` was mounted."



## Preparing clients for access to protection systems

Find documentation online.

### Procedure

1. Log into the Online Support ([support.emc.com](http://support.emc.com)) web site.
2. In the Search field, enter the name of the document that you are looking for.
3. Select the appropriate document, such as the *CIFS and Data Domain Systems Tech Note*.
4. Follow the instructions in the document.

## Enabling CIFS services

Enable the client to access the system using the CIFS protocol.

### About this task

After configuring a client for access to protection systems, enable CIFS services, which allows the client to access the system using the CIFS protocol.

### Procedure

1. For the system selected in the DD System Manager Navigation tree, click **Protocols > CIFS**.
2. In the CIFS Status area, click **Enable**.

## Naming the CIFS server

The hostname for the protection system that serves as the CIFS server is set during the system's initial configuration.

To change a CIFS server name, see the procedures in the section regarding setting authentication parameters.

A system's hostname should match the name assigned to its IP address, or addresses, in the DNS table. Otherwise authentication, as well as attempts to join a domain, can fail. If you need to change the system's hostname, use the `net set hostname` command, and also modify the system's entry in the DNS table.

When the system acts as a CIFS server, it takes the hostname of the system. For compatibility purposes, it also creates a NetBIOS name. The NetBIOS name is the first component of the hostname in all uppercase letters. For example, the hostname `jp9.oasis.local` is truncated to the NetBIOS name `JP9`. The CIFS server responds to both names.

You can have the CIFS server respond to different names at the NetBIOS levels by changing the NetBIOS hostname.

## Changing the NetBIOS hostname

Change the NetBIOS hostname with the CLI.

### Procedure

1. Display the current NetBIOS name by entering:
 

```
# cifs show config
```
2. Use the
 

```
cifs set nb-hostname nb-hostname
```

 command.

## Setting authentication parameters

Set the authentication parameters for working with CIFS.

Click the **Configure** link in to the left of the **Authentication** label in the **Configuration** tab. The system will navigate to the **Administration > Access > Authentication** tab where you can configure authentication for Active Directory, Kerberos, Workgroups, and NIS.

### Setting CIFS options

View CIFS configuration, restrict anonymous connections.

#### Procedure

1. Select **Protocols > CIFS > Configuration**.
2. In the **Options** area, click **Configure Options**.
3. To restrict anonymous connections, click the checkbox of the **Enable** option in the **Restrict Anonymous Connections** area.
4. In the **Log Level** area, click the drop-down list to select the level number.

The level is an integer from 1 (one) to 5 (five). One is the default system level that sends the least-detailed level of CIFS-related log messages, five results in the most detail. Log messages are stored in the file `/ddvar/log/debug/cifs/cifs.log`.

① Note: A log level of 5 degrades system performance. Click the **Default** in the **Log Level** area after debugging an issue. This sets the level back to 1.

5. In the **Server Signing** area, select:
  - **Enabled** to enable server signing
  - **Disabled** to disable server signing
  - **Required** when server signing is required

## Disabling CIFS services

Prevent clients from accessing the protection system.

#### Procedure

1. Select **Protocols > CIFS**.
2. In the **Status** area, click **Disable**.
3. Click **OK**.

Even after disabling CIFS access, CIFS authentication services continue to run on the system. This continuation is required to authenticate active directory domain users for management access.

## Working with shares

To share data, create shares on the protection system.

Shares are administered on the protection system and the CIFS systems.

## Creating shares

When creating shares, you have to assign client access to each directory separately and remove access from each directory separately. For example, a client can be removed from `/advax` and still have access to `/data/col1/backup`

### About this task

A protection system supports a maximum number of 3000 CIFS shares,<sup>1</sup> and 600 simultaneous connections are allowed. However, the maximum number of connections that are supported is based on system memory. See the section regarding setting the maximum open files on a connection for more information.

**Note:** If Replication is to be implemented, a system can receive backups from both CIFS clients and NFS clients as long as separate directories are used for each. Do not mix CIFS and NFS data in the same directory.

Do not use the top level of an MTtree to host a CIFS share. Create a subdirectory within the MTtree, and specify that subdirectory as the path for the CIFS share.

### Procedure

1. Select **Protocols > CIFS** tabs to go to the CIFS view.
2. Ensure that authentication has been configured, as described in the section regarding setting authentication parameters.
3. On the CIFS client, set shared directory permissions or security options.
4. On the CIFS view, click the Shares tab.
5. Click **Create**.
6. In the Create Shares dialog box, enter the following information:

Table 106 Shares dialog box information

Item	Description
Share Name	A descriptive name for the share.
Directory Path	The path to the target directory (for example, <code>/data/col1/backup/dir1</code> ). <b>Note:</b> col1 uses the lower case letter L followed by the number 1.
Comment	A descriptive comment about the share.

**Note:** The share name can be a maximum of 80 characters and cannot contain the following characters: `\ / : * ? " < > | + [ ] ; , =` or extended ASCII characters.

7. Add a client by clicking **Add (+)** in the Clients area. The Client dialog box is displayed. Enter the name of the client in the Client text box and click **OK**.

Consider the following when entering the client name.

- No blanks or tabs (white space) characters are enabled.
- It is not recommended to use both an asterisk (\*) and individual client name or IP address for a given share. When an asterisk (\*) is present, any other client entries for that share are not used.

<sup>1</sup> May be affected by hardware limitations.

- It is not required to use both client name and client IP address for the same client on a given share. Use client names when the client names are defined in the DNS table.
- To make share available to all clients, specify an asterisk (\*) as the client. All users in the client list can access the share, unless one or more user names are specified, in which case only the listed names can access the share.

Repeat this step for each client that you need to configure.

8. In the Max Connections area, select the text box and enter the maximum number of connections to the share that are enabled at one time. The default value of zero (also settable through the Unlimited button) enforces no limit on the number of connections.
9. Click **OK**.

The newly created share is displayed at the end of the list of shares, which are located in the center of the Shares panel.

## CLI equivalent

### Procedure

1. Run the `cifs status` command to verify that CIFS is enabled.
2. Run the `filesystem status` command to verify that file system is enabled.
3. Run the `hostname` command to determine the system hostname.
4. Create the CIFS share.

```
cifs share create <share> path <path> {max-connections <max
connections> | clients <clients> | users <users> | comment
<comment>}
```

```
# cifs share create backup path /backup
```

5. Grant client access to the share.

```
cifs share modify <share> {max-connections <max connections> |
clients <clients> | browsing {enabled | disabled} | writeable
{enabled | disabled} | users <users> | comment <comment>}
```

```
# cifs share modify backup clients
*svr24.yourdomain.com,svr24,10.24.160.116
```

6. Optionally make the share visible.

```
cifs share <share> browsing enabled
```

```
# cifs share backup browsing enabled
```

7. Optionally make the share writeable.

```
cifs share <share> writeable enabled
```

```
# cifs share backup writeable enabled
```

8. From the Windows system, select **Start > Run**, and type the hostname and directory of the CIFS share.

```
\\<DDhostname>.<DDdomain.com>\<sharename>
```

9. If there are problems connecting to the CIFS share, run the `cifs share show` command to verify the status of the share.

The warning `WARNING: The share path does not exist!` is displayed if the share does not exist or was misspelled on creation.

```
# cifs share show
----- share backup -----
enabled: yes
path: /backup
```

10. If the CIFS share is still not accessible, verify that all client information is in the access list, and all network connections are functional.

## Modifying a share

Change share information and connections.

### Procedure

1. Select **Protocols > CIFS > Shares** to navigate to the CIFS view, Shares tab.
2. Click the checkbox next the share that you wish to modify in the Share Name list.
3. Click **Modify**.
4. Modify share information:
  - a. To change the comment, enter new text in the Comment text field.
  - b. To modify a User or Group names, in the User/Group list, click the checkbox of the user or group and click **Edit** (pencil icon) or **Delete** (X). To add a user or group, click (+), and in the User/Group dialog box select the Type for User or Group, and enter the user or group name.
  - c. To modify a client name, in the Client list click the checkbox of the client and click **Edit** (pencil icon) or **Delete** (X). To add a client, click the Add (+) and add the name in the Client dialog box.
 

**Note:** To make the share available to all clients, specify an asterisk (\*) as the client. All users in the client list can access the share, unless one or more user names are specified, in which case only the listed names can access the share.
  - d. Click **OK**.
5. In the Max Connections area, in the text box, change the maximum number of connections to the share that are allowed at one time. Or select Unlimited to enforce no limit on the number of connections.
6. Click **OK**.

## Creating a share from an existing share

Create a share from an existing share and modify the new share if necessary.

### About this task

- Note:** User permissions from the existing share are carried over to the new share.

### Procedure

1. In the CIFS Shares tab, click the checkbox for the share you wish to use as the source.
2. Click **Create From**.
3. Modify the share information, as described in the section about modifying a share.

## Disabling a share

Disable one or more existing shares.

### Procedure

1. In the Shares tab, click the checkbox of the share you wish to disable in the Share Name list.
2. Click **Disable**.
3. Click **Close**.

## Enabling a share

Enable one or more existing shares.

### Procedure

1. In the Shares tab, click the checkbox of the shares you wish to enable in the Share Name list.
2. Click **Enable**.
3. Click **Close**.

## Deleting a share

Delete one or more existing shares.

### Procedure

1. In the Shares tab, click the checkbox of the shares you wish to delete in the Share Name list.
2. Click **Delete**.  
The Warning dialog box appears.
3. Click **OK**.  
The shares are removed.

## Performing MMC administration

Use the Microsoft Management Console (MMC) for administration.

DD OS supports these MMC features:

- Share management, except for browsing when adding a share, or the changing of the offline settings default, which is a manual procedure.
- Session management.
- Open file management, except for deleting files.

## Connecting to a protection system from a CIFS client

Use CIFS to connect to a protection system and create a read-only backup subfolder.

### Procedure

1. On the system CIFS page, verify that CIFS Status shows that CIFS is enabled and running.
2. In the Control Panel, open Administrative Tools and select **Computer Management**.
3. In the Computer Management dialog box, right-click **Computer Management (Local)** and select **Connect to another computer** from the menu.

4. In the **Select Computer** dialog box, select **Another computer** and enter the name or IP address for the protection system.
5. Create a `\backup` subfolder as read-only. For more information, see the section on creating a `/data/col1/backup` subfolder as read-only.

### Creating a `\data\col1\backup` subfolder as read-only

Enter a path, share name, and select permissions.

#### Procedure

1. Right-click **Shares** in the Shared Folders directory.
2. Select **New File Share** from the menu.  
The **Create a Shared Folder** wizard opens. The computer name should be the name or IP address of the protection system.
3. Enter the path for the Folder to share, for example, enter `C:\data\col1\backup\newshare`.
4. Enter the Share name, for example, enter `newshare`. Click **Next**.
5. For the Share Folder Permissions, selected Administrators have full access. Other users have read-only access. Click **Next**.
6. The Completing dialog box shows that you have successfully shared the folder with all Microsoft Windows clients in the network. Click **Finish**.

The newly created shared folder is listed in the Computer Management dialog box.

## Displaying CIFS information

Display information about shared folders, sessions, and open files.

#### Procedure

1. In the Control Panel, open Administrative Tools and select **Computer Management**.
2. Select one of the Shared Folders (**Shares**, **Sessions**, or **Open Files**) in the System Tools directory.

Information about shared folders, sessions, and open files is shown in the right panel.

## Configuring SMB signing

On a DD OS version that supports it, you can configure the SMB signing feature using the CIFS option called `server signing`.

This feature is disabled by default because it degrades performance. When enabled, SMB signing can cause a 29 percent (reads) to 50 percent (writes) throughput performance drop, although individual system performance will vary. There are three possible values for SMB signing: disabled, auto and mandatory:

- When SMB signing is set to disabled, SMB signing is disabled, this is the default.
- When SMB signing is set to required, SMB signing is required, and both computers in the SMB connection must have SMB signing enabled.

#### SMB Signing CLI Commands

```
cifs option set "server-signing" required
Sets server signing to required.
```

```
cifs option reset "server-signing"
```



Resets server signing to the default (disabled).

As a best practice, whenever you change the SMB signing options, disable and then enable (restart) CIFS service using the following CLI commands:

```
cifs disable
cifs enable
```

The DD System Manager interface displays whether the SMB signing option is disabled or set to auto or mandatory. To view this setting in the interface, navigate to: **Protocols > CIFS > Configuration tab**. In the Options area, the value for the SMB signing option will be disabled, auto or mandatory reflecting the value set using the CLI commands.

## Managing access control

Access shared from a Windows client, provide administrative access, and allow access from trusted domain users.

### Accessing shares from a Windows client

Use the command line to map a share.

#### Procedure

- From the Windows client use this DOS command:  

```
net use drive: backup-location
```

For example, enter:

```
# \\PP02\backup /USER:PP02\backup22
```

This command maps the backup share from PowerProtect system PP02 to drive H on the Windows system and gives the user named backup22 access to the \\PP\_sys\backup directory.

DD OS supports the SMB Change Notify functionality. This improves CIFS performance on the Windows client by allowing the CIFS server to automatically notify the Windows client about changes on the CIFS share, and eliminate the need for the client to poll the protection system to look for changes to the share.

### Providing domain users administrative access

Use the command line to add CIFS and include the domain name in the ssh instruction.

#### Procedure

- Enter: `adminaccess authentication add cifs`

The SSH, Telnet, or FTP command that accesses the protection system must include, in double quotation marks, the domain name, a backslash, and the user name. For example:

```
C:> ssh "domain2\djones" @dd22
```


## Allowing administrative access to a protection system for domain users

Use the command line to map a DD system default group number, and then enable CIFS administrative access.

### Procedure

1. To map a protection system default group number to a Windows group name that differs from the default group name, use the `cifs option set "dd admin group2" ["windows grp-name"]` command.

The Windows group name is a group (based on one of the user roles—admin, user, or back-up operator) that exists on a Windows domain controller, and you can have up to 50 groups (`dd admin group1` to `dd admin group50`).

 **Note:** For a description of DD OS user roles and Windows groups, see the section about managing protection systems.

2. Enable CIFS administrative access by entering:

```
adminaccess authentication add cifs
```

- The default system group `dd admin group1` is mapped to the Windows group Domain Admins.
- You can map the default system group `dd admin group2` to a Windows group named Data Domain that you create on a Windows domain controller.
- Access is available through SSH, Telnet, FTP, HTTP, and HTTPS.
- After setting up administrative access to the protection system from the Windows group Data Domain, you must enable CIFS administrative access using the `adminaccess` command.

## Restricting administrative access from Windows

Use the command line to prohibit access to users without a DD account.

### Procedure

- Enter: `adminaccess authentication del cifs`


This command prohibits Windows users access to the protection system if they do not have an account on the system.

## File access

This sections contains information about ACLs, setting DACL and SACL permissions using Windows Explorer, and so on.

### NT access control lists

Access control lists (ACLs) are enabled by default on the protection system.

 **CAUTION** Dell EMC recommends that you do not disable NTFS ACLs once they have been enabled. Contact Dell EMC Support prior to disabling NTFS ACLs.

### Default ACL Permissions

The default permissions, which are assigned to new objects created through the CIFS protocol when ACLs are enabled, depend on the status of the parent directory. There are three different possibilities:

- The parent directory has no ACL because it was created through NFS protocol.
- The parent directory has an inheritable ACL, either because it was created through the CIFS protocol or because ACL had been explicitly set. The inherited ACL is set on new objects.
- The parent directory has an ACL, but it is not inheritable. The permissions are as follows:

Table 107 Permissions

Type	Name	Permission	Apply To
Allow	SYSTEM	Full control	This folder only
Allow	CREATOR OWNER	Full control	This folder only

① Note: CREATOR OWNER is replaced by the user creating the file/folder for normal users and by Administrators for administrative users.

### Permissions for a New Object when the Parent Directory Has No ACL

The permissions are as follows:

- BUILTIN\Administrators:(OI)(CI)F
- NT AUTHORITY\SYSTEM:(OI)(CI)F
- CREATOR OWNER:(OI)(CI)(IO)F
- BUILTIN\Users:(OI)(CI)R
- BUILTIN\Users:(CI)(special access:)FILE\_APPEND\_DATA
- BUILTIN\Users:(CI)(IO)(special access:)FILE\_WRITE\_DATA
- Everyone:(OI)(CI)R

These permissions are described in more detail as follows:

Table 108 Permissions Detail

Type	Name	Permission	Apply To
Allow	Administrators	Full control	This folder, subfolders, and files
Allow	SYSTEM	Full control	This folder, subfolders, and files
Allow	CREATOR OWNER	Full control	Subfolders and files only
Allow	Users	Read & execute	This folder, subfolders, and files
Allow	Users	Create subfolders	This folder and subfolders only
Allow	Users	Create files	Subfolders only
Allow	Everyone	Read & execute	This folder, subfolders, and files

### Setting ACL Permissions and Security

Windows-based backup and restore tools such as NetBackup can be used to back up DACL- and SACL-protected files to, and restore them from, the protection system.

#### Granular and Complex Permissions (DACL)

You can set granular and complex permissions (DACL) on any file or folder object within the file system, either through using Windows commands such as `cacls`, `xcaccls`, `xcopy` and `scoopy`, or through the CIFS protocol using the Windows Explorer GUI.

#### Audit ACL (SACL)

You can set audit ACL (SACL) on any object in the file system, either through commands or through the CIFS protocol using the Windows Explorer GUI.

## Setting DACL permissions using the Windows Explorer

Use Explorer properties settings to select DACL permissions.

### Procedure

1. Right-click the file or folder and select **Properties**.
2. In the Properties dialog box, click the Security tab.
3. Select the group or user name, such as **Administrators**, from the list. The permissions appear, in this case for *Administrators, Full Control*.
4. Click the **Advanced** button, which enables you to set special permissions.
5. In the Advanced Security Settings for ACL dialog box, click the Permissions tab.
6. Select the permission entry in the list.
7. To view more information about a permission entry, select the entry and click **Edit**.
8. Select the Inherit from parent option to have the permissions of parent entries inherited by their child objects, and click **OK**.

## Setting SACL permissions using the Windows Explorer

Use Explorer properties settings to select SACL permissions.

### Procedure

1. Right-click the file or folder and select **Properties** from the menu.
2. In the Properties dialog box, click the Security tab.
3. Select the group or user name, such as **Administrators**, from the list, which displays its permissions, in this case, *Full Control*.
4. Click the **Advanced** button, which enables you to set special permissions.
5. In the Advanced Security Settings for ACL dialog box, click the Auditing tab.
6. Select the auditing entry in the list.
7. To view more information about special auditing entries, select the entry and click **Edit**.
8. Select the Inherit from parent option to have the permissions of parent entries inherited by their child objects, and click **OK**.

## Viewing or changing the current owner security ID (owner SID)

Use the Advanced Security Settings for ACL dialog box.

### Procedure

1. In the Advanced Security Settings for ACL dialog box, click the Owner tab.

- To change the owner, select a name from the Change owner list, and click **OK**.

## Controlling ID account mapping

The CIFS option `idmap-type` controls ID account mapping behavior.

This option has two values: `rid` (the default) and `none`. When the option is set to `rid`, the ID-to-id mapping is performed internally. When the option is set to `none`, all CIFS users are mapped to a local UNIX user named "cifsuser" belonging to the local UNIX group users.

Consider the following information while managing this option.

- CIFS must be disabled to set this option. If CIFS is running, disable CIFS services.
- The `idmap-type` can be set to `none` only when ACL support is enabled.
- Whenever the `idmap` type is changed, a file system metadata conversion might be required for correct file access. Without any conversion, the user might not be able to access the data. To convert the metadata, consult your contracted support provider.

## Monitoring CIFS operation

Monitoring CIFS Operation topics.

### Displaying CIFS status

View and enable/disable CIFS status.

#### Procedure

- In the DD System Manager, select **Protocols > CIFS**.
  - Status is either enabled and running, or disabled but CIFS authentication is running. To enable CIFS, see the section regarding enabling CIFS services. To disable CIFS, see the section regarding disabling CIFS services.
  - Connections** lists the tally of open connections and open files.

Table 109 Connections Details information

Item	Description
Open Connections	Open CIFS connections
Connection Limit	Maximum allowed connections
Open Files	Current open files
Max Open Files	Maximum number of open files

- Click **Connection Details** to see more connection information.

Table 110 Connections Details information

Item	Description
Sessions	Active CIFS sessions
Computer	IP address or computer name connected with DDR for the session
User	User operating the computer connected with the DDR

Table 110 Connections Details information (continued)

Item	Description
Open Files	Number of open files for each session
Connection Time	Connection length in minutes
User	Domain name of computer
Mode	File permissions
Locks	Number of locks on the file
Files	File location

## Display CIFS configuration

This section displays CIFS Configuration.

### Authentication configuration

The information in the Authentication panel changes, depending on the type of authentication that is configured.

Click the Configure link in to the left of the Authentication label in the Configuration tab. The system will navigate to the **Administration > Access > Authentication** page where you can configure authentication for Active Directory, Kerberos, Workgroups, and NIS.

#### Active directory configuration

Table 111 Active directory configuration information

Item	Description
Mode	The Active Directory mode displays.
Realm	The configured realm displays.
DDNS	The status of the DDNS Server displays: either enabled or disabled.
Domain Controllers	The name of the configured domain controllers display or a * if all controllers are permitted.
Organizational Unit	The name of the configured organizational units displays.
CIFS Server Name	The name of the configured CIFS server displays.
WINS Server Name	The name of the configured WINS server displays.
Short Domain Name	The short domain name displays.

#### Workgroup configuration

Table 112 Workgroup configuration authentication information

Item	Description
Mode	The Workgroup mode displays.
Workgroup Name	The configured workgroup name displays.

**Table 112** Workgroup configuration authentication information (continued)

Item	Description
DDNS	The status of the DDNS Server displays: either enabled or disabled.
CIFS Server Name	The name of the configured CIFS server displays.
WINS Server Name	The name of the configured WINS server displays.


## Display shares information

This section displays shares information.

### Viewing configured shares

View the list of configured shares.

**Table 113** Configured shares information


Item	Description
Share Name	The name of the share (for example, share1).
Share Status	The status of the share: either enabled or disabled.
Directory Path	The directory path to the share (for example, /data/col1/backup/dir1).  Note: col1 uses the lower case letter L followed by the number 1.
Directory Path Status	The status of the directory path.

- To list information about a specific share, enter the share name in the Filter by Share Name text box and click **Update**.
- Click **Update** to return to the default list.
- To page through the list of shares, click the < and > arrows at the bottom right of the view to page forward or backward. To skip to the beginning of the list, click |< and to skip to the end, click >|.
- Click the **Items per Page** drop-down arrow to change the number of share entries listed on a page. Choices are 15, 30, or 45 entries.

### Viewing detailed share information

Display detailed information about a share by clicking a share name in the share list.

**Table 114** Share information

Item	Description
Share Name	The name of the share (for example, share1).
Directory Path	The directory path to the share (for example, /data/col1/backup/dir1).  Note: col1 uses the lower case letter L followed by the number 1.



**Table 114** Share information (continued)

Item	Description
Directory Path Status	Indicates whether the configured directory path exists on the DDR. Possible values are Path Exists or Path Does Not Exist, the later indicating an incorrect or incomplete CIFS configuration.
Max Connections	The maximum number of connections allowed to the share at one time. The default value is Unlimited.
Comment	The comment that was configured when the share was created.
Share Status	The status of the share: either enabled or disabled.

- The Clients area lists the clients that are configured to access the share, along with a client tally beneath the list.
- The User/Groups area lists the names and type of users or groups that are configured to access the share, along with a user or group tally beneath the list.
- The Options area lists the name and value of configured options.

## Displaying CIFS statistics

Use the command line to display CIFS statistics.


### Procedure

- Enter: `cifs show detailed-stats`

The output shows number of various SMB requests received and the time taken to process them.

## Performing CIFS troubleshooting

This section provides basic troubleshooting procedures.

-  **Note:** The `cifs troubleshooting` commands provide detailed information about CIFS users and groups.

## Displaying clients current activity

Use the command line to display CIFS sessions and open files information.

### Procedure

- Enter: `cifs show active`

### Results

**Table 115** Sessions

Computer	User	Open files	Connect time (sec)	Idle time (sec)
::ffff:10.25.132.	ddve-25179109\sysadmin	1	92	0

84

Table 116 Open files

User	Mode	Locks	File
ddve-25179109\sysadmin	1	0	C:\data\col1\backup

## Setting the maximum open files on a connection

Use the command line to set the maximum number of files that can be open concurrently.

### Procedure

- Enter: `cifs option set max-global-open-files value`.

The *value* for the maximum global open files can be between 1 and the open files maximum limit. The maximum limit is based on the DDR system memory. For systems with greater than 12 GB, the maximum open files limit is 30,000. For systems with less than or equal to 12 GB, the maximum open files limit is 10,000.

Table 117 Connection and maximum open file limits

Memory	Connection Limit	Open File Maximum Limit
8 GB	300	10,000
16 GB and higher	600	30,000

- ① Note: The system has a maximum limit of 600 CIFS connections and 250,000 open files. However, if the system runs out of open files, the number of files can be increased.
- ① Note: File access latencies are affected by the number of files in a directory. To the extent possible, we recommend directory sizes of less than 250,000. Larger directory sizes might experience slower responses to metadata operations such as listing the files in the directory and opening or creating a file.

## System clock

When using active directory mode for CIFS access, the system clock time can differ by no more than five minutes from that of the domain controller.

When configured for Active Directory authentication, the system regularly syncs time with the Windows domain controller. Therefore, it is important for the domain controller to obtain the time from a reliable time source. Refer to the Microsoft documentation for your Windows operating system version to configure the domain controller with a time source.

- ⚠ **WARNING** When the system is configured for Active Directory authentication, it uses an alternate mechanism to sync time with the domain controller. To avoid time sync conflicts, do not enable NTP when the system is configured for Active Directory authentication.

## Synchronize from an NTP server

Configure the time server synchronization, as described in the section regarding working with time and date settings.

# CHAPTER 9

## NFS

This chapter includes:

- NFS overview.....248
- Managing NFS client access to the protection system.....248
- Displaying NFS information.....252
- Integrating a DDR into a Kerberos domain.....253
- Add and delete KDC servers after initial configuration.....254

## NFS overview

Network File System (NFS) clients can have access to the system directories or MTrees on the protection system.

- The `/backup` directory is the default destination for non-MTree compressed backup server data.
- The `/data/coll/backup` path is the root destination when using MTrees for compressed backup server data.
- The `/ddvar/core` directory contains system core and log files (remove old logs and core files to free space in this area).

① **Note:** On protection systems, the `/ddvar/core` is on a separate partition. If you mount `/ddvar` only, you will not be able to navigate to `/ddvar/core` from the `/ddvar` mountpoint.

Clients, such as backup servers that perform backup and restore operations need access to the `/backup` or `/data/coll/backup` areas, at a minimum. Clients that have administrative access need to be able to access the `/ddvar/core` directory to retrieve core and log files.

As part of the initial system configuration, NFS clients were configured to access these areas. This chapter describes how to modify these settings and how to manage data access.

① **Note:**

- The `nfs` command manages backups and restores between NFS clients and protection systems, and it displays NFS statistics and status. For complete information about the `nfs` command, see the *DD OS Command Reference Guide*.
- For information about setting up third-party clients to use the protection system as a server, see the related tuning guide, such as the *Solaris System Tuning*, which is available from the Dell EMC support web site.

## HA systems and NFS

HA systems are compatible with NFS. If a NFS job is in progress during a failover, the job will **not** need to be restarted.

① **Note:** `/ddvar` is an ext3 file system, and cannot be shared like a normal MTree-based share. The information in `/ddvar` will become stale when the active node fails over to the standby node because the filehandles are different on the two nodes. If `/ddvar` is mounted to access log files or upgrade the system, unmount and remount `/ddvar` if a failover has occurred since the last time `/ddvar` was mounted.

To create valid NFS exports that will failover with HA, the export needs to be created from the Active HA node, and generally shared over the failover network interfaces.

## Managing NFS client access to the protection system

The topics in this section describe how to manage NFS client access to a protection System.

The KB article *NFS Best Practices for Data Domain and client OS*, available at <https://support.emc.com/kb/180552>, provides additional information about best practices for NFS.

## Enabling NFS services

Enable NFS services to allow the client to access the system using the NFS protocol.

### Procedure

1. Select **Protocols > NFS**.  
The NFS view opens displaying the Exports tab.
2. Click **Enable**.

## Disabling NFS services

Disable NFS services to prevent the client access to the system using the NFS protocol.

### Procedure

1. Select the **Protocols > NFS** tabs.  
The NFS view opens displaying the Exports tab.
2. Click **Disable**.

## Creating an export

You can use DD SM's Create button on the NFS view or use the Configuration Wizard to specify the NFS clients that can access the `/backup`, `/data/coll/backup`, `/ddvar`, `/ddvar/core` areas, or the `/ddvar/ext` area if it exists.

### About this task

A protection system supports a maximum of 2048 exports<sup>2</sup>, with the number of connections scaling in accordance with system memory.

**Note:** You have to assign client access to each export separately and remove access from each export separately. For example, a client can be removed from `/ddvar` and still have access to `/data/coll/backup`.

**CAUTION** If Replication is to be implemented, a single destination system can receive backups from both CIFS clients and NFS clients as long as separate directories or MTrees are used for each. Do not mix CIFS and NFS data in the same area.

Do not use the top level of an MTree to host an NFS export. Create a subdirectory within the MTree, and specify that subdirectory as the path for the NFS export.

### Procedure

1. Select **Protocols****NFS**.  
The NFS view opens displaying the Exports tab.
2. Click **Create**.
3. Enter the pathname in the Directory Path text box (for example, `/data/coll/backup/dir1`).  
**Note:** `coll` uses the lower-case letter L followed by the number 1.
4. In the Clients area, select an existing client or click the + icon to create a client.  
The Client dialog box is displayed.

<sup>2</sup> May be affected by hardware limitations.

- a. Enter a server name in the text box.

Enter fully qualified domain names, hostnames, or IP addresses. A single asterisk (\*) as a wild card indicates that all backup servers are to be used as clients.

- ① **Note:** Clients given access to the `/data/coll/backup` directory have access to the entire directory. A client given access to a subdirectory of `/data/coll/backup` has access only to that subdirectory.
- A client can be a fully-qualified domain hostname, an IPv4 or IPv6 IP address, an IPv4 address with either a netmask or prefix length, an IPv6 address with prefix length, an NIS netgroup name with the prefix `g`, or an asterisk (\*) wildcard with a domain name, such as `*.yourcompany.com`.
- A client added to a subdirectory under `/data/coll/backup` has access only to that subdirectory.
- Enter an asterisk (\*) as the client list to give access to all clients on the network.

- b. Select the checkboxes of the NFS options for the client.

General:

- Read-only permission (ro).
- Allow connections from ports below 1024 (secure) (default).

Anonymous UID/GID:

- Map requests from UID (user identifier) or GID (group identifier) 0 to the anonymous UID/GID (root\_squash).
- Map all user requests to the anonymous UID/GID (all\_squash).
- Use Default Anonymous UID/GID.

Allowed Kerberos Authentication Modes:

- Unauthenticated connections (sec=sys). Select to not use authentication.
- Authenticated Connections (sec=krb5).

- ① **Note:** Integrity and Privacy are supported, although they might slow performance considerably.

- c. Click **OK**.

5. Click **OK** to create the export.

## Modifying an export

Change the directory path, domain name, and other options using the GUI.

### Procedure

1. Select **Protocols > NFS**.  
The NFS view opens displaying the Exports tab.
2. Click the checkbox of an export in the NFS Exports table.
3. Click **Modify**.
4. Modify the pathname in the Directory Path text box.
5. In the Clients area, select another client and click the pencil icon (modify), or click the + icon to create a client.

- a. Enter a server name in the Client text box.

Enter fully qualified domain names, hostnames, or IP addresses. A single asterisk (\*) as a wild card indicates that all backup servers are to be used as clients.

① **Note:** Clients given access to the `/data/coll/backup` directory have access to the entire directory. A client given access to a subdirectory of `/data/coll/backup` has access only to that subdirectory.

- A client can be a fully-qualified domain hostname, an IPv4 or IPv6 IP address, an IPv4 address with either a netmask or prefix length, an IPv6 address with prefix length, an NIS netgroup name with the prefix `@`, or an asterisk (\*) wildcard with a domain name, such as `*.yourcompany.com`.  
A client added to a subdirectory under `/data/coll/backup` has access only to that subdirectory.
- Enter an asterisk (\*) as the client list to give access to all clients on the network.

- b. Select the checkboxes of the NFS options for the client.

General:

- Read-only permission (`ro`).
- Allow connections from ports below 1024 (`secure`) (default).

Anonymous UID/GID:

- Map requests from UID (user identifier) or GID (group identifier) 0 to the anonymous UID/GID (`root_squash`).
- Map all user requests to the anonymous UID/GID (`all_squash`).
- Use Default Anonymous UID/GID.

Allowed Kerberos Authentication Modes:

- Unauthenticated connections (`sec=sys`). Select to not use authentication.
- Authenticated Connections (`sec=krb5`).

① **Note:** Integrity and Privacy are not supported.

- c. Click **OK**.

6. Click **OK** to modify the export.

## Creating an export from an existing export

Create an export from an existing export and then modify it as needed.

### Procedure

1. In the NFS Exports tab, click the checkbox of the export you wish to use as the source.
2. Click **Create From**.
3. Modify the export information, as described in section about modifying an export.



## Deleting an export

Delete an export from the NFS Exports tab.

### Procedure

1. In the NFS Exports tab, click the checkbox of the export you wish to delete.
2. Click **Delete**.
3. Click **OK** and **Close** to delete the export.

## Displaying NFS information

The topics in this section describe how to use the DD System Manager to monitor NFS client status and NFS configuration.

### Viewing NFS status

Display whether NFS is active and Kerberos is enabled.

#### Procedure

- Click **Protocols > NFS**.

The top panel shows the operational status of NFS; for example, whether NFS is currently active and running, and whether Kerberos mode is enabled.

① **Note:** Click **Configure** to view the **Administration > Access > Authentication** tab where you can configure Kerberos authentication.

### Viewing NFS exports

See the list of clients allowed to access the protection system.

#### Procedure

1. Click **Protocols > NFS**.

The Exports view shows a table of NFS exports that are configured for system and the mount path, status, and NFS options for each export.

2. Click an export in the table to populate the Detailed Information area, below the Exports table.

In addition to the export's directory path, configured options, and status, the system displays a list of clients.

Use the **Filter By** text box to sort by mount path.

Click **Update** for the system to refresh the table and use the filters supplied.

Click **Reset** for the system to clear the Path and Client filters.

### Viewing active NFS clients

Display all clients that have been connected in the past 15 minutes and their mount path.

#### Procedure

- Select the **Protocols > NFS > Active Clients** tab.

The Active Clients view displays, showing all clients that have been connected in the past 15 minutes and their mount path.

Use the Filter By text boxes to sort by mount path and client name.

Click **Update** for the system to refresh the table and use the filters supplied.


Click **Reset** for the system to clear the Path and Client filters.



## Integrating a DDR into a Kerberos domain

Set the domain name, the host name, and the DNS server for the DDR.

### About this task

Enable the DDR to use the authentication server as a Key Distribution Center (for UNIX) and as a Distribution Center (for Windows Active Directory).


 **CAUTION** The examples provided in this description are specific to the operating system (OS) used to develop this exercise. You must use commands specific to your OS.

-  **Note:** For UNIX Kerberos mode, a keytab file must be transferred from the Key Distribution Center (KDC) server, where it is generated, to the DDR. If you are using more than one DDR, each DDR requires a separate keytab file. The keytab file contains a shared secret between the KDC server and the DDR.
-  **Note:** When using a UNIX KDC, the DNS server does not have to be the KDC server, it can be a separate server.

### Procedure

1. Set the host name and the domain name for the DDR, using DDR commands.


```
net set hostname <host>
net set (domainname <local-domain-name>)
```

 **Note:** The host name is the name of the DDR.

2. Configure NFS principal (node) for the DDR on the Key Distribution Center (KDC).

Example:

```
addprinc nfs/hostname@realm
```

 **Note:** Hostname is the name for the DDR.

3. Verify that there are nfs entries added as principals on the KDC.

Example:

```
listprincs
nfs/hostname@realm
```

4. Add the DDR principal into a keytab file.

Example:

```
ktadd <keytab_file> nfs/hostname@realm
```

5. Verify that there is an nfs keytab file configured on the KDC.

Example:

```
klist -k <keytab_file>
```

① | Note: The <keytab\_file> is the keytab file used to configure keys in a previous step.

6. Copy the keytab file from the location where the keys for NFS DDR are generated to the DDR in the /ddvar/ directory.

**Table 118** Keytab destination

Copy file from:	Copy file to:
<keytab_file> (The keytab file configured in a previous step.)	/ddvar/

7. Set the realm on the DDR, using the following DDR command:

```
authentication kerberos set realm <home realm> kdc-type <unix, windows.>
kdc <IP address of server>
```

8. When the kdc-type is UNIX, import the keytab file from /ddvar/ to /ddr/etc/, where the Kerberos configuration file expects it. Use the following DDR command to copy the file:

```
authentication kerberos keytab import
```

① | NOTICE This step is required only when the kdc-type is UNIX.

Kerberos setup is now complete.

9. To add a NFS mount point to use Kerberos, use the nfs add command.

See the *DD OS Command Reference Guide* for more information.

10. Add host, NFS and relevant user principals for each NFS client on the Key Distribution Center (KDC).

Example: listprincs

```
host/hostname@realm
nfs/hostname@realm
root/hostname@realm
```

11. For each NFS client, import all its principals into a keytab file on the client.

Example:

```
ktadd -k <keytab_file> host/hostname@realm
```

```
ktadd -k <keytab_file> nfs/hostname@realm
```

## Add and delete KDC servers after initial configuration

After you have integrated a DDR into a Kerberos domain, and thereby enabled the DDR to use the authentication server as a Key Distribution Center (for UNIX) and as a Distribution Center (for Windows Active Directory), you can use the following procedure to add or delete KDC servers.

### Procedure

1. Join the DDR to a Windows Active Directory (AD) server or a UNIX Key Distribution Center (KDC).

```
authentication kerberos set realm <home-realm> kdc-type {windows [kdc
<kdc-list>] | unix kdc <kdc-list>}
```

Example: authentication kerberos set realm krb5.test kdc-type unix kdc
nfskrb-kdc.krb5.test

This command joins the system to the krb5.test realm and enables Kerberos authentication for NFS clients.

**Note:** A keytab generated on this KDC must exist on the DDR to authenticate using Kerberos.

2. Verify the Kerberos authentication configuration.

```
authentication kerberos show config
Home Realm:          krb5.test
KDC List:            nfskrb-kdc.krb5.test
KDC Type:           unix
```

3. Add a second KDC server.

```
authentication kerberos set realm <home-realm> kdc-type {windows [kdc
<kdc-list>] | unix kdc <kdc-list>}
```

Example: `authentication kerberos set realm krb5.test kdc-type unix kdc ostqa-sparc2.krb5.test nfskrb-kdc.krb5.test`

**Note:** A keytab generated on this KDC must exist on the DDR to authenticate using Kerberos.

4. Verify that two KDC servers are added.

```
authentication kerberos show config
Home Realm:          krb5.test
KDC List:            ostqa-sparc2.krb5.test, nfskrb-kdc.krb5.test
KDC Type:           unix
```

5. Display the value for the Kerberos configuration key.

```
reg show config.kerberos
config.kerberos.home_realm = krb5.test
config.kerberos.home_realm.kdc1 = ostqa-sparc2.krb5.test
config.kerberos.home_realm.kdc2 = nfskrb-kdc.krb5.test
config.kerberos.kdc_count = 2
config.kerberos.kdc_type = unix
```

6. Delete a KDC server.

Delete a KDC server by using the `authentication kerberos set realm <home-realm> kdc-type {windows [kdc <kdc-list>] | unix kdc <kdc-list>}` command without listing the KDC server that you want to delete. For example, if the existing KDC servers are `kdc1`, `kdc2`, and `kdc3`, and you want to remove `kdc2` from the realm, you could use the following example:

```
authentication kerberos set realm <realm-name> kdc-type <kdc_type> kdc
kdc1,kdc3
```



# CHAPTER 10

## NFSv4

This chapter includes:

• Introduction to NFSv4.....	258
• ID Mapping Overview.....	259
• External formats.....	259
• Internal Identifier Formats.....	260
• When ID mapping occurs.....	260
• NFSv4 and CIFS/SMB Interoperability.....	262
• NFS Referrals.....	263
• NFSv4 and High Availability.....	264
• NFSv4 Global Namespaces.....	264
• NFSv4 Configuration.....	265
• Kerberos and NFSv4.....	266
• Enabling Active Directory.....	269

## Introduction to NFSv4

Because NFS clients are increasingly using NFSv4.x as the default NFS protocol level, protection systems can now employ NFSv4 instead of requiring the client to work in a backwards-compatibility mode.

Clients can work in mixed environments in which NFSv4 and NFSv3 must be able to access the same NFS exports.

The DD OS NFS server can be configured to support NFSv4 and NFSv3, depending on site requirements. You can make each NFS export available to only NFSv4 clients, only NFSv3 clients, or both.

Several factors might affect whether you choose NFSv4 or NFSv3:

- **NFS client support**  
Some NFS clients may support only NFSv3 or NFSv4, or may operate better with one version.
- **Operational requirements**  
An enterprise might be strictly standardized to use either NFSv4 or NFSv3.
- **Security**  
If you require greater security, NFSv4 provides a greater security level than NFSv3, including ACL and extended owner and group configuration.
- **Feature requirements**  
If you need byte-range locking or UTF-8 files, you should choose NFSv4.
- **NFSv3 submounts**  
If your existing configuration uses NFSv3 submounts, NFSv3 might be the appropriate choice.

## NFSv4 compared to NFSv3

NFSv4 provides enhanced functionality and features compared to NFSv3.

The following table compares NFSv3 features to those for NFSv4.

Table 119 NFSv4 compared to NFSv3

Feature	NFSv3	NFSv4
Standards-based Network Filesystem	Yes	Yes
Kerberos support	Yes	Yes
Kerberos with LDAP	Yes	Yes
Quota reporting	Yes	Yes
Multiple exports with client-based access lists	Yes	Yes
ID mapping	Yes	Yes
UTF-8 character support	No	Yes
File/directory-based Access Control Lists (ACL)	No	Yes
Extended owner/group (OWNER@)	No	Yes
File share locking	No	Yes
Byte range locking	No	Yes
DD-CIFS integration (locking, ACL, AD)	No	Yes



Table 119 NFSv4 compared to NFSv3 (continued)

Feature	NFSv3	NFSv4
Stateful file opens and recovery	No	Yes
Global namespace and pseudoFS	No	Yes
Multi-system namespace using referrals	No	Yes

## NFSv4 ports

You can enable or disable NFSv4 and NFSv3 independently. In addition, you can move NFS versions to different ports; both versions do not need to occupy the same port.

With NFSv4, you do not need to restart the file system if you change ports. Only an NFS restart is required in such instances.

Like NFSv3, NFSv4 runs on Port 2049 as the default if it is enabled.

NFSv4 does not use portmapper (Port 111) or mountd (Port 2052).

## ID Mapping Overview

NFSv4 identifies owners and groups by a common external format, such as `joe@example.com`. These common formats are known as identifiers, or IDs.

Identifiers are stored within an NFS server and use internal representations such as ID 12345 or ID S-123-33-667-2. The conversion between internal and external identifiers is known as ID mapping.

Identifiers are associated with the following:

- Owners of files and directories
- Owner groups of files and directories
- Entries in Access Control Lists (ACLs)

Protection systems use a common internal format for NFS and CIFS/SMB protocols, which allows files and directories to be shared between NFS and CIFS/SMB. Each protocol converts the internal format to its own external format with its own ID mapping.

## External formats

The external format for NFSv4 identifiers follows NFSv4 standards (for example, RFC-7530 for NFSv4.0). In addition, supplemental formats are supported for interoperability.

## Standard identifier formats

Standard external identifiers for NFSv4 have the format `identifier@domain`. This identifier is used for NFSv4 owners, owner-groups, and access control entries (ACEs). The domain must match the configured NFSv4 domain that was set using the `nfs` option command.

The following CLI example sets the NFSv4 domain to `mycorp.com` for the NFS server:

```
nfs option set nfs4-domain mycorp.com
```

See client-specific documentation you have for setting the client NFS domain. Depending on the operating system, you might need to update a configuration file (for example, `/etc/idmapd.conf`) or use a client administrative tool.

- i** Note: If you do not set the default value, it will follow the DNS name for the protection system.
- i** Note: The file system must be restarted after changing the DNS domain for the nfs4-domain to automatically update.

## ACE extended identifiers

For ACL ACE entries, protection system NFS servers also support the following standard NFSv4 ACE extended identifiers defined by the NFSv4 RFC:

- OWNER@, The current owner of the file or directory
- GROUP@, the current owner group of the file or directory.
- The special identifiers INTERACTIVE@, NETWORK@, DIALUP@, BATCH@, ANONYMOUS@, AUTHENTICATED@, SERVICE@.

## Alternative formats

To allow interoperability, NFSv4 servers on protection systems support some alternative identifier formats for input and output.

- Numeric identifiers; for example, "12345".
- Windows compatible Security identifiers (SIDs) expressed as "S-NNN-NNN-..."

See the sections on input mapping and output mapping for more information about restrictions to these formats.

## Internal Identifier Formats

The DD file system stores identifiers with each object (file or directory) in the filesystem. All objects have a numeric user ID (UID) and group ID (GID). These, along with a set of mode bits, allow for traditional UNIX/Linux identification and access controls.

Objects created by the CIFS/SMB protocol, or by the NFSv4 protocol when NFSv4 ACLs are enabled, also have an extended security descriptor (SD). Each SD contains the following:

- An owner security identifier (SID)
- An owner group SID
- A discretionary ACL (DACL)
- (Optional) A system ACL (SACL)

Each SID contains a relative ID (RID) and a distinct domain in a similar manner to Windows SIDs. See the section on NFSv4 and CIFS interoperability for more information on SIDs and the mapping of SIDs.

## When ID mapping occurs

The protection system NFSv4 server performs mapping in the following circumstances:

- Input mapping  
The NFS server receives an identifier from an NFSv4 client. See Input mapping on page 261.
- Output mapping:  
An identifier is sent from the NFS server to the NFSv4 client. See Output mapping on page 261.
- Credential mapping

The RPC client credentials are mapped to an internal identity for access control and other operations. See *Credential mapping* on page 261.

## Input mapping

Input mapping occurs when an NFSv4 client sends an identifier to the protection system NFSv4 server—setting up the owner or owner-group of a file, for example. Input mapping is distinct from credential mapping.

Standard format identifiers such as `joe@mycorp.com` are converted into an internal UID/GID based on the configured conversion rules. If NFSv4 ACLs are enabled, a SID will also be generated, based on the configured conversion rules.

Numeric identifiers (for example, "12345") are directly converted into corresponding UID/GIDs if the client is not using Kerberos authentication. If Kerberos is being used, an error will be generated as recommended by the NFSv4 standard. If NFSv4 ACLs are enabled, a SID will be generated based on the conversion rules.

Windows SIDs (for example, "S-NNN-NNN-...") are validated and directly converted into the corresponding SIDs. A UID/GID will be generated based on the conversion rules.

## Output mapping

Output mapping occurs when the NFSv4 server sends an identifier to the NFSv4 client; for example, if the server returns the owner or owner-group of a file.

1. If configured, the output might be the numeric ID.  
This can be useful for NFSv4 clients that are not configured for ID mapping (for example, some Linux clients).
2. Mapping is attempted using the configured mapping services, (for example, NIS or Active Directory).
3. The output is a numeric ID or SID string if mapping fails and the configuration is allowed.
4. Otherwise, nobody is returned.

The `nfs` option `nfs4-idmap-out-numeric` configures the mapping on output:

- If `nfs` option `nfs4-idmap-out-numeric` is set to `map-first`, mapping will be attempted. On error, a numeric string is output if allowed. This is the default.
- If `nfs` option `nfs4-idmap-out-numeric` is set to `always`, output will always be a numeric string if allowed.
- If `nfs` option `nfs4-idmap-out-numeric` is set to `never`, mapping will be attempted. On error, `nobody@nfs4-domain` is the output.  
If the RPC connection uses GSS/Kerberos, a numeric string is never allowed and `nobody@nfs4-domain` is the output.

The following example configures the protection system NFS server to always attempt to output a numeric string on output. For Kerberos the name `nobody` is returned:

```
nfs option set nfs4-idmap-out-numeric always
```

## Credential mapping

The NFSv4 server provides credentials for the NFSv4 client.

These credentials perform the following functions:

- Determine the access policy for the operation; for example, the ability to read a file.
- Determine the default owner and owner-group for new files and directories.

Credentials sent from the client may be `john_doe@mycorp.com`, or system credentials such as `UID=1000, GID=2000`. System credentials specify a UID/GID along with auxiliary group IDs.

If NFSv4 ACLs are disabled, then the UID/GID and auxiliary group IDs are used for the credentials.

If NFSv4 ACLs are enabled, then the configured mapping services are used to build an extended security descriptor for the credentials:

- SIDs for the owner, owner-group, and auxiliary group mapped and added to the Security Descriptor (SD).
- Credential privileges, if any, are added to the SD.

## NFSv4 and CIFS/SMB Interoperability

The security descriptors used by NFSv4 and CIFS are similar from an ID mapping perspective, although there are differences.

You should be aware of the following to ensure for optimal interoperability:

- Active Directory should be configured for both CIFS and NFSv4, and the NFS ID mapper should be configured to use Active Directory for ID mapping.
- If you are using CIFS ACLs extensively, you can usually improve compatibility by also enabling NFSv4 ACLs.
  - Enabling NFSv4 ACLs allows NFSv4 credentials to be mapped to the appropriate SID when evaluating DACL access.
- The CIFS server receives credentials from the CIFS client, including default ACL and user privileges.
  - In contrast, the NFSv4 server receives a more limited set of credentials, and constructs credentials at runtime using its ID mapper. Because of this, the filesystem might see different credentials.

## CIFS/SMB Active Directory Integration

The protection system NFSv4 server can be configured to use the Windows Active Directory configuration that is set with the protection system CIFS server.

The system is mapped to use Active Directory if possible. This functionality is disabled by default, but you can enable it using the following command:

```
nfs option set nfs4-idmap-active-directory enabled
```

## Default DACL for NFSv4

NFSv4 sets a different default DACL (discretionary access control list) than the default DACL supplied by CIFS.

Only `OWNER@`, `GROUP@` and `EVERYONE@` are defined in the default NFSv4 DACL. You can use ACL inheritance to automatically add CIFS-significant ACEs by default if appropriate.

## System Default SIDs

Files and directories created by NFSv3, and NFSv4 without ACLs, use the default system domain, sometimes referred to as the default UNIX domain:

- User SIDs in the system domain have format `S-1-22-1-N`, where `N` is the UID.
- Group SIDs in the system domain have format `S-1-22-2-N`, when `N` is the GID.

For example, a user with UID 1234 would have an owner SID of S-1-22-1-1234.

## Common identifiers in NFSv4 ACLs and SIDs

The EVERYONE@ identifier and other special identifiers (such as BATCH@, for example) in NFSv4 ACLs use the equivalent CIFS SIDs and are compatible.

The OWNER@ and GROUP@ identifiers have no direct correspondence in CIFS; they appear as the current owner and current owner-group of the file or directory.

## NFS Referrals

The referral feature allows an NFSv4 client to access an export (or file system) in one or multiple locations. Locations can be on the same NFS server or on different NFS servers, and use either the same or different path to reach the export.

Because referrals are an NFSv4 feature, they apply only to NFSv4 mounts.

Referrals can be made to any server that uses NFSv4 or later, including the following:

- A protection system running NFS with NFSv4 enabled
- Other servers that support NFSv4 including Linux servers, NAS appliances, and VNX systems.

A referral can use an NFS export point with or without a current underlying path in the DD file system.

NFS exports with referrals can be mounted through NFSv3, but NFSv3 clients will not be redirected since referrals are a NFSv4 feature. This characteristic is useful in scaleout systems to allow exports to be redirected at a file-management level.

## Referral Locations

NFSv4 referrals always have one or more locations.

These locations consist of the following:

- A path on a remote NFS server to the referred filesystem.
- One or more server network addresses that allow the client to reach the remote NFS server.

Typically when multiple server addresses are associated with the same location, those addresses are found on the same NFS server.

## Referral location names

You can name each referral location within an NFS export. You can use the name to access the referral as well as to modify or delete it.

A referral name can contain a maximum of 80 characters from the following character sets:

- a-z
- A-Z
- 0-9
- "."
- ","
- "\_"
- "-"

- i** Note: You can include spaces as long as those spaces are embedded within the name. If you use embedded spaces, you must enclose the entire name in double quotes.

Names that begin with "." are reserved for automatic creation by the protection system. You can delete these names but you cannot create or modify them using the command line interface (CLI) or system management services (SMS).

## Referrals and Scaleout Systems

NFSv4 referrals and locations can better enable access if you are scaling out your protection systems.

Because your system might or might not already contain a global namespace, the following two scenarios describe how you might use NFSv4 referrals:

- Your system does not contain a global namespace.
  - You can use NFSv4 referrals to build that global namespace. System administrators can build these global namespaces, or you can use smart system manager (SM) element building referrals as necessary.
- Your system already has a global namespace.
  - If your system has a global namespace with MTrees placed in specific nodes, NFS referrals can be created to redirect access to those MTrees to the nodes added to the scaled-out system. You can create these referrals or have them performed automatically within NFS if the necessary SM or file manager (FM) information is available.

## NFSv4 and High Availability

With NFSv4, protocol exports (for example, `/data/coll/<mtree>`) are mirrored in a High Availability (HA) setup. However, configuration exports such as `/ddvar` are not mirrored.

The `/ddvar` filesystem is unique to each node of an HA pair. As a result, `/ddvar` exports and their associated client access lists are not mirrored to the standby node in an HA environment.

The information in `/ddvar` becomes stale when the active node fails over to the standby node. Any client permissions granted to `/ddvar` on the original active node must be recreated on the newly active node after a failover occurs.

You must also add any additional `/ddvar` exports and their clients (for example, `/ddvar/core`) that were created on the original active node to the newly active node after a failover occurs.

Finally, any desired `/ddvar` exports must be unmounted from the client and then remounted after a failover occurs.

## NFSv4 Global Namespaces

The NFSv4 server provides a virtual directory tree known as a PseudoFS to connect NFS exports into a searchable set of paths.

The use of a PseudoFS distinguishes NFSv4 from NFSv3, which uses the MOUNTD auxiliary protocol.

In most configurations, the change from NFSv3 MOUNTD to NFSv4 global namespace is transparent and handled automatically by the NFSv4 client and server.



## NFSv4 global namespaces and NFSv3 submounts

If you use NFSv3 export submounts, the global namespaces characteristic of NFSv4 might prevent submounts from being seen on the NFSv4 mount.

### Example 1 NFSv3 main exports and submount exports

If NFSv3 has a main export and a submount export, these exports might use the same NFSv3 clients yet have different levels of access:

Table 120 NFSv3 main exports and submount exports

Export	Path	Client	Options
Mt1	/data/coll/mt1	client1.example.com	ro
Mt1-sub	/data/coll/mt1/subdir	client1.example.com	rw

In the previous table, the following applies to NFSv3:

- If client1.example.com mounts /data/coll/mt1, the client gets read-only access.
- If client1.example.com mounts /data/coll/mt1/subdir, the client gets read-write access.

NFSv4 operates in the same manner in regard to highest-level export paths. For NFSv4, client1.example.com navigates the NFSv4 PseudoFS until it reaches the highest-level export path, /data/coll/mt1, where it gets read-only access.

However, because the export has been selected, the submount export (Mt1-sub) is not part of the PseudoFS for the client and read-write access is not given.

### Best practice

If your system uses NFSv3 exports submounts to give the client read-write access based on the mount path, you must consider this before using NFSv4 with these submount exports.

With NFSv4, each client has an individual PseudoFS.

Table 121 NFSv3 submount exports

Export	Path	Client	Options
Mt1	/data/coll/mt1	client1.example.com	ro
Mt1-sub	/data/coll/mt1/subdir	client2.example.com	rw

## NFSv4 Configuration

The default protection system configuration only enables NFSv3. To use NFSv4, you must first enable the NFSv4 server.



## Enabling the NFSv4 Server

### Procedure

1. Enter `nfs enable version 4` to enable NFSv4:

```
# nfs enable version 4
NFS server version(s) 3:4 enabled.
```

2. (Optional) If you want to disable NFSv3, enter `nfs disable version 3`.

```
# nfs disable version 3
NFS server version(s) 3 disabled.
NFS server version(s) 4 enabled.
```

### After you finish

After the NFSv4 server is enabled, you might need to perform additional NFS configuration tasks specifically for your site. These tasks can include:

- Setting the NFSv4 domain
- Configuring NFSv4 ID mapping
- Configuring ACL (Access Control Lists)

## Setting the default server to include NFSv4

### About this task

The NFS command option `default-server-version` controls which NFS version is enabled when you enter the `nfs enable` command without specifying a version.

### Procedure

1. Enter the `nfs option set default-server-version 3:4` command:

```
# nfs option set default-server-version 3:4
NFS option 'default-server-version' set to '3:4'.
```

## Updating existing exports

You can update existing exports to change the NFS version used by your protection system.

### Procedure

1. Enter the `nfs export modify all` command:

```
# nfs export modify all clients all options version=version number
```

To ensure all existing clients have either version 3, 4, or both, you can modify the NFS version to the appropriate string. The following example shows NFS modified to include versions 3 and 4:

```
#nfs export modify all clients all options version=3:4
```

For more information about the `nfs export` command, see the *DD OS Command Reference Guide* for more information.

## Kerberos and NFSv4

Both NFSv4 and NFSv3 use the Kerberos authentication mechanism to secure user credentials.

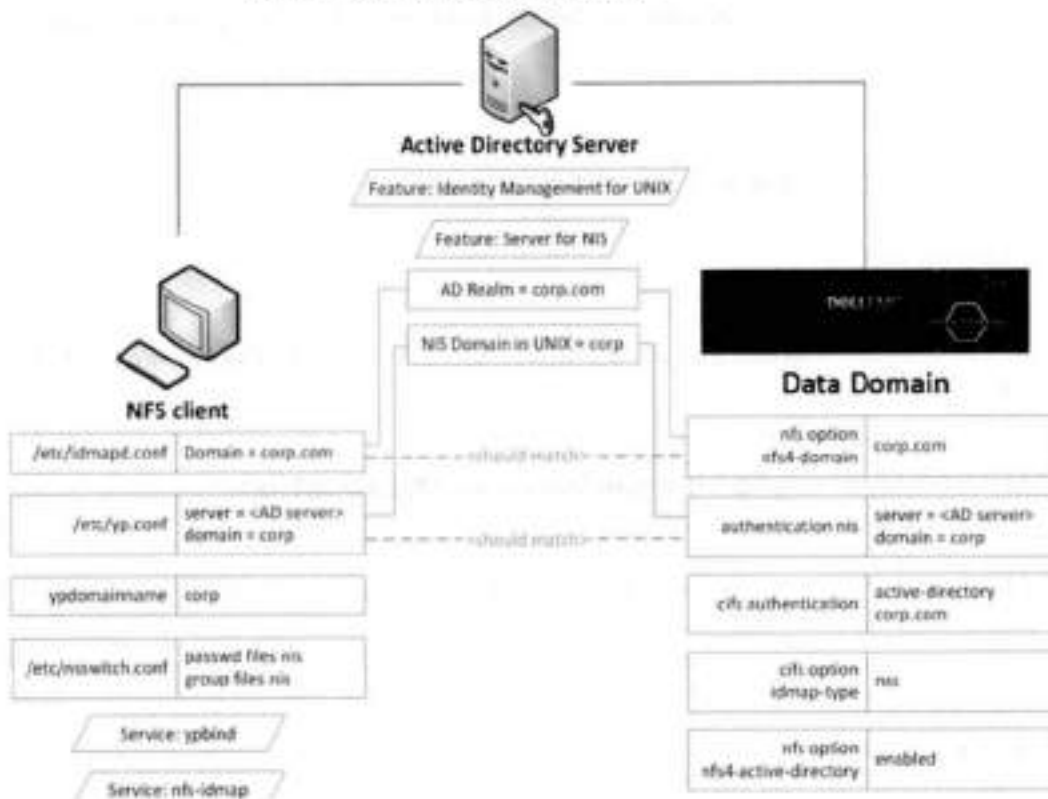
Kerberos prevents user credentials from being spoofed in NFS packets and protects them from tampering en route to the protection system.

There are distinct types of Kerberos over NFS:

- Kerberos 5 (`sec=krb5`)  
Use Kerberos for user credentials.
- Kerberos 5 with integrity (`sec=krb5i`)  
Use Kerberos and check the integrity of the NFS payload using an encrypted checksum.
- Kerberos 5 with security (`sec=krb5p`)  
Use Kerberos 5 with integrity and encrypt the entire NFS payload.

① Note: `krb5i` and `krb5p` can both cause performance degradation due to additional computational overhead on both the NFS client and the protection system.

Figure 7 Active Directory Configuration



You employ existing commands that are used for NFSv3 when configuring your system for Kerberos. See the `nfsv3` chapter of the *DD OS Command Reference Guide* for more information.

## Configuring Kerberos with a Linux-Based KDC

### Before you begin

You should ensure that all your systems can access the Key Distribution Center (KDC).

If the systems cannot reach the KDC, check the domain name system (DNS) settings.

### About this task

The following steps allow you to create keytab files for the client and the protection system:

- In Steps 1-3, you create the keytab file for the protection system.

- In Steps 4-5, you create the keytab file for the client.

#### Procedure

1. Create the `nfs/<ddr_dns_name>@<realm>` service principal.

```
kadmin.local: addprinc -randkey nfs/ddr12345.<domain-name>@<domain-name>
```

2. Export `nfs/<ddr_dns_name>@<realm>` to a keytab file.

```
kadmin.local: ktadd -k /tmp/ddr.keytab nfs/ddr12345.corp.com@CORP.COM
```

3. Copy the keytab file to the protection system at the following location:

```
/ddr/var/krb5.keytab
```

4. Create one of the following principals for the client and export that principal to the keytab file:

```
nfs/<client_dns_name>@<REALM>  
root/<client_dns_name>@<REALM>
```

5. Copy the keytab file to the client at the following location:

```
/etc/krb5.keytab
```

- ① Note: It is recommended that you use an NTP server to keep the time synchronized on all entities.

## Configuring the protection System to Use Kerberos Authentication

#### Procedure

1. Configure the KDC and Kerberos realm on the protection system by using the `authentication` command:

```
# authentication kerberos set realm <realm> kdc-type unix kdc <kdc-server>
```

2. Import the keytab file:

```
# authentication kerberos keytab import
```

3. (Optional) Configure the NIS server by entering the following commands:

```
# authentication nis servers add <server>  
# authentication nis domain set <domain-name>  
# authentication nis enable  
# filesys restart
```

4. (Optional) Make the `nfs4-domain` the same as the Kerberos realm using the `nfs option` command:

```
nfs option set nfs4-domain <kerberos-realm>
```

5. Add a client to an existing export by adding `sec=krb5` to the `nfs export add` command:

```
nfs export add <export-name> clients * options version=4,sec=krb5
```

## Configuring Clients

### Procedure

1. Configure the DNS server and verify that forward and reverse lookups are working.
2. Configure the KDC and Kerberos realm by editing the `/etc/krb5.conf` configuration file.  
You might need to perform this step based on the client operating system you are using.
3. Configure NIS or another external name mapping service.
4. (Optional) Edit the `/etc/idmapd.conf` file to ensure it is the same as the Kerberos realm.  
You might need to perform this step based on the client operating system you are using.
5. Verify the keytab file `/etc/krb5.keytab` contains an entry for the `nfs/` service principal or the `root/` principal.

```
[root@fc22 ~]# klist -k
Keytab name: FILE:/etc/krb5.keytab
KVNO Principal
-----
```

```
3 nfs/fc22.domain-name@domain-name
```

6. Mount the export using the `sec=krb5` option.

```
[root@fc22 ~]# mount ddrl2345.<domain-name>:/data/coll/mtreel /mnt/nfs4 -
o sec=krb5,vers=4
```

## Enabling Active Directory

### About this task

Configuring Active Directory authentication makes the protection system part of a Windows Active Directory realm. CIFS clients and NFS clients use Kerberos authentication.

### Procedure

1. Join an active directory realm using the `cifs set` command:

```
# cifs set authentication active-directory <realm>
```

Kerberos is automatically set up on the system, and the required `NFS/` service principal is automatically created on the KDC.

2. Configure NIS using the `authentication nis` command:

```
# authentication nis servers add <windows-ad-server>
# authentication nis domain set <ad-realm>
# authentication nis enable
```

3. Configure CIFS to use NSS for ID mapping by using `cifs` commands:

```
# cifs disable
# cifs option set idmap-type nss
# cifs enable
# fileys restart
```

4. Set the `nfs4-domain` to be the same as the Active Directory realm:

```
# nfs option set nfs4-domain <ad-realm>
```

5. Enable Active Directory for NFSv4 id mapping by using the `nfs` command:

```
# nfs option set nfs4-idmap-active-directory enabled
```

## Configuring Active Directory

### Procedure

1. Install the Active Directory Domain Services (AD DS) role on the Windows server.
2. Install the Identity Management for UNIX components.

```
C:\Windows\system32>Dism.exe /online /enable-feature /
featurename:adadminui /all
C:\Windows\system32>Dism.exe /online /enable-feature /featurename:nis /all
```

3. Verify the NIS domain is configured on the server.

```
C:\Windows\system32>nisadmin
The following are the settings on localhost

Push Interval : 1 days
Logging Mode   : Normal

NIS Domains
NIS Domain in AD  Master server  NIS Domain in UNIX
-----
corp              win-ad-server  corp
```

4. Assign AD users and groups UNIX UID/GIDs for the NFSv4 server.
  - a. Go to **Server Manager > Tools > Active Directory**.
  - b. Open the **Properties** for an AD user or group.
  - c. Under the **UNIX Attributes** tab, fill in the NIS domain, UID, and Primary GID fields.

## Configuring clients on Active Directory

### Procedure

1. Create a new AD user on the AD server to represent the NFS client's service principal.
2. Create the nfs/ service principal for the NFS client.

```
> ktpass -princ nfs/<client_dns_name>@<REALM> -mapuser nfsuser -pass ****
-out nfsclient.keytab
/crypt rc4-hmac-nt /ptype KRB5_NT_PRINCIPAL
```

3. (Optional) Copy the keytab file to /etc/krb5.keytab on the client.

The need to perform this step depends on which client OS you are using.

# CHAPTER 11

## Storage Migration

This chapter includes:

- Storage migration overview ..... 272
- Migration planning considerations ..... 272
- Viewing migration status ..... 274
- Evaluating migration readiness ..... 274
- Migrating storage using DD System Manager ..... 275
- Storage migration dialog descriptions ..... 276
- Migrating storage using the CLI ..... 278
- CLI storage migration example ..... 279

## Storage migration overview

Storage migration supports the replacement of existing storage enclosures with new enclosures that may offer higher performance, higher capacity, and a smaller footprint.

After new enclosures are installed, you can migrate the data from the older enclosures to the new enclosures while the system continues to support other processes such as data access, expansion, cleaning, and replication. The storage migration does require system resources, but you can control this with throttle settings that give the migration a relatively higher or lower priority. You can also suspend a migration to make more resources available to other processes, then resume the migration when resource demand is lower.

During the migration, the system uses data on the source and destination enclosures. New data is written to the new enclosures. Non-migrated data is updated on the source enclosures, and migrated data is updated on the destination enclosures. If the migration is interrupted, the migration can resume migrating blocks that have not been marked as migrated.

During the migration, each block of data is copied and verified, the source block is freed and marked as migrated, and the system index is updated to use the new location. New data that was destined to land in the source block will now be redirected to destination block. All new data block allocations that would have been allocated from source are allocated from the destination.

The Migration copy process is done at the shelf level, not the logical data level, so all disk sectors on the source shelf are accessed and copied over regardless of whether there is data on them. Therefore, the Storage Migration Utility cannot be used to shrink a logical data footprint.

**i** Note: Because the data set is divided between the source and destination enclosures during migration, you cannot halt a migration and resume use of only the source enclosures. Once started, the migration must complete. If a failure, such as a faulty disk drive, interrupts the migration, address the issue and resume the migration.

Depending on the amount of data to migrate and the throttle settings selected, a storage migration can take days or weeks. When all data is migrated, the finalize process, which must be manually initiated using the `storage migration finalize` command, restarts the filesystem. During the restart, the source enclosures are removed from the system configuration and the destination enclosures become part of the filesystem. When the finalize process is complete, the source enclosures can be removed from the system.


After a storage migration, the disk shelf numbers reported by DD OS might not be sequential. This is because shelf numbering is tied to the serial number of each individual disk shelf. KB article 499019, *Data Domain: Storage enclosure numbering is not sequential*, available on <https://support.emc.com>, provides additional details. In DD OS version 5.7.3.0 and later, the `enclosure show persistent-id` command described in the KB article requires administrator access, not SE access.

## Migration planning considerations

Consider the following guidelines before starting a storage migration.

- Storage migration requires a single-use license and operates on system models supported by DD OS version 5.7 or later.
  - i** Note: Multiple storage migration operations require multiple licenses. However, multiple source enclosures can be migrated to multiple destination enclosures during a single operation.
- Two licenses are required for storage migration:
  - The storage migration feature license



- The capacity and shelf type license for the destination enclosures
- Storage migration is based on capacity, not enclosure count. Therefore:
  - One source enclosure can be migrated to one destination enclosure.
  - One source enclosure can be migrated to multiple destination enclosures.
  - Multiple source enclosures can be migrated to one destination enclosure.
  - Multiple source enclosures can be migrated to multiple destination enclosures.
- The storage migration licensing process consists of:
  1. Updating the license installed on the system with the storage migration feature license and the capacity and shelf type license for the destination enclosures before running the migration operation.
  2. Updating the license installed on the system to remove the original capacity and shelf type license and the storage migration feature license after the migration operation is complete.
- The destination enclosures must:
  - Be unassigned shelves with the drives in an unused state.
  - Be licensed for sufficient capacity to receive the data from the source enclosures, with the license installed on the system
  - Be supported on the DD system model.
  - Contain at least as much usable capacity as the enclosures they are replacing.
- ① Note: It is not possible to determine the utilization of the source shelf. The system performs all calculations based on the capacity of the shelf.
- The DD system model must have sufficient memory to support the active tier storage capacity of the new enclosures.
- Data migration is not supported for disks in the system controller.
-  **CAUTION** Do not upgrade DD OS until the in-progress storage migration is complete.
- Storage migration cannot start when the file system is disabled or while a DD OS upgrade is in progress, another migration is in progress, or a RAID reconstruction is in progress.
- ① Note: If a storage migration is in progress, a new storage migration license is required to start a new storage migration operation after the in-progress migration completes. The presence or absence of a storage migration license is reported as part of the upgrade precheck.
- All specified source enclosures must be in the same tier (active).
- There can be only one disk group in each source enclosure, and all disks in the disk group must be installed in within the same enclosure.
- All disks in each destination enclosure must be of the same type (for example, all SATA or all SAS).
- After migration begins, the destination enclosures cannot be removed.
- Source enclosures cannot be removed until migration is complete and finalized.
- The storage migration duration depends on the system resources (which differ for different system models), the availability of system resources, and the data quantity to migrate. Storage migration can take days or weeks to complete.

## DS60 shelf considerations

The DS60 dense shelf can hold 60 disks, allowing the customer to use the full amount of space in the rack. The drives are accessed from the top of the shelf, by extending the shelf from the

cabinet. Due to the weight of the shelves, approximately 225 lbs when fully loaded, read this section before proceeding with a storage migration to DS60 shelves.

Be aware of the following considerations when working with the DS60 shelf:

 **CAUTION**

- Storage migrations are not supported when the source DS60 shelves contain 8 TB drives.
- Loading shelves at the top of the rack may cause the shelf to tip over.
- Validate that the floor can support the total weight of the DS60 shelves.
- Validate that the racks can provide enough power to the DS60 shelves.
- When adding more than five DS60s in the first rack, or more than six DS60s in the second rack, stabilizer bars and a ladder are required to maintain the DS60 shelves.

## Viewing migration status


DD System Manager provides two ways to view storage migration status.

### Procedure

1. Select **Hardware > Storage**.

In the Storage area, review the Storage Migration Status line. If the status is Not Licensed, you must add a license before using any storage migration features. If the storage migration license is installed, the status can be one of the following: None, Starting, Migrating, Paused by User, Paused by System, Copy Completed - Pending Finalization, Finalizing, Failed during Copy, or Failed during Finalize.

2. If a storage migration is in progress, click **View Storage Migration** to view the progress dialogs.

 Note: The migration status shows the percentage of blocks transferred. In a system with many free blocks, the free blocks are not migrated, but they are included in the progress indication. In this situation, the progress indication will climb quickly and then slow when the data migration starts.

3. When a storage migration is in progress, you can also view the status by selecting **Health > Jobs**.

## Evaluating migration readiness

You can use the system to evaluate storage migration readiness without committing to start the migration.

### Procedure

1. Install the destination enclosures using the instructions in the product installation guides.
2. Select **Administration > Licenses** and verify that the storage migration license is installed.
3. If the storage migration license is not installed, click **Add Licenses** and add the license.
4. Select **Hardware > Storage**, then click **Migrate Data**.
5. In the Select a Task dialog, select **Estimate**, then click **Next**.
6. In the Select Existing Enclosures dialog, use the checkboxes to select each of the source enclosures for the storage migration, then click **Next**.

- In the **Select New Enclosures** dialog, use the checkboxes to select each of the destination enclosures for the storage migration, then click **Next**.

The **Add Licenses** button allows you to add storage licenses for the new enclosures as needed, without interrupting the current task.

- In the **Review Migration Plan** dialog, review the estimated migration schedule, then click **Next**.
- Review the precheck results in the **Verify Migration Preconditions** dialog, then click **Close**.

### Results

If any of the precheck tests fail, resolve the issue before you start the migration.

## Migrating storage using DD System Manager

The storage migration process evaluates system readiness, prompts you to confirm that you want to start the migration, migrates the data, and then prompts you to finalize the process.

### Procedure

- Install the destination enclosures using the instructions in the product installation guides.
- Select **Administration > Licenses** and verify that the storage migration license is installed.
- If the storage migration license is not installed, click **Add Licenses** and add the license.
- Select **Hardware > Storage**, then click **Migrate Data**.
- In the **Select a Task** dialog, select **Migrate**, then click **Next**.
- In the **Select Existing Enclosures** dialog, use the checkboxes to select each of the source enclosures for the storage migration, then click **Next**.
- In the **Select New Enclosures** dialog, use the checkboxes to select each of the destination enclosures for the storage migration, then click **Next**.  
The **Add Licenses** button allows you to add storage licenses for the new enclosures as needed, without interrupting the current task.
- In the **Review Migration Plan** dialog, review the estimated migration schedule, then click **Start**.
- In the **Start Migration** dialog, click **Start**.  
The **Migrate** dialog appears and updates during the three phases of the migration: **Starting Migration**, **Migration in Progress**, and **Copy Complete**.
- When the **Migrate** dialog title displays **Copy Complete** and a filesystem restart is acceptable, click **Finalize**.

**Note:** This task restarts the filesystem and typically takes 10 to 15 minutes. The system is unavailable during this time.

### Results

When the migration finalize task is complete, the system is using the destination enclosures and the source enclosures can be removed.

## Storage migration dialog descriptions

The DD System Manager dialog descriptions provide additional information on storage migration. This information is also available by clicking the help icon in the dialogs.

### Select a Task dialog

The configuration in this dialog determines whether the system will evaluate storage migration readiness and stop, or evaluate readiness and begin storage migration.

Select **Estimate** to evaluate system readiness and stop.

Select **Migrate** to start migration after the system evaluation. Between the system evaluation and the start of the migration, a dialog prompts you to confirm or cancel the storage migration.

### Select Existing Enclosures dialog

The configuration in this dialog selects either the active or the retention tier and the source enclosures for the migration.

The Existing Enclosures list displays the enclosures that are eligible for storage migration. Select the checkbox for each of the enclosures to migrate. Click **Next** when you are ready to continue.

### Select New Enclosures dialog

The configuration in this dialog selects the destination enclosures for the migration. This dialog also displays the storage license status and an **Add Licenses** button.

The Available Enclosures list displays the enclosures that are eligible destinations for storage migration. Select the checkbox for each of the desired destination enclosures.

The license status bar represents all of the storage licenses installed on the system. The green portion represents licenses that are in use, and the and clear portion represents the licensed storage capacity available for destination enclosures. If you need to install additional licenses to support the selected destination controllers, click **Add Licenses**.

Click **Next** when you are ready to continue.

### Review Migration Plan dialog

This dialog presents an estimate of the storage migration duration, organized according to the three stages of storage migration.

Stage 1 of the storage migration runs a series of tests to verify that the system is ready for the migration. The test results appear in the Verify Migration Preconditions dialog.

During Stage 2, the data is copied from the source enclosures to the destination enclosures. When a large amount of data is present, the copy can take days or weeks to complete because the copy takes place in the background, while the system continues to serve backup clients. A setting in the Migration in Progress dialog allows you to change the migration priority, which can speed up or slow down the migration.

Stage 3, which is manually initiated from the Copy Complete dialog, updates the system configuration to use the destination enclosures and removes the configuration for the source controllers. During this stage, the file system is restarted and the system is unavailable to backup clients.

## Verify Migration Preconditions dialog

This dialog displays the results of the tests that execute before the migration starts.

The following list shows the test sequence and provides additional information on each of the tests.

- P1. This system's platform is supported.**  
Older DD system models do not support storage migration.
- P2. A storage migration license is available.**  
A storage migration license is required.
- P3. No other migration is currently running.**  
A previous storage migration must complete before you can start another.
- P4. The current migration request is the same as the interrupted migration request.**  
Resume and complete the interrupted migration.
- P5. Check the disk group layout on the existing enclosures.**  
Storage migration requires that each source enclosure contain only one disk group, and all the disks in the group must be in that enclosure.
- P6. Verify the final system capacity.**  
The total system capacity after migration and the removal of the source enclosures must not exceed the capacity supported by the DD system model.
- P7. Verify the replacement enclosures' capacity.**  
The usable capacity of the destination enclosures must be greater than that of the source enclosures.
- P8. Source enclosures are in the same active tier or retention unit.**  
The system supports storage migration from either the active tier or the retention tier. It does not support migration of data from both tiers at the same time.
- P9. Source enclosures are not part of the head unit.**  
Although the system controller is listed as an enclosure in the CLI, storage migration does not support migration from disks installed in the system controller.
- P10. Replacement enclosures are addable to storage.**  
All disks in each destination enclosure must be of the same type (for example, all SATA or all SAS).
- P11. No RAID reconstruction is occurring in the source controllers.**  
Storage migration cannot start while a RAID reconstruction is in progress.
- P12. Source shelf belongs to a supported tier.**  
The source disk enclosure must be part of a tier supported on the migration destination.

## Migration progress dialogs

This series of dialogs presents the storage migration status and the controls that apply at each stage.

### Migrate - Starting Migration

During the first stage, the progress is shown on the progress bar and no controls are available.



### Migrate - Migration in Progress

During the second stage, data is copied from the source enclosures to the destination enclosures and the progress is shown on the progress bar. Because the data copy can take days or weeks to complete, controls are provided so that you can manage the resources used during migration and suspend migration when resources are needed for other processes.

You can click **Pause** to suspend the migration and later click **Resume** to continue the migration.

The **Low**, **Medium**, and **High** buttons define throttle settings for storage migration resource demands. A low throttle setting gives storage migration a lower resource priority, which results in a slower migration and requires fewer system resources. Conversely, A high throttle setting gives storage migration a higher resource priority, which results in a faster migration and requires more system resources. The medium setting selects an intermediate priority.

You do not have to leave this dialog open for the duration of the migration. To check the status of the migration after closing this dialog, select **Hardware > Storage** and view the migration status. To return to this dialog from the Hardware/Storage page, click **Manage Migration**. The migration progress can also be viewed by selecting **Health > Jobs**.

### Migrate - Copy Complete

When the copy is complete, the migration process waits for you to click **Finalize**. During this final stage, , which takes 10 to 15 minutes, the filesystem is restarted and the system is not available. It is a good practice to start this stage during a maintenance window or a period of low system activity.

## Migrating storage using the CLI

### About this task

A migration simply requires moving all of the allocated blocks from the blocksets formatted over source DGs (e.g., source blocksets) to the blocksets formatted over destination DGs (e.g., destination blocksets). Once all of the allocated blocks have been moved from the source blocksets, those blocksets can be removed from the file system, their disks can be removed from their storage tier, and the physical disks and enclosures can be removed from the DDR.

① **Note:** The preparation of new enclosures for storage migration is managed by the storage migration process. Do not prepare destination enclosures as you would for an enclosure addition. For example, use of the `filesys expand` command is appropriate for an enclosure addition, but this command prevents enclosures from being used as storage migration destinations.

A DS60 disk shelf contains four disk packs, of 15 disks each. When a DS60 shelf is the migration source or destination, the disk packs are referenced as `enclosure:pack`. In this example, the source is enclosure 7, pack 2 (7:2), and the destination is enclosure 7, pack 4 (7:4).

### Procedure

1. Install the destination enclosures using the instructions in the product installation guides.
2. Check to see if the storage migration feature license is installed.
 

```
# elicence show
```
3. If the license is not installed, update the elicence to add the storage migration feature license
 

```
# elicence update
```
4. View the disk states for the source and destination disks.
 

```
# disk show state
```

The source disks should be in the active state, and the destination disks should be in the unknown state.

- Run the storage migration precheck command to determine if the system is ready for the migration.

```
# storage migration precheck source-enclosures 7:2 destination-enclosures 7:4
```

- View the migration throttle setting.

```
storage migration option show throttle
```

- When the system is ready, begin the storage migration.

```
# storage migration start source-enclosures 7:2 destination-enclosures 7:4
```

- Optionally, view the disk states for the source and destination disks during the migration.

```
# disk show state
```

During the migration, the source disks should be in the migrating state, and the destination disks should be in the destination state.

- Review the migration status as needed.

```
# storage migration status
```

- View the disk states for the source and destination disks.

```
# disk show state
```

During the migration, the source disks should be in the migrating state, and the destination disks should be in the destination state.

- When the migration is complete, update the configuration to use the destination enclosures.

**i** Note: This task restarts the file system and typically takes 10 to 15 minutes. The system is unavailable during this time.

```
storage migration finalize
```

- If you want to remove all data from each of the source enclosures, remove the data now.

```
storage sanitize start enclosure <enclosure-id>[:<pack-id>]
```

**i** Note: The storage sanitize command does not produce a certified data erasure. Dell EMC offers certified data erasure as a service. For more information, contact your Dell EMC representative.

- View the disk states for the source and destination disks.

```
# disk show state
```

After the migration, the source disks should be in the unknown state, and the destination disks should be in the active state.

### Results

When the migration finalize task is complete, the system is using the destination storage and the source storage can be removed.

## CLI storage migration example

```
elicense show
```

```
# elicense show
Feature licenses:
## Feature      Count Mode      Expiration Date
-----
```



Storage Migration

```
1 REPLICATION 1 permanent (int) n/a
2 VTL 1 permanent (int) n/a
-----
```

**elicense update**

# elicense update mylicense.lic

New licenses: Storage Migration

Feature licenses:

#	Feature	Count	Mode	Expiration Date
1	REPLICATION	1	permanent (int)	n/a
2	VTL	1	permanent (int)	n/a
3	Storage Migration	1	permanent (int)	

\*\* This will replace all existing Data Domain licenses on the system with the above EMC ELMS licenses.

Do you want to proceed? [yes|no] [yes]: yes

elicense(s) updated.

**disk show state**

Figure 8 disk show state

```
# disk show state
Enclosure      Disk
Row(disk:rd)  1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
-----
1              .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
2              U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
3              U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
4              U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
5              *  *  *  *  *  *  *  *  *  *  *  *  *  *  *
6              U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
7
              Pack 1  Pack 2  Pack 3  Pack 4
K(49-60)      U  U  U  .  .  *  U  U  U  U  U  U  .  .  .
D(37-48)      U  U  U  .  .  .  U  U  U  U  U  U  .  .  .
C(28-34)      U  U  U  .  .  .  U  U  U  U  U  U  .  .  .
S(13-24)      U  U  U  .  .  .  U  U  U  U  U  U  .  .  .
A( 1-12)      U  U  U  .  .  .  U  U  U  U  U  U  .  .  .
-----

Legend  State      Count
-----
.       In Use Disks  15
*       Spare Disks   1
U       Available Disks 15
U       Unknown Disks  105
-----
```

**storage migration precheck**

#storage migration precheck source-enclosures 2 destination-enclosures 11

Source enclosures:

Disks	Count	Disk Group	Disk Size	Enclosure Model	Enclosure Serial No.
2.1-2.15	15	dgl	1.81 TiB	ES30	APM00111103820

Total source disk size: 27.29 TiB

Destination enclosures:

Disks	Count	Disk Group	Disk Size	Enclosure Model	Enclosure Serial No.
11.1-11.15	15	unknown	931.51 GiB	ES30	APM00111103840

Total destination disk size: 13.64 TiB

1 "Verifying platform support.....PASS"  
 2 "Verifying valid storage migration license exists.....PASS"

```

3 "Verifying no other migration is running.....PASS"
4 "Verifying request matches interrupted migration.....PASS"
5 "Verifying data layout on the source shelves.....PASS"
6 "Verifying final system capacity.....PASS"
7 "Verifying destination capacity.....PASS"
8 "Verifying source shelves belong to same tier.....PASS"
9 "Verifying enclosure 1 is not used as source.....PASS"
10 "Verifying destination shelves are addable to storage.....PASS"
11 "Verifying no RAID reconstruction is going on in source shelves.....PASS"
Migration pre-check PASSED

Expected time to migrate data: 8 hrs 33 min

```

### storage migration show history

Figure 9 storage migration show history

```

# storage migration show history

```

ID	Source Enclosure*	Source Enclosure Serial No.	Dest Enclosure*	Dest Enclosure Serial No.	Status	Start Time	End Time
2	R:0	88U952408400521	T:0	88U952408400528	Finalized	Sat Aug 4 11:59:27 2015	Mon Aug 10 12:10:11 2015
1	R:0	88U952408400521	R:0	88U952408400528	Finalized	Thu Aug 6 16:33:55 2015	Fri Aug 7 10:28:07 2015

(\*) Enclosure ID at migration start time.

### storage migration start

```

#storage migration start source-enclosures 2 destination-enclosures 11

```

#### Source enclosures:

Disks	Count	Disk Group	Disk Size	Enclosure Model	Enclosure Serial No.
2.1-2.15	15	dq1	1.81 TiB	ES30	APM00111103820

Total source disk size: 27.29 TiB

#### Destination enclosures:

Disks	Count	Disk Group	Disk Size	Enclosure Model	Enclosure Serial No.
11.1-11.15	15	unknown	931.51 GiB	ES30	APM00111103840

Total destination disk size: 13.64 TiB

Expected time to migrate data: 84 hrs 40 min

```

** Storage migration once started cannot be aborted.
Existing data on the destination shelves will be overwritten.
Do you want to continue with the migration? (yes/no) [no]: yes

```

#### Performing migration pre-check:

```

1 Verifying platform support.....PASS
2 Verifying valid storage migration license exists.....PASS
3 Verifying no other migration is running.....PASS
4 Verifying request matches interrupted migration.....PASS
5 Verifying data layout on the source shelves.....PASS
6 Verifying final system capacity.....PASS
7 Verifying destination capacity.....PASS
8 Verifying source shelves belong to same tier.....PASS
9 Verifying enclosure 1 is not used as source.....PASS
10 Verifying destination shelves are addable to storage.....PASS
11 Verifying no RAID reconstruction is going on in source shelves.....PASS

```

Migration pre-check PASSED

Storage migration will reserve space in the filesystem to migrate data.  
Space reservation may add up to an hour or more based on system resources.

## Storage Migration

Storage migration process initiated.  
Check storage migration status to monitor progress.

### storage migration status

Figure 10 storage migration status

```
# storage migration status
```

Id	Source Enclosure (s)	Destination Enclosure (s)	State	Percent Complete	Estimated Time to Complete	Current Throttle Setting
1	7:2	7:4	migrating	15%	30 hrs 18 mins	high

### disk show state, migration in progress

Figure 11 disk show state, migration in progress

```
# disk show state
```

Enclosure Row(disk-ID)	Disk																																																																																																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15																																																																																					
1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.																																																																																					
2	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U																																																																																					
3	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U																																																																																					
4	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U																																																																																					
5	v	x	x	x	v	v	v	v	x	x	x	x	x	x	v																																																																																					
6	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U																																																																																					
7	<table border="1"> <thead> <tr> <th></th> <th>Pack 1</th> <th>Pack 2</th> <th>Pack 3</th> <th>Pack 4</th> </tr> </thead> <tbody> <tr> <td>E(43-60)</td> <td>U</td><td>U</td><td>U</td><td>m</td><td>m</td><td>m</td><td>U</td><td>U</td><td>U</td><td>w</td><td>d</td><td>d</td><td>d</td><td>d</td><td>d</td> </tr> <tr> <td>D(37-42)</td> <td>U</td><td>U</td><td>U</td><td>m</td><td>m</td><td>m</td><td>U</td><td>U</td><td>U</td><td>d</td><td>d</td><td>d</td><td>d</td><td>d</td><td>d</td> </tr> <tr> <td>C(23-36)</td> <td>U</td><td>U</td><td>U</td><td>m</td><td>m</td><td>m</td><td>U</td><td>U</td><td>U</td><td>d</td><td>d</td><td>d</td><td>d</td><td>d</td><td>d</td> </tr> <tr> <td>S(13-24)</td> <td>U</td><td>U</td><td>U</td><td>m</td><td>m</td><td>m</td><td>v</td><td>v</td><td>v</td><td>d</td><td>d</td><td>d</td><td>d</td><td>d</td><td>d</td> </tr> <tr> <td>A( 1-12)</td> <td>U</td><td>U</td><td>U</td><td>m</td><td>m</td><td>m</td><td>U</td><td>U</td><td>U</td><td>d</td><td>d</td><td>d</td><td>d</td><td>d</td><td>d</td> </tr> </tbody> </table>																Pack 1	Pack 2	Pack 3	Pack 4	E(43-60)	U	U	U	m	m	m	U	U	U	w	d	d	d	d	d	D(37-42)	U	U	U	m	m	m	U	U	U	d	d	d	d	d	d	C(23-36)	U	U	U	m	m	m	U	U	U	d	d	d	d	d	d	S(13-24)	U	U	U	m	m	m	v	v	v	d	d	d	d	d	d	A( 1-12)	U	U	U	m	m	m	U	U	U	d	d	d	d	d	d
	Pack 1	Pack 2	Pack 3	Pack 4																																																																																																
E(43-60)	U	U	U	m	m	m	U	U	U	w	d	d	d	d	d																																																																																					
D(37-42)	U	U	U	m	m	m	U	U	U	d	d	d	d	d	d																																																																																					
C(23-36)	U	U	U	m	m	m	U	U	U	d	d	d	d	d	d																																																																																					
S(13-24)	U	U	U	m	m	m	v	v	v	d	d	d	d	d	d																																																																																					
A( 1-12)	U	U	U	m	m	m	U	U	U	d	d	d	d	d	d																																																																																					

Legend	State	Count
.	In Use Disks	4
s	Spare Disks	2
v	Available Disks	15
U	Unknown Disks	50
m	Migrating Disks	16
d	Destination Disks	14

## storage migration finalize

Figure 12 storage migration finalize

```

# storage migration finalize

Storage migration finalize restarts the filesystem.
This can take several minutes and the filesystem is unavailable until the operation completes.
Do you want to continue? (yes/no) [no]: yes

Performing migration finalization pre-check:
(P1) Verifying storage migration is ready for finalization....PASS
(P2) Verifying there are no foreign disks.....PASS
(P3) Verifying data layout on the source shelves.....PASS

Migration finalization pre-check PASSED
Finalizing the storage migration with id 5:

Notifying filesystem to finalize migration...

Done.

Disabling the filesystem
Please wait.....
The filesystem is now disabled.
Removing source enclosures from filesystem...

Done.

Removing source enclosures from storage tier...

Done.

Enabling the filesystem
Please wait.....
The filesystem is now enabled.
Storage migration with id 5 from enclosure(s) 7.2 to enclosure(s) 7.4 has been finalized.

```

## disk show state, migration complete

Figure 13 disk show state, migration complete

```

# disk show state
Enclosure      Disk
Row/Disk-ID    1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
-----
1              .  .  .  .
2              U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
3              U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
4              U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
5              v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
6              U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
7
           Pack 1  Pack 2  Pack 3  Pack 4
E(49-50)    U  U  U  U  U  U  U  U  U  .  .  .
D(27-48)    U  U  U  U  U  U  U  U  U  .  .  .
C(25-26)    U  U  U  U  U  U  U  U  U  .  .  .
B(13-24)    U  U  U  U  U  U  U  U  U  .  .  .
A( 1-12)    U  U  U  U  U  U  U  U  U  .  .  .
-----

Legend  State      Count
-----
.       In Use Disks  18
v       Spare Disks  1
U       Available Disks  13
U       Unknown Disks  135
-----

```

**i** Note: Currently storage migration is only supported on the active node. Storage migration is not supported on the standby node of an HA cluster.



# CHAPTER 12

## Metadata on Flash

This chapter includes:

• Overview of Metadata on Flash (MDoF) .....	286
• SSD cache licensing and capacity .....	286
• SSD cache tier .....	288
• SSD cache tier - system management .....	288
• SSD alerts .....	291

## Overview of Metadata on Flash (MDoF)

MDoF creates caches for file system metadata using flash technologies. The SSD Cache is a low latency, high input/output operations per second (IOPS) cache to accelerate metadata and data access.

① **Note:** The minimum software version required is DD OS 6.0.

Caching the file system metadata on SSDs improves I/O performance for both traditional and random workloads.

For traditional workloads, offloading random access to metadata from HDDs to SSDs allows the hard drives to accommodate streaming write and read requests.

For random workloads, SSD cache provides low latency metadata operations, which allows the HDDs to serve data requests instead of cache requests.

Read cache on SSD improves random read performance by caching frequently accessed data. Writing data to NVRAM combined with low latency metadata operations to drain the NVRAM faster improve random write latency. The absence of cache does not prevent file system operation, it only impacts file system performance.

When the cache tier is first created, a file system restart is only required if the cache tier is being added after the file system is running. For new systems that come with cache tier disks, no file system restart is required if the cache tier is created before enabling the file system for the first time. Additional cache can be added to a live system, without the need to disable and enable the file system.

One specific condition with regard to SSDs is when the number of spare blocks remaining gets close to zero, the SSD enters a read only condition. When a read only condition occurs, DD OS treats the drive as read-only cache and sends an alert.

MDoF is supported on the following systems:

- DD6300
- DD6800
- DD6900
- DD9300
- DD9400
- DD9500
- DD9800
- DD9900
- DD VE instances, including DD3300 systems, in capacity configurations of 16 TB and higher (SSD Cache Tier for DD VE)

## SSD cache licensing and capacity

Depending on your system model, the SSD cache feature will either be enabled by default with no need for a license, or it will require an ELMS license to enable

The following table describes the various SSD capacity and licensing requirements for the supported systems:



Table 122 SSD capacity and licensing requirements

Model	Memory	Number of SSDs	SSD capacity	License required	Enabled by default
DD6300	48 GB (Base)	1	800 GB	Y	N
	96 GB (Expanded)	2	1600 GB	Y	N
DD6800	192 GB (Base)	2	1600 GB	Y	N
	192 GB (Expanded)	4	3200 GB	Y	N
DD6900	288 GB	2	3840 GB	N	Y
DD9300	192 GB (Base)	5	4000 GB	Y	N
	384 GB (Expanded)	8	6400 GB	Y	N
DD9400	576 GB	5	19200 GB	N	Y
DD9500	256 GB (Base)	8	6400 GB	Y	N
	512 GB (Expanded)	15	12000 GB	Y	N
DD9800	256 GB (Base)	8	6400 GB	Y	N
	768 GB (Expanded)	15	12000 GB	Y	N
DD9900	1152 GB	10	38400 GB	N	Y

#### SSD Cache Tier for DD VE

DD VE instances and DD3300 systems do not require a license for the SSD Cache Tier. The maximum supported SSD capacity is 1% of the Active Tier capacity.

The following table describes the various SSD capacity licenses and the SSD capacities for the given system:

Table 123 DD VE and DD3300 SSD capacity

Capacity configuration	Maximum SSD capacity
DD VE 16 TB	160 GB
DD VE 32 TB	320 GB
DD VE 48 TB	480 GB
DD VE 64 TB	640 GB
DD VE 96 TB	960 GB
DD3300 8 TB	160 GB
DD3300 16 TB	160 GB

Table 123 DD VE and DD3300 SSD capacity (continued)

Capacity configuration	Maximum SSD capacity
DD3300 32 TB	320 GB

## SSD cache tier

The SSD cache tier provides the SSD cache storage for the file system. The file system draws the required storage from the SSD cache tier without active intervention from the user.

## SSD cache tier - system management

Be aware of the following considerations for SSD cache:

- When SSDs are deployed within a controller, those SSDs are treated as internal root drives. They display as enclosure 1 in the output of the `storage show all` command.
- Manage individual SSDs with the `disk` command the same way HDDs are managed.
- Run the `storage add` command to add an individual SSD or SSD enclosure to the SSD cache tier.
- The SSD cache tier space does not need to be managed. The file system draws the required storage from the SSD cache tier and shares it among its clients.
- The `filesys create` command creates an SSD volume if SSDs are available in the system.
  - ① **Note:** If SSDs are added to the system later, the system should automatically create the SSD volume and notify the file system. SSD Cache Manager notifies its registered clients so they can create their cache objects.
- If the SSD volume contains only one active drive, the last drive to go offline will come back online if the active drive is removed from the system.

The next section describes how to manage the SSD cache tier from DD System Manager, and with the DD OS CLI.

## Managing the SSD cache tier

Storage configuration features allow you to add and remove storage from the SSD cache tier.

### Procedure

1. Select **Hardware > Storage > Overview**.
2. Expand the **Cache Tier** dialog.
3. Click **Configure**.
  - ① **Note:** The licensed capacity bar shows the portion of licensed capacity (used and remaining) for the installed enclosures.
4. Select the checkbox for the Shelf to be added.
5. Click the **Add to Tier** button.
6. Click **OK** to add the storage.
  - ① **Note:** To remove an added shelf, select it in the Tier Configuration list, click **Remove from Configuration**, and click **OK**.

**CLI Equivalent**

When the cache tier SSDs are installed in the head unit:

- a. Add the SSDs to the cache tier.

```
# storage add disks 1.13,1.14 tier cache
Checking storage requirements...done
Adding disk 1.13 to the cache tier...done

Updating system information...done

Disk 1.13 successfully added to the cache tier.

Checking storage requirements...
done
Adding disk 1.14 to the cache tier...done

Updating system information...done

Disk 1.14 successfully added to the cache tier.
```

- b. Verify the state of the newly added SSDs.

```
# disk show state
Enclosure  Disk
-----
1          1  2  3  4  5  6  7  8  9 10 11 12 13 14 15
-----
1          .  .  .  .  s  .  .  s  s  s  s  s  v  v
2          U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
3          U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
-----

Legend      State          Count
-----
.           In Use Disks    6
s           Spare Disks    6
v           Available Disks 2
U           Unknown Disks 30
-----
Total 44 disks
```

When the cache tier SSDs are installed in an external shelf:

- a. Verify the system recognizes the SSD shelf. In the example below, the SSD shelf is enclosure 2.

```
# disk show state
Enclosure  Disk
Row(disk-id) 1  2  3  4  5  6  7  8  9 10 11 12 13 14 15
-----
1          .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
2          U  U  U  U  U  U  U  U  -  -  -  -  -  -  -
3          .  .  .  .  .  .  .  .  .  .  .  .  .  .  v
4          .  .  .  .  .  .  .  .  .  .  .  .  .  .  v
5          v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
6          v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
7          v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
8          v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
9          v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
10         |-----|
           | Pack 1 | Pack 2 | Pack 3 | Pack 4 |
           |-----|
           Z(49-60) |v  v  v|v  v  v|v  v  v|v  v  v|
           D(37-48) |v  v  v|v  v  v|v  v  v|v  v  v|
           C(25-36) |v  v  v|v  v  v|v  v  v|v  v  v|
           B(13-24) |v  v  v|v  v  v|v  v  v|v  v  v|
           A( 1-12) |v  v  v|v  v  v|v  v  v|v  v  v|
           |-----|
11         v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
12         v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
13         v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
-----
```

```

Legend   State           Count
-----
.        In Use Disks       32
v        Available Disks 182
0        Unknown Disks   8
-        Not Installed Disks 7
-----
Total 222 disks
    
```

b. Identify the shelf ID of the SSD shelf. SSDs will display as SAS-SSD or SATA-SSD in the Type column.

```
# disk show hardware
```

Figure 14



c. Add the SSD shelf to the cache tier

```
# storage add enclosure 2 tier cache
```

```
Checking storage requirements...done
Adding enclosure 2 to the cache tier...Enclosure 2 successfully added
to the cache tier.
```

```
Updating system information...done
```

```
Successfully added: 2 done
```

d. Verify the state of the newly added SSDs.

```
# disk show state
```

```

Enclosure  Disk
Row(disk-id) 1  2  3  4  5  6  7  8  9 10 11 12 13 14 15
-----
1             .  .  .  .
2             .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
3             .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
4             .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
5             v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
6             v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
7             v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
8             v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
9             v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
10            -----
              | Pack 1 | Pack 2 | Pack 3 | Pack 4 |
E(49-60)     | v  v  v | v  v  v | v  v  v | v  v  v |
D(37-48)     | v  v  v | v  v  v | v  v  v | v  v  v |
C(25-36)     | v  v  v | v  v  v | v  v  v | v  v  v |
B(13-24)     | v  v  v | v  v  v | v  v  v | v  v  v |
A( 1-12)     | v  v  v | v  v  v | v  v  v | v  v  v |
              -----
11            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
12            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
13            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
-----
    
```

```

Legend   State           Count
-----
.        In Use Disks       32
v        Available Disks 182
    
```

```

U          Unknown Disks      8
-          Not Installed Disks 7
-----
Total 222 disks

To remove a controller-mounted SSD from the cache tier:
# storage remove disk 1.13

Removing disk 1.13...done
Updating system information...done
Disk 1.13 successfully removed.

To remove an SSD shelf from the system:
# storage remove enclosure 2

Removing enclosure 2...Enclosure 2 successfully removed.
Updating system information...done
Successfully removed: 2 done

```

## SSD alerts

There are three alerts specific to the SSD cache tier.

The SSD cache tier alerts are:

- Licensing**  
 If the file system is enabled and less physical cache capacity present than what the license permits is configured, an alert is generated with the current SSD capacity present, and the capacity license. This alert is classified as a warning alert. The absence of cache does not prevent file system operation, it only impacts file system performance. Additional cache can be added to a live system, without the need to disable and enable the file system.
- Read only condition**  
 When the number of spare blocks remaining gets close to zero, the SSD enters a read only condition. When a read only condition occurs, DD OS treats the drive as read-only cache.  
 Alert `EVT-STORAGE-00001` displays when the SSD is in a read-only state and should be replaced.
- SSD end of life**  
 When an SSD reaches the end of its lifespan, the system generates a hardware failure alert identifying the location of the SSD within the SSD shelf. This alert is classified as a critical alert.  
 Alert `EVT-STORAGE-00016` displays when the EOL counter reaches 98. The drive is failed proactively when the EOL counter reaches 99.

2016 Q2

# CHAPTER 13

## SCSI Target

This chapter includes:

- SCSI Target overview.....294
- Fibre Channel view.....295
- Port monitoring.....304



## SCSI Target overview

SCSI (Small Computer System Interface) Target is a unified management daemon for all SCSI services and transports. SCSI Target supports DD VTL (Virtual Tape Library), DD Boost over FC (Fibre Channel), and vDisk/ProtectPoint Block Services, as well as anything that has a target LUN (logical unit number) on a DD system.

### SCSI Target Services and Transports

The SCSI Target daemon starts when FC ports are present or DD VTL is licensed. It provides unified management for all SCSI Target *services* and *transports*.

- A *service* is anything that has a target LUN on a DD system that uses SCSI Target commands, such as DD VTL (tape drives and changers), DD Boost over FC (processor devices), or vDisk (Virtual Disk Device).
- A *transport* enables *devices* to become visible to *initiators*.
- An *initiator* is a backup client that connects to a system to read and write data using the FC protocol. A specific initiator can support DD Boost over FC, vDisk, or DD VTL, but not all three.
- *Devices* are visible on a SAN (storage area network) through physical ports. Host initiators communicate with the DD system through the SAN.
- *Access groups* manage access between devices and initiators.
- An *endpoint* is the logical target on a DD system to which an initiator connects. You can disable, enable, and rename endpoints. To delete endpoints, the associated transport hardware must no longer exist. Endpoints are automatically discovered and created when a new transport connection occurs. Endpoints have the following attributes: port topology, FCP2-RETRY status, WWPN, and WWNN.
- *NPIV* (N\_port ID Virtualization) is an FC feature that lets multiple endpoints share a single physical port. NPIV eases hardware requirements and provides failover capabilities.
- In DD OS 6.0, users can specify the sequence of secondary system addresses for failover. For example, if the system specifies 0a, 0b, 1a, 1b and the user specifies 1b, 1a, 0a, 0b, the user-specified sequence is used for failover. The `scsitarget endpoint show detailed` command displays the user-specified sequence.

Only one initiator should be present per access group. Each access group is assigned a type (DD VTL, vDisk/ProtectPoint Block Services, or DD Boost over FC).

### SCSI Target Architectures - Supported and Unsupported

SCSI Target supports the following architectures:

- **DD VTL plus DD Boost over FC from different initiators:** Two different initiators (on the same or different clients) may access a DD system using DD VTL and DD Boost over FC, through the same or different DD system target endpoints.
- **DD VTL plus DD Boost over FC from one initiator to two different DD systems:** A single initiator may access two different DD systems using any service.

SCSI Target does not support the following architecture:

- **DD VTL plus DD Boost over FC from one initiator to the same DD system:** A single initiator may not access the same DD system through different services.

### Thin Protocol

The thin protocol is a lightweight daemon for vDisk and DD VTL that responds to SCSI commands when the primary protocol can't. For Fibre Channel environments with multiple protocols, thin protocol:

- Prevents initiator hangs
- Prevents unnecessary initiator aborts
- Prevents initiator devices from disappearing
- Supports a standby mode
- Supports fast and early discoverable devices
- Enhances protocol HA behavior
- Doesn't require fast registry access

#### For More Information about DD Boost and the `scsitarget` Command (CLI)

For more information about using DD Boost through the DD System Manager, see the related chapter in this book. For other types of information about DD Boost, see the *DD Boost for OpenStorage Administration Guide*.

This chapter focuses on using SCSI Target through the DD System Manager. After you have become familiar with basic tasks, the `scsitarget` command in the *DD OS Command Reference Guide* provides more advanced management tasks.

When there is heavy DD VTL traffic, avoid running the `scsitarget group use` command, which switches the in-use endpoint lists for one or more SCSI Target or vdisk devices in a group between primary and secondary endpoint lists.

## Fibre Channel view

The Fibre Channel view displays the current status of whether Fibre Channel and/or NPIV is enabled. It also displays two tabs: Resources and Access Groups. Resources include ports, endpoints, and initiators. An access group holds a collection of initiator WWPNs (worldwide port names) or aliases and the drives and changers they are allowed to access.

## Enabling NPIV

NPIV (N\_Port ID Virtualization), is a Fibre Channel feature in which multiple endpoints can share a single physical port. NPIV eases hardware requirements and provides endpoint failover/failback capabilities. NPIV is not configured by default; you must enable it.

#### About this task

**Note:** NPIV is enabled by default in HA configuration.

NPIV provides simplified multiple-system consolidation:

- NPIV is an ANSI T11 standard that allows a single HBA physical port to register with a Fibre Channel fabric using multiple WWPNs
- The virtual and physical ports have the same port properties and behave exactly the same.
- There may be m:1 relationships between the endpoints and the port, that is, multiple endpoints can share the same physical port.

Specifically, enabling NPIV enables the following features:

- Multiple endpoints are allowed per physical port, each using a virtual (NPIV) port. The base port is a placeholder for the physical port and is not associated with an endpoint.
- Endpoint failover/failback is automatically enabled when using NPIV.
  - Note:** After NPIV is enabled, the "Secondary System Address" must be specified at each of the endpoints. If not, endpoint failover will not occur.
- Multiple DD systems can be consolidated into a single DD system, however, the number of HBAs remains the same on the single DD system.

- The endpoint failover is triggered when FC-SSM detects when a port goes from online to offline. In the case where the physical port is offline before `scsitarget` is enabled and the port is still offline after `scsitarget` is enabled, a endpoint failover is not possible because FC-SSM does not generate a port offline event. If the port comes back online and auto-failback is enabled, any failed over endpoints that use that port as a primary port will fail-back to the primary port.

The HA feature requires NPIV to move WWNs between the nodes of an HA pair during the failover process.

**i** Note: Before enabling NPIV, the following conditions must be met:

- The DD system must be running DD OS 5.7 or higher.
- All ports must be connected to 4Gb, 8Gb, and 16 Gb Fibre Channel HBA and SLIC.
- The DD system ID must be valid, that is, it must not be 0.

In addition, port topologies and port names will be reviewed and may prevent NPIV from being enabled:

- NPIV is allowed if the topology for *all* ports is loop-preferred.
- NPIV is allowed if the topology for *some* of the ports is loop-preferred; however, NPIV must be disabled for ports that are loop-only, or you must reconfigure the topology to loop-preferred for proper functionality.
- NPIV is *not* allowed if *none* of the ports has a topology of loop-preferred.
- If port names are present in access groups, the port names are replaced with their associated endpoint names.

#### Procedure

1. Select **Hardware > Fibre Channel**.
2. Next to NPIV: Disabled, select **Enable**.
3. In the Enable NPIV dialog, you will be warned that all Fibre Channel ports must be disabled before NPIV can be enabled. If you are sure that you want to do this, select **Yes**.

#### CLI Equivalent

- a. Make sure (global) NPIV is enabled.

```
# scsitarget transport option show npiv
SCSI Target Transport Options
Option      Value
-----
npiv        disabled
-----
```

- b. If NPIV is disabled, then enable it. You must first disable all ports.

```
# scsitarget port disable all
All ports successfully disabled.
# scsitarget transport option set npiv enabled
Enabling FiberChannel NPIV mode may require SAN zoning to
be changed to configure both base port and NPIV WWPNS.
Any FiberChannel port names used in the access groups will
be converted to their corresponding endpoint names in order
to prevent ambiguity.
Do you want to continue? [yes|no] [no]:
```

- c. Re-enable the disabled ports.

```
# scsitarget port enable all
All ports successfully enabled.
```

- d. Make sure the physical ports have an NPIV setting of "auto".

```
# scsitarget port show detailed 0a
System Address:    0a
```

```

Enabled:          Yes
Status:          Online
Transport:       FibreChannel
Operational Status: Normal
FC NPIV:         Enabled (auto)
+
+
+

```

- e. Create a new endpoint using the primary and secondary ports you have selected.

```
# scsitarget endpoint add test0a0b system-address 0a
primary-system-address 0a secondary-system-address 0b
```

Note that the endpoint is disabled by default, so enable it.

```
# scsitarget endpoint enable test0a0b
```

Then display the endpoint information.

```
# scsitarget endpoint show detailed test0a0b
Endpoint:          test0a0b
Current System Address: 0b
Primary System Address: 0a
Secondary System Address: 0b
Enabled:          Yes
Status:          Online
Transport:       FibreChannel
FC WNN:          50:02:18:80:08:a0:00:91
FC WWP:          50:02:18:84:08:b6:00:91
```

- f. Zone a host system to the auto-generated WWPN of the newly created endpoint.
- g. Create a DD VTL, vDisk, or DD Boost over Fibre Channel (DFC) device, and make this device available on the host system.
- h. Ensure that the DD device chosen can be accessed on the host (read and/or written).
- i. Test the endpoint failover by using the "secondary" option to move the endpoint to the SSA (secondary system address).
- ```
# scsitarget endpoint use test0a0b secondary
```
- j. Ensure that the DD device chosen can still be accessed on the host (read and/or written). Test the fallback by using the "primary" option to move the endpoint back to the PSA (primary system address).
- ```
# scsitarget endpoint use test0a0b primary
```
- k. Ensure that the DD device chosen can still be accessed on the host (read and/or written).

## Disabling NPIV

Before you can disable NPIV, you must not have any ports with multiple endpoints.

### About this task

- ① **Note:** NPIV is required for HA configuration. It is enabled by default and cannot be disabled.

### Procedure

1. Select **Hardware > Fibre Channel**.
2. Next to NPIV: Enabled, select **Disable**.
3. In the Disable NPIV dialog, review any messages about correcting the configuration, and when ready, select **OK**.

## Resources tab

The **Hardware > Fibre Channel > Resources** tab displays information about ports, endpoints, and initiators.

**Table 124** Ports

Item	Description
System Address	System address for port
WWPN	Unique worldwide port name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the Fibre Channel (FC) port.
WWNN	Unique worldwide node name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the FC node
Enabled	Port operational status; either Enabled or Disabled.
NPIV	NPIV status; either Enabled or Disabled.
Link Status	Link status; either Online or Offline; that is, whether or not the port is up and capable of handling traffic.
Operation Status	Operation status; either Normal or Marginal.
# of Endpoints	Number of endpoints associated with this port.

**Table 125** Endpoints

Item	Description
Name	Name of endpoint.
WWPN	Unique worldwide port name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the Fibre Channel (FC) port.
WWNN	Unique worldwide node name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the FC node
System Address	System address of endpoint.
Enabled	Port operational state; either Enabled or Disabled.
Link Status	Either Online or Offline; that is, whether or not the port is up and capable of handling traffic.

**Table 126** Initiators

Item	Description
Name	Name of initiator.
Service	Service support by the initiator, which is either DD VTL, DD Boost, or vDisk.



Table 126 Initiators (continued)

Item	Description
WWPN	Unique worldwide port name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the Fibre Channel (FC) port.
WWNN	Unique worldwide node name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the FC node.
Vendor Name	Initiator's model.
Online Endpoints	Endpoints seen by this initiator. Displays <i>none</i> or <i>offline</i> if the initiator is not available.

## Configuring a port

Ports are discovered, and a single endpoint is automatically created for each port, at startup.

### About this task

The properties of the base port depend on whether NPIV is enabled:

- In non-NPIV mode, ports use the same properties as the endpoint, that is, the WWPN for the base port and the endpoint are the same.
- In NPIV mode, the base port properties are derived from default values, that is, a new WWPN is generated for the base port and is preserved to allow consistent switching between NPIV modes. Also, NPIV mode provides the ability to support multiple endpoints per port.

### Procedure

1. Select **Hardware > Fibre Channel > Resources**.
2. Under **Ports**, select an port, and then select **Modify** (pencil).
3. In the Configure Port dialog, select whether to automatically enable or disable NPIV for this port.
4. For **Topology**, select Loop Preferred, Loop Only, Point to Point, or Default.
5. For **Speed**, select 1, 2, 4, 8, or 16 Gbps, or auto.
6. Select **OK**.

## Enabling a port

Ports must be enabled before they can be used.

### Procedure

1. Select **Hardware > Fibre Channel > Resources**.
2. Select **More Tasks > Ports > Enable**. If all ports are already enabled, a message to that effect is displayed.
3. In the Enable Ports dialog, select one or more ports from the list, and select **Next**.
4. After the confirmation, select **Next** to complete the task.

## Disabling a port

You can simply disable a port (or ports), or you can choose to failover all endpoints on the port (or ports) to another port.

### Procedure

1. Select **Hardware > Fibre Channel > Resources**.
2. Select **More Tasks > Ports > Disable**.
3. In the Disable Ports dialog, select one or more ports from the list, and select **Next**.
4. In the confirmation dialog, you can continue with simply disabling the port, or you can choose to failover all endpoints on the ports to another port.

## Adding an endpoint

An endpoint is a virtual object that is mapped to a underlying virtual port. In non-NPIV mode (not available on HA configuration), only a single endpoint is allowed per physical port, and the base port is used to configure that endpoint to the fabric. When NPIV is enabled, multiple endpoints are allowed per physical port, each using a virtual (NPIV) port, and endpoint failover/failback is enabled.

### About this task

- ① **Note:** Non-NPIV mode is not available on HA configurations. NPIV is enabled by default and cannot be disabled.
- ① **Note:** In NPIV mode, endpoints:
  - have a primary system address.
  - may have zero or more secondary system addresses.
  - are all candidates for failover to an alternate system address on failure of a port; however, failover to a marginal port is not supported.
  - may be failed back to use their primary port when the port comes back up online.
- ① **Note:** When using NPIV, it is recommended that you use only one protocol (that is, DD VTL Fibre Channel, DD Boost-over-Fibre Channel, or vDisk Fibre Channel) per endpoint. For failover configurations, secondary endpoints should also be configured to have the same protocol as the primary.

### Procedure

1. Select **Hardware > Fibre Channel > Resources**.
2. Under **Endpoints**, select **Add (+ sign)**.
3. In the Add Endpoint dialog, enter a Name for the endpoint (from 1 to 128 characters). The field cannot be empty or be the word "all," and cannot contain the characters asterisk (\*), question mark (?), front or back slashes (/, \), or right or left parentheses [(,)].
4. For Endpoint Status, select Enabled or Disabled.
5. If NPIV is enabled, for Primary system address, select from the drop-down list. The primary system address must be different from any secondary system address.
6. If NPIV is enabled, for Fails over to secondary system addresses, check the appropriate box next to the secondary system address.
7. Select **OK**.



## Configuring an endpoint

After you have added an endpoint, you can modify it using the Configure Endpoint dialog.

### About this task

- ① **Note:** When using NPIV, it is recommended that you use only one protocol (that is, DD VTL Fibre Channel, DD Boost-over-Fibre Channel, or vDisk Fibre Channel) per endpoint. For failover configurations, secondary endpoints should also be configured to have the same protocol as the primary.

### Procedure

1. Select **Hardware > Fibre Channel > Resources**.
2. Under **Endpoints**, select an endpoint, and then select **Modify** (pencil).
3. In the Configure Endpoint dialog, enter a Name for the endpoint (from 1 to 128 characters). The field cannot be empty or be the word "all," and cannot contain the characters asterisk (\*), question mark (?), front or back slashes (/, \), or right or left parentheses [(,)].
4. For Endpoint Status, select Enabled or Disabled.
5. For Primary system address, select from the drop-down list. The primary system address must be different from any secondary system address.
6. For Fails over to secondary system addresses, check the appropriate box next to the secondary system address.
7. Select **OK**.

## Modifying an endpoint's system address

You can modify the active system address for a SCSI Target endpoint using the `scsitarget endpoint modify` command option. This is useful if the endpoint is associated with a system address that no longer exists, for example after a controller upgrade or when a controller HBA (host bus adapter) has been moved. When the system address for an endpoint is modified, all properties of the endpoint, including WWPN and WWNN (worldwide port and node names, respectively), if any, are preserved and are used with the new system address.

### About this task

In the following example, endpoint ep-1 was assigned to system address 5a, but this system address is no longer valid. A new controller HBA was added at system address 10a. The SCSI Target subsystem automatically created a new endpoint, ep-new, for the newly discovered system address. Because only a single endpoint can be associated with a given system address, ep-new must be deleted, and then ep-1 must be assigned to system address 10a.

- ① **Note:** It may take some time for the modified endpoint to come online, depending on the SAN environment, since the WWPN and WWNN have moved to a different system address. You may also need to update SAN zoning to reflect the new configuration.

### Procedure

1. Show all endpoints to verify the endpoints to be changed:  
# `scsitarget endpoint show list`
2. Disable all endpoints:  
# `scsitarget endpoint disable all`
3. Delete the new, unnecessary endpoint, ep-new:  
# `scsitarget endpoint del ep-new`

4. Modify the endpoint you want to use, ep-1, by assigning it the new system address 10a:

```
# scsitarget endpoint modify ep-1 system-address 10a
```

5. Enable all endpoints:

```
# scsitarget endpoint enable all
```

### Enabling an endpoint

Enabling an endpoint enables the port only if it is currently disabled, that is, you are in non-NPIV mode.

#### Procedure

1. Select **Hardware > Fibre Channel > Resources**.
2. Select **More Tasks > Endpoints > Enable**. If all endpoints are already enabled, a message to that effect is displayed.
3. In the Enable Endpoints dialog, select one or more endpoints from the list, and select **Next**.
4. After the confirmation, select **Next** to complete the task.

### Disabling an endpoint

Disabling an endpoint does not disable the associated port, unless all endpoints using the port are disabled, that is, you are in non-NPIV mode.

#### Procedure

1. Select **Hardware > Fibre Channel > Resources**.
2. Select **More Tasks > Endpoints > Disable**.
3. In the Disable Endpoints dialog, select one or more endpoints from the list, and select **Next**. If an endpoint is in use, you are warned that disabling it might disrupt the system.
4. Select **Next** to complete the task.

### Deleting an endpoint

You may want to delete an endpoint if the underlying hardware is no longer available. However, if the underlying hardware is still present, or becomes available, a new endpoint for the hardware is discovered automatically and configured based on default values.

#### Procedure

1. Select **Hardware > Fibre Channel > Resources**.
2. Select **More Tasks > Endpoints > Delete**.
3. In the Delete Endpoints dialog, select one or more endpoints from the list, and select **Next**. If an endpoint is in use, you are warned that deleting it might disrupt the system.
4. Select **Next** to complete the task.

### Adding an initiator

Add initiators to provide backup clients to connect to the system to read and write data using the FC (Fibre Channel) protocol. A specific initiator can support DD Boost over FC, or DD VTL, but not both. A maximum of 1024 initiators can be configured for a DD system.

#### Procedure

1. Select **Hardware > Fibre Channel > Resources**.
2. Under Initiators, select Add (+ sign)

3. In the Add Initiator dialog, enter the port's unique WWPN in the specified format.
4. Enter a Name for the initiator.
5. Select the Address Method: **Auto** is used for standard addressing, and **VSA** (Volume Set Addressing) is used primarily for addressing virtual buses, targets, and LUNs.
6. Select **OK**.

#### CLI Equivalent

```
# scsitaraget group add My_Group initiator My_Initiator
```

## Modifying or deleting an initiator

Before you can delete an initiator, it must be offline and not attached to any group. Otherwise, you will get an error message, and the initiator will not be deleted. You must delete all initiators in an access group before you can delete the access group. If an initiator remains visible, it may be automatically rediscovered.

#### Procedure

1. Select **Hardware > Fibre Channel > Resources**.
2. Under Initiators, select one of the initiators. If you want to delete it, select **Delete (X)**. If you want to modify it, select **Modify** (pencil) to display the Modify Initiator dialog.
3. Change the initiator's Name and/or Address Method [**Auto** is used for standard addressing, and **VSA** (Volume Set Addressing) is used primarily for addressing virtual buses, targets, and LUNs.]
4. Select **OK**.

#### Recommendation to Set Initiator Aliases - CLI only

It is strongly recommended that Initiator aliases be set to reduce confusion and human error during the configuration process.

```
# vtl initiator set alias NewAliasName wwpn 21:00:00:e0:8b:9d:0b:e8
# vtl initiator show
```

Initiator	Group	Status	WWNN	WWPN	Port
NewVTL	aussia1	Online	20:00:00:e0:8b:9d:0b:e8	21:00:00:e0:8b:9d:0b:e8	6a
		Offline	20:00:00:e0:8b:9d:0b:e8	21:00:00:e0:8b:9d:0b:e8	6b

Initiator	Symbolic Port Name	Address Method
NewVTL		auto

## Setting a hard address (loop ID)

Some backup software requires that all private-loop targets have a hard address (loop ID) that does not conflict with another node. The range for a loop ID is from 0 to 125.

#### Procedure

1. Select **Hardware > Fibre Channel > Resources**.
2. Select **More Tasks > Set Loop ID**.
3. In the Set Loop ID dialog, enter the loop ID (from 0 to 125), and select **OK**.

## Setting failover options

You can set options for automatic failover and fallback when NPIV is enabled.

### About this task

Here is the expected behavior for Fibre Channel port failover, by application:

- DD Boost-over-Fibre Channel operation is expected to continue without user intervention when the Fibre Channel endpoints failover.
- DD VTL Fibre Channel operation is expected to be interrupted when the DD VTL Fibre Channel endpoints failover. You may need to perform discovery (that is, operating system discovery and configuration of DD VTL devices) on the initiators using the affected Fibre Channel endpoint. You should expect to re-start active backup and restore operations.
- vDisk Fibre Channel operation is expected to continue without user intervention when the Fibre Channel endpoints failover.

Automatic fallback is not guaranteed if all ports are disabled and then subsequently enabled (which could be triggered by the administrator), as the order in which ports get enabled is unspecified.

### Procedure

1. Select **Hardware > Fibre Channel > Resources**.
2. Select **More Tasks > Set Failover Options**.
3. In the Set Failover Options dialog, enter the Failover and Fallback Delay (in seconds) and whether to enable Automatic Fallback, and select **OK**.

## Access Groups tab

The **Hardware > Fibre Channel > Access Groups** tab provides information about DD Boost and DD VTL access groups. Selecting the link to *View DD Boost Groups* or *View VTL Groups* takes you to the DD Boost or DD VTL pages.

Table 127 Access Groups

Item	Description
Group Name	Name of access group.
Service	Service for this access group: either DD Boost or DD VTL.
Endpoints	Endpoints associated with this access group.
Initiators	Initiators associated with this access group.
Number of Devices	Number of devices associated with this access group.

## Port monitoring

Port monitoring detects an FC port at system startup and raises an alert if the port is enabled and offline.

To clear the alert, disable an unused port using the `scsitarget port` commands.

# CHAPTER 14

## Working with DD Boost

This chapter includes:

• About DD Boost.....	306
• Managing DD Boost with DD System Manager.....	306
• About interface groups.....	320
• Destroying DD Boost.....	326
• Configuring DD Boost-over-Fibre Channel.....	327
• Using DD Boost on HA systems.....	331
• About the DD Boost tabs.....	331

## About DD Boost

DD Boost provides advanced integration with backup and enterprise applications for increased performance and ease of use. DD Boost distributes parts of the deduplication process to the backup server or application clients, enabling client-side deduplication for faster, more efficient backup and recovery.

DD Boost is an optional product that requires a separate license to operate on the protection system. You can purchase a DD Boost software license key directly from Dell EMC.

**Note:** A special license, BLOCK-SERVICES-PROTECTPOINT, is available to enable clients using ProtectPoint block services to have DD Boost functionality without a DD Boost license. If DD Boost is enabled for ProtectPoint clients only—that is, if only the BLOCK-SERVICES-PROTECTPOINT license is installed—the license status indicates that DD Boost is enabled for ProtectPoint only.

There are two components to DD Boost: one component that runs on the backup server and another that runs on the protection system.

- In the context of the NetWorker backup application, Avamar backup application and other DDBoost partner backup applications, the component that runs on the backup server (DD Boost libraries) is integrated into the particular backup application.
- In the context of Veritas backup applications (NetBackup and Backup Exec) and the Oracle RMAN plug-in, you need to download an appropriate version of the DD Boost plugin that is installed on each media server. The DD Boost plugin includes the DD Boost libraries for integrating with the DD Boost server running on the protection system.

The backup application (for example, Avamar, NetWorker, NetBackup, or Backup Exec) sets policies that control when backups and duplications occur. Administrators manage backup, duplication, and restores from a single console and can use all of the features of DD Boost, including WAN-efficient replicator software. The application manages all files (collections of data) in the catalog, even those created by the protection system.

In the protection system, storage units that you create are exposed to backup applications that use the DD Boost protocol. For Veritas applications, storage units are viewed as disk pools. For NetWorker, storage units are viewed as logical storage units (LSUs). A storage unit is an MTree; therefore, it supports MTree quota settings. (Do not create an MTree in place of a storage unit.)

This chapter does not contain installation instructions; refer to the documentation for the product you want to install. For example, for information about setting up DD Boost with Veritas backup applications (NetBackup and Backup Exec), see the *DD Boost for OpenStorage Administration Guide*. For information on setting up DD Boost with any other application, see the application-specific documentation.

Additional information about configuring and managing DD Boost on the protection system can also be found in the *DD Boost for OpenStorage Administration Guide* (for NetBackup and Backup Exec) and the *DD Boost for Partner Integration Administration Guide* (for other backup applications).

## Managing DD Boost with DD System Manager

Access the DD Boost view in DD System Manager.

### Before you begin

NFSv3 must be enabled to use DD Boost.

### Procedure

1. Select **Data Management > File System**. Verify that the file system is enabled and running by checking its state.



2. Select **Protocols > DD Boost**.

If you go to the DD Boost page without a license, the Status states that DD Boost is not licensed. Click **Add License** and enter a valid license in the Add License Key dialog box.

**Note:** A special license, BLOCK-SERVICES-PROTECTPOINT, is available to enable clients using ProtectPoint block services to have DD Boost functionality without a DD Boost license. If DD Boost is enabled for ProtectPoint clients only—that is, if only the BLOCK-SERVICES-PROTECTPOINT license is installed—the license status indicates that DD Boost is enabled for ProtectPoint only.

Use the DD Boost tabs—Settings, Active Connections, IP Network, Fibre Channel, and Storage Units—to manage DD Boost.

## Specifying DD Boost user names

A DD Boost user is also a DD OS user. Specify a DD Boost user either by selecting an existing DD OS user name or by creating a new DD OS user name and making that name a DD Boost user.

### About this task

Backup applications use the DD Boost user name and password to connect to the protection system. You must configure these credentials on each backup server that connects to this system. The system supports multiple DD Boost users. For complete information about setting up DD Boost with Veritas NetBackup and Backup Exec, see the *DD Boost for OpenStorage Administration Guide*. For information on setting up DD Boost with other applications, see the *DD Boost for Partner Integration Administration Guide* and the application-specific documentation.

### Procedure

1. Select **Protocols > DD Boost**.
2. Select **Add (+)** above the Users with DD Boost Access list.  
The Add User dialog appears.
3. To select an existing user, select the user name in the drop-down list.  
If possible, select a user name with management role privileges set to *none*.
4. To create and select a new user, select **Create a new Local User** and do the following:
  - a. Enter the new user name in the User field.  
The user must be configured in the backup application to connect to the protection system.
  - b. Enter the password twice in the appropriate fields.
5. Click **Add**.

## Changing DD Boost user passwords

Change a DD Boost user password.

### Procedure

1. Select **Protocols > DD Boost > Settings**.
2. Select a user in the Users with DD Boost Access list.
3. Click the **Edit** button (pencil icon) above the DD Boost user list.  
The Change Password dialog appears.



4. Enter the password twice in the appropriate boxes.
5. Click **Change**.

## Troubleshooting DD Boost user access issues

### DD Boost user is locked out

The most common reason a user becomes locked out of the system is that the password expired. Passwords must be changed at intervals specified by the system administrator (90 days by default). Refer to KB article 520213 Data Domain: DDBoost user shows locked status for information on resolving and preventing this issue.

## Removing a DD Boost user name

Remove a user from the DD Boost access list.

### Procedure

1. Select **Protocols > DD Boost > Settings**.
2. Select the user in the Users with DD Boost Access list that needs to be removed.
3. Click **Remove (X)** above the DD Boost user list.

The Remove User dialog appears.

4. Click **Remove**.

After removal, the user remains in the DD OS access list.

## Enabling DD Boost

Use the DD Boost Settings tab to enable DD Boost and to select or add a DD Boost user.

### Procedure

1. Select **Protocols > DD Boost**.
2. Click **Enable** in the DD Boost Status area.  
The Enable DD Boost dialog box is displayed.
3. Select an existing user name from the menu, or add a new user by supplying the name, password, and role.


## Configuring Kerberos

You can configure Kerberos by using the DD Boost Settings tab.

### Procedure

1. Select **Protocols > DD Boost > Settings**.
2. Click **Configure** in the Kerberos Mode status area.

The Authentication tab under **Administration > Access** is displayed.

 **Note:** You can also enable Kerberos by going directly to Authentication under **Administration > Access** in System Manager.

3. Under Active Directory/Kerberos Authentication, click **Configure**.

The Active Directory/Kerberos Authentication dialog box is displayed.

Choose the type of Kerberos Key Distribution Center (KDC) you want to use:

- **Disabled**
  - ① Note: If you select **Disabled**, NFS clients do not use Kerberos authentication. CIFS clients use Workgroup authentication.
- **Windows/Active Directory**
  - ① Note: Enter the Realm Name, Under Name, and Password for Active Directory authentication.
- **Unix**
  - a. Enter the Realm Name, the IP Address/Host Names of one to three KDC servers.
  - b. Upload the keytab file from one of the KDC servers.

## Disabling DD Boost

Disabling DD Boost drops all active connections to the backup server. When you disable or destroy DD Boost, the DD Boost FC service is also disabled.

### Before you begin

Ensure there are no jobs running from your backup application before disabling.

### About this task

① Note: File replication started by DD Boost between two restore operations is not canceled.

### Procedure

1. Select **Protocols > DD Boost**.
2. Click **Disable** in the DD Boost Status area.
3. Click **OK** in the Disable DD Boost confirmation dialog box.

## Viewing DD Boost storage units

Access the Storage Units tab to view and manage DD Boost storage units.

The DD Boost Storage Unit tab:

- Lists the storage units and provides the following information for each storage unit:

**Table 128** Storage unit information

Item	Description
Storage Unit	The name of the storage unit.
User	The DD Boost user owning the storage unit.
Quota Hard Limit	The percentage of hard limit quota used.
Last 24 hr Pre-Comp	The amount of raw data from the backup application that has been written in the last 24 hours.
Last 24 hr Post-Comp	The amount of storage used after compression in the last 24 hours.
Last 24 hr Comp Ratio	The compression ratio for the last 24 hours.
Weekly Avg Post-Comp	The average amount of compressed storage used in the last five weeks.
Last Week Post-Comp	The average amount of compressed storage used in the last seven days.

**Table 128** Storage unit information (continued)

Item	Description
Weekly Avg Comp Ratio	The average compression ratio for the last five weeks.
Last Week Comp Ratio	The average compression ratio for the last seven days.

- Allows you to create, modify, and delete storage units.
- Displays four related tabs for a storage unit selected from the list: Storage Unit, Space Usage, Daily Written, and Data Movement.
  - ① **Note:** The Data Movement tab is available only if an optional Cloud Tier license is installed.
- Takes you to **Replication > On-Demand > File Replication** when you click the **View DD Boost Replications** link.
  - ① **Note:** A DD Replicator license is required for DD Boost to display tabs other than the File Replication tab.

## Creating a storage unit

You must create at least one storage unit on the protection system, and a DD Boost user must be assigned to that storage unit. Use the Storage Units tab to create a storage unit.

### About this task

Each storage unit is a top-level subdirectory of the `/data/coll` directory; there is no hierarchy among storage units.

### Procedure

1. Select **Protocols > DD Boost > Storage Units**.
2. Click **Create (+)**.

The Create Storage Unit dialog box is displayed.

3. Enter the storage unit name in the Name box.

Each storage unit name must be unique. Storage unit names can be up to 50 characters. The following characters are acceptable:

- upper- and lower-case alphabetical characters: A-Z, a-z
- numbers: 0-9
- embedded space

① **Note:** The storage-unit name must be enclosed in double quotes (") if the name has an embedded space.

- comma (,)
- period (.), as long as it does not precede the name
- exclamation mark (!)
- number sign (#)
- dollar sign (\$)
- per cent sign (%)
- plus sign (+)
- at sign (@)
- equal sign (=)

- ampersand (&)
  - semi-colon (;)
  - parenthesis [(and)]
  - square brackets {[and]}
  - curly brackets ({and})
  - caret (^)
  - tilde (~)
  - apostrophe (unslanted single quotation mark)
  - single slanted quotation mark (')
  - minus sign (-)
  - underscore (\_)
4. To select an existing username that will have access to this storage unit, select the user name in the dropdown list.  
If possible, select a username with management role privileges set to *none*.
  5. To create and select a new username that will have access to this storage unit, select **Create a new Local User** and:
    - a. Enter the new user name in the User box.  
The user must be configured in the backup application to connect to the protection system.
    - b. Enter the password twice in the appropriate boxes.
  6. To set storage space restrictions to prevent a storage unit from consuming excess space: enter either a soft or hard limit quota setting, or both a hard and soft limit. With a soft limit an alert is sent when the storage unit size exceeds the limit, but data can still be written to it. Data cannot be written to the storage unit when the hard limit is reached.
    - ⓘ Note: Quota limits are pre-compressed values. To set quota limits, select **Set to Specific Value** and enter the value. Select the unit of measurement: MiB, GiB, TiB, or PiB.
    - ⓘ Note: When setting both soft and hard limits, a quota's soft limit cannot exceed the quota's hard limit.
  7. Click **Create**.
  8. Repeat the above steps for each DD Boost-enabled system.

## Viewing storage unit information

From the DD Boost Storage Units tab, you can select a storage unit and access the Storage Unit, Space Usage, Daily Written, and Data Movement tabs for the selected storage unit.

### Storage Unit tab

The Storage Unit tab shows detailed information for a selected storage unit in its Summary and Quota panels. The Snapshot panel shows snapshot details, allows you to create new snapshots and schedules, and provides a link to the **Data Management > Snapshots** tab.

- The Summary panel shows summarized information for the selected storage unit.

Table 129 Summary panel

Summary item	Description
Total Files	The total number of file images on the storage unit. For compression details that you can download to a log file, click the Download Compression Details link. The generation can take up to several minutes. After it has completed, click Download.
Full Path	<code>/data/coll/filename</code>
Status	R: read; W: write; Q: quota defined
Pre-Comp Used	The amount of pre-compressed storage already used.

- The Quota panel shows quota information for the selected storage unit.

Table 130 Quota panel

Quota item	Description
Quota Enforcement	Enabled or disable. Clicking Quota takes you to the <b>Data Management &gt; Quota</b> tab where you can configure quotas.
Pre-Comp Soft Limit	Current value of soft quota set for the storage unit.
Pre-Comp Hard Limit	Current value of hard quota set for the storage unit.
Quota Summary	Percentage of Hard Limit used.

To modify the pre-comp soft and hard limits shown in the tab:

- Click the **Quota** link in the Quota panel.
  - In the Configure Quota dialog box, enter values for hard and soft quotas and select the unit of measurement: MiB, GiB, TiB, or PiB. Click **OK**.
- Snapshots**  
The Snapshots panel shows information about the storage unit's snapshots.

Table 131 Snapshots panel

Item	Description
Total Snapshots	The total number of snapshots created for this MTree. A total of 750 snapshots can be created for each MTree.
Expired	The number of snapshots in this MTree that have been marked for deletion, but have not been removed with the clean operation as yet.
Unexpired	The number of snapshots in this MTree that are marked for keeping.
Oldest Snapshot	The date of the oldest snapshot for this MTree.
Newest Snapshot	The date of the newest snapshot for this MTree.
Next Scheduled	The date of the next scheduled snapshot.
Assigned Snapshot Schedules	The name of the snapshot schedule assigned to this MTree.

Using the Snapshots panel, you can:

- Assign a snapshot schedule to a selected storage unit: Click **Assign Schedules**. Select the schedule's checkbox; click **OK** and **Close**.
- Create a new schedule: Click **Assign Snapshot Schedules > Create Snapshot Schedule**. Enter the new schedule's name.
  - ① Note: The snapshot name can be composed only of letters, numbers, `_`, `-`, `%d` (numeric day of the month: 01-31), `%a` (abbreviated weekday name), `%m` (numeric month of the year: 01-12), `%B` (abbreviated month name), `%Y` (year, two digits), `%Y` (year, four digits), `%H` (hour: 00-23), and `%M` (minute: 00-59), following the pattern shown in the dialog box. Enter the new pattern and click **Validate Pattern & Update Sample**. Click **Next**.
    - Select when the schedule is to be executed: weekly, every day (or selected days), monthly on specific days that you select by clicking that date in the calendar, or on the last day of the month. Click **Next**.
    - Enter the times of the day when the schedule is to be executed: Either select **At Specific Times** or **In Intervals**. If you select a specific time, select the time from the list. Click **Add (+)** to add a time (24-hour format). For intervals, select **In Intervals** and set the start and end times and how often (**Every**), such as every eight hours. Click **Next**.
    - Enter the retention period for the snapshots in days, months, or years. Click **Next**.
    - Review the **Summary** of your configuration. Click **Back** to edit any of the values. Click **Finish** to create the schedule.
- Click the **Snapshots** link to go to the **Data Management > Snapshots** tab.

#### Space Usage tab

The Space Usage tab graph displays a visual representation of data usage for the storage unit over time.

- Click a point on a graph line to display a box with data at that point.
- Click **Print** (at the bottom on the graph) to open the standard Print dialog box.
- Click **Show in new window** to display the graph in a new browser window.

There are two types of graph data displayed: Logical Space Used (Pre-Compression) and Physical Capacity Used (Post-Compression).

#### Daily Written tab

The Daily Written view contains a graph that displays a visual representation of data that is written daily to the system over a period of time, selectable from 7 to 120 days. The data amounts are shown over time for pre- and post-compression amounts.

#### Data Movement tab

A graph in the same format as the Daily Written graph that shows the amount of disk space moved to Cloud Tier storage (if the Cloud Tier license is enabled).

## Modifying a storage unit

Use the Modify Storage Unit dialog to rename a storage unit, select a different existing user, create and select a new user, and edit quota settings.

#### About this task

##### Procedure

1. Select **Protocols > DD Boost > Storage Units**.
2. In the Storage Unit list, select the storage unit to modify.

3. Click the pencil icon.  
The Modify Storage Unit dialog appears.
4. To rename the storage unit, edit the text in the **Name** field.
5. To select a different existing user, select the user name in the drop-down list.  
If possible, select a username with management role privileges set to *none*.
6. To create and select a new user, select **Create a new Local User** and do the following:
  - a. Enter the new user name in the User box.  
The user must be configured in the backup application to connect to the protection system.
  - b. Enter the password twice in the appropriate boxes.
7. Edit the Quota Settings as needed.

To set storage space restrictions to prevent a storage unit from consuming excess space: enter either a soft or hard limit quota setting, or both a hard and soft limit. With a soft limit an alert is sent when the storage unit size exceeds the limit, but data can still be written to it. Data cannot be written to the storage unit when the hard limit is reached.

① **Note:** Quota limits are pre-compressed values. To set quota limits, select **Set to Specific Value** and enter the value. Select the unit of measurement: MiB, GiB, TiB, or PiB.

② **Note:** When setting both soft and hard limits, a quota's soft limit cannot exceed the quota's hard limit.

8. Click **Modify**.

## Renaming a storage unit

Use the Modify Storage Unit dialog to rename a storage unit.

### About this task

Renaming a storage unit changes the name of the storage unit while retaining its:

- Username ownership
- Stream limit configuration
- Capacity quota configuration and physical reported size
- AIR association on the local protection system

### Procedure

1. Go to **Protocols > DD Boost > Storage Units**.
2. In the Storage Unit list, select the storage unit to rename.
3. Click the pencil icon.  
The Modify Storage Unit dialog appears.
4. Edit the text in the **Name** field.
5. Click **Modify**.



## Deleting a storage unit

Use the Storage Units tab to delete a storage unit from your protection system. Deleting a storage unit removes the storage unit, as well as any images contained in the storage unit, from your system.

### Procedure

1. Select **Protocols > DD Boost > Storage Units**.
2. Select the storage unit to be deleted from the list.
3. Click **Delete (X)**.
4. Click **OK**.

### Results

The storage unit is removed from your system. You must also manually remove the corresponding backup application catalog entries.

## Undeleting a storage unit

Use the Storage Units tab to undelete a storage unit.

### About this task

Undeleting a storage unit recovers a previously deleted storage unit, including its:

- Username ownership
- Stream limit configuration
- Capacity quota configuration and physical reported size
- AIR association on the local protection system

**Note:** Deleted storage units are available until the next `filesys clean` command is run.

### Procedure

1. Select **Protocols > DD Boost > Storage Units > More Tasks > Undelete Storage Unit....**
2. In the Undelete Storage Units dialog box, select the storage unit(s) that you want to undelete.
3. Click **OK**.

## Selecting DD Boost options

Use the Set DD Boost Options dialog to specify settings for distributed segment processing, virtual synthetics, low bandwidth optimization for file replication, file replication encryption, and file replication network preference (IPv4 or IPv6).

### Procedure

1. To display the DD Boost option settings, select **Protocols > DD Boost > Settings > Advanced Options**.
2. To change the settings, select **More Tasks > Set Options**.

The Set DD Boost Options dialog appears.

3. Select any option to be enabled.
4. Deselect any option to be disabled.

To deselect a File Replication Network Preference option, select the other option.

5. Set the DD Boost security options.
  - a. Select the **Authentication Mode**:
    - None
    - Two-way
    - Two-way Password
  - b. Select the **Encryption Strength**:
    - None
    - Medium
    - High

The protection system compares the global authentication mode and encryption strength against the per-client authentication mode and encryption strength to calculate the effective authentication mode and authentication encryption strength. The system does not use the highest authentication mode from one entry, and the highest encryption settings from a different entry. The effective authentication mode and encryption strength come from the single entry that provides the highest authentication mode.

6. Click **OK**.

① **Note:** You can also manage distributed segment processing via the `ddboost` option commands, which are described in detail in the *DD OS Command Reference Guide*.

### Distributed segment processing

Distributed segment processing increases backup throughput in almost all cases by eliminating duplicate data transmission between the media server and the protection system.

You can manage distributed segment processing via the `ddboost` option commands, which are described in detail in the *DD OS Command Reference Guide*.

### Virtual synthetics

A virtual synthetic full backup is the combination of the last full (synthetic or full) backup and all subsequent incremental backups. Virtual synthetics are enabled by default.

### Low-bandwidth optimization

If you use file replication over a low-bandwidth network (WAN), you can increase replication speed by using low bandwidth optimization. This feature provides additional compression during data transfer. Low bandwidth compression is available to protection systems with an installed Replication license.

Low-bandwidth optimization, which is disabled by default, is designed for use on networks with less than 5 Mbps aggregate bandwidth. Do not use this option if maximum file system write performance is required.

① **Note:** You can also manage low bandwidth optimization via the `ddboost file-replication` commands, which are described in detail in the *DD OS Command Reference Guide*.

## File replication encryption

You can encrypt the data replication stream by enabling the DD Boost file replication encryption option.

- ① **Note:** If DD Boost file replication encryption is used on systems without the Data at Rest option, it must be set to on for both the source and destination systems.

### Managed file replication TCP port setting

For DD Boost managed file replication, use the same global listen port on both the source and target protection systems. To set the listen port, use the `replication option` command as described in the *DD OS Command Reference Guide*.

## File replication network preference

Use this option to set the preferred network type for DD Boost file replication to either IPv4 or IPv6.

## Managing certificates for DD Boost

A host certificate allows DD Boost client programs to verify the identity of the system when establishing a connection. CA certificates identify certificate authorities that should be trusted by the system. The topics in this section describe how to manage host and CA certificates for DD Boost.

### Adding a host certificate for DD Boost

Add a host certificate to your system. DD OS supports one host certificate for DD Boost.

#### Procedure

1. If you have not yet requested a host certificate, request one from a trusted CA.
2. When you have received a host certificate, copy or move it to the computer from which you run DD Service Manager.
3. Start DD System Manager on the system to which you want to add a host certificate.
 

① **Note:** DD System Manager supports certificate management only on the management system (which is the system running DD System Manager).
4. Select **Protocols > DD Boost > More Tasks > Manage Certificates....**

① **Note:** If you try to remotely manage certificates on a managed system, DD System Manager displays an information message at the top of the certificate management dialog. To manage certificates for a system, you must start DD System Manager on that system.
5. In the Host Certificate area, click **Add**.
6. To add a host certificate enclosed in a .p12 file, do the following:
  - a. Select **I want to upload the certificate as a .p12 file**.
  - b. Type the password in the **Password** box.
  - c. Click **Browse** and select the host certificate file to upload to the system.
  - d. Click **Add**.
7. To add a host certificate enclosed in a .pem file, do the following:

- a. Select **I want to upload the public key as a .pem file and use a generated private key.**
- b. Click **Browse** and select the host certificate file to upload to the system.
- c. Click **Add**.

## Adding CA certificates for DD Boost

Add a certificate for a trusted CA to your system. DD OS supports multiple certificates for trusted CAs.

### Procedure

1. Obtain a certificate for the trusted CA.
2. Copy or move the trusted CA certificate to the computer from which you run DD Service Manager.
3. Start DD System Manager on the system to which you want to add the CA certificate.
  - ① **Note:** DD System Manager supports certificate management only on the management system (which is the system running DD System Manager).
4. Select **Protocols > DD Boost > More Tasks > Manage Certificates...**
  - ① **Note:** If you try to remotely manage certificates on a managed system, DD System Manager displays an information message at the top of the certificate management dialog. To manage certificates for a system, you must start DD System Manager on that system.
5. In the CA Certificates area, click **Add**.  
The Add CA Certificate for DD Boost dialog appears.
6. To add a CA certificate enclosed in a .pem file, do the following:
  - a. Select **I want to upload the certificate as a .pem file.**
  - b. Click **Browse**, select the host certificate file to upload to the system, and click **Open**.
  - c. Click **Add**.
7. To add a CA certificate using copy and paste, do the following:
  - a. Copy the certificate text to the clipboard using the controls in your operating system.
  - b. Select **I want to copy and paste the certificate text.**
  - c. Paste the certificate text in the box below the copy and paste selection.
  - d. Click **Add**.

## Managing DD Boost client access and encryption

Use the DD Boost Settings tab to configure which specific clients, or set of clients, can establish a DD Boost connection with the protection System and whether or not the client will use encryption. By default, the system is configured to allow all clients to have access, with no encryption.

- ① **Note:** Enabling in-flight encryption will impact system performance.
- ① **Note:** DD Boost offers global authentication and encryption options to defend your system against man-in-the-middle (MITM) attacks. You specify authentication and encryption settings using the GUI, or CLI commands on the protection system. For details, see the *DD Boost for*

*OpenStorage 3.4 Administration Guide*, and *Adding a DD Boost client* on page 319 or the *DD OS Command Reference Guide*.

## Adding a DD Boost client

Create an allowed DD Boost client and specify whether the client will use encryption.

### Procedure

1. Select **Protocols > DD Boost > Settings**.
2. In the Allowed Clients section, click **Create (+)**.  
The Add Allowed Client dialog appears.
3. Enter the hostname of the client.  
This can be a fully-qualified domain name (e.g. host1.example.com) or a hostname with a wildcard (e.g. \*.example.com).
4. Select the Encryption Strength.  
The options are None (no encryption), Medium (AES128-SHA1), or High (AES256-SHA1).
5. Select the Authentication Mode.  
The options are One Way, Two Way, Two Way Password, or Anonymous.
6. Click **OK**.

## Modifying a DD Boost client

Change the name, encryption strength, and authentication mode of an allowed DD Boost client.

### Procedure

1. Select **Protocols > DD Boost > Settings**.
2. In the Allowed Clients list, select the client to modify.
3. Click the **Edit** button, which displays a pencil icon.  
The Modify Allowed Client dialog appears.
4. To change the name of a client, edit the Client text.
5. To change the Encryption Strength, select the option.  
The options are None (no encryption), Medium (AES128-SHA1), or High (AES256-SHA1).
6. To change the Authentication Mode, select the option.  
The options are One Way, Two Way, or Anonymous.
7. Click **OK**.

## Removing a DD Boost client

Delete an allowed DD Boost client.

### Procedure

1. Select **Protocols > DD Boost > Settings**.
2. Select the client from the list.
3. Click **Delete (X)**.  
The Delete Allowed Clients dialog appears.



4. Confirm and select the client name. Click **OK**.

## About interface groups

This feature lets you combine multiple Ethernet links into a group and register only one interface on the protection system with the backup application. The DD Boost Library negotiates with the system to obtain the best interface to send data. Load balancing provides higher physical throughput to the system.

Configuring an interface group creates a private network within the system, comprised of the IP addresses designated as a group. Clients are assigned to a single group, and the group interface uses load balancing to improve data transfer performance and increase reliability.

For example, in the Veritas NetBackup environment, media server clients use a single public network IP address to access the system. All communication with the system is initiated via this administered IP connection, which is configured on the NetBackup server.

If an interface group is configured, when the system receives data from the media server clients, the data transfer is load-balanced and distributed on all the interfaces in the group, providing higher input/output throughput, especially for customers who use multiple 1 GigE connections.

The data transfer is load-balanced based on the number of connections outstanding on the interfaces. Only connections for backup and restore jobs are load-balanced. Check the Active Connections for more information on the number of outstanding connections on the interfaces in a group.

Should an interface in the group fail, all the in-flight jobs to that interface are automatically resumed on healthy operational links (unbeknownst to the backup applications). Any jobs that are started subsequent to the failure are also routed to a healthy interface in the group. If the group is disabled or an attempt to recover on an alternate interface fails, the administered IP is used for recovery. Failure in one group will not utilize interfaces from another group.

Consider the following information when managing interface groups.

- The IP address must be configured on the system, and its interface enabled. To check the interface configuration, select **Hardware > Ethernet > Interfaces** page, and check for free ports. See the *net* chapter of the *DD OS Command Reference Guide* for information about configuring an IP address for an interface.
- You can use the `ifgroup` commands to manage interface groups; these commands are described in detail in the *DD OS Command Reference Guide*.
- Interface groups provide full support for static IPv6 addresses, providing the same capabilities for IPv6 as for IPv4. Concurrent IPv4 and IPv6 client connections are allowed. A client connected with IPv6 sees IPv6 ifgroup interfaces only. A client connected with IPv4 sees IPv4 ifgroup interfaces only. Individual ifgroups include all IPv4 addresses or all IPv6 addresses. For details, see the *DD Boost for Partner Integration Administration Guide* or the *DD Boost for OpenStorage Administration Guide*.
- Configured interfaces are listed in Active Connections, on the lower portion of the Activities page.

**Note:** See Using DD Boost on HA systems on page 331 for important information about using interface groups with HA systems.

The topics that follow describe how to manage interface groups.

## Interfaces

IFGROUP supports physical and virtual interfaces.

An IFGROUP interface is a member of a single IFGROUP *<group-name>* and may consist of:

- Physical interface such as `eth0a`
- Virtual interface, created for link failover or link aggregation, such as `veth1`
- Virtual alias interface such as `eth0a:2` or `veth1:2`
- Virtual VLAN interface such as `eth0a.1` or `veth1.1`
- Within an IFGROUP `<group-name>`, all interfaces must be on unique interfaces (Ethernet, virtual Ethernet) to ensure failover in the event of network error.

IFGROUP provides full support for static IPv6 addresses, providing the same capabilities for IPv6 as for IPv4. Concurrent IPv4 and IPv6 client connections are allowed. A client connected with IPv6 sees IPv6 IFGROUP interfaces only. A client connected with IPv4 sees IPv4 IFGROUP interfaces only. Individual IFGROUPs include all IPv4 addresses or all IPv6 addresses.

For more information, see the *DD Boost for Partner Integration Administration Guide* or the *DD Boost for OpenStorage Administration Guide*.

## Interface enforcement

IFGROUP lets you enforce private network connectivity, ensuring that a failed job does not reconnect on the public network after network errors.

When interface enforcement is enabled, a failed job can only retry on an alternative private network IP address. Interface enforcement is only available for clients that use IFGROUP interfaces.

Interface enforcement is off (FALSE) by default. To enable interface enforcement, you must add the following setting to the system registry:

```
system.ENFORCE_IFGROUP_RW=TRUE
```

After you've made this entry in the registry, you must do a `filesys restart` for the setting to take effect.

For more information, see the *DD Boost for Partner Integration Administration Guide* or the *DD Boost for OpenStorage Administration Guide*.

## Clients

IFGROUP supports various naming formats for clients. Client selection is based on a specified order of precedence.

An IFGROUP client is a member of a single `ifgroup <group-name>` and may consist of:

- A fully qualified domain name (FQDN) such as `ddbboost.exampledomain.com`
- A partial host, allowing search on the first `n` characters of the hostname. For example, when `n=3`, valid formats are `rtp_.*example.com` and `dur_.*example.com`. Five different values of `n` (1-5) are supported.
- Wild cards such as `*.exampledomain.com` or `**`
- A short name for the client, such as `ddbboost`
- Client public IP range, such as `128.5.20.0/24`

Prior to write or read processing, the client requests an IFGROUP IP address from the server. To select the client IFGROUP association, the client information is evaluated according to the following order of precedence.

1. IP address of the connected protection system. If there is already an active connection between the client and the system, and the connection exists on the interface in the IFGROUP, then the IFGROUP interfaces are made available for the client.



2. Connected client IP range. An IP mask check is done against the client source IP; if the client's source IP address matches the mask in the IFGROUP clients list, then the IFGROUP interfaces are made available for the client.

- For IPv4, you can select five different range masks, based on network.
- For IPv6, fixed masks /64, /112, and /128 are available.

This host-range check is useful for separate VLANs with many clients where there isn't a unique partial hostname (domain).

3. Client Name: `abc-11.d1.com`
4. Client Domain Name: `*.d1.com`
5. All Clients: `*`

For more information, see the *DD Boost for Partner Integration Administration Guide*.

## Creating interface groups

Use the IP Network tab to create interface groups and to add interfaces and clients to the groups.

### About this task

Multiple interface groups improve the efficiency of DD Boost by allowing you to:

- Configure DD Boost to use specific interfaces configured into groups.
- Assign clients to one of those interface groups.
- Monitor which interfaces are active with DD Boost clients.

Create interface groups first, and then add clients (as new media servers become available) to an interface group.

### Procedure

1. Select **Protocols > DD Boost > IP Network**.
2. In the Interface Groups section, click **Add (+)**.
3. Enter the interface group name.
4. Select one or more interfaces. A maximum of 32 interfaces can be configured.
 

**i** Note: Depending upon aliasing configurations, some interfaces may not be selectable if they are sharing a physical interface with another interface in the same group. This is because each interface within the group must be on a different physical interface to ensure fail-over recovery.
5. Click **OK**.
6. In the Configured Clients section, click **Add (+)**.
7. Enter a fully qualified client name or `*.mydomain.com`.
 

**i** Note: The `*` client is initially available to the default group. The `*` client may only be a member of one ifgroup.
8. Select a previously configured interface group, and click **OK**.

## Enabling and disabling interface groups

Use the IP Network tab to enable and disable interface groups.

### Procedure

1. Select **Protocols > DD Boost > IP Network**.
2. In the Interface Groups section, select the interface group in the list.
  - ⓘ Note: If the interface group does not have both clients and interfaces assigned, you cannot enable the group.
3. Click **Edit** (pencil).
4. Click **Enabled** to enable the interface group; clear the checkbox to disable.
5. Click **OK**.

## Modifying an interface group's name and interfaces

Use the IP Network tab to change an interface group's name and the interfaces associated with the group.

### Procedure

1. Select **Protocols > DD Boost > IP Network**.
2. In the Interface Groups section, select the interface group in the list.
3. Click **Edit** (pencil).
4. Retype the name to modify the name.
  - ⓘ The group name must be one to 24 characters long and contain only letters, numbers, underscores, and dashes. It cannot be the same as any other group name and cannot be "default", "yes", "no", or "all."
5. Select or deselect client interfaces in the Interfaces list.
  - ⓘ Note: If you remove all interfaces from the group, it will be automatically disabled.
6. Click **OK**.

## Deleting an interface group

Use the IP Network tab to delete an interface group. Deleting an interface group deletes all interfaces and clients associated with the group.

### Procedure

1. Select **Protocols > DD Boost > IP Network**.
2. In the Interface Groups section, select the interface group in the list. The default group cannot be deleted.
3. Click **Delete (X)**.
4. Confirm the deletion.

## Adding a client to an interface group

Use the IP Network tab to add clients to interface groups.

### Procedure

1. Select **Protocols > DD Boost > IP Network**.
2. In the Configured Clients section, click **Add (+)**.
3. Enter a name for the client.

Client names must be unique and may consist of:

- FQDN
- \*.domain
- Client public IP range:
  - For IPv4, `xx.xx.xx.0/24` provides a 24-bit mask against the connecting IP. The /24 represents what bits are masked when the client's source IP address is evaluated for access to the IFGROUP.
  - For IPv6, `xxxx::0/112` provides a 112-bit mask against the connecting IP. The /112 represents what bits are masked when the client's source IP address is evaluated for access to the IFGROUP.

Client names have a maximum length of 128 characters.

4. Select a previously configured interface group, and click **OK**.

## Modifying a client's name or interface group

Use the IP Network tab to change a client's name or interface group.

### Procedure

1. Select **Protocols > DD Boost > IP Network**.
2. In the Configured Clients section, select the client.
3. Click **Edit** (pencil).
4. Type a new client name.

Client names must be unique and may consist of:

- FQDN
- \*.domain
- Client public IP range:
  - For IPv4, `xx.xx.xx.0/24` provides a 24-bit mask against the connecting IP. The /24 represents what bits are masked when the client's source IP address is evaluated for access to the IFGROUP.
  - For IPv6, `xxxx::0/112` provides a 112-bit mask against the connecting IP. The /112 represents what bits are masked when the client's source IP address is evaluated for access to the IFGROUP.

Client names have a maximum length of 128 characters.

5. Select a new interface group from the menu.

 Note: The old interface group is disabled if it has no clients.

6. Click OK.

## Deleting a client from the interface group

Use the IP Network tab to delete a client from an interface group.

### Procedure

1. Select **Protocols > DD Boost > IP Network**.
2. In the Configured Clients section, select the client.
3. Click Delete (X).

**i** Note: If the interface group to which the client belongs has no other clients, the interface group is disabled.

4. Confirm the deletion.

## Using interface groups for Managed File Replication (MFR)

Interface groups can be used to control the interfaces used for DD Boost MFR, to direct the replication connection over a specific network, and to use multiple network interfaces with high bandwidth and reliability for failover conditions. All protection system IP types are supported—IPv4 or IPv6, Alias IP/VLAN IP, and LACP/failover aggregation.

**i** Note: Interface groups used for replication are different from the interface groups previously explained and are supported for DD Boost Managed File Replication (MFR) only. For detailed information about using interface groups for MFR, see the *DD Boost for Partner Integration Administration Guide* or the *DD Boost for OpenStorage Administration Guide*.

Without the use of interface groups, configuration for replication requires several steps:

1. Adding an entry in the `/etc/hosts` file on the source system for the target system and hard coding one of the private LAN network interfaces as the destination IP address.
2. Adding a route on the source system to the target system specifying a physical or virtual port on the source system to the remote destination IP address.
3. Configuring LACP through the network on all switches between the systems for load balancing and failover.
4. Requiring different applications to use different names for the target system to avoid naming conflicts in the `/etc/hosts` file.

Using interface groups for replication simplifies this configuration through the use of the DD OS System Manager or DD OS CLI commands. Using interface groups to configure the replication path lets you:

- Redirect a hostname-resolved IP address away from the public network, using another private system IP address.
- Identify an interface group based on configured selection criteria, providing a single interface group where all the interfaces are reachable from the target system.
- Select a private network interface from a list of interfaces belonging to a group, ensuring that the interface is healthy.
- Provide load balancing across multiple system interfaces within the same private network.
- Provide a failover interface for recovery for the interfaces of the interface group.
- Provide host failover if configured on the source system.
- Use Network Address Translation (NAT)

The selection order for determining an interface group match for file replication is:

1. Local MTree (storage-unit) path and a specific remote system hostname
2. Local MTree (storage-unit) path with any remote system hostname
3. Any MTree (storage-unit) path with a specific system hostname

The same MTree can appear in multiple interface groups only if it has a different system hostname. The same system hostname can appear in multiple interface groups only if it has a different MTree path. The remote hostname is expected to be an FQDN, such as dd9900-1.example.com.

The interface group selection is performed locally on both the source system and the target system, independent of each other. For a WAN replication network, only the remote interface group needs to be configured since the source IP address corresponds to the gateway for the remote IP address.

## Adding a replication path to an interface group

Use the IP Network tab to add replication paths to interface groups.

### Procedure

1. Select **Protocols > DD Boost > IP Network**.
2. In the Configured Replication Paths section, click **Add (+)**.
3. Enter values for **MTree** and/or **Remote Host**.
4. Select a previously configured interface group, and click **OK**.

## Modifying a replication path for an interface group

Use the IP Network tab to modify replication paths for interface groups.

### Procedure

1. Select **Protocols > DD Boost > IP Network**.
2. In the Configured Replication Paths section, select the replication path.
3. Click **Edit** (pencil).
4. Modify any or all values for **MTree**, **Remote Host**, or **Interface Group**.
5. Click **OK**.

## Deleting a replication path for an interface group

Use the IP Network tab to delete replication paths for interface groups.

### Procedure

1. Select **Protocols > DD Boost > IP Network**.
2. In the Configured Replication Paths section, select the replication path.
3. Click **Delete (X)**.
4. In the Delete Replication Path(s) dialog, click **OK**.

## Destroying DD Boost

Use this option to permanently remove all of the data (images) contained in the storage units. When you disable or destroy DD Boost, the DD Boost FC service is also disabled. Only an administrative user can destroy DD Boost.

### Procedure

1. Manually remove (expire) the corresponding backup application catalog entries.

**i** Note: If multiple backup applications are using the same protection system, then remove all entries from each of those applications' catalogs.

2. Select **Protocols > DD Boost > More Tasks > Destroy DD Boost....**
3. Enter your administrative credentials when prompted.
4. Click **OK**.

## Configuring DD Boost-over-Fibre Channel

In earlier versions of DD OS, all communication between the DD Boost Library and any protection system was performed using IP networking. DD OS now offers Fibre Channel as an alternative transport mechanism for communication between the DD Boost Library and the system.

**i** Note: Windows, Linux, HP-UX (64-bit Itanium architecture), AIX, and Solaris client environments are supported.

### Enabling DD Boost users

Before you can configure the DD Boost-over-FC service on a protection system, you must add one or more DD Boost users and enable DD Boost.

#### Before you begin

- Log in to DD System Manager. For instructions, see "Logging In and Out of DD System Manager."

#### CLI equivalent

```
login as: sysadmin
Data Domain OS 5.7.x.x-12345
Using keyboard-interactive authentication.
Password:
```

- If you are using the CLI, ensure that the SCSI target daemon is enabled:

```
# scsitarget enable
Please wait ...
SCSI Target subsystem is enabled.
```

**i** Note: If you are using DD System Manager, the SCSI target daemon is automatically enabled when you enable the DD Boost-over-FC service (later in this procedure).

- Verify that the DD Boost license is installed. In DD System Manager, select **Protocols > DD Boost > Settings**. If the Status indicates that DD Boost is not licensed, click **Add License** and enter a valid license in the Add License Key dialog box.

#### CLI equivalents

```
# elicense show
# elicense update license-file
```

#### Procedure

1. Select **Protocols > DD Boost > Settings**.
2. In the Users with DD Boost Access section, specify one or more DD Boost user names.

A DD Boost user is also a DD OS user. When specifying a DD Boost user name, you can select an existing DD OS user name, or you can create a new DD OS user name and make that name a DD Boost user. This release supports multiple DD Boost users. For detailed instructions, see "Specifying DD Boost User Names."

#### CLI equivalents

```
# user add username [password password]
```



```
# ddbboost set user-name exampleuser
```

3. Click **Enable** to enable DD Boost.

#### CLI equivalent

```
# ddbboost enable
Starting DDBOOST, please wait.....
DDBOOST is enabled.
```

#### Results

You are now ready to configure the DD Boost-over-FC service.

## Configuring DD Boost

After you have added user(s) and enabled DD Boost, you need to enable the Fibre Channel option and specify the DD Boost Fibre Channel server name. Depending on your application, you may also need to create one or more storage units and install the DD Boost API/plugin on media servers that will access the protection system.

#### Procedure

1. Select **Protocols > DD Boost > Fibre Channel**.
2. Click **Enable** to enable Fibre Channel transport.

#### CLI equivalent

```
# ddbboost option set fc enabled
Please wait...
DD Boost option "FC" set to enabled.
```

3. To change the DD Boost Fibre Channel server name from the default (hostname), click **Edit**, enter a new server name, and click **OK**.

#### CLI equivalent

```
# ddbboost fc dfc-server-name set DFC-ddbeta2
DDBOOST dfc-server-name is set to "DFC-ddbeta2" for DDBOOST FC.
Configure clients to use "DFC-DFC-ddbeta2" for DDBOOST FC.
```

4. Select **Protocols > DD Boost > Storage Units** to create a storage unit (if not already created by the application).

You must create at least one storage unit on the system, and a DD Boost user must be assigned to that storage unit. For detailed instructions, see "Creating a Storage Unit."

#### CLI equivalent

```
# ddbboost storage-unit create storage_unit_name-su
```

5. Install the DD Boost API/plugin (if necessary, based on the application).

The DD Boost OpenStorage plug-in software must be installed on NetBackup media servers that need to access the system. This plug-in includes the required DD Boost Library that integrates with the system. For detailed installation and configuration instructions, see the *DD Boost for Partner Integration Administration Guide* or the *DD Boost for OpenStorage Administration Guide*.



## Results

You are now ready to verify connectivity and create access groups.

## Verifying connectivity and creating access groups

Go to **Hardware > Fibre Channel > Resources** to manage initiators and endpoints for access points. Go to **Protocols > DD Boost > Fibre Channel** to create and manage DD Boost-over-FC access groups.

### About this task

- ① **Note:** Avoid making access group changes on a protection system during active backup or restore jobs. A change may cause an active job to fail. The impact of changes during active jobs depends on a combination of backup software and host configurations.

### Procedure

1. Select **Hardware > Fibre Channel > Resources > Initiators** to verify that initiators are present.

It is recommended that you assign aliases to initiators to reduce confusion during the configuration process.

#### CLI equivalent

```
# scsitarget initiator show list
```

Initiator	System Address	Group	Service
initiator-1	21:00:00:24:ff:31:b7:16	n/a	n/a
initiator-2	21:00:00:24:ff:31:b8:32	n/a	n/a
initiator-3	25:00:00:21:88:00:73:ee	n/a	n/a
initiator-4	50:06:01:6d:3c:e0:68:14	n/a	n/a
initiator-5	50:06:01:6a:46:e0:55:9a	n/a	n/a
initiator-6	21:00:00:24:ff:31:b7:17	n/a	n/a
initiator-7	21:00:00:24:ff:31:b8:33	n/a	n/a
initiator-8	25:10:00:21:88:00:73:ee	n/a	n/a
initiator-9	50:06:01:6c:3c:e0:68:14	n/a	n/a
initiator-10	50:06:01:6b:46:e0:55:9a	n/a	n/a
tasm5_p23	21:00:00:24:ff:31:ce:f8	SetUp_Test	VTL

2. To assign an alias to an initiator, select one of the initiators and click the pencil (edit) icon. In the Name field of the Modify Initiator dialog, enter the alias and click **OK**.

#### CLI equivalents

```
# scsitarget initiator rename initiator-1 initiator-renamed
Initiator 'initiator-1' successfully renamed.
```

```
# scsitarget initiator show list
```

Initiator	System Address	Group	Service
initiator-2	21:00:00:24:ff:31:b8:32	n/a	n/a
initiator-renamed	21:00:00:24:ff:31:b7:16	n/a	n/a

3. On the Resources tab, verify that endpoints are present and enabled.

#### CLI equivalent

```
# scsitarget endpoint show list
```

Endpoint	System Address	Group	Service
endpoint-fc-0	5a	FibreChannel	Yes Online
endpoint-fc-1	5b	FibreChannel	Yes Online

- Go to **Protocols > DD Boost > Fibre Channel**.
- In the DD Boost Access Groups area, click the + icon to add an access group.
- Enter a unique name for the access group. Duplicate names are not supported.

**CLI equivalent**

```
# ddbboost fc group create test-dfc-group
DDBoost FC Group "test-dfc-group" successfully created.
```

- Select one or more initiators. Optionally, replace the initiator name by entering a new one. Click **Next**.

**CLI equivalent**

```
# ddbboost fc group add test-dfc-group initiator initiator-5
Initiator(s) "initiator-5" added to group "test-dfc-group".
```

An initiator is a port on an HBA attached to a backup client that connects to the system for the purpose of reading and writing data using the Fibre Channel protocol. The WWPN is the unique World-Wide Port Name of the Fibre Channel port in the media server.

- Specify the number of DD Boost devices to be used by the group. This number determines which devices the initiator can discover and, therefore, the number of I/O paths to the system. The default is one, the minimum is one, and the maximum is 64.

**CLI equivalent**

```
# ddbboost fc group modify Test device-set count 5
Added 3 devices.
```

See the *DD Boost for OpenStorage Administration Guide* for the recommended value for different clients.

- Indicate which endpoints to include in the group: all, none, or select from the list of endpoints. Click **Next**.

**CLI equivalents**

```
# scsitarget group add Test device ddbboost-dev8 primary-endpoint all
secondary-endpoint all
Device 'ddbboost-dev8' successfully added to group.


# scsitarget group add Test device ddbboost-dev8 primary-endpoint
endpoint-fc-1 secondary-endpoint fc-port-0
Device 'ddbboost-dev8' is already in group 'Test'.
```

When presenting LUNs via attached FC ports on HBAs, ports can be designated as primary, secondary or none. A primary port for a set of LUNs is the port that is currently advertizing those LUNs to a fabric. A secondary port is a port that will broadcast a set of LUNs in the event of primary path failure (this requires manual intervention). A setting of none is used in the case where you do not wish to advertize selected LUNs. The presentation of LUNs is dependent upon the SAN topology.

- Review the Summary and make any modifications. Click **Finish** to create the access group, which is displayed in the DD Boost Access Groups list.

**CLI equivalent**

```
# scsitarget group show detailed
```


-  Note: To change settings for an existing access group, select it from the list and click the pencil icon (Modify).

## Deleting access groups

Use the Fibre Channel tab to delete access groups.

### Procedure

1. Select **Protocols > DD Boost > Fibre Channel**.
2. Select the group to be deleted from the DD Boost Access Groups list.

 Note: You cannot delete a group that has initiators assigned to it. Edit the group to remove the initiators first.

3. Click **Delete (X)**.

## Using DD Boost on HA systems

HA provides seamless failover of any application using DD Boost—that is, any backup or restore operation continues with no manual intervention required. All other DD Boost user scenarios are supported on HA systems as well, including managed file replication (MFR), distributed segment processing (DSP), filecopy, and dynamic interface groups (DIG).

Note these special considerations for using DD Boost on HA systems:

- On HA-enabled protection systems, failovers of the DD server occur in less than 10 minutes. However, recovery of DD Boost applications may take longer than this, because Boost application recovery cannot begin until the DD server failover is complete. In addition, Boost application recovery cannot start until the application invokes the Boost library.
- DD Boost on HA systems requires that the Boost applications be using Boost HA libraries; applications using non-HA Boost libraries do not see seamless failover.
- MFR will fail over seamlessly when both the source and destination systems are HA-enabled. MFR is also supported on partial HA configurations (that is, when either the source or destination system is enabled, but not both) when the failure occurs on the HA-enabled system. For more information, see the *DD Boost for OpenStorage Administration Guide* or the *DD Boost for Partner Integration Administration Guide*.
- Dynamic interface groups should not include IP addresses associated with the direct interconnection between the active and standby nodes.
- DD Boost clients must be configured to use floating IP addresses.

## About the DD Boost tabs

Learn to use the DD Boost tabs in DD System Manager.

### Settings

Use the Settings tab to enable or disable DD Boost, select clients and users, and specify advanced options.

The Settings tab shows the DD Boost status (Enabled or Disabled). Use the **Status** button to switch between **Enabled** or **Disabled**.

Under **Allowed Clients**, select the clients that are to have access to the system. Use the **Add**, **Modify**, and **Delete** buttons to manage the list of clients.

Under **Users with DD Boost Access**, select the users that are to have DD Boost access. Use the **Add**, **Change Password**, and **Remove** buttons to manage the list of users.

Expand **Advanced Options** to see which advanced options are enabled. Go to **More Tasks > Set Options** to reset these options.

## Active Connections

Use the **Active Connections** tab to see information about clients, interfaces, and outbound files.

**Table 132** Connected client information

Item	Description
Client	The name of the connected client.
Idle	Whether the client is idle (Yes) or not (No).
Plug-In Version	The DD Boost plug-in version installed, such as 7.0.0.1.
OS Version	The operating system version installed, such as Linux 3.0.101-108.57-default x86_64
Application Version	The backup application version installed, such as NetWorker 19.1.
Encrypted	Whether the connection is encrypted (Yes) or not (No).
DSP	Whether or not the connection is using Distributed Segment Processing (DSP) or not.
Transport	Type of transport being used, such as IPv4, IPv6 or FCoE (Fibre Channel).

**Table 133** Configured interface connection information

Item	Description
Interface	The IP address of the interface.
Interface Group	One of the following: <ul style="list-style-type: none"> <li>• The name of the interface group.</li> <li>• None, if not a member of one.</li> </ul>
Backup	The number of active backup connections.
Restore	The number of active restore connections.
Replication	The number of active replication connections.
Synthetic	The number of synthetic backups.
Total	The total number of connections for the interface.

**Table 134** Outbound file replication information

Outbound files item	Description
File Name	The name of the outgoing image file.
Target Host	The name of the host receiving the file.
Logical Bytes to Transfer	The number of logical bytes to be transferred.
Logical Bytes Transferred	The number of logical bytes already transferred.

**Table 134** Outbound file replication information (continued)

Outbound files item	Description
Low Bandwidth Optimization	The number of low-bandwidth bytes already transferred.

## IP Network

The IP Network tab lists configured interface groups. Details include whether or not a group is enabled and any configured client interfaces. Administrators can use the Interface Group menu to view which clients are associated with an interface group.

## Fibre Channel

The Fibre Channel tab lists configured DD Boost access groups. Use the Fibre Channel tab to create and delete access groups and to configure initiators, devices, and endpoints for DD Boost access groups.

## Storage Units

Use the **Storage Units** tab to view, create, modify, and delete storage units.

**Table 135** Storage Units tab

Item	Description
Storage Units	
View DD Boost Replications	View DD Boost replication contexts.
Storage Unit	The name of the storage unit.
User	Username associated with the storage unit.
Quota Hard Limit	The hard quota set for the storage unit.
Last 24hr Pre-Comp	The amount of data written to the storage unit in the last 24 hours, before compression.
Last 24hr Post-Comp	The amount of data written to the storage unit in the last 24 hours, after compression.
Last 24hr Comp Ratio	Compression ratio of the data written to the storage unit in the last 24 hours.
Weekly Avg Post-Comp	Average amount of data written to the storage unit each week, after compression.
Last Week Post-Comp	Amount of data written to the storage unit in the last week, after compression.
Weekly Avg Comp Ratio	Average compression ratio of data written to the storage unit each week.
Last Week Comp Ratio	Compression ratio of the data written to the storage unit in the last week.

Select a storage unit to see detailed information about it. Detailed information is available on three tabs:

- Storage Unit tab

**Table 136** Storage unit details: Storage Unit tab

Item	Description
Total Files	The total number of file images on the storage unit.
Full Path	The full path of the storage unit.
Status	The current status of the storage unit (combinations are supported). Status can be: <ul style="list-style-type: none"> <li>D—Deleted</li> <li>RO—Read-only</li> <li>RW—Read/write</li> <li>RD—Replication destination</li> <li>RLE—DD Retention lock enabled</li> <li>RLD—DD Retention lock disabled</li> </ul>
Pre-Comp Used	The amount of pre-compressed storage already used.
Used (Post-Comp)	The total size after compression of the files in the storage unit.
Compression	The compression ratio achieved on the files.
Schedules	The number of physical capacity measurement schedules assigned to the storage unit.
Submitted Measurements	The number of times the physical capacity of the storage unit has been measured.
Quota Enforcement	Click Quota to go to the Data Management Quota page, which lists hard and soft quota values/percentage used by MTrees.
Pre-Comp Soft Limit	Current value of soft quota set for the storage unit.
Pre-Comp Hard Limit	Current value of hard quota set for the storage unit.
Quota Summary	Percentage of Hard Limit used.
Total Snapshots	Total number of snapshots of the storage unit.
Expired	Number of expired snapshots of the storage unit.
Unexpired	Number of unexpired snapshots of the storage unit.
Oldest Snapshot	The oldest snapshot of the storage unit.
Newest Snapshot	The newest snapshot of the storage unit.
Next Scheduled	The next scheduled snapshot of the storage unit.
Assigned Snapshot Schedules	The snapshot schedules assigned to the storage unit.

- Space Usage tab: Displays a graph showing pre-compression bytes used, post-compression bytes used, and compression factor.
- Daily Written tab: Displays a graph showing pre-compression bytes written, post-compression bytes written, and total compression factor.

# CHAPTER 15

## DD Virtual Tape Library

This chapter includes:

• DD Virtual Tape Library overview.....	336
• Planning a DD VTL.....	336
• Managing a DD VTL.....	342
• Working with libraries.....	346
• Working with a selected library.....	350
• Viewing changer information.....	357
• Working with drives.....	358
• Working with a selected drive.....	360
• Working with tapes.....	361
• Working with the vault.....	362
• Working with the cloud-based vault.....	363
• Working with access groups.....	369
• Working with a selected access group.....	373
• Working with resources.....	375
• Working with pools.....	379
• Working with a selected pool.....	382



## DD Virtual Tape Library overview

DD Virtual Tape Library (DD VTL) is a disk-based backup system that emulates the use of physical tapes. It enables backup applications to connect to and manage DD system storage using functionality almost identical to a physical tape library.

Virtual tape drives are accessible to backup software in the same way as physical tape drives. After you create these drives in a DD VTL, they appear to the backup software as SCSI tape drives. The DD VTL, itself, appears to the backup software as a SCSI robotic device accessed through standard driver interfaces. However, the backup software (not the DD system that is configured as a DD VTL) manages the movement of the media changer and backup images.

The following terms have special meaning when used with DD VTL:

- **Library:** A library emulates a physical tape library with drives, changer, CAPs (cartridge access ports), and slots (cartridge slots).
- **Tape:** A tape is represented as a file. Tapes can be imported from the vault to a library. Tapes can be exported from a library to the vault. Tapes can be moved within a library across drives, slots, and CAPs.
- **Pool:** A pool is a collection of tapes that maps to a directory on the file system. Pools are used to replicate tapes to a destination. By default, pools are created as MTree pools unless you specify them as directory pools when they are created. You can convert directory-based pools to MTree-based pools to take advantage of the greater functionality of MTrees.
- **Vault:** The vault holds tapes not being used by any library. Tapes reside in either a library or the vault.

DD VTL has been tested with, and is supported by, specific backup software and hardware configurations. For more information, see the appropriate *Backup Compatibility Guide* on the Online Support Site.

DD VTL supports simultaneous use of the tape library and file system (NFS/CIFS/DD Boost) interfaces.

When DR (disaster recovery) is needed, pools and tapes can be replicated to a remote DD system using the DD Replicator.

To protect data on tapes from modification, tapes can be locked using DD Retention Lock Governance software.

**i** Note: At present, 16 Gb/s is supported for fabric and point-to-point topologies. Other topologies will present issues.

The KB article *Data Domain: VTL Best Practices Guide*, available at <https://support.emc.com/kb/180591>, provides additional information about best practices for DD VTL.

The KB article *Data Domain: Create a Virtual Tape Library via CLI*, available at <https://support.emc.com/kb/181043>, provides more information.

## Planning a DD VTL

The DD VTL (Virtual Tape Library) feature has very specific requirements, such as proper licensing, interface cards, user permissions, etc. These requirements are listed here, complete with details and recommendations.

- An appropriate DD VTL license.
  - DD VTL is a licensed feature, and you must use NDMP (Network Data Management Protocol) over IP (Internet Protocol) or DD VTL directly over FC (Fibre Channel).

- An additional license is required for IBM i systems – the I/OS license.
- Adding a DD VTL license through the DD System Manager automatically disables and enables the DD VTL feature.
- An installed FC interface card or DD VTL configured to use NDMP.
  - If the DD VTL communication between a backup server and a DD system is through an FC interface, the DD system must have an FC interface card installed. Notice that whenever an FC interface card is removed from (or changed within) a DD system, any DD VTL configuration associated with that card must be updated.
  - If the DD VTL communication between a backup server and a DD system is through NDMP, no FC interface card is required. However, you must configure the TapeServer access group. Also, when using NDMP, all initiator and port functionality does not apply.
  - The net filter must be configured to allow the NDMP client to send information to the DD system. Run the `net filter add operation allow clients <client-IP-address>` command to allow access for the NDMP client.
    - For added security, run the `net filter add operation allow clients <client-IP-address> interfaces <DD-interface-IP-address>` command.
    - Add the `seq-id 1` option to the command to enforce this rule before any other net filter rules.
- A backup software minimum record (block) size.
  - If possible, set backup software to use a minimum record (block) size of 64 KiB or larger. Larger sizes usually give faster performance and better data compression.
  - Depending on your backup application, if you change the size after the initial configuration, data written with the original size might become unreadable.
- Appropriate user access to the system.
  - For basic tape operations and monitoring, only a user login is required.
  - To enable and configure DD VTL services and perform other configuration tasks, a `sysadmin` login is required.

## DD VTL limits

Before setting up or using a DD VTL, review these limits on size, slots, etc.

- I/O Size – The maximum supported I/O size for any DD system using DD VTL is 1 MB.
- Libraries – DD VTL supports a maximum of 64 libraries per DD system (that is, 64 DD VTL instances on each DD system).
- Initiators – DD VTL supports a maximum of 1024 initiators or WWPNs (world-wide port names) per DD system.
- Tape Drives – Information about tape drives is presented in the next section.
- Data Streams – Information about data streams is presented in the following table.

Table 137 Data streams sent to a protection system

Model	RAM / NVRAM	Backup write streams	Backup read streams	Repl <sup>a</sup> source streams	Repl <sup>a</sup> dest streams	Mixed
DD2200	8 GB	35	6	18	20	w<=35; r<=6; ReplSrc<=18; ReplDest<=20; ReplDest +w<=35; Total<=35

Table 137 Data streams sent to a protection system (continued)

Model	RAM / NVRAM	Backup write streams	Backup read streams	Repl <sup>®</sup> source streams	Repl <sup>®</sup> dest streams	Mixed
DD2200	16 GB	60	16	30	60	w<=60; r<=16; ReplSrc<=30; ReplDest<=60; ReplDest +w<=60; Total<=60
DD5300	48 or 96 GB / 8 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD6800	192 GB / 8 GB	400	110	220	400	w<=400; r<=110; ReplSrc<=220; ReplDest<=400; ReplDest +w<=400; Total<=400
DD6900	288 GB / 16 GB	400	110	220	400	w<=400; r<=110; ReplSrc<=220; ReplDest<=400; ReplDest +w<=400; Total<=400
DD9300	192 or 384 GB / 8 GB	800	220	440	800	w<=800; r<=220; ReplSrc<=440; ReplDest<=800; ReplDest+w<=800; Total<=800
DD9400	576 GB / 16 GB	800	220	440	800	w<=800; r<=220; ReplSrc<=440; ReplDest<=800; ReplDest+w<=800; Total<=800
DD9500	256 or 512 GB / 8 GB	1885	300	540	1080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest +w<=1080; Total<=1885
DD9800	256 or 768 GB / 8 GB	1885	300	540	1080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest +w<=1080; Total<=1885
DD9900	1152 GB / 16 GB	1885	300	540	1080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest +w<=1080; Total<=1885
DD VE 8 TB	8 GB / 512 MB	20	16	20	20	w<= 20 ; r<= 16 ReplSrc<=20; ReplDest<=20; ReplDest +w<=20; w+r+ReplSrc <=20; Total<=20
DD VE 16 TB	16 GB / 512 MB or 24 GB / 1 GB	45	30	45	45	w<= 45 ; r<= 30 ReplSrc<=45; ReplDest<=45; ReplDest +w<=45; w+r+ReplSrc <=45; Total<=45
DD VE 32 TB	24 GB / 1 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest +w<=90; w+r+ReplSrc <=90; Total<=90

Table 137 Data streams sent to a protection system (continued)

Model	RAM / NVRAM	Backup write streams	Backup read streams	Repl <sup>a</sup> source streams	Repl <sup>a</sup> dest streams	Mixed
DD VE 48 TB	36 GB / 1 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest +w<=90; w+r+ReplSrc <=90;Total<=90
DD VE 64 TB	48 GB / 1 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest +w<=90; w+r+ReplSrc <=90;Total<=90
DD VE 96 TB	64 GB / 2 GB	180	50	90	180	w<= 180 ; r<= 50 ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; w+r+ReplSrc <=180;Total<=180
DD3300 4 TB	12 GB (virtual memory) / 512 MB	20	16	30	20	w<= 20 ; r<= 16 ReplSrc<=30; ReplDest<=20; ReplDest +w<=20; w+r+ReplSrc <=30;Total<=30
DD3300 8 TB	32 GB (virtual memory) / 1.536 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest +w<=90; w+r+ReplSrc <=90;Total<=90
DD3300 16 TB	32 GB (virtual memory) / 1.536 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest +w<=90; w+r+ReplSrc <=90;Total<=90
DD3300 32 TB	48 GB (virtual memory) / 1.536 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest +w<=90; w+r+ReplSrc <=90;Total<=140

a. DirRepl, OptDup, MTreeRepl streams

- Slots – DD VTL supports a maximum of:
  - 32,000 slots per library
  - 64,000 slots per DD system

The DD system automatically adds slots to keep the number of slots equal to, or greater than, the number of drives.

① Note: Some device drivers (for example, IBM AIX stape device drivers) limit library configurations to specific drive/slot limits, which may be less than what the DD system supports. Backup applications, and drives used by those applications, may be affected by this limitation.

- CAPs (cartridge access ports) – DD VTL supports a maximum of:
  - 100 CAPs per library

- 1000 CAPs per DD system

## Number of drives supported by a DD VTL

The maximum number of drives supported by a DD VTL depends on the number of CPU cores and the amount of memory installed (both RAM and NVRAM, if applicable) on a DD system.

- (i) Note: There are no references to model numbers in this table because there are many combinations of CPU cores and memories for each model, and the number of supported drives depends *only* on the CPU cores and memories – not on the particular model, itself.

Table 138 Number of drives supported by a DD VTL

Number of CPU cores	RAM (in GB)	NVRAM (in GB)	Maximum number of supported drives
Fewer than 32	4 or less	NA	64
	More than 4, up to 38	NA	128
	More than 38, up to 128	NA	256
	More than 128	NA	540
32 to 39	Up to 128	Less than 4	270
	Up to 128	4 or more	540
	More than 128	NA	540
40 to 59	NA	NA	540
60 or more	NA	NA	1080

## Tape barcodes

When you create a tape, you must assign a unique *barcode* (never duplicate barcodes as this can cause unpredictable behavior). Each barcode consists of eight characters: the first six are numbers or uppercase letters (0-9, A-Z), and the last two are the tape code for the supported tape type, as shown in the following table.

- (i) Note: Although a DD VTL barcode consists of eight characters, either six or eight characters may be transmitted to a backup application, depending on the changer type.

Table 139 Tape Codes by Tape Type

Tape Type	Default Capacity (unless noted)	Tape Code
LTO-1	100 GiB	L1
LTO-1	50 GiB (non-default)	LA <sup>B</sup>
LTO-1	30 GiB (non-default)	LB
LTO-1	10 GiB (non-default)	LC
LTO-2	200 GiB	L2
LTO-3	400 GiB	L3

**Table 139** Tape Codes by Tape Type (continued)

Tape Type	Default Capacity (unless noted)	Tape Code
LTO-4	800 GiB	L4
LTO-5 (default)	1.5 TiB	L5

a. For TSM, use the L2 tape code if the LA code is ignored.

For multiple tape libraries, barcodes are automatically incremented, if the sixth character (just before the "L") is a number. If an overflow occurs (9 to 0), numbering moves one position to the left. If the next character to increment is a letter, incrementation stops. Here are a few sample barcodes and how each will be incremented:

- 00000L1 creates tapes of 100 GiB capacity and can accept a count of up to 100,000 tapes (from 000000 to 99999).
- AA0000LA creates tapes of 50 GiB capacity and can accept a count of up to 10,000 tapes (from 0000 to 9999).
- AAAA00LB creates tapes of 30GiB capacity and can accept a count of up to 100 tapes (from 00 to 99).
- AAAAAALC creates one tape of 10 GiB capacity. Only one tape can be created with this name.
- AAA350L1 creates tapes of 100 GiB capacity and can accept a count of up to 650 tapes (from 350 to 999).
- 00CAAALA creates one tape of 50 GiB capacity. Only one tape can be created with this name.
- 5M7Q3KLB creates one tape of 30 GiB capacity. Only one tape can be created with this name.

## LTO tape drive compatibility

You may have different generations of LTO (Linear Tape-Open) technology in your setup; the compatibility between these generations is presented in tabular form.

In this table:

- RW = read and write compatible
- R = read-only compatible
- — = not compatible

**Table 140** LTO tape drive compatibility

tape format	LTO-5 drive	LTO-4 drive	LTO-3 drive	LTO-2 drive	LTO-1 drive
LTO-5 tape	RW	—	—	—	—
LTO-4 tape	RW	RW	—	—	—
LTO-3 tape	R	RW	RW	—	—
LTO-2 tape	—	R	RW	RW	—
LTO-1 tape	—	—	R	RW	RW



## Setting up a DD VTL

To set up a simple DD VTL, use the Configuration Wizard, which is described in the *Getting Started* chapter.

Then, continue with the following topics to enable the DD VTL, create libraries, and create and import tapes.

- ① **Note:** If the deployment environment includes an AS400 system as a DD VTL client, refer to *Configuring DD VTL default options* on page 345 to configure the serial number prefix for VTL changers and drives before configuring the DD VTL relationship between the protection system and the AS400 client system.

## HA systems and DD VTL

HA systems are compatible with DD VTL; however, if a DD VTL job is in progress during a failover, the job will need to be restarted manually after the failover is complete.

The *DD Operating System Backup Compatibility Guide* provides additional details about the HBA, switch, firmware, and driver requirements for using DD VTL in an HA environment.

## DD VTL tape out to cloud

DD VTL supports storing the VTL vault on Cloud Tier storage. To use this functionality, the protection system must be a supported Cloud Tier configuration, and have a Cloud Tier license in addition to the VTL license.

Configure and license the Cloud Tier storage before configuring DD VTL to use cloud storage for the vault. Cloud Tier on page 441 provides additional information about the requirements for Cloud Tier, and how to configure Cloud Tier.

The FC and network interface requirements for VTL are the same for both cloud-based and local vault storage. DD VTL does not require special configuration to use cloud storage for the vault. When configuring the DD VTL, select the cloud storage as the vault location. However, when working with a cloud-based vault, there are some data management options that are unique to the cloud-based vault. Working with the cloud-based vault on page 363 provides more information.

## Managing a DD VTL

You can manage a DD VTL using the DD System Manager or the CLI. After you login, you can check the status of your DD VTL process, check your license information, and review and configure options.

### Logging In

To use a graphical user interface (GUI) to manage your DD Virtual Tape Library (DD VTL), log in to the DD System Manager.

### CLI Equivalent

You can also log in at the CLI:

```
login as: sysadmin
Data Domain OS
Using keyboard-interactive authentication.
Password:
```



### Enabling SCSI Target Daemon (CLI only)

If you do log in from the CLI, you must enable the `scsitarget` daemon (the Fibre Channel service). This daemon is enabled during the DD VTL or DD Boost-FC enable selections in DD System Manager. In the CLI, these processes need to be enabled separately.

```
# scsitarget enable
Please wait ...
SCSI Target subsystem is enabled.
```

### Accessing DD VTL

From the menu at the left of the DD System Manager, select **Protocols > VTL**.

#### Status

In the **Virtual Tape Libraries > VTL Service** area, you can see the status of your DD VTL process is displayed at the top, for example, **Enabled: Running**. The first part of the status will be **Enabled** (on) or **Disabled** (off). The second part will be one of the following process states.

Table 141 DD VTL process states

State	Description
Running	DD VTL process is enabled and active (shown in green).
Starting	DD VTL process is starting.
Stopping	DD VTL process is being shut down.
Stopped	DD VTL process is disabled (shown in red).
Timing out	DD VTL process crashed and is attempting an automatic restart.
Stuck	After several failed automatic restarts, the DD VTL process is unable to shut down normally, so an attempt is being made to kill it.

### DD VTL License

The VTL License line tells you whether your DD VTL license has been applied. If it says **Unlicensed**, select **Add License**. Enter your license key in the Add License Key dialog. Select **Next** and **OK**.

**Note:** All license information should have been populated as part of the factory configuration process; however, if DD VTL was purchased later, the DD VTL license key may not have been available at that time.

### CLI Equivalent

You can also verify that the DD VTL license has been installed at the CLI:

```
# elicense show
## License Key                               Feature
-----
1  DEFA-EPCD-FCDE-CDEF                       Replication
2  EPCD-FCDE-CDEF-DEFA                       VTL
-----
```

If the license is not present, each unit comes with documentation – a quick install card – which will show the licenses that have been purchased. Enter the following command to populate the license key.

```
# elicense update <license-file>
```

**I/OS License (for IBM i users)**

For customers of IBM i, the I/OS License line tells you whether your I/OS license has been applied. If it says **Unlicensed**, select **Add License**. You must enter a valid I/OS license in either of these formats: `xxxx-xxxx-xxxx-xxxx` or `xxxx-xxxx-xxxx-xxxx-xxxx`. Your I/OS license must be installed before creating a library and drives to be used on an IBM i system. Select **Next** and **OK**.

**Enabling DD VTL**

Enabling DD VTL broadcasts the WWN of the protection system HBA to customer fabric and enables all libraries and library drives. If a forwarding plan is required in the form of change control processes, this process should be enabled to facilitate zoning.

**Procedure**

1. Make sure that you have a DD VTL license and that the file system is enabled.
2. Select **Virtual Tape Libraries > VTL Service**.
3. To the right of the Status area, select **Enable**.
4. In the Enable Service dialog box, select **OK**.
5. After DD VTL has been enabled, note that Status will change to **Enabled: Running** in green. Also note that the configured DD VTL options are displayed in the Option Defaults area.

**CLI Equivalent**

```
# vtl enable
Starting VTL, please wait ...
VTL is enabled.
```

**Disabling DD VTL**

Disabling DD VTL closes all libraries and shuts down the DD VTL process.

**Procedure**

1. Select **Virtual Tape Libraries > VTL Service**.
2. To the right of the Status area, select **Disable**.
3. In the Disable Service dialog, select **OK**.
4. After DD VTL has been disabled, notice that the Status has changed to **Disabled: Stopped** in red.

**CLI Equivalent**

```
# vtl disable
```

**DD VTL option defaults**

The Option Default area of the VTL Service page displays the current settings for default DD VTL options (auto-eject, auto-offline, and barcode-length) that you can configure.

In the **Virtual Tape Libraries > VTL Service** area, the current default options for your DD VTL are displayed. Select **Configure** to change any of these values.

Table 142 Option Defaults

Item	Description
Property	Lists the configured options: <ul style="list-style-type: none"> <li>• auto-eject</li> <li>• auto-offline</li> <li>• barcode-length</li> </ul>
Value	Provides the value for each configured option: <ul style="list-style-type: none"> <li>• auto-eject: default (disabled), enabled, or disabled</li> <li>• auto-offline: default (disabled), enabled, or disabled</li> <li>• barcode-length: default (8), 6, or 8</li> </ul>

## Configuring DD VTL default options

You can configure DD VTL default options when you add a license, create a library, or any time thereafter.

### About this task

- ① **Note:** DD VTLs are assigned global options, by default, and those options are updated whenever global options change, unless you change them manually using this method.

### Procedure

1. Select **Virtual Tape Libraries > VTL Service**.
2. In the Option Defaults area, select **Configure**. In the Configure Default Options dialog box, change any of the default options, and then click **OK**.

Table 143 DD VTL default options

Option	Values	Notes
auto-eject	default (disabled), enable, or disable	Enabling auto-eject causes any tape put into a CAP (cartridge access port) to automatically move to the virtual vault, unless: <ul style="list-style-type: none"> <li>• the tape came from the vault, in which case the tape stays in the CAP.</li> <li>• an <code>ALLOW_MEDIUM_REMOVAL</code> command with a 0 value (false) has been issued to the library to prevent the removal of the medium from the CAP to the outside world.</li> </ul>

Table 143 DD VTL default options (continued)

Option	Values	Notes
auto-offline	default (disabled), enable, or disable	Enabling auto-offline takes a drive offline automatically before a tape move operation is performed.
barcode-length	default (8), 6 or 8 [automatically set to 6 for L180, RESTORER-L180, and DDVTL changer models]	Although a DD VTL barcode consists of 8 characters, either 6 or 8 characters may be transmitted to a backup application, depending on the changer type.

① Note: To disable all of these service options, select **Reset to Factory**, and the values will be immediately reset to factory defaults.

#### After you finish

If the DD VTL environment contains an AS400 as a DD VTL client, configure the DD VTL option for serial-number-prefix manually before adding the AS400 to the DD VTL environment. This is required to avoid duplicate serial numbers when there are multiple protection systems using DD VTL. The serial-number-prefix value must:

- Be a unique six digit value such that no other DD VTL on any system in the environment has the same prefix number
- Not end with a zero

Configure this value only once during the deployment of the system and the configuration of DD VTL. It will persist with any future DD OS upgrades on the system. Setting this value does not require a DD VTL service restart. Any DD VTL library created after setting this value will use the new prefix for the serial number.

CLI equivalent

```
# vtl option set serial-number-prefix value
# vtl option show serial-number-prefix
```

## Working with libraries

A library emulates a physical tape library with drives, changer, CAPs (cartridge access ports), and slots (cartridge slots). Selecting **Virtual Tape Libraries > VTL Service > Libraries** displays detailed information for all configured libraries.

Table 144 Library information

Item	Description
Name	The name of a configured library.
Drives	The number of drives configured in the library.
Slots	The number of slots configured in the library.
CAPs	The number of CAPs (cartridge access ports) configured in the library.

From the More Tasks menu, you can create and delete libraries, as well as search for tapes.

## Creating libraries

DD VTL supports a maximum of 64 libraries per system, that is, 64 concurrently active virtual tape library instances on each DD system.

### Before you begin

If the deployment environment includes an AS400 system as a DD VTL client, refer to *Configuring DD VTL default options* on page 345 to configure the serial number prefix for VTL changers and drives before creating the DD VTL library and configuring the DD VTL relationship between the protection system and the AS400 client system.

### Procedure

1. Select **Virtual Tape Libraries > VTL Service > Libraries**.
2. Select **More Tasks > Library > Create**
3. In the Create Library dialog, enter the following information:

Table 145 Create Library dialog

Field	User input
Library Name	Enter a name of from 1 to 32 alphanumeric characters.
Number of Drives	<p>① Note: The maximum number of drives supported by a DD VTL depends on the number of CPU cores and the amount of memory installed (both RAM and NVRAM, if applicable) on a DD system.</p> <p>Enter the number of drives from 1 to 98. The number of drives to be created will correspond to the number of data streams that will write to a library.</p>
Drive Model	<p>Select the desired model from the drop-down list:</p> <ul style="list-style-type: none"> <li>• IBM-LTO-1</li> <li>• IBM-LTO-2</li> <li>• IBM-LTO-3</li> <li>• IBM-LTO-4</li> <li>• IBM-LTO-5 (default)</li> <li>• HP-LTO-3</li> <li>• HP-LTO-4</li> </ul> <p>Do not mix drive types, or media types, in the same library. This can cause unexpected results and/or errors in the backup operation.</p>
Number of Slots	<p>Enter the number of slots in the library. Here are some things to consider:</p> <ul style="list-style-type: none"> <li>• The number of slots must be equal to or greater than the number of drives.</li> <li>• You can have up to 32,000 slots per individual library</li> <li>• You can have up to 64,000 slots per system.</li> </ul>

Table 145 Create Library dialog (continued)

Field	User input
	<ul style="list-style-type: none"> <li>Try to have enough slots so tapes remain in the DD VTL and never need to be exported to a vault – to avoid reconfiguring the DD VTL and to ease management overhead.</li> <li>Consider any applications that are licensed by the number of slots.</li> </ul> <p>As an example, for a standard 100-GB cartridge you might configure 5000 slots. This would be enough to hold up to 500 TB (assuming reasonably compressible data).</p>
Number of CAPs	<p>(Optional) Enter the number of cartridge access ports (CAPs).</p> <ul style="list-style-type: none"> <li>You can have up to 100 CAPs per library.</li> <li>You can have up to 1000 CAPs per system.</li> </ul> <p>Check your particular backup software application documentation on the Online Support Site for guidance.</p>
Changer Model Name	<p>Select the desired model from the drop-down list:</p> <ul style="list-style-type: none"> <li>L180 (default)</li> <li>RESTORER-L180</li> <li>TS3500</li> <li>I2000</li> <li>I6000</li> <li>DDVTL</li> </ul> <p>Check your particular backup software application documentation on the Online Support Site for guidance. Also refer to the DD VTL support matrix to see the compatibility of emulated libraries to supported software.</p>
<b>Options</b>	
auto-eject	default (disabled), enable, disable
auto-offline	default (disabled), enable, disable
barcode-length	default (8), 6, 8 [automatically set to 6 for L180, RESTORER-L180, and DD VTL changer models]

## 4. Select OK.

After the Create Library status dialog shows **Completed**, select **OK**.

The new library appears under the Libraries icon in the VTL Service tree, and the options you have configured appear as icons under the library. Selecting the library displays details about the library in the Information Panel.

Note that access to VTLs and drives is managed with Access Groups.

**CLI Equivalent**

```
# vtl add NewVTL model L180 slots 50 caps 5
This adds the VTL library, NewVTL. Use 'vtl show config NewVTL' to view it.
```

```
# vtl drive add NewVTL count 4 model IBM-LTO-3
This adds 4 IBM-LTO-3 drives to the VTL library, NewVTL.
```

## Deleting libraries

When a tape is in a drive within a library, and that library is deleted, the tape is moved to the vault. However, the tape's pool does not change.

### Procedure

1. Select **Virtual Tape Libraries > VTL Service > Libraries**.
2. Select **More Tasks > Library > Delete**.
3. In the Delete Libraries dialog, select or confirm the checkbox of the items to delete:
  - The name of each library, or
  - Library Names, to delete all libraries
4. Select **Next**.
5. Verify the libraries to delete, and select **Submit** in the confirmation dialogs.
6. After the Delete Libraries Status dialog shows *Completed*, select **Close**. The selected libraries are deleted from the DD VTL.

### CLI Equivalent

```
# vtl del OldVTL
```

## Searching for tapes

You can use a variety of criteria – location, pool, and/or barcode – to search for a tape.

### Procedure

1. Select **Virtual Tape Libraries or Pools**.
2. Select the area to search (library, vault, pool).
3. Select **More Tasks > Tapes > Search**.
4. In the Search Tapes dialog, enter information about the tape(s) you want to find.

Table 146 Search Tapes dialog

Field	User input
Location	Specify a location, or leave the default (All).
Pool	Select the name of the pool in which to search for the tape. If no pools have been created, use the Default pool.
Barcode	Specify a unique barcode, or leave the default (*) to return a group of tapes. Barcode allows the wildcards ? and *, where ? matches any single character and * matches 0 or more characters.
Count	Enter the maximum number of tapes you want to be returned to you. If you leave this blank, the barcode default (*) is used.

5. Select **Search**.



## Working with a selected library

Selecting **Virtual Tape Libraries > VTL Service > Libraries > library** displays detailed information for a selected library.

Table 147 Devices

Item	Description
Device	The elements in the library, such as drives, slots, and CAPs (cartridge access ports).
Loaded	The number of devices with media loaded.
Empty	The number of devices with no media loaded.
Total	The total number of loaded and empty devices.

Table 148 Options

Property	Value
auto-eject	enabled or disabled
auto-offline	enabled or disabled
barcode-length	6 or 8

Table 149 Tapes

Item	Description
Pool	The name of the pool where the tapes are located.
Tape Count	The number of tapes in that pool.
Capacity	The total configured data capacity of the tapes in that pool, in GiB (Gibibytes, the base-2 equivalent of GB, Gigabytes).
Used	The amount of space used on the virtual tapes in that pool.
Average Compression	The average amount of compression achieved on the data on the tapes in that pool.

From the **More Tasks** menu, you can delete, rename, or set options for a library; create, delete, import, export, or move tapes; and add or delete slots and CAPs.

## Creating tapes

You can create tapes in either a library or a pool. If initiated from a pool, the system first creates the tapes, then imports them to the library.

### Procedure

1. Select **Virtual Tape Libraries > VTL Service > Libraries > library** or **Vault or Pools > Pools > pool**.
2. Select **More Tasks > Tapes > Create**.
3. In the **Create Tapes** dialog, enter the following information about the tape:


Table 150 Create Tapes dialog

Field	User input
Library (if initiated from a library)	If a drop-down menu is enabled, select the library or leave the default selection.
Pool Name	Select the name of the pool in which the tape will reside, from the drop-down list. If no pools have been created, use the Default pool.
Number of Tapes	For a library, select from 1 to 20. For a pool, select from 1 to 100,000, or leave the default (20). [Although the number of supported tapes is unlimited, you can create no more than 100,000 tapes at a time.]
Starting Barcode	Enter the initial barcode number (using the format A99000LA).
Tape Capacity	(optional) Specify the number of GiBs from 1 to 4000 for each tape (this setting overrides the barcode capacity setting). For efficient use of disk space, use 100 GiB or fewer.

4. Select **OK** and **Close**.

#### CLI Equivalent

```
# vtl tape add A00000L1 capacity 100 count 5 pool VTL_Pool
... added 5 tape(s)...
```

 Note: You must auto-increment tape volume names in base10 format.

## Deleting tapes

You can delete tapes from either a library or a pool. If initiated from a library, the system first exports the tapes, then deletes them. The tapes must be in the vault, not in a library. On a Replication destination DD system, deleting a tape is not permitted.

#### Procedure

1. Select **Virtual Tape Libraries > VTL Service > Libraries > library** or **Vault** or **Pools > Pools > pool**.
2. Select **More Tasks > Tapes > Delete**.
3. In the Delete Tapes dialog, enter search information about the tapes to delete, and select **Search**:

Table 151 Delete Tapes dialog

Field	User input
Location	If there is a drop-down list, select a library, or leave the default <b>Vault</b> selection.
Pool	Select the name of the pool in which to search for the tape. If no pools have been created, use the Default pool.
Barcode	Specify a unique barcode, or leave the default (*) to search for a group of tapes. Barcode allows the wildcards ? and *, where ? matches any single character and * matches 0 or more characters.
Count	Enter the maximum number of tapes you want to be returned to you. If you leave this blank, the barcode default (*) is used.

Table 151 Delete Tapes dialog (continued)

Field	User input
Tapes Per Page	Select the maximum number of tapes to display per page – possible values are 15, 30, and 45.
Select all pages	Select the <b>Select All Pages</b> checkbox to select all tapes returned by the search query.
Items Selected	Shows the number of tapes selected across multiple pages – updated automatically for each tape selection.

- Select the checkbox of the tape that should be deleted or the checkbox on the heading column to delete all tapes, and select **Next**.
- Select **Submit** in the confirmation window, and select **Close**.

① Note: After a tape is removed, the physical disk space used for the tape is not reclaimed until after a file system cleaning operation.

#### CLI Equivalent

```
# vtl tape del barcode [count count] [pool pool]
```

For example:

```
# vtl tape del A00000L1
```

① Note: You can act on ranges; however, if there is a missing tape in the range, the action will stop.

## Importing tapes

*Importing a tape* means that an existing tape will be moved from the vault to a library slot, drive, or cartridge access port (CAP).

#### About this task

The number of tapes you can import at one time is limited by the number of empty slots in the library, that is, you cannot import more tapes than the number of currently empty slots.

To view the available slots for a library, select the library from the stack menu. The information panel for the library shows the count in the Empty column.

- If a tape is in a drive, and the tape origin is known to be a slot, a slot is reserved.
- If a tape is in a drive, and the tape origin is unknown (slot or CAP), a slot is reserved.
- If a tape is in a drive, and the tape origin is known to be a CAP, a slot is not reserved. (The tape returns to the CAP when removed from the drive.)
- To move a tape to a drive, see the section on moving tapes, which follows.

#### Procedure

- You can import tapes using either step a. or step b.
  - Select **Virtual Tape Libraries > VTL Service > Libraries > library**. Then, select **More Tasks > Tapes > Import**. In the Import Tapes dialog, enter search information about the tapes to import, and select **Search**:

Table 152 Import Tapes dialog

Field	User input
Location	If there is a drop-down list, select the location of the tape, or leave the default of <b>Vault</b> .
Pool	Select the name of the pool in which to search for the tape. If no pools have been created, use the Default pool.
Barcode	Specify a unique barcode, or leave the default (*) to return a group of tapes. Barcode allows the wildcards ? and *, where ? matches any single character and * matches 0 or more characters.
Count	Enter the maximum number of tapes you want to be returned to you. If you leave this blank, the barcode default (*) is used.
Select Destination > Device	Select the destination device where the tape will be imported. Possible values are Drive, CAP, and Slot.
Tapes Per Page	Select the maximum number of tapes to display per page. Possible values are 15, 30, and 45.
Items Selected	Shows the number of tapes selected across multiple pages – updated automatically for each tape selection.

Based on the previous conditions, a default set of tapes is searched to select the tapes to import. If pool, barcode, or count is changed, select **Search** to update the set of tapes available from which to choose.

b. Select **Virtual Tape Libraries > VTL Service > Libraries > library > Changer > Drives > drive > Tapes**. Select tapes to import by selecting the checkbox next to:

- An individual tape, or
- The **Barcode** column to select all tapes on the current page, or
- The **Select all pages** checkbox to select all tapes returned by the search query.

Only tapes showing Vault in the Location can be imported.

Select **Import from Vault**. This button is disabled by default and enabled only if all of the selected tapes are from the Vault.

- From the Import Tapes: library view, verify the summary information and the tape list, and select **OK**.
- Select **Close** in the status window.

### CLI Equivalent

```
# vtl tape show pool VTL_Pool
Processing tapes...
Barcode Pool Location State Size Used (%) Comp ModTime
-----
A00000L3 VTL_Pool vault RW 100 GiB 0.0 GiB (0.00%) 0x 2010/07/16 09:50:41
A00001L3 VTL_Pool vault RW 100 GiB 0.0 GiB (0.00%) 0x 2010/07/16 09:50:41
A00002L3 VTL_Pool vault RW 100 GiB 0.0 GiB (0.00%) 0x 2010/07/16 09:50:41
A00003L3 VTL_Pool vault RW 100 GiB 0.0 GiB (0.00%) 0x 2010/07/16 09:50:41
A00004L3 VTL_Pool vault RW 100 GiB 0.0 GiB (0.00%) 0x 2010/07/16 09:50:41
-----
VTL Tape Summary
-----
Total number of tapes: 5
Total pools: 1
```

```

Total size of tapes:      500 GiB
Total space used by tapes: 0.0 GiB
Average Compression:    0.0x

# vtl import NewVTL barcode A00000L3 count 5 pool VTL_Pool
... imported 5 tape(s)...

# vtl tape show pool VTL_Pool
Processing tapes....

VTL Tape Summary
-----
Total number of tapes:    5
Total pools:              1
Total size of tapes:     500 GiB
Total space used by tapes: 0.0 GiB
Average Compression:    0.0x

```

## Exporting tapes

*Exporting a tape* removes that tape from a slot, drive, or cartridge-access port (CAP) and sends it to the vault.

### Procedure

- You can export tapes using either step a. or step b.
  - Select **Virtual Tape Libraries > VTL Service > Libraries > library**. Then, select **More Tasks > Tapes > Export**. In the Export Tapes dialog, enter search information about the tapes to export, and select **Search**:

**Table 153** Export Tapes dialog

Field	User input
Location	If there is a drop-down list, select the name of the library where the tape is located, or leave the selected library.
Pool	Select the name of the pool in which to search for the tape. If no pools have been created, use the Default pool.
Barcode	Specify a unique barcode, or leave the default (*) to return a group of tapes. Barcode allows the wildcards ? and *, where ? matches any single character and * matches 0 or more characters.
Count	Enter the maximum number of tapes you want to be returned to you. If you leave this blank, the barcode default (*) is used.
Tapes Per Page	Select the maximum number of tapes to display per page. Possible values are 15, 30, and 45.
Select all pages	Select the <b>Select All Pages</b> checkbox to select all tapes returned by the search query.
Items Selected	Shows the number of tapes selected across multiple pages – updated automatically for each tape selection.

- Select **Virtual Tape Libraries > VTL Service > Libraries > library > Changer > Drives > drive > Tapes**. Select tapes to export by selecting the checkbox next to:
  - An individual tape, or
  - The **Barcode** column to select all tapes on the current page, or
  - The **Select all pages** checkbox to select all tapes returned by the search query.

Only tapes with a library name in the Location column can be exported.

Select **Export from Library**. This button is disabled by default and enabled only if all of the selected tapes have a library name in the Location column.

- From the Export Tapes: library view, verify the summary information and the tape list, and select **OK**.
- Select **Close** in the status window.

#### CLI Equivalent

```
# vtl export NewVTL cap address 1 count 4
... exported 4 tape(s)...
```

## Moving tapes between devices within a library

Tapes can be moved between physical devices within a library to mimic backup software procedures for physical tape libraries (which move a tape in a library from a slot to a drive, a slot to a CAP, a CAP to a drive, and the reverse). In a physical tape library, backup software never moves a tape outside the library. Therefore, the destination library cannot change and is shown only for clarification.

#### Procedure

- Select **Virtual Tape Libraries > VTL Service > Libraries > library**.  
Note that when started from a library, the Tapes panel allows tapes to be moved only between devices.
- Select **More Tasks > Tapes > Move**.  
Note that when started from a library, the Tapes panel allows tapes to be moved only between devices.
- In the Move Tape dialog, enter search information about the tapes to move, and select **Search**:

Table 154 Move Tape dialog

Field	User input
Location	Location cannot be changed.
Pool	Select a pool.
Barcode	Specify a unique barcode, or leave the default (*) to return a group of tapes. Barcode allows the wildcards ? and *, where ? matches any single character and * matches 0 or more characters.
Count	Enter the maximum number of tapes you want to be returned to you. If you leave this blank, the barcode default (*) is used.
Tapes Per Page	Select the maximum number of tapes to display per page. Possible values are 15, 30, and 45.
Items Selected	Shows the number of tapes selected across multiple pages – updated automatically for each tape selection.

- From the search results list, select the tape or tapes to move.
- Do one of the following:

- a. Select the device from the Device list (for example, a slot, drive, or CAP), and enter a starting address using sequential numbers for the second and subsequent tapes. For each tape to be moved, if the specified address is occupied, the next available address is used.
  - b. Leave the address blank if the tape in a drive originally came from a slot and is to be returned to that slot; or if the tape is to be moved to the next available slot.
6. Select **Next**.
  7. In the Move Tape dialog, verify the summary information and the tape listing, and select **Submit**.
  8. Select **Close** in the status window.

## Adding slots

You can add slots from a configured library to change the number of storage elements.

### About this task

- ① **Note:** Some backup applications do not automatically recognize that slots have been added to a DD VTL. See your application documentation for information on how to configure the application to recognize this type of change.

### Procedure

1. Select **Virtual Tape Libraries > VTL Service > Libraries > library**.
2. Select **More Tasks > Slots > Add**.
3. In the Add Slots dialog, enter the Number of Slots to add. The total number of slots in a library, or in all libraries on a system, cannot exceed 32,000 for a library and 64,000 for a system.
4. Select **OK** and **Close** when the status shows *Completed*.

## Deleting slots

You can delete slots from a configured library to change the number of storage elements.

### About this task

- ① **Note:** Some backup applications do not automatically recognize that slots have been deleted from a DD VTL. See your application documentation for information on how to configure the application to recognize this type of change.

### Procedure

1. If the slot that you want to delete contains cartridges, move those cartridges to the vault. The system will delete only empty, uncommitted slots.
2. Select **Virtual Tape Libraries > VTL Service > Libraries > library**.
3. Select **More Tasks > Slots > Delete**.
4. In the Delete Slots dialog, enter the Number of Slots to delete.
5. Select **OK** and **Close** when the status shows *Completed*.



## Adding CAPs

You can add CAPs (cartridge access ports) from a configured library to change the number of storage elements.

### About this task

- ① **Note:** CAPs are used by a limited number of backup applications. See your application documentation to ensure that CAPs are supported.

### Procedure

1. Select **Virtual Tape Libraries > VTL Service > Libraries > library**.
2. Select **More Tasks > CAPs > Add**.
3. In the Add CAPs dialog, enter the Number of CAPs to add. You can add from 1 to 100 CAPs per library and from 1 to 1,000 CAPs per system.
4. Select **OK** and **Close** when the status shows *Completed*.

## Deleting CAPs

You can delete CAPs (cartridge access ports) from a configured library to change the number of storage elements.

### About this task

- ① **Note:** Some backup applications do not automatically recognize that CAPs have been deleted from a DD VTL. See your application documentation for information on how to configure the application to recognize this type of change.

### Procedure

1. If the CAP that you want to delete contains cartridges, move those cartridges to the vault, or this will be done automatically.
2. Select **Virtual Tape Libraries > VTL Service > Libraries > library**.
3. Select **More Tasks > CAPs > Delete**.
4. In the Delete CAPs dialog, enter the Number of CAPs to delete. You can delete a maximum of 100 CAPs per library or 1000 CAPs per system.
5. Select **OK** and **Close** when the status shows *Completed*.

## Viewing changer information

There can be only one changer per DD VTL. The changer model you select depends on your specific configuration.

### Procedure

1. Select **Virtual Tape Libraries > VTL Service > Libraries**.
2. Select a specific library.
3. If not expanded, select the plus sign (+) on the left to open the library, and select a Changer element to display the Changer information panel, which provides the following information.

Table 155 Changer information panel

Item	Description
Vendor	The name of the vendor who manufactured the changer
Product	The model name
Revision	The revision level
Serial Number	The changer serial number

## Working with drives

Selecting **Virtual Tape Libraries > VTL Service > Libraries > library > Drives** displays detailed information for all drives for a selected library.

### About this task

Table 156 Drives information panel

Column	Description
Drive	The list of drives by name, where name is "Drive #" and # is a number between 1 and n representing the address or location of the drive in the list of drives.
Vendor	The manufacturer or vendor of the drive, for example, IBM.
Product	The product name of the drive, for example, ULTRIUM-TD5.
Revision	The revision number of the drive product.
Serial Number	The serial number of the drive product.
Status	Whether the drive is Empty, Open, Locked, or Loaded. A tape must be present for the drive to be locked or loaded.
Tape	The barcode of the tape in the drive (if any).
Pool	The pool of the tape in the drive (if any).

**Tape and library drivers** – To work with drives, you must use the tape and library drivers supplied by your backup software vendor that support the IBM LTO-1, IBM LTO-2, IBM LTO-3, IBM LTO-4, IBM LTO-5 (default), HP-LTO-3, or HP-LTO-4 drives and the StorageTek L180 (default), RESTORER-L180, IBM TS3500, I2000, I6000, or DDVTL libraries. For more information, see the *Application Compatibility Matrices and Integration Guides* for your vendors. When configuring drives, also keep in mind the limits on backup data streams, which are determined by the platform in use.

**LTO drive capacities** – Because the DD system treats LTO drives as virtual drives, you can set a maximum capacity to 4 TiB (4000 GiB) for each drive type. The default capacities for each LTO drive type are as follows:

- LTO-1 drive: 100 GiB
- LTO-2 drive: 200 GiB
- LTO-3 drive: 400 GiB
- LTO-4 drive: 800 GiB
- LTO-5 drive: 1.5 TiB

**Migrating LTO-1 tapes** – You can migrate tapes from existing LTO-1 type VTLs to VTLs that include other supported LTO-type tapes and drives. The migration options are different for each

backup application, so follow the instructions in the LTO tape migration guide specific to your application. To find the appropriate guide, go to the Online Support Site, and in the search text box, type in **LTO Tape Migration for VTLs**.

**Tape full: Early warning** – You will receive a warning when the remaining tape space is almost completely full, that is, greater than 99.9, but less than 100 percent. The application can continue writing until the end of the tape to reach 100 percent capacity. The last write, however, is not recoverable.

From the More Tasks menu, you can create or delete a drive.

## Creating drives

See the *Number of drives supported by a DD VTL* section to determine the maximum number of drives supported for your particular DD VTL.

### Procedure

1. Select **Virtual Tape Libraries > VTL Service > Libraries > library > Changer > Drives**.
2. Select **More Tasks > Drives > Create**.
3. In the Create Drive dialog, enter the following information:

Table 157 Create Drive dialog

Field	User input
Location	Select a library name, or leave the name selected.
Number of Drives	See the table in the <i>Number of Drives Supported by a DD VTL</i> section, earlier in this chapter.
Model Name	Select the model from the drop-down list. If another drive already exists, this option is inactive, and the existing drive type must be used. You cannot mix drive types in the same library. <ul style="list-style-type: none"> <li>• IBM-LTO-1</li> <li>• IBM-LTO-2</li> <li>• IBM-LTO-3</li> <li>• IBM-LTO-4</li> <li>• IBM-LTO-5 (default)</li> <li>• HP-LTO-3</li> <li>• HP-LTO-4</li> </ul>

4. Select **OK**, and when the status shows *Completed*, select **OK**.

The added drive appears in the Drives list.

## Deleting drives

A drive must be empty before it can be deleted.

### Procedure

1. If there is a tape in the drive that you want to delete, remove the tape.
2. Select **Virtual Tape Libraries > VTL Service > Libraries > library > Changer > Drives**.
3. Select **More Tasks > Drives > Delete**.

4. In the Delete Drives dialog, select the checkboxes of the drives to delete, or select the **Drive** checkbox to delete all drives.
5. Select **Next**, and after verifying that the correct drive(s) has been selected for deletion, select **Submit**.
6. When the Delete Drive Status dialog shows **Completed**, select **Close**.

The drive will have been removed from the Drives list.

## Working with a selected drive

Selecting **Virtual Tape Libraries > VTL Service > Libraries > library > Drives > drive** displays detailed information for a selected drive.

Table 158 Drive Tab

Column	Description
Drive	The list of drives by name, where name is "Drive #" and # is a number between 1 and n representing the address or location of the drive in the list of drives.
Vendor	The manufacturer or vendor of the drive, for example, IBM.
Product	The product name of the drive, for example, ULTRIUM-TD5.
Revision	The revision number of the drive product.
Serial Number	The serial number of the drive product.
Status	Whether the drive is Empty, Open, Locked, or Loaded. A tape must be present for the drive to be locked or loaded.
Tape	The barcode of the tape in the drive (if any).
Pool	The pool of the tape in the drive (if any).

Table 159 Statistics Tab

Column	Description
Endpoint	The specific name of the endpoint.
Ops/s	The operations per second.
Read KiB/s	The speed of reads in KiB per second.
Write KiB/s	The speed of writes in KiB per second.

From the More Tasks menu, you can delete the drive or perform a refresh.

## Working with tapes

A tape is represented as a file. Tapes can be imported from the vault to a library. Tapes can be exported from a library to the vault. Tapes can be moved within a library across drives, slots (cartridge slots), and CAPs (cartridge access ports).

### About this task

When tapes are created, they are placed into the vault. After they have been added to the vault, they can be imported, exported, moved, searched, or removed.

Selecting **Virtual Tape Libraries > VTL Service > Libraries > library > Tapes** displays detailed information for all tapes for a selected library.

**Table 160** Tape description

Item	Description
Barcode	The unique barcode for the tape.
Pool	The name of the pool that holds the tape. The Default pool holds all tapes unassigned to a user-created pool.
Location	The location of the tape - whether in a library (and which drive, CAP, or slot number) or in the virtual vault.
State	The state of the tape: <ul style="list-style-type: none"> <li>• RW – Read-writable</li> <li>• RL – Retention-locked</li> <li>• RO – Readable only</li> <li>• WP – Write-protected</li> <li>• RD – Replication destination</li> </ul>
Capacity	The total capacity of the tape.
Used	The amount of space used on the tape.
Compression	The amount of compression performed on the data on a tape.
Last Modified	The date of the last change to the tape's information. Modification times used by the system for age-based policies might differ from the last modified time displayed in the tape information sections of the DD System Manager.
Locked Until	If a DD Retention Lock deadline has been set, the time set is shown. If no retention lock exists, this value is <i>Not specified</i> .

From the information panel, you can import a tape from the vault, export a tape to the library, set a tape's state, create a tape, or delete a tape.

From the More Tasks menu, you can move a tape.

## Changing a tape's write or retention lock state

Before changing a tape's write or retention lock state, the tape must have been created and imported. DD VTL tapes follow the standard DD Retention Lock policy. After the retention period for a tape has expired, it cannot be written to or changed (however, it can be deleted).

### Procedure

1. Select **Virtual Tape Libraries > VTL Service > Libraries > library > Tapes**.
2. Select the tape to modify from the list, and select **Set State** (above the list).
3. In the Set Tape State dialog, select **Read-Writeable**, **Write-Protected**, or **Retention-Lock**.
4. If the state is Retention-Lock, either
  - enter the tape's expiration date in a specified number of days, weeks, months, years, or
  - select the calendar icon, and select a date from the calendar. The Retention-Lock expires at noon on the selected date.
5. Select **Next**, and select **Submit** to change the state.

## Working with the vault

The vault holds tapes not being used by any library. Tapes reside in either a library or the vault.

Selecting **Virtual Tape Libraries > VTL Service > Vault** displays detailed information for the Default pool and any other existing pools in the vault.

Systems with Cloud Tier and DD VTL provide the option of storing the vault on cloud storage.

**Table 161** Pool Summary

Item	Description
Pool Count	The number of VTL pools.
Tape Count	The number of tapes in the pools.
Size	The total amount of space in the pools.
Logical Used	The amount of space used in the pools.
Compression	The average amount of compression in the pools.

The **Protection Distribution** pane displays the following information.

 **Note:** This table only appears if Cloud Tier is enabled on the protection system.

**Table 162** Protection Distribution

Item	Description
Storage type	Vault or Cloud.
Cloud provider	For systems with tapes in Cloud Tier, there is a column for each cloud provider.
Logical Used	The amount of space used in the pools.
Pool Count	The number of VTL pools.
Tape Count	The number of tapes in the pools.

From the **More Tasks** menu, you can create, delete, and search for tapes in the vault.

## Working with the cloud-based vault

DD VTL supports several parameters that are unique to configurations where the vault is stored on Cloud Tier storage.

The following operations are available for working with cloud-based vault storage.

- Configure the data movement policy and cloud unit information for the specified VTL pool. Run the `vtl pool modify <pool-name> data-movement-policy {user-managed | age-threshold <days> | none} to-tier {cloud} cloud-unit <cloud-unit-name>` command.

The available data movement policies are:

- **User-managed:** The administrator can set this policy on a pool, to manually select tapes from the pool for migration to the cloud tier. The tapes migrate to the cloud tier on the first data movement operation after the tapes are selected.
- **Age-threshold:** The administrator can set this policy on a pool, to allow the DD VTL to automatically select tapes from the pool for migration to the cloud tier based on the age of the tape. The tapes are selected for migration within six hours after they meet the age threshold, and are migrated on the first data movement operation after the tapes are selected.
- Select a specified tape for migration to the cloud tier. Run the `vtl tape select-for-move barcode <barcode> [count <count>] pool <pool> to-tier {cloud}` command.
- Deselect a specified tape for migration to the cloud tier. Run the `vtl tape deselect-for-move barcode <barcode> [count <count>] pool <pool> to-tier {cloud}` command.
- Recall a tape from the cloud tier. Run the `vtl tape recall start barcode <barcode> [count <count>] pool <pool>` command.

After the recall, the tape resides in a local DD VTL vault and must be imported to the library for access.

- ① **Note:** Run the `vtl tape show` command at any time to check the current location of a tape. The tape location updates within one hour of the tape moving to or from the cloud tier.

## Prepare the VTL pool for data movement

Set the data movement policy on the VTL pool to manage migration of VTL data from the local vault to Cloud Tier.

### About this task

Data movement for VTL occurs at the tape volume level. Individual tape volumes or collections of tape volumes can be moved to the cloud tier but only from the vault location. Tapes in other elements of a VTL cannot be moved.

- ① **Note:** The default VTL pool and vault, `/data/coll/backup` directories or legacy library configurations cannot be used for Tape out to Cloud.

### Procedure

1. Select **Protocols > DD VTL**.
2. Expand the list of pools, and select a pool on which to enable migration to Cloud Tier.
3. In the **Cloud Data Movement** pane, click **Create** under **Cloud Data Movement Policy**.
4. In the **Policy** drop-down list, select a data movement policy:



- **Age of tapes in days**
  - **Manual selection**
5. Set the data movement policy details.
    - For **Age of tapes in days**, select an age threshold after which tapes are migrated to Cloud Tier, and specify a destination cloud unit.
    - For **Manual selection**, specify a destination cloud unit.
  6. Click **Create**.
    - ① **Note:** After creating the data movement policy, the **Edit** and **Clear** buttons can be used to modify or delete the data movement policy.

## CLI equivalent

### Procedure

1. Set the data movement policy to user-managed or age-threshold

① **Note:** VTL pool and cloud unit names are case sensitive and commands will fail if the case is not correct.

- To set the data movement policy to user-managed, run the following command:  
`vtl pool modify cloud-vtl-pool data-movement-policy user-managed to-tier cloud cloud-unit ecs-unit1`

\*\* Any tapes that are already selected will be migrated on the next data-movement run. VTL data-movement policy is set to "user-managed" for VTL pool "cloud-vtl-pool".

- To set the data movement policy to age-threshold, run the following command:

① **Note:** The minimum is 14 days, and the maximum is 182,250 days.

```
vtl pool modify cloud-vtl-pool data-movement-policy age-threshold
14 to-tier cloud cloud-unit ecs-unit1
```

\*\* Any tapes that are already selected will be migrated on the next data-movement run. VTL data-movement policy "age-threshold" is set to 14 days for the VTL pool "cloud-vtl-pool".

2. Verify the data movement policy for the VTL pool.

Run the following command:

```
vtl pool show all
```

```
VTL Pools
Pool          Status  Tapes  Size (GiB)  Used (GiB)  Comp  Cloud Unit
Cloud Policy
-----
cloud-vtl-pool  RW      50     250         41         45x   ecs-unit1
user-managed
Default
none          RW      0       0           0           0x    -
-----
```

8080 tapes in 5 pools

```
RO : Read Only
RD : Replication Destination
BCM : Backwards-Compatibility
```

3. Verify the policy for the VTL pool MTree is app-managed.

Run the following command:

```
data-movement policy show all
```

Mtree	Target(Tier/Unit Name)	Policy	Value
/data/coll/cloud-vtl-pool	Cloud/ecs-unit1	app-managed	enabled

## Remove tapes from the backup application inventory

Use the backup application verify the tape volumes that will move to the cloud are marked and inventoried according to the backup application requirements.

## Select tape volumes for data movement

Manually select tapes for migration to Cloud Tier (immediately or at the next scheduled data migration), or manually remove tapes from the migration schedule.

### Before you begin

Verify the backup application is aware of status changes for volumes moved to cloud storage. Complete the necessary steps for the backup application to refresh its inventory to reflect the latest volume status.

If the tape is not in the vault, it cannot be migrated to Cloud Tier.

### About this task

#### Procedure

1. Select **Protocols > DD VTL**.
2. Expand the list of pools, and select the pool which is configured to migrate tapes to Cloud Tier.
3. In the pool pane, click the **Tape** tab.
4. Select tapes for migration to Cloud Tier.
5. Click **Select for Cloud Move** to migrate the tape at the next scheduled migration, or **Move to Cloud Now** to immediately migrate the tape.

**Note:** If the data movement policy is based on tape ages, the **Select for Cloud Move** is not available, as the protection system automatically selects tapes for migration.

6. Click **Yes** at the confirmation dialog.

## Unselect tape volumes for data movement

### About this task

Tapes selected for migration to Cloud Tier can be removed from the migration schedule.

#### Procedure

1. Select **Protocols > DD VTL**.
2. Expand the list of pools, and select the pool which is configured to migrate tapes to Cloud Tier.
3. In the pool pane, click the **Tape** tab.
4. Select tapes for migration to Cloud Tier.
5. Click **Unselect Cloud Move** to remove the tape from the migration schedule.
6. Click **Yes** at the confirmation dialog.

## CLI equivalent

## Procedure

1. Identify the slot location of the tape volume to move.

Run the following command:

```
vtl tape show cloud-vtl
```

```
Processing tapes....
Barcode Pool Location State Size Used (%) Comp
Modification Time
-----
T00001L3 cloud-vtl-pool cloud-vtl slot 1 RW 5 GiB 5.0 GiB (99.07%) 205x
2017/05/05 10:43:43
T00002L3 cloud-vtl-pool cloud-vtl slot 2 RW 5 GiB 5.0 GiB (99.07%) 36x
2017/05/05 10:45:10
T00003L3 cloud-vtl-pool cloud-vtl slot 3 RW 5 GiB 5.0 GiB (99.07%) 73x
2017/05/05 10:45:26
```

2. Specify the numeric slot value to export the tape from the DD VTL.

Run the following command:

```
vtl export cloud-vtl-pool slot 1 count 1
```

3. Verify the tape is in the vault.

Run the following command:

```
vtl tape show vault
```

4. Select the tape for data movement.

Run the following command:

```
vtl tape select-for-move barcode T00001L3 count 1 pool cloud-vtl-
pool to-tier cloud
```

**(i)** Note: If the data movement policy is age-threshold, data movement occurs automatically after 15-20 minutes.

5. View the list of tapes scheduled to move to cloud storage during the next data movement operation. The tapes selected for movement display an (S) in the location column.

Run the following command:

```
vtl tape show vault
```

```
Processing tapes.....
Barcode Pool Location State Size Used (%) Comp
Modification Time
-----
T00003L3 cloud-vtl-pool vault (S) RW 5 GiB 5.0 GiB (99.07%) 63x
2017/05/05 10:43:43
T00006L3 cloud-vtl-pool ecs-unit1 n/a 5 GiB 5.0 GiB (99.07%) 62x
2017/05/05 10:45:49
-----
* RD : Replication Destination
(S) Tape selected for migration to cloud. Selected tapes will move to cloud on the next
data-movement run.
(R) Recall operation is in progress for the tape.

VTL Tape Summary
-----
Total number of tapes: 4024
Total pools: 3
Total size of tapes: 40175 GiB
Total space used by tapes: 39.6 GiB
Average Compression: 9.7x
```

- If the data movement policy is user-managed, initiate the data movement operation.

Run the following command:  
`data-movement start`

- Observe the status of the data movement operation.

Run the following command:  
`data-movement watch`

- Verify the tape volumes successfully move to cloud storage.

Run the following command:  
`vtl tape show all cloud-unit ecs-unit1`

```
Processing tapes....
Barcode Pool Location State Size Used (%) Comp Modification Time
-----
T00001L3 cloud-vtl-pool ecs-unit1 n/a 5 GiB 5.0 GiB (99.07%) 89x 2017/05/05 10:41:41
T00006L3 cloud-vtl-pool ecs-unit1 n/a 5 GiB 5.0 GiB (99.07%) 62x 2017/05/05 10:45:49
-----
(S) Tape selected for migration to cloud. Selected tapes will move to cloud on the next
data-movement run.
(R) Recall operation is in progress for the tape.

VTL Tape Summary
-----
Total number of tapes: 4
Total pools: 2
Total size of tapes: 16 GiB
Total space used by tapes: 14.9 GiB
Average Compression: 59.5x
```

## Restore data held in the cloud

When a client requests data for restore from the backup application server, the backup application should generate an alert or message requesting the required volumes from the cloud unit.

The volume must be recalled from the cloud and checked into the DD VTL library before the backup application must be notified of the presence of the volumes.

- ① Note: Verify the backup application is aware of status changes for volumes moved to cloud storage. Complete the necessary steps for the backup application to refresh its inventory to reflect the latest volume status.

## Manually recall a tape volume from cloud storage

Recall a tape from Cloud Tier to the local VTL vault.

### Procedure

- Select **Protocols > DD VTL**.
- Expand the list of pools, and select the pool which is configured to migrate tapes to Cloud Tier.
- In the pool pane, click the **Tape** tab.
- Select one or more tapes that are located in a cloud unit.
- Click **Recall Cloud Tapes** to recall tapes from Cloud Tier.

### Results

After the next scheduled data migration, the tapes are recalled from the cloud unit to the vault. From the vault, the tapes can be returned to a library.

## CLI equivalent

## Procedure

1. Identify the volume required to restore data.

2. Recall the tape volume from the vault.

Run the following command:

```
vtl tape recall start barcode T00001L3 count 1 pool cloud-vtl-pool
```

3. Verify the recall operation started.

Run the following command:

```
data-movement status
```

4. Verify the recall operation completed successfully.

Run the following command:

```
vtl tape show all barcode T00001L3
```

```
Processing tapes....
Barcode Pool Location State Size Used (%) Comp
Modification Time
-----
T00001L3 cloud-vtl-pool cloud-vtl slot 1 RW 5 GiB 5.0 GiB (99.07%) 239x
2017/05/05 10:41:41
-----
```

(S) Tape selected for migration to cloud. Selected tapes will move to cloud on the next data-movement run.

(R) Recall operation is in progress for the tape.

## VTL Tape Summary

```
-----
Total number of tapes: 1
Total pools: 1
Total size of tapes: 5 GiB
Total space used by tapes: 5.0 GiB
Average Compression: 239.1x
-----
```

5. Validate the file location.

Run the following command:

```
filesys report generate file-location path /data/coll/cloud-vtl-pool
```

```
filesys report generate file-location path /data/coll/cloud-vtl-pool
-----
File Name Location(Unit Name)
-----
/data/coll/cloud-vtl-pool/.vtl_pool Active
/data/coll/cloud-vtl-pool/.vtc/T00001L3 Active
-----
```

6. Import the recalled tape to the DD VTL.

Run the following command:

```
vtl import cloud-vtl barcode T00001L3 count 1 pool cloud-vtl-pool
element slot
```

```
imported 1 tape(s)...sysadmin@ddb708 vtl tape show cloud-vtlProcessing tapes.....
```

7. Check the volume into the backup application inventory.

8. Restore data through the backup application.

9. When restore is completed check the tape volume out of the backup application inventory.

10. Export the tape volume from the DD VTL to the vault.
11. Move the tape back to the cloud unit.

## Working with access groups

*Access groups* hold a collection of initiator WWPNs (worldwide port names) or aliases and the drives and changers they are allowed to access. A DD VTL default group named *TapeServer* lets you add devices that will support NDMP (Network Data Management Protocol)-based backup applications.

Access group configuration allows initiators (in general backup applications) to read and write data to devices in the same access group.

Access groups let clients access only selected LUNs (media changers or virtual tape drives) on a system. A client set up for an access group can access only devices in its access group.

Avoid making access group changes on a DD system during active backup or restore jobs. A change may cause an active job to fail. The impact of changes during active jobs depends on a combination of backup software and host configurations.

Selecting **Access Groups > Groups** displays the following information for all access groups.

**Table 163** Access group information

Item	Description
Group Name	Name of group.
Initiators	Number of initiators in group.
Devices	Number of devices in group.

If you select **View All Access Groups**, you are taken to the Fibre Channel view.

From the **More Tasks** menu, you can create or delete a group.

## Creating an access group

Access groups manage access between devices and initiators. Do not use the default *TapeServer* access group unless you are using NDMP.

### Procedure

1. Select **Access Groups > Groups**.
2. Select **More Tasks > Group > Create**
3. In the Create Access Group dialog, enter a name, from 1 to 128 characters, and select **Next**.
4. Add devices, and select **Next**.
5. Review the summary, and select **Finish** or **Back**, as appropriate.

### CLI Equivalent

```
# vtl group create My_Group
```



## Adding an access group device

Access group configuration allows initiators (in general backup applications) to read and write data to devices in the same access group.

### Procedure

1. Select **Access Groups > Groups**. You can also select a specific *group*.
2. Select **More Tasks > Group > Create or Group > Configure**.
3. In the Create or Modify Access Group dialog, enter or modify the **Group Name** if desired. (This field is required.)
4. To configure initiators to the access group, check the box next to the initiator. You can add initiators to the group later.
5. Select **Next**.
6. In the Devices display, select Add (+) to display the Add Devices dialog.
  - a. Verify that the correct library is selected in the Library Name drop-down list, or select another library.
  - b. In the Device area, select the checkboxes of the devices (changer and drives) to be included in the group.
  - c. Optionally, specify a starting LUN in the LUN Start Address text box.

This is the LUN that the DD system returns to the initiator. Each device is uniquely identified by the library and the device name. (For example, it is possible to have drive 1 in Library 1 and drive 1 in Library 2). Therefore, a LUN is associated with a device, which is identified by its library and device name.

When presenting LUNs via attached FC ports on FC HBA/SLIC, ports can be designated as primary, secondary, or none. A Primary port for a set of LUNs is the port that is currently advertising those LUNs to a fabric. A secondary port is a port that will broadcast a set of LUNs in the event of primary path failure (this requires manual intervention). A setting of none is used in the case where you do not wish to advertise selected LUNs. The presentation of LUNs depends on the SAN topology in question.

The initiators in the access group interact with the LUN devices that are added to the group.

The maximum LUN accepted when creating an access group is 16383.

A LUN can be used only once for an individual group. The same LUN can be used with multiple groups.

Some initiators (clients) have specific rules for target LUN numbering; for example, requiring LUN 0 or requiring contiguous LUNs. If these rules are not followed, an initiator may not be able to access some or all of the LUNs assigned to a DD VTL target port.

Check your initiator documentation for special rules, and if necessary, alter the device LUNs on the DD VTL target port to follow the rules. For example, if an initiator requires LUN 0 to be assigned on the DD VTL target port, check the LUNs for devices assigned to ports, and if there is no device assigned to LUN 0, change the LUN of a device so it is assigned to LUN 0.

- d. In the Primary and Secondary Endpoints area, select an option to determine from which ports the selected device will be seen. The following conditions apply for designated ports:
  - all – The checked device is seen from all ports.
  - none – The checked device is not seen from any port.



- **select** – The checked device is to be seen from selected ports. Select the checkboxes of the appropriate ports.

If only primary ports are selected, the checked device is visible only from primary ports.

If only secondary ports are selected, the checked device is visible only from secondary ports. Secondary ports can be used if the primary ports become unavailable.

The switchover to a secondary port is not an automatic operation. You must manually switch the DD VTL device to the secondary ports if the primary ports become unavailable.

The port list is a list of physical port numbers. A port number denotes the PCI slot and a letter denotes the port on a PCI card. Examples are 1a, 1b, or 2a, 2b.

A drive appears with the same LUN on all the ports that you have configured.

e. **Select OK.**

You are returned to the Devices dialog box where the new group is listed. To add more devices, repeat these five substeps.

7. **Select Next.**
8. **Select Close** when the **Completed** status message is displayed.

#### CLI Equivalent

```
# vtl group add VTL_Group vtl NewVTL changer lun 0 primary-port all secondary-port all
# vtl group add VTL_Group vtl NewVTL drive 1 lun 1 primary-port all secondary-port all
# vtl group add Setup_Test vtl Setup_Test drive 3 lun 3 primary-port endpoint-fc-0
secondary-port endpoint-fc-1
```

```
# vtl group show Setup_Test
Group: Setup_Test
```

```
Initiators:
Initiator Alias      Initiator WWPN
-----
tsm6_p23             21:00:00:24:ff:31:ce:f8
-----
```

```
Devices:
Device Name          LUN   Primary Ports   Secondary Ports   In-use Ports
-----
Setup_Test changer   0     all             all              all
Setup_Test drive 1   1     all             all              all
Setup_Test drive 2   2     5a              5b              5a
Setup_Test drive 3   3     endpoint-fc-0   endpoint-fc-1    endpoint-fc-0
-----
```

## Modifying or deleting an access group device

You may need to modify or delete a device from an access group.

### Procedure

1. **Select Protocols > VTL > Access Groups > Groups > *group*.**
2. **Select More Tasks > Group > Configure.**
3. In the Modify Access Group dialog, enter or modify the **Group Name**. (This field is required.)
4. To configure initiators to the access group, check the box next to the initiator. You can add initiators to the group later.

5. Select **Next**.
6. Select a device, and select the edit (pencil) icon to display the Modify Devices dialog. Then, follow steps a-e. If you simply want to delete the device, select the delete (X) icon, and skip to step e.

- a. Verify that the correct library is selected in the Library drop-down list, or select another library.
- b. In the Devices to Modify area, select the checkboxes of the devices (Changer and drives) to be modified.
- c. Optionally, modify the starting LUN (logical unit number) in the LUN Start Address box.

This is the LUN that the DD system returns to the initiator. Each device is uniquely identified by the library and the device name. (For example, it is possible to have drive 1 in Library 1 and drive 1 in Library 2). Therefore, a LUN is associated with a device, which is identified by its library and device name.

The initiators in the access group interact with the LUN devices that are added to the group.

The maximum LUN accepted when creating an access group is 16383.

A LUN can be used only once for an individual group. The same LUN can be used with multiple groups.

Some initiators (clients) have specific rules for target LUN numbering; for example, requiring LUN 0 or requiring contiguous LUNs. If these rules are not followed, an initiator may not be able to access some or all of the LUNs assigned to a DD VTL target port.

Check your initiator documentation for special rules, and if necessary, alter the device LUNs on the DD VTL target port to follow the rules. For example, if an initiator requires LUN 0 to be assigned on the DD VTL target port, check the LUNs for devices assigned to ports, and if there is no device assigned to LUN 0, change the LUN of a device so it is assigned to LUN 0.

- d. In the Primary and Secondary Ports area, change the option that determines the ports from which the selected device is seen. The following conditions apply for designated ports:

- all – The checked device is seen from all ports.
- none – The checked device is not seen from any port.
- select – The checked device is seen from selected ports. Select the checkboxes of the ports from which it will be seen.

If only primary ports are selected, the checked device is visible only from primary ports.

If only secondary ports are selected, the checked device is visible only from secondary ports. Secondary ports can be used if primary ports become unavailable.

The switchover to a secondary port is not an automatic operation. You must manually switch the DD VTL device to the secondary ports if the primary ports become unavailable.

The port list is a list of physical port numbers. A port number denotes the PCI slot, and a letter denotes the port on a PCI card. Examples are 1a, 1b, or 2a, 2b.

A drive appears with the same LUN on all ports that you have configured.

- e. Select **OK**.

## Deleting an access group

Before you can delete an access group, you must remove all of its initiators and LUNs.

### Procedure

1. Remove all of the initiators and LUNs from the group.
2. Select **Access Groups > Groups**.
3. Select **More Tasks > Group > Delete**.
4. In the Delete Group dialog, select the checkbox of the group to be removed, and select **Next**.
5. In the groups confirmation dialog, verify the deletion, and select **Submit**.
6. Select **Close** when the Delete Groups Status displays *Completed*.

### CLI Equivalent

```
# scsitarget group destroy My_Group
```

## Working with a selected access group

Selecting **Access Groups > Groups > group** displays the following information for a selected access group.

**Table 164** LUNs tab

Item	Description
LUN	Device address – maximum number is 15383. A LUN can be used only once within a group, but can be used again within another group. DD VTL devices added to a group must use contiguous LUNs.
Library	Name of library associated with LUN.
Device	Changers and drives.
In-Use Endpoints	Set of endpoints currently being used: primary or secondary.
Primary Endpoints	Initial (or default) endpoint used by backup application. In the event of a failure on this endpoint, the secondary endpoints may be used, if available.
Secondary Endpoints	Set of fail-over endpoints to use if primary endpoint fails.

**Table 165** initiators tab

Item	Description
Name	Name of initiator, which is either the WWPN or the alias assigned to the initiator.
WWPN	Unique worldwide port name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the Fibre Channel port.

From the More Tasks menu, with a group selected, you can configure that group, or set endpoints in use.

## Selecting endpoints for a device

Since endpoints connect a device to an initiator, use this process to set up the endpoints before you connect the device.

### Procedure

1. Select **Access Groups > Groups > group**.
2. Select **More Tasks > Endpoints > Set In-Use**.
3. In the Set in-Use Endpoints dialog, select only specific devices, or select **Devices** to select all devices in the list.
4. Indicate whether the endpoints are primary or secondary.
5. Select **OK**.

## Configuring the NDMP device TapeServer group

The DD VTL TapeServer group holds tape drives that interface with NDMP (Network Data Management Protocol)-based backup applications and that send control information and data streams over IP (Internet Protocol) instead of Fibre Channel (FC). A device used by the NDMP TapeServer must be in the DD VTL group TapeServer and is available *only* to the NDMP TapeServer.

### Procedure

1. Add tape drives to a new or existing library (in this example, named "dd9900-16").
2. Create slots and CAPs for the library.
3. Add the created devices in a library (in this example, "dd9900-16") to the TapeServer access group.
4. Enable the NDMP daemon by entering at the command line:

```
# ndmpd enable
Starting NDMP daemon, please wait.....
NDMP daemon is enabled.
```

5. Ensure that the NDMP daemon sees the devices in the TapeServer group:

```
# ndmpd show devicenames
NDMP Device      Virtual Name      Vendor  Product      Serial Number
-----
/dev/dd_ch_c0t010 dd9900-16 changer STK      L180        6290820000
/dev/dd_st_c0t110 dd9900-16 drive 1  IBM     ULTRIUM-TD3 6290820001
/dev/dd_st_c0t210 dd9900-16 drive 2  IBM     ULTRIUM-TD3 6290820002
/dev/dd_st_c0t310 dd9900-16 drive 3  IBM     ULTRIUM-TD3 6290820003
/dev/dd_st_c0t410 dd9900-16 drive 4  IBM     ULTRIUM-TD3 6290820004
-----
```

6. Add an NDMP user (ndmp in this example) with the following command:

```
# ndmpd user add ndmp
Enter password:
Verify password:
```

7. Verify that user ndmp is added correctly:

```
# ndmpd user show
ndmp
```

8. Display the NDMP configuration:

```
# ndmpd option show all
Name      Value
-----
```

```

authentication    text
debug            disabled
port            10000
preferred-ip
-----

```

- Change the default user password authentication to use MD5 encryption for enhanced security, and verify the change (notice the authentication value changed from text to md5):

```

# ndmpd option set authentication md5
# ndmpd option show all
Name            Value
-----
authentication  md5
debug          disabled
port          10000
preferred-ip
-----

```

### Results

NDMP is now configured, and the TapeServer access group shows the device configuration. See the `ndmpd` chapter of the *DD OS Command Reference Guide* for the complete command set and options.

## Working with resources

Selecting **Resources > Resources** displays information about initiators and endpoints. An *initiator* is a backup client that connects to a system to read and write data using the Fibre Channel (FC) protocol. A specific initiator can support DD Boost over FC or DD VTL, but not both. An *endpoint* is the logical target on a DD system to which the initiator connects.

**Table 166** Initiators tab

Item	Description
Name	Name of initiator, which is either the WWPN or the alias assigned to the initiator.
WWPN	Unique worldwide port name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the Fibre Channel (FC) port.
WWNN	Unique worldwide node name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the FC node.
Online Endpoints	Group name where ports are seen by initiator. Displays <code>None</code> or <code>Offline</code> if the initiator is unavailable.

**Table 167** Endpoints tab

Item	Description
Name	Specific name of endpoint.
WWPN	Unique worldwide port name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the Fibre Channel (FC) port.

Table 167 Endpoints tab (continued)

Item	Description
WWNN	Unique worldwide node name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the FC node.
System Address	System address for the endpoint.
Enabled	HBA (host bus adapter) port operational state, which is either <i>Yes</i> (enabled) or <i>No</i> (not enabled).
Status	DD VTL link status, which is either <i>Online</i> (capable of handling traffic) or <i>Offline</i> .

### Configure Resources

Selecting **Configure Resources** takes you to the Fibre Channel area, where you can configure endpoints and initiators.

## Working with initiators

Selecting **Resources > Resources > Initiators** displays information about initiators. An *initiator* is a client system FC HBA (fibre channel host bus adapter) WWPN (worldwide port name) with which the DD system interfaces. An *initiator name* is an alias for the client's WWPN, for ease of use.

While a client is mapped as an initiator – but before an access group has been added – the client cannot access any data on a DD system.

After adding an access group for the initiator or client, the client can access only the devices in that access group. A client can have access groups for multiple devices.

An access group may contain multiple initiators, but an initiator can exist in only one access group.

 **Note:** A maximum of 1024 initiators can be configured for a DD system.

Table 168 Initiator information

Item	Description
Name	Name of initiator.
Group	Group associated with initiator.
Online Endpoints	Endpoints seen by initiator. Displays <i>none</i> or <i>offline</i> if initiator is unavailable.
WWPN	Unique worldwide port name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the Fibre Channel (FC) port.
WWNN	Unique worldwide node name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the FC node.
Vendor Name	Name of vendor for initiator.

Selecting **Configure Initiators** takes you to the Fibre Channel area, where you can configure endpoints and initiators.



## CLI Equivalent

```
# vtl initiator show
Initiator Group Status WWNN WPN Port
-----
tsm6_p1 tsm3500_a Online 20:00:00:24:ff:31:ce:f8 21:00:00:24:ff:31:ce:f8 10b

Initiator Symbolic Port Name Address Method
-----
tsm6_p1 QLE2562 FW:v5.06.03 DVR:v8.03.07.15.05.09-x auto
```

## Working with endpoints

Selecting **Resources > Resources > Endpoints** provides information about endpoint hardware and connectivity.

Table 169 Hardware Tab

Item	Description
System Address	System address of endpoint.
WWPN	Unique worldwide port name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the Fibre Channel (FC) port.
WWNN	Unique worldwide node name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the FC node.
Enabled	HBA (host bus adapter) port operational state, which is either <i>Yes</i> (enabled) or <i>No</i> (not enabled).
NPIV	NPIV status of this endpoint: either <i>Enabled</i> or <i>Disabled</i> .
Link Status	Link status of this endpoint: either <i>Online</i> or <i>Offline</i> .
Operation Status	Operation status of this endpoint: either <i>Normal</i> or <i>Marginal</i> .
# of Endpoints	Number of endpoints associated with this endpoint.

Table 170 Endpoints Tab

Item	Description
Name	Specific name of endpoint.
WWPN	Unique worldwide port name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the Fibre Channel (FC) port.
WWNN	Unique worldwide node name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the FC node.
System Address	System address of endpoint.
Enabled	HBA (host bus adapter) port operational state, which is either <i>Yes</i> (enabled) or <i>No</i> (not enabled).
Link Status	Link status of this endpoint: either <i>Online</i> or <i>Offline</i> .



### Configure Endpoints

Selecting **Configure Endpoints** takes you to the Fibre Channel area, where you can change any of the above information for the endpoint.

### CLI Equivalent

```
# scsitarget endpoint show list
Endpoint      System Address  Transport      Enabled  Status
-----
endpoint-fc-0 5a              FibreChannel  Yes     Online
endpoint-fc-1 5b              FibreChannel  Yes     Online
```

## Working with a selected endpoint

Selecting **Resources > Resources > Endpoints > endpoint** provides information about the endpoint's hardware, connectivity, and statistics.

Table 171 Hardware tab

Item	Description
System Address	System address of endpoint.
WWPN	Unique worldwide port name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the Fibre Channel port.
WWNN	Unique worldwide node name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the FC node.
Enabled	HBA (host bus adapter) port operational state, which is either <i>Yes</i> (enabled) or <i>No</i> (not enabled).
NPIV	NPIV status of this endpoint: either <i>Enabled</i> or <i>Disabled</i> .
Link Status	Link status of this endpoint: either <i>Online</i> or <i>Offline</i> .
Operation Status	Operation status of this endpoint: either <i>Normal</i> or <i>Marginal</i> .
# of Endpoints	Number of endpoints associated with this endpoint.

Table 172 Summary tab

Item	Description
Name	Specific name of endpoint.
WWPN	Unique worldwide port name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the Fibre Channel port.
WWNN	Unique worldwide node name, which is a 64-bit identifier (a 60-bit value preceded by a 4-bit <i>Network Address Authority</i> identifier), of the FC node.
System Address	System address of endpoint.
Enabled	HBA (host bus adapter) port operational state, which is either <i>Yes</i> (enabled) or <i>No</i> (not enabled).
Link Status	Link status of this endpoint: either <i>Online</i> or <i>Offline</i> .

Table 173 Statistics tab

Item	Description
Endpoint	Specific name of endpoint.
Library	Name of library containing the endpoint.
Device	Number of device.
Ops/s	Operations per second.
Read KiB/s	Speed of reads in KiB per second.
Write KiB/s	Speed of writes in KiB per second.

Table 174 Detailed Statistics tab

Item	Description
Endpoint	Specific name of endpoint.
# of Control Commands	Number of control commands.
# of Read Commands	Number of read commands.
# of Write Commands	Number of write commands.
In (MiB)	Number of MiB written (the binary equivalent of MB).
Out (MiB)	Number of MiB read.
# of Error Protocol	Number of error protocols.
# of Link Fail	Number of link failures.
# of Invalid Crc	Number of invalid CRCs (cyclic redundancy checks).
# of Invalid TxWord	Number of invalid tx (transmission) words.
# of Lip	Number of LIPs (loop initialization primitives).
# of Loss Signal	Number of signals or connections that have been lost.
# of Loss Sync	Number of signals or connections that have lost synchronization.

## Working with pools

Selecting **Pools > Pools** displays detailed information for the Default pool and any other existing pools. A *pool* is a collection of tapes that maps to a directory on the file system. Pools are used to replicate tapes to a destination. You can convert directory-based pools to MTree-based pools to take advantage of the greater functionality of MTrees.

Note the following about pools:

- Pools can be of two types: MTree (recommended), or Directory, which is backward-compatible.
- A pool can be replicated no matter where individual tapes are located. Tapes can be in the vault or in a library (slot, cap, or drive).
- You can copy and move tapes from one pool to another.
- Pools are not accessible by backup software.

- No DD VTL configuration or license is needed on a replication destination when replicating pools.
- You must create tapes with unique barcodes. Duplicate barcodes may cause unpredictable behavior in backup applications and can be confusing to users.
- Two tapes in two different pools on a DD system may have the same name, and in this case, neither tape can be moved to the other tape's pool. Likewise, a pool sent to a replication destination must have a name that is unique on the destination.

Table 175 Pools tab

Item	Description
Name	The name of the pool.
Type	Whether it is a Directory or MTree pool.
Status	The status of the pool.
Tape Count	The number of tapes in the pool.
Size	The total configured data capacity of tapes in the pool, in GiB (Gibibytes base-2 equivalent of GB, Gigabytes).
Physical Used	The amount of space used on virtual tapes in the pool.
Compression	The average amount of compression achieved for data on tapes in the pool.
Cloud Unit	The name of the cloud unit where the DD VTL pool migrates data.
Cloud Data Movement Policy	The data movement policy that governs migration of DD VTL data to Cloud Tier storage.

Table 176 Replication tab

Item	Description
Name	The name of the pool.
Configured	Whether replication is configured for the pool: yes or no.
Remote Source	Contains an entry only if the pool is replicated from another DD system.
Remote Destination	Contains an entry only if the pool replicates to another DD system.

From the More Tasks menu, you can create and delete pools, as well as search for tapes.

## Creating pools

You can create backward-compatible pools, if necessary for your setup, for example, for replication with a pre-5.2 DD OS system.

### Procedure

1. Select **Pools > Pools**.
2. Select **More Tasks > Pool > Create**.
3. In the Create Pool dialog, enter a Pool Name, noting that a pool name:

- cannot be "all," "vault," or "summary."
  - cannot have a space or period at its beginning or end.
  - is case-sensitive.
4. If you want to create a directory pool (which is backward compatible with the previous version of DD System Manager), select the option "Create a directory backwards compatibility mode pool." However, be aware that the advantages of using an MTree pool include the ability to:
    - make individual snapshots and schedule snapshots.
    - apply retention locks.
    - set an individual retention policy.
    - get compression information.
    - get data migration policies to the Retention Tier.
    - establish a storage space usage policy (quota support) by setting hard limits and soft limits.
  5. Select **OK** to display the Create Pool Status dialog.
  6. When the Create Pool Status dialog shows **Completed**, select **Close**. The pool is added to the Pools subtree, and you can now add virtual tapes to it.

#### CLI Equivalent

```
# vtl pool add VTL_Pool
A VTL pool named VTL_Pool is added.
```

## Deleting pools

Before a pool can be deleted, you must have deleted any tapes contained within it. If replication is configured for the pool, the replication pair must also be deleted. Deleting a pool corresponds to renaming the MTree and then deleting it, which occurs at the next cleaning process.

#### Procedure

1. Select **Pools > Pools > pool**.
2. Select **More Tasks > Pool > Delete**.
3. In the Delete Pools dialog, select the checkbox of items to delete:
  - The name of each pool, or
  - **Pool Names**, to delete all pools.
4. Select **Submit** in the confirmation dialogs.
5. When the Delete Pool Status dialog shows **Completed**, select **Close**.  
The pool will have been removed from the Pools subtree.

## Working with a selected pool

Both **Virtual Tape Libraries > VTL Service > Vault > pool and Pools > Pools > pool** display detailed information for a selected pool. Notice that pool "Default" always exists.

### Pool tab

Table 177 Summary

Item	Description
Convert to MTree Pool	Select this button to convert a Directory pool to an MTree pool.
Type	Whether it is a Directory or MTree pool.
Tape Count	The number of tapes in the pool.
Capacity	The total configured data capacity of tapes in the pool, in GiB (Gibibytes, base-2 equivalent of GB, Gigabytes).
Logical Used	The amount of space used on virtual tapes in the pool.
Compression	The average amount of compression achieved for data on tapes in the pool.

Table 178 Pool Tab: Cloud Data Movement - Protection Distribution

Item	Description
Pool type (%)	VTL Pool and Cloud (if applicable), with the current percentage of data in parentheses.
Name	Name of the local VTL pool, or cloud provider.
Logical Used	The amount of space used on virtual tapes in the pool.
Tape Count	The number of tapes in the pool.

Table 179 Pool Tab: Cloud Data Movement - Cloud Data Movement Policy

Item	Description
Policy	Age of tapes in days, or manual selection.
Older Than	Age threshold for an age-based data movement policy.
Cloud Unit	Destination cloud unit.

### Tape tab

Table 180 Tape controls

Item	Description
Create	Create a new tape.
Delete	Delete the selected tapes.
Copy	Make a copy of a tape.

Table 180 Tape controls (continued)

Item	Description
<b>Move between Pool</b>	Move the selected tapes to a different pool.
<b>Select for Cloud Move<sup>a</sup></b>	Schedule the selected tapes for migration to Cloud Tier.
<b>Unselect from Cloud Move<sup>a</sup></b>	Remove the selected tapes from the schedule for migration to Cloud Tier.
<b>Recall Cloud Tapes</b>	Recall the selected tapes from Cloud Tier.
<b>Move to Cloud Now</b>	Migrate the selected tapes to Cloud Tier without waiting for the next scheduled migration.

a. This option is only available if the data movement policy is configured for manual selection.

Table 181 Tape information

Item	Description
Barcode	Tape barcode.
Size	Maximum size of the tape.
Physical Used	Physical storage capacity used by the tape.
Compression	Compression ratio on the tape.
Location	Location of the tape.
Modification Time	Last time the tape was modified.
Recall Time	Last time the tape was recalled.

#### Replication tab

Table 182 Replication

Item	Description
Name	The name of the pool.
Configured	Whether replication is configured for this pool: yes or no.
Remote Source	Contains an entry only if the pool is replicated from another DD system.
Remote Destination	Contains an entry only if the pool replicates to another DD system.

You can also select the **Replication Detail** button, at the top right, to go directly to the Replication information panel for the selected pool.

From either the Virtual Tape Libraries or Pools area, from the More Tasks menu, you can create, delete, move, copy, or search for a tape in the pool.

From the Pools area, from the More Tasks menu, you can rename or delete a pool.

## Converting a directory pool to an MTree pool

MTree pools have many advantages over directory pools. See the *Creating pools* section for more information.

### Procedure

1. Make sure the following prerequisites have been met:
  - The source and destination pools must have been synchronized, so that the number of tapes, and the data on each side, remains intact.
  - The directory pool must not be a replication source or destination.
  - The file system must not be full.
  - The file system must not have reached the maximum number of MTrees allowed (100).
  - There must not already be an MTree with the same name.
  - If the directory pool is being replicated on multiple systems, those replicating systems must be known to the managing system.
  - If the directory pool is being replicated to an older DD OS (for example, from DD OS 5.5 to DD OS 5.4), it cannot be converted. As a workaround:
    - Replicate the directory pool to a second DD system.
    - Replicate the directory pool from the second DD system to a third DD system.
    - Remove the second and third DD systems from the managing DD system's network.
    - On any of the systems running DD OS 5.5, from the Pools submenu, select **Pools** and a directory pool. In the Pools tab, select **Convert to MTree Pool**.
2. With the directory pool you wish to convert highlighted, choose **Convert to MTree Pool**.
3. Select **OK** in the Convert to MTree Pool dialog.
4. Be aware that conversion affects replication in the following ways:
  - DD VTL is temporarily disabled on the replicated systems during conversion.
  - The destination data is copied to a new pool on the destination system to preserve the data until the new replication is initialized and synced. Afterward, you may safely delete this temporarily copied pool, which is named **CONVERTED-pool**, where *pool* is the name of the pool that was upgraded (or the first 18 characters for long pool names). [This applies only to DD OS 5.4.1.0 and later.]
  - The target replication directory will be converted to MTree format. [This applies only to DD OS 5.2 and later.]
  - Replication pairs are broken before pool conversion and re-established afterward if no errors occur.
  - DD Retention Lock cannot be enabled on systems involved in MTree pool conversion.

## Moving tapes between pools

If they reside in the vault, tapes can be moved between pools to accommodate replication activities. For example, pools are needed if all tapes were created in the Default pool, but you later



need independent groups for replicating groups of tapes. You can create named pools and re-organize the groups of tapes into new pools.

#### About this task

① **Note:** You cannot move tapes from a tape pool that is a directory replication source. As a workaround, you can:

- Copy the tape to a new pool, then delete the tape from the old pool.
- Use an MTree pool, which allows you to move tapes from a tape pool that is a directory replication source.

#### Procedure

1. With a pool highlighted, select **More Tasks > Tapes > Move**.

Note that when started from a pool, the Tapes Panel allows tapes to be moved only between pools.

2. In the Move Tapes dialog, enter information to search for the tapes to move, and select **Search**:

Table 183 Move Tapes dialog

Field	User input
Location	Location cannot be changed.
Pool	Select the name of the pool where the tapes reside. If no pools have been created, use the Default pool.
Barcode	Specify a unique barcode, or leave the default (*) to import a group of tapes. Barcode allows the wildcards ? and *, where ? matches any single character and * matches 0 or more characters.
Count	Enter the maximum number of tapes you want to be returned to you. If you leave this blank, the barcode default (*) is used.
Tapes Per Page	Select the maximum number of tapes to display per page. Possible values are 15, 30, and 45.
Items Selected	Shows the number of tapes selected across multiple pages – updated automatically for each tape selection.

3. From the search results list, select the tapes to move.
4. From the Select Destination: Location list, select the location of the pool to which tapes are to be moved. This option is available only when started from the (named) Pool view.
5. Select **Next**.
6. From the Move Tapes view, verify the summary information and tape list, and select **Submit**.
7. Select **Close** in the status window.

## Copying tapes between pools

Tapes can be copied between pools, or from the vault to a pool, to accommodate replication activities. This option is available only when started from the (named) Pool view.

#### Procedure

1. With a pool highlighted, select **More Tasks > Tapes > Copy**.

- In the Copy Tapes Between Pools dialog, select the checkboxes of tapes to copy, or enter information to search for the tapes to copy, and select **Search**:

Table 184 Copy Tapes Between Pools dialog

Field	User input
Location	Select either a library or the <b>Vault</b> for locating the tape. While tapes always show up in a pool (under the Pools menu), they are technically in either a library or the vault, but not both, and they are never in two libraries at the same time. Use the Import/export options to move tapes between the vault and a library.
Pool	To copy tapes between pools, select the name of the pool where the tapes currently reside. If no pools have been created, use the <b>Default</b> pool.
Barcode	Specify a unique barcode, or leave the default (*) to import a group of tapes. Barcode allows the wildcards ? and *, where ? matches any single character and * matches 0 or more characters.
Count	Enter the maximum number of tapes you want to be imported. If you leave this blank, the barcode default (*) is used.
Tapes Per Page	Select the maximum number of tapes to display per page. Possible values are 15, 30, and 45.
Items Selected	Shows the number of tapes selected across multiple pages – updated automatically for each tape selection.

- From the search results list, select the tapes to copy.
- From the Select Destination: Pool list, select the pool where tapes are to be copied. If a tape with a matching barcode already resides in the destination pool, an error is displayed, and the copy aborts.
- Select **Next**.
- From the Copy Tapes Between Pools dialog, verify the summary information and the tape list, and select **Submit**.
- Select **Close** on the Copy Tapes Between Pools Status window.

## Renaming pools

A pool can be renamed only if none of its tapes is in a library.

### Procedure

- Select **Pools > Pools > pool**.
- Select **More Tasks > Pool > Rename**.
- In the Rename Pool dialog, enter the new Pool Name, with the caveat that this name:
  - cannot be "all," "vault," or "summary."
  - cannot have a space or period at its beginning or end.
  - is case-sensitive.
- Select **OK** to display the Rename Pool status dialog.
- After the Rename Pool status dialog shows **Completed**, select **OK**.

The pool will have been renamed in the Pools subtree in both the Pools and the Virtual Tape Libraries areas.

# CHAPTER 16

## DD Replicator

This chapter includes:

• DD Replicator overview.....	388
• Prerequisites for replication configuration.....	389
• Replication version compatibility.....	391
• Replication types.....	393
• Using DD Encryption with DD Replicator.....	398
• Replication topologies.....	399
• Managing replication.....	403
• Monitoring replication.....	418
• Replication with HA.....	419
• Replicating a system with quotas to one without.....	420
• Replication Scaling Context.....	420
• Directory-to-MTree replication migration.....	420
• Using collection replication for disaster recovery with SMT.....	424

## DD Replicator overview

DD Replicator provides automated, policy-based, network-efficient, and encrypted replication for DR (disaster recovery) and multi-site backup and archive consolidation. DD Replicator asynchronously replicates only compressed, deduplicated data over a WAN (wide area network).

DD Replicator performs two levels of deduplication to significantly reduce bandwidth requirements: *local* and *cross-site* deduplication. Local deduplication determines the unique segments to be replicated over a WAN. Cross-site deduplication further reduces bandwidth requirements when multiple sites are replicating to the same destination system. With cross-site deduplication, any redundant segment previously transferred by any other site, or as a result of a local backup or archive, will not be replicated again. This improves network efficiency across all sites and reduces daily network bandwidth requirements up to 99%, making network-based replication fast, reliable, and cost-effective.

In order to meet a broad set of DR requirements, DD Replicator provides flexible replication topologies, such as full system mirroring, bi-directional, many-to-one, one-to-many, and cascaded. In addition, you can choose to replicate either all or a subset of the data on your DD system. For the highest level of security, DD Replicator can encrypt data being replicated between DD systems using the standard SSL (Secure Socket Layer) protocol.

DD Replicator scales performance and supported fan-in ratios to support large enterprise environments.

Before getting started with DD Replicator, note the following general requirements:

- DD Replicator is a licensed product. See your Dell EMC sales representative to purchase licenses.
- You can usually replicate only between machines that are within two releases of each other, for example, from 6.0 to 6.2. However, there may be exceptions to this (as a result of atypical release numbering), so review the tables in the *Replication version compatibility* section, or check with your Dell EMC representative.
- If you are unable to manage and monitor DD Replicator from the current version of the DD System Manager, use the `replication` commands described in the *DD OS Command Reference Guide*.

## Prerequisites for replication configuration

Before configuring a replication, review the following prerequisites to minimize initial data transfer time, prevent overwriting of data, etc.

- **Contexts** – Determine the maximum number of contexts for your DD systems by reviewing the replication streams numbers in the following table.

Table 185 Data streams sent to a protection system

Model	RAM / NVRAM	Backup write streams	Backup read streams	Repl <sup>a</sup> source streams	Repl <sup>a</sup> dest streams	Mixed
DD2200	8 GB	35	6	18	20	w<=35; r<=6; ReplSrc<=18; ReplDest<=20; ReplDest+w<=35; Total<=35
DD2200	16 GB	60	16	30	60	w<=60; r<=16; ReplSrc<=30; ReplDest<=60; ReplDest+w<=60; Total<=60
DD6300	48 or 96 GB / 8 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest+w<=270; Total<=270
DD6800	192 GB / 8 GB	400	110	220	400	w<=400; r<=110; ReplSrc<=220; ReplDest<=400; ReplDest+w<=400; Total<=400
DD6900	288 GB / 16 GB	400	110	220	400	w<=400; r<=110; ReplSrc<=220; ReplDest<=400; ReplDest+w<=400; Total<=400
DD9300	192 or 384 GB / 8 GB	800	220	440	800	w<=800; r<=220; ReplSrc<=440; ReplDest<=800; ReplDest+w<=800; Total<=800
DD9400	576 GB / 16 GB	800	220	440	800	w<=800; r<=220; ReplSrc<=440; ReplDest<=800; ReplDest+w<=800; Total<=800
DD9500	256 or 512 GB / 8 GB	1885	300	540	1080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest+w<=1080; Total<=1885
DD9800	256 or 768 GB / 8 GB	1885	300	540	1080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest+w<=1080; Total<=1885
DD9900	1152 GB / 16 GB	1885	300	540	1080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest+w<=1080; Total<=1885
DD VE 8 TB	8 GB / 512 MB	20	16	20	20	w<= 20 ; r<= 16 ReplSrc<=20; ReplDest<=20; ReplDest

Table 185 Data streams sent to a protection system (continued)

Model	RAM / NVRAM	Backup write streams	Backup read streams	Repl <sup>a</sup> source streams	Repl <sup>a</sup> dest streams	Mixed
DD VE 16 TB	16 GB / 512 MB or 24 GB / 1 GB	45	30	45	45	+w<=20; w+r+ReplSrc<=20; Total<=20 w<= 45 ; r<= 30 ReplSrc<=45; ReplDest<=45; ReplDest +w<=45; w+r+ReplSrc<=45; Total<=45
DD VE 32 TB	24 GB / 1 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest +w<=90; w+r+ReplSrc<=90; Total<=90
DD VE 48 TB	36 GB / 1 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest +w<=90; w+r+ReplSrc<=90; Total<=90
DD VE 64 TB	48 GB / 1 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest +w<=90; w+r+ReplSrc<=90; Total<=90
DD VE 96 TB	64 GB / 2 GB	180	50	90	180	w<= 180 ; r<= 50 ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; w+r+ReplSrc<=180; Total<=180
DD3300 4 TB	12 GB (virtual memory) / 512 MB	20	16	30	20	w<= 20 ; r<= 16 ReplSrc<=30; ReplDest<=20; ReplDest +w<=20; w+r+ReplSrc<=30; Total<=30
DD3300 8 TB	32 GB (virtual memory) / 1.536 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest +w<=90; w+r+ReplSrc<=90; Total<=90
DD3300 16 TB	32 GB (virtual memory) / 1.536 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest +w<=90; w+r+ReplSrc<=90; Total<=90
DD3300 32 TB	46 GB (virtual memory) / 1.536 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest +w<=90; w+r+ReplSrc<=90; Total<=140

a. DirRepl, CptDup, MTreeRepl streams

- **Compatibility** – If you are using DD systems running different versions of DD OS, review the next section on Replication Version Compatibility.



- **Initial Replication** – If the source holds a lot of data, the initial replication operation can take many hours. Consider putting both DD systems in the same location with a high-speed, low-latency link. After the first replication, you can move the systems to their intended locations because only new data will be sent.
- **Bandwidth Delay Settings** – Both the source and destination must have the same bandwidth delay settings. These tuning controls benefit replication performance over higher latency links by controlling the TCP (transmission control protocol) buffer size. The source system can then send enough data to the destination while waiting for an acknowledgment.
- **Only One Context for Directories/Subdirectories** – A directory (and its subdirectories) can be in only one context at a time, so be sure that a subdirectory under a source directory is not used in another directory replication context.
- **Adequate Storage** – At a minimum, the destination must have the *same amount of space* as the source.
- **Destination Empty for Directory Replication** – The destination directory must be empty for directory replication, or its contents no longer needed, because it will be overwritten.
- **Security** – DD OS requires that port 3009 be open in order to configure secure replication over an Ethernet connection.

## Replication version compatibility

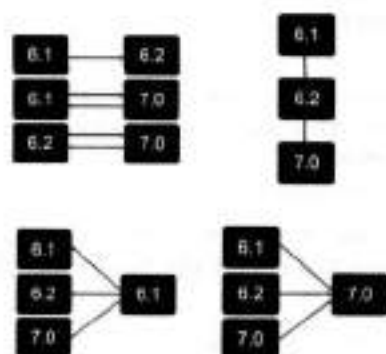
To use DD systems running different versions of DD OS for a source or destination, the following tables provide compatibility information for single-node, DD Retention Lock, MTree, directory, collection, delta (low bandwidth optimization), and cascaded replication.

In general:

- For DD Boost or DD Boost OST, see the *DD Boost for Partner Integration Administration Guide* or the *DD Boost for OpenStorage Administration Guide* for supported configurations.
- MTree and directory replication cannot be used simultaneously for replicating the same data.
- The recovery procedure is valid for all supported replication configurations.
- File migration is supported whenever collection replication is supported.
- For MTree replication, directory replication, or managed file replication, if a DD OS 7.0 source is configured to replicate to a target running DD OS 6.2 with gz or gzfast compression, the target system must be upgraded to DD OS 6.2.0.35 or higher.
- For collection replication, if a DD OS 7.0 source is configured to replicate to a target running DD OS 6.2 or DD OS 6.1, the target system must use gzfast for local compression.
- For MTree replication from a source DD system running DD OS 6.0 to a target DD system running an earlier version of DD OS, the replication process behaves according to the older version of DD OS on the destination DD system. If a restore operation or cascade replication is performed from the destination DD system, no virtual synthetics are applied.
- For cascaded configurations, the maximum number of hops is two, that is, three DD systems. Directory-to-MTree migration supports backward compatibility up to two previous releases. See *Directory-to-MTree replication migration* on page 420 for more information about *directory-to-Mtree-migration*.
- One-to-many, many-to-one, and cascaded replication support up to three consecutive DD OS release families, as seen in these figures.



Figure 15 Valid replication configurations



In these tables:

- Each DD OS release includes all releases in that family, for example, DD OS 6.1 includes 6.1.0, 6.1.1, 6.1.2, etc.
- c = collection replication
- dir = directory replication
- m = MTree replication
- del = delta (low bandwidth optimization) replication
- dest = destination
- src = source
- NA = not applicable

Table 186 Configuration: single-node to single-node

src/dest	6.0 (dest)	6.1 (dest)	6.2 (dest)	7.0 (dest)
6.0 (src)	c, dir, del, m	dir, del, m	dir, del, m	NA
6.1 (src)	dir, del, m	c, dir, del, m	dir, del, m	dir, del, m
6.2 (src)	dir, del, m	dir, del, m	c, dir, del, m	dir, del, m
7.0 (src)	NA	dir, del, m	dir, del, m	c, dir, del, m

### TLS version support

By default, the system supports TLS versions 1.0, 1.1, and 1.2. However, it is possible to configure the system to support TLS version 1.2 only by changing the system parameter `REPL_SSL_DISABLE_TLSV1_0`. Changing the system parameter requires SE access to the system. Contact Dell EMC Support if this change is required.

## Replication types

Replication typically consists of a *source* DD system (which receives data from a backup system) and one or more *destination* DD systems. Each DD system can be the source and/or the destination for replication contexts. During replication, each DD system can perform normal backup and restore operations.

Each replication type establishes a *context* associated with an existing directory or MTree on the source. The replicated context is created on the destination when a context is established. The context establishes a replication pair, which is always active, and any data landing in the source will be copied to the destination at the earliest opportunity. Paths configured in replication contexts are absolute references and do not change based on the system in which they are configured.

A protection system can be set up for directory, collection, or MTree replication.

- *Directory replication* provides replication at the level of individual directories.
- *Collection replication* duplicates the entire data store on the source and transfers that to the destination, and the replicated volume is read-only.
- *MTree replication* replicates entire MTrees (that is, a virtual file structure that enables advanced management). Media pools can also be replicated, and by default, an MTree is created for replication. (A media pool can also be created in backward-compatibility mode that, when replicated, will be a directory replication context.)

For any replication type, note the following requirements:

- A destination system must have available storage capacity that is at least the size of the expected maximum size of the source directory. Be sure that the destination system has enough network bandwidth and disk space to handle all traffic from replication sources.
- The file system must be enabled or, based on the replication type, will be enabled as part of the replication initialization.
- The source must exist.
- The destination must not exist.
- The destination will be created when a context is built and initialized.
- After replication is initialized, ownership and permissions of the destination are always identical to those of the source.
- In the replication command options, a specific replication pair is always identified by the destination.

- Both systems must have an active, visible route through the IP network so that each system can resolve its partner's host name.

The choice of replication type depends on your specific needs. The next sections provide descriptions and features of these three types, plus a brief introduction to Managed File Replication, which is used by DD Boost.

## Managed file replication

*Managed file replication*, which is used by DD Boost, is a type of replication that is managed and controlled by backup software.

With managed file replication, backup images are directly transferred from one DD system to another, one at a time, at the request of the backup software.

The backup software keeps track of all copies, allowing easy monitoring of replication status and recovery from multiple copies.

Managed file replication offers flexible replication topologies including full system mirroring, bi-directional, many-to-one, one-to-many, and cascaded, enabling efficient cross-site deduplication.

Here are some additional points to consider about managed file replication:

- Replication contexts do not need to be configured.
- Lifecycle policies control replication of information with no intervention from the user.
- DD Boost will build and tear down contexts as needed on the fly.

For more information, see the `ddboost file-replication` commands in the *DD OS Command Reference Guide*.

## Directory replication

*Directory replication* transfers deduplicated data within a DD file system directory configured as a replication source to a directory configured as a replication destination on a different system.

With directory replication, a DD system can simultaneously be the source of some replication contexts and the destination of other contexts. And that DD system can also receive data from backup and archive applications while it is replicating data.

Directory replication has the same flexible network deployment topologies and cross-site deduplication effects as managed file replication (the type used by DD Boost).

Here are some additional points to consider when using directory replication:

- Do not mix CIFS and NFS data within the same directory. A single destination DD system can receive backups from both CIFS clients and NFS clients as long as separate directories are used for CIFS and NFS.
- Any directory can be in only one context at a time. A parent directory may not be used in a replication context if a child directory of that parent is already being replicated.
- Renaming (moving) files or tapes *into or out of* a directory replication source directory is *not* permitted. Renaming files or tapes *within* a directory replication source directory *is* permitted.
- A destination DD system must have available storage capacity of at least the post-compressed size of the expected maximum post-compressed size of the source directory.
- When replication is initialized, a destination directory is created automatically.
- After replication is initialized, ownership and permissions of the destination directory are always identical to those of the source directory. As long as the context exists, the destination directory is kept in a read-only state and can receive data only from the source directory.
- At any time, due to differences in global compression, the source and destination directory can differ in size.

### Folder Creation Recommendations

Directory replication replicates data at the level of individual subdirectories under `/data/coll/backup/`.

To provide a granular separation of data you must create, from a host system, other directories (DirA, DirB, etc.) within the `/backup` Mtree. Each directory should be based on your environment and the desire to replicate those directories to another location. You will not replicate the entire `/backup` MTree, but instead would set up replication contexts on each subdirectory underneath `/data/coll/backup/` (ex. `/data/coll/backup/DirC`). The purpose of this threefold:

- It allows control of the destination locations as DirA may go to one site and DirB may go to another.
- This level of granularity allows management, monitoring, and fault isolation. Each replication context can be paused, stopped, destroyed, or reported on.
- Performance is limited on a single context. The creation of multiple contexts can improve aggregate replication performance.
- As a general recommendation, approximately 5 - 10 contexts may be required to distribute replication load across multiple replication streams. This must be validated against the site design and the volume and composition of the data at the location.

**i** Note: Recommending a number of contexts is a design-dependent issue, and in some cases, significant implications are attached to the choices made about segregating data for the purposes of optimizing replication. Data is usually optimized for the manner in which it will rest – not in manner with which it will replicate. Keep this in mind when altering a backup environment.

## MTree replication

*MTree replication* is used to replicate MTrees between DD systems. Periodic snapshots are created on the source, and the differences between them are transferred to the destination by leveraging the same cross-site deduplication mechanism used for directory replication. This ensures that the data on the destination is always a point-in-time copy of the source, with file consistency. This also reduces replication of churn in the data, leading to more efficient utilization of the WAN.

While directory replication must replicate every change to the content of the source directory in order, the use of snapshots with MTree replication enables some intermediate changes to the source to be skipped. Skipping these changes further reduces the amount of data that is sent over the network, and therefore reduces replication lag.

With MTree replication, a DD system can be simultaneously the source of some replication contexts and the destination of other contexts. And that DD system can also receive data from backup and archive applications while it is replicating data.

MTree replication has the same flexible network deployment topologies and cross-site deduplication effects as managed file replication (the type used by DD Boost).

Here are some additional points to consider when using MTree replication:

- When replication is initialized, a destination read-only MTree is created automatically.
- Data can be logically segregated into multiple MTrees to promote greater replication performance.
- Snapshots must be created on source contexts.
- Snapshots cannot be created on a replication destination.
- Snapshots are replicated with a fixed retention of one year; however, the retention is adjustable on the destination and must be adjusted there.

- Snapshots are not automatically deleted after breaking a replication context, and must be expired when they are no longer required to prevent the system from filling up. The following KB articles provide more information:
  - *Data Domain - Checking for Snapshots that are No Longer Needed*, available at <https://support.emc.com/kb/336461>.
  - *Data Domain - Identifying Why a DDR is Filling Up*, available at <https://support.emc.com/kb/306203>.
  - *Data Domain - Mtree\_replication\_resync\_Snapshot\_retention*, available at <https://support.emc.com/kb/446176>.
- Replication contexts must be configured on both the source and the destination.
- Replicating DD VTL tape cartridges (or pools) simply means replicating MTree or directories that contain DD VTL tape cartridges. Media pools are replicated by MTree replication, as a default. A media pool can be created in backward-compatibility mode and can then be replicated via directory-based replication. You cannot use the `pool://` syntax to create replication contexts using the command line. When specifying pool-based replication in DD System Manager, either directory or MTree replication will be created, based on the media pool type.
- Replicating directories under an MTree is not permitted.
- A destination DD system must have available storage capacity of at least the post-compressed size of the expected maximum post-compressed size of the source MTree.
- After replication is initialized, ownership and permissions of the destination MTree are always identical to those of the source MTree. If the context is configured, the destination MTree is kept in a read-only state and can receive data only from the source MTree.
- At any time, due to differences in global compression, the source and destination MTree can differ in size.
- DD Retention Lock Compliance is supported with MTree replication, by default. If DD Retention Lock is licensed on a source, the destination must also have a DD Retention Lock license, or replication will fail. (To avoid this situation, you must disable DD Retention Lock.) If DD Retention Lock is enabled on a replication context, a replicated destination context will always contain data that is retention locked.
- DD Boost users should have the same user ID (UID) and primary group ID (GID) on both the source and destination systems.

#### MTree replication details

MTree replication involves the following steps:

1. A snapshot is created on the source replication context.
2. This snapshot is compared to the last previous snapshot.
3. Any differences between the two snapshots are sent to the destination replication context.
4. On the destination, the MTree is updated but no files are exposed to the user until all changes are received by the destination system.

These steps are repeated any time a snapshot is created on the source MTree. The following situations trigger the creation of a snapshot on the source system:

- System-generated periodic snapshot—When the replication lag is more than 15 minutes and there is no snapshot being currently replicated.
- User-created snapshot—At a time specified by the user, such as after the completion of a backup job.

For examples showing the interaction of different types of snapshots, see the KB article *How MTree Replication Works*, available at <https://support.emc.com/kb/180832>.



After the snapshot is replicated, the connection to the destination is closed. A new connection between the source and destination is established when the next snapshot is replicated.

#### Automatic Multi-Streaming (AMS)

Automatic Multi-Streaming (AMS) improves MTree replication performance. It uses multiple streams to replicate a single large file (32 GB or larger) to improve network bandwidth utilization during replication. By increasing the replication speed for individual files, AMS also improves the pipeline efficiency of the replication queue, and provides improved replication throughput and reduced replication lag.

When the workload presents multiple optimization choices, AMS automatically selects the best option for the workload. For example, if the workload is a large file with fastcopy attributes, the replication operation uses fastcopy optimization to avoid the overhead of scanning the file to identify unique segments between the replication pair. If the workload uses synthetics, replication uses synthetic replication on top of AMS to leverage local operations on the destination system for each replication stream to generate the file.


AMS is always enabled, and cannot be disabled.

## Collection replication

*Collection replication* performs whole-system mirroring in a one-to-one topology, continuously transferring changes in the underlying collection, including all of the logical directories and files of the DD file system.

Collection replication does not have the flexibility of the other types, but it can provide higher throughput and support more objects with less overhead, which may work better for high-scale enterprise cases.

Collection replication replicates the entire `/data/coll` area from a source DD system to a destination DD system.

 **Note:** Collection replication is not supported for cloud-tier enabled systems.

Here are some additional points to consider when using collection replication:

- No granular replication control is possible. All data is copied from the source to the destination producing a read-only copy.
- Collection replication requires that the storage capacity of the destination system be equal to, or greater than, the capacity of the source system. If the destination capacity is less than the source capacity, the available capacity on the source is reduced to the capacity of the destination.
- The DD system to be used as the collection replication destination must be empty before configuring replication. After replication is configured, this system is dedicated to receive data from the source system.
- With collection replication, all user accounts and passwords are replicated from the source to the destination. However, as of DD OS 5.5.1.0, other elements of configuration and user settings of the DD system are not replicated to the destination; you must explicitly reconfigure them after recovery.
- Collection replication is supported with DD Secure Multitenancy (SMT). Core SMT information, contained in the registry namespace, including the tenant and tenant-unit definitions with matching UUIDs is automatically transferred during replication operation. However, the following SMT information is not automatically included for replication, and must be configured manually on the destination system:
  - Alert notification lists for each tenant-unit

- All users assigned to the DD Boost protocol for use by SMT tenants, if DD Boost is configured on the system
- The default-tenant-unit associated with each DD Boost user, if any, if DD Boost is configured on the system

Using collection replication for disaster recovery with SMT on page 424 describes how to manually configure these items on the replication destination.

- DD Retention Lock Compliance supports collection replication.
- Collection replication is not supported in cloud tier-enabled systems.
- With collection replication, data in a replication context on the source system that has not been replicated cannot be processed for file system cleaning. If file system cleaning cannot complete because the source and destination systems are out of sync, the system reports the cleaning operation status as `partial`, and only limited system statistics are available for the cleaning operation. If collection replication is disabled, the amount of data that cannot be processed for file system cleaning increases because the replication source and destination systems remain out of sync. The KB article *Data Domain: An overview of Data Domain File System (DDFS) clean/garbage collection (GC) phases*, available from the Online Support site at <https://support.emc.com>, provides additional information.
- To enhance throughput in a high bandwidth environment, run the `replication modify <destination> crepl-gc-gw-optim` command to disable collection replication bandwidth optimization.

## Using DD Encryption with DD Replicator

DD Replicator can be used with the optional *DD Encryption* feature, enabling encrypted data to be replicated using collection, directory, or MTree replication

Replication contexts are always authenticated with a *shared secret*. That shared secret is used to establish a session key using a Diffie-Hellman key exchange protocol, and that session key is used to encrypt and decrypt the protection system encryption key when appropriate.

Each replication type works uniquely with encryption and offers the same level of security.

- *Collection replication* requires the source and destination to have the same encryption configuration, because the destination data is expected to be an exact replica of the source data. In particular, the encryption feature must be turned on or off at both the source and destination, and if the feature is turned on, the encryption algorithm and the system passphrases must also match. The parameters are checked during the replication association phase.  
During collection replication, the source transmits the data in encrypted form, and also transmits the encryption keys to the destination. The data can be recovered at the destination because the destination has the same passphrase and the same system encryption key.  
① | Note: Collection replication is not supported for cloud-tier enabled systems.
- *MTree or directory replication* does not require encryption configuration to be the same at both the source and destination. Instead, the source and destination securely exchange the destination's encryption key during the replication association phase, and the data is re-encrypted at the source using the destination's encryption key before transmission to the destination.  
If the destination has a different encryption configuration, the data transmitted is prepared appropriately. For example, if the feature is turned off at the destination, the source decrypts the data, and it is sent to the destination un-encrypted.
- In a *cascaded replication* topology, a replica is chained among three systems. The last system in the chain can be configured as a collection, MTree, or directory. If the last system is a



collection replication destination, it uses the same encryption keys and encrypted data as its source. If the last system is an MTree or directory replication destination, it uses its own key, and the data is encrypted at its source. The encryption key for the destination at each link is used for encryption. Encryption for systems in the chain works as in a replication pair.

## Replication topologies

DD Replicator supports five replication topologies (one-to-one, one-to-one bidirectional, one-to-many, many-to-one, and cascaded). The tables in this section show (1) how these topologies work with three types of replication (MTree, directory, and collection) and (2) how mixed topologies are supported with cascaded replication.

In general:

- Single node (SN) systems support all replication topologies.
- Single node-to-single node (SN -> SN) can be used for all replication types.
- Collection replication cannot be configured from either an SN system to a DD high availability-enabled system, nor from a DD high availability-enabled system to an SN system.
- For MTree and Directory replication, DD high availability systems are treated like SN systems.
- Collection replication cannot be configured on Cloud Tier-enabled systems.

In this table:

- SN = single node DD system without Cloud Tier
- SN + CT = single node DD system with Cloud Tier

**Table 187** Topology Support by Replication Type and DD System Type

Topologies	MTree Replication	Directory Replication	Collection Replication
one-to-one	SN -> {SN   SN + CT}	SN -> SN SN -> SN + CT	SN -> SN
one-to-one bidirectional	SN -> {SN   SN + CT}	SN -> SN	not supported
one-to-many	SN -> {SN   SN + CT}	SN -> SN SN -> SN + CT	not supported
many-to-one	SN -> {SN   SN + CT}	SN -> SN SN -> SN + CT	not supported
cascaded	SN -> {SN   SN + CT} -> {SN   SN + CT}	SN -> SN -> SN SN -> SN -> SN + CT	SN -> SN -> SN

Cascaded replication supports mixed topologies where the second leg in a cascaded connection is different from the first type in a connection (for example, A -> B is directory replication, and B -> C is collection replication).

**Table 188** Mixed Topologies Supported with Cascaded Replication

Mixed Topologies	
SN - Dir Repl -> SN + CT - MTree Repl -> SN + CT - MTree Repl	SN - Dir Repl -> SN + CT - Col Repl -> SN + CT - Col Repl

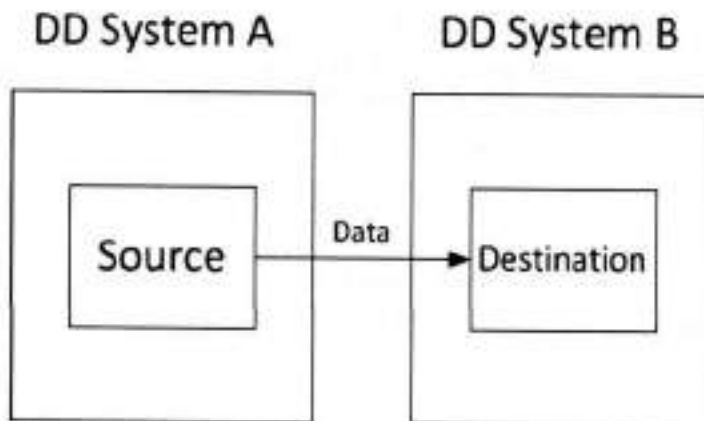
Table 188 Mixed Topologies Supported with Cascaded Replication (continued)

Mixed Topologies	
SN - MTree Repl -> SN - Col Repl -> SN - Col Repl	SN - MTree Repl -> SN + CT - Col Repl -> SN + CT - Col Repl

## One-to-one replication

The simplest type of replication is from a DD source system to a DD destination system, otherwise known as a *one-to-one* replication pair. This replication topology can be configured with directory, MTree, or collection replication types.

Figure 16 One-to-one replication pair

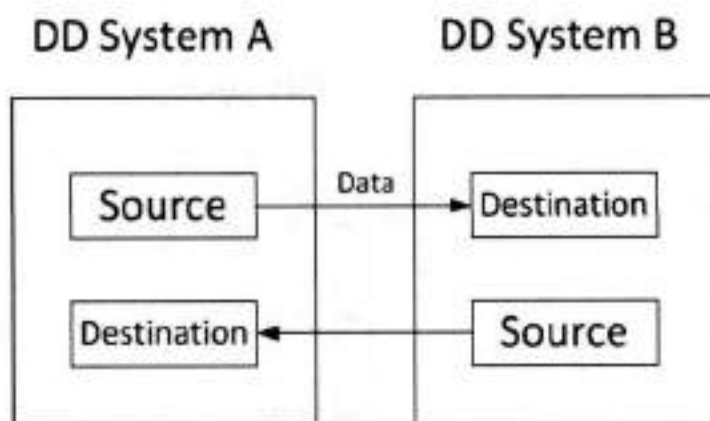


Data flows from the source to the destination system.

## Bi-directional replication

In a bi-directional replication pair, data from a directory or MTree on DD system A is replicated to DD system B, and from another directory or MTree on DD system B to DD system A.

Figure 17 Bi-directional replication

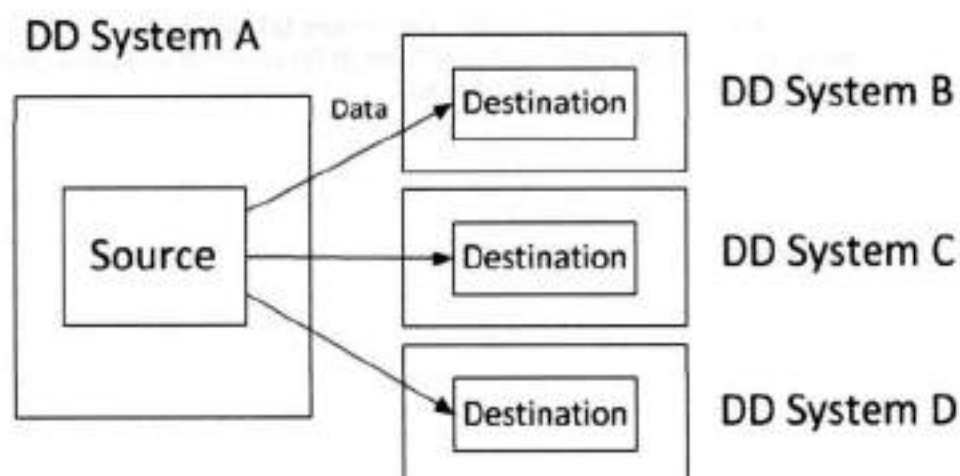


Data flows in both directions  
between two systems.

## One-to-many replication

In one-to-many replication, data flows from a source directory or MTree on one DD system to several destination DD systems. You could use this type of replication to create more than two copies for increased data protection, or to distribute data for multi-site usage.

Figure 18 One-to-many replication

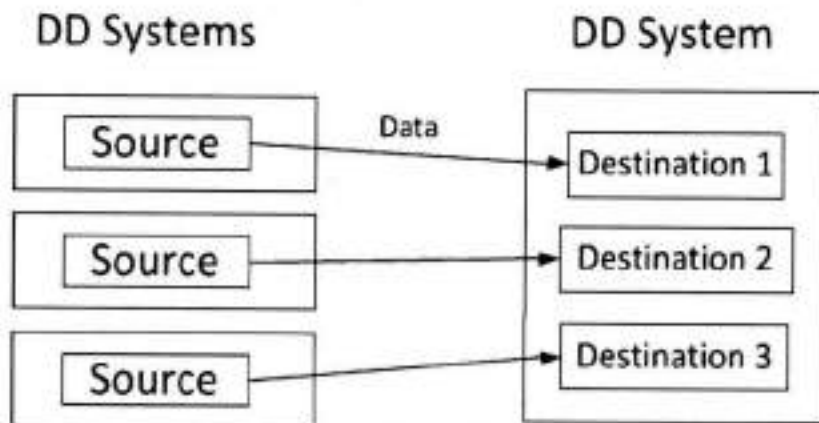


Data flows from a directory or MTree source system  
to many destination systems.

## Many-to-one replication

In many-to-one replication, whether with MTree or directory, replication data flows from several source DD systems to a single destination DD system. This type of replication can be used to provide data recovery protection for several branch offices on a corporate headquarter's IT system.

Figure 19 Many-to-one replication



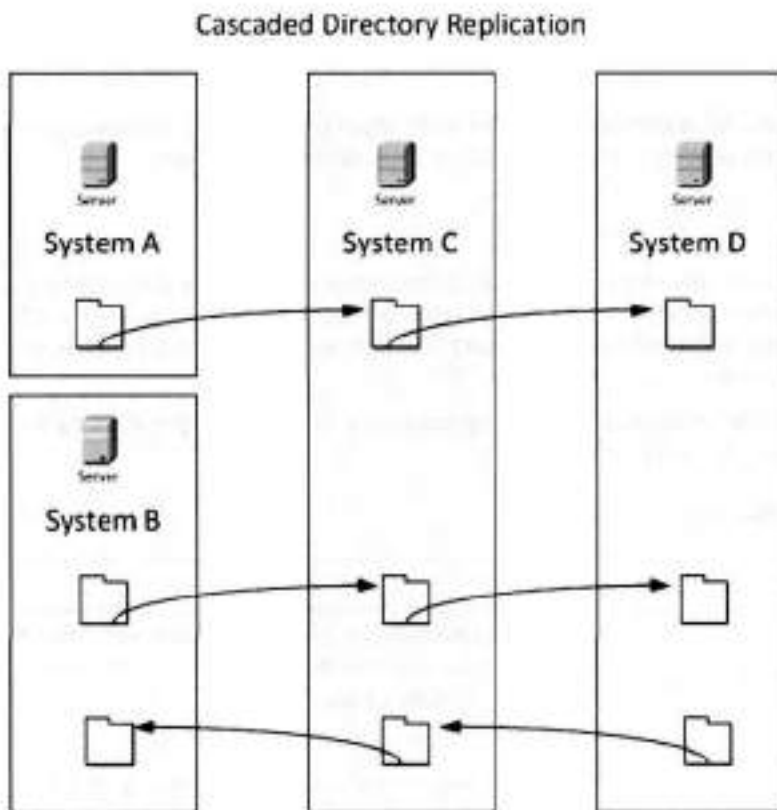
Data flows from many source systems to one destination system.

## Cascaded replication

In a cascaded replication topology, a source directory or MTree is chained among three DD systems. The last hop in the chain can be configured as collection, MTree, or directory replication, depending on whether the source is directory or MTree.

For example, DD system A replicates one or more MTrees to DD system B, which then replicates those MTrees to DD system C. The MTrees on DD system B are both a destination (from DD system A) and a source (to DD system C).

Figure 20 Cascaded directory replication



Data recovery can be performed from the non-degraded replication pair context. For example:

- In the event DD system A requires recovery, data can be recovered from DD system B.
- In the event DD system B requires recovery, the simplest method is to perform a replication resync from DD system A to (the replacement) DD system B. In this case, the replication context from DD system B to DD system C should be broken first. After the DD system A to DD system B replication context finishes resync, a new DD system B to DD System C context should be configured and resynced.

## Managing replication

You can manage replication using the DD System Manager) or the DD OS CLI.

### About this task

To use a graphical user interface (GUI) to manage replication, log in to the DD System Manager.

### Procedure

1. From the menu at the left of the DD System Manager, select **Replication**. If your license has not been added yet, select **Add License**.
2. Select **Automatic** or **On-Demand** (you must have a DD Boost license for on-demand).

### CLI Equivalent

You can also log in at the CLI:

```
login as: sysadmin
Data Domain OS 6.0.x.x-12345
```

```
Using keyboard-interactive authentication.
Password:
```

## Replication status

*Replication Status* shows the system-wide count of replication contexts exhibiting a warning (yellow text) or error (red text) state, or if conditions are normal.

## Summary view

The Summary view lists the configured replication contexts for a DD system, displaying aggregated information about the selected DD system – that is, summary information about the inbound and outbound replication pairs. The focus is the DD system, itself, and the inputs to it and outputs from it.

The Summary table can be filtered by entering a Source or Destination name, or by selecting a State (Error, Warning, or Normal).

**Table 189** Replication Summary view

Item	Description
Source	System and path name of the source context, with format <i>system.path</i> . For example, for directory <i>dir1</i> on system <i>dd9900-22</i> , you would see <i>dd9900-22.chaos.local/data/coll/dir1</i> .
Destination	System and path name of destination context, with format <i>system.path</i> . For example, for MTree <i>MTree1</i> on system <i>dd9900-44</i> , you would see <i>dd9900-44.chaos.local/data/coll/MTree1</i> .
Type	Type of context: MTree, directory (Dir), or Pool.
State	Possible states of replication pair status include: <ul style="list-style-type: none"> <li>• Normal – If the replica is initializing, Replicating, Recovering, Resyncing, or Migrating.</li> <li>• Idle – For MTree replication, this state can display if the replication process is not currently active or for network errors (such as the destination system being inaccessible).</li> <li>• Warning – If there is an unusual delay for the first five states, or for the Uninitialized state.</li> <li>• Error – Any possible error states, such as Disconnected.</li> </ul>
Synced As Of Time	Timestamp for last automatic replication sync operation performed by the source. For MTree replication, this value is updated when a snapshot is exposed on the destination. For directory replication, it is updated when a sync point inserted by the source is applied. A value of unknown displays during replication initialization.
Pre-Comp Remaining	Amount of pre-compressed data remaining to be replicated.
Completion Time (Est.)	Value is either <i>Completed</i> , or the estimated amount of time required to complete the replication data transfer based on the last 24 hours' transfer rate.

## Detailed information for a replication context

Selecting one replication context from the Summary view populates that context's information in Detailed Information, Performance Graph, Completion Stats, and Completion Predictor.

**Table 190** Detailed Information

Item	Description
State Description	Message about state of replica.
Source	System and path name of source context, with format <code>system.path</code> . For example, for directory <code>dir1</code> on system <code>dd9900-22</code> , you would see <code>dd9900-22.chaos.local/data/coll/dir1</code> .
Destination	System and path name of destination context, with format <code>system.path</code> . For example, for MTree <code>MTree1</code> on system <code>dd9900-44</code> , you would see <code>dd9900-44.chaos.local/data/coll/MTree1</code> .
Connection Port	System name and listen port used for replication connection.

**Table 191** Performance Graph

Item	Description
Pre-Comp Remaining	Pre-compressed data remaining to be replicated.
Pre-Comp Written	Pre-compressed data written on the source.
Post-Comp Replicated	Post-compressed data that has been replicated.

**Table 192** Completion Stats

Item	Description
Synced As Of Time	Timestamp for last automatic replication sync operation performed by the source. For MTree replication, this value is updated when a snapshot is exposed on the destination. For directory replication, it is updated when a sync point inserted by the source is applied. A value of unknown displays during replication initialization.
Completion Time (Est.)	Value is either <code>Completed</code> or the estimated amount of time required to complete the replication data transfer based on the last 24 hours' transfer rate.
Pre-Comp Remaining	Amount of data remaining to be replicated.
Files Remaining	(Directory Replication Only) Number of files that have not yet been replicated.
Status	For source and destination endpoints, shows status (Enabled, Disabled, Not Licensed, etc.) of major components on the system, such as: <ul style="list-style-type: none"> <li>• Replication</li> <li>• File System</li> </ul>



Table 192 Completion Stats (continued)

Item	Description
	<ul style="list-style-type: none"> <li>• DD Retention Lock</li> <li>• DD Encryption at Rest</li> <li>• DD Encryption over Wire</li> <li>• Available Space</li> <li>• Low Bandwidth Optimization</li> <li>• Compression Ratio</li> <li>• Low Bandwidth Optimization Ratio</li> </ul>

#### Completion Predictor

The Completion Predictor is a widget for tracking a backup job's progress and for predicting when replication will complete, for a selected context.

### Creating a replication pair

Before creating a replication pair, make sure the destination does not *exist*, or you will get an error.

#### Procedure

1. Select **Replication > Automatic > Summary tab > Create Pair**.
2. In the Create Pair dialog, add information to create an inbound or outbound MTree, directory, collection, or pool replication pair, as described in the next sections.

### Adding a DD system for replication

You may need to add a DD system as either a host or a destination before you can create a replication pair.

#### About this task

- Note:** Make sure the system being added is running a compatible DD OS version as described in Replication version compatibility on page 391.

#### Procedure

1. In the Create Pair dialog, select **Add System**.
2. For **System**, enter the hostname or IP address of the system to be added.
3. For **User Name and Password**, enter the sysadmin's user name and password.
4. Optionally, select **More Options** to enter a proxy IP address (or system name) of a system that cannot be reached directly. If configured, enter a custom port instead of the default port 3009.

- Note:** IPv6 addresses are supported only when adding a DD OS 5.5 or later system to a management system using DD OS 5.5 or later.

5. Select **OK**.

- Note:** If the system is unreachable after adding it to DD System Manager, make sure that there is a route from the managing system to the system being added. If a hostname (either a fully qualified domain name (FQDN) or non-FQDN) is entered, make sure it is resolvable on the managed system. Configure a domain name for the managed

system, ensure a DNS entry for the system exists, or ensure an IP address to hostname mapping is defined.

6. If the system certificate is not verified, the Verify Certificate dialog shows details about the certificate. Check the system credentials. Select **OK** if you trust the certificate, or select **Cancel**.

### Creating a collection replication pair

See the *Collection replication* section for general information about this type of replication.

#### About this task

Before creating a collection replication pair, make sure:

- The storage capacity of the destination system is equal to, or greater than, that of the source system. (If the destination capacity is less than that of the source, the available capacity on the source is reduced to that of the destination.)
- The destination has been destroyed, and subsequently re-created, but not enabled.
- Each destination and each source is in only one context at a time.
- The file system is disabled on the replica, while configuring and enabling encryption on the source.
- The file system is disabled on the source, while configuring and enabling encryption on the replica.

#### Procedure

1. In the Create Pair dialog, select **Collection** from the **Replication Type** menu.
2. Select the source system hostname from the **Source System** menu.
3. Select the destination system hostname from the **Destination System** menu. The list includes only those hosts in the DD-Network list.
4. If you want to change any host connection settings, select the **Advanced** tab.
5. Select **OK**. Replication from the source to the destination begins.

#### Results

Test results returned the following performance guidelines for replication initialization. These are guidelines *only*, and actual performance seen in production environments may vary.

- Over a gigabit LAN: With a high enough shelf count to drive maximum input/output and ideal conditions, collection replication can saturate a 1GigE link (modulo 10% protocol overhead), as well as 400-900 MB/sec on 10GigE, depending on the platform.
- Over a WAN, performance is governed by the WAN link line speed, bandwidth, latency, and packet loss rate.

### Creating an MTree, directory, or pool replication pair

See the *MTree replication* and *Directory replication* sections for general information about these types of replication.

#### About this task

When creating an MTree, directory, or pool replication pair:

- Make sure the replication is transiting/exiting the correct interface. When defining a replication context, the host names of the source and destination must resolve with forward and reverse lookups. To make the data transit alternate interfaces on the system, other than the default resolving interface, the replication context must be modified after creation. It may

be necessary to set up host files to ensure that contexts are defined on non-resolving (cross-over) interfaces.

- You can "reverse" the context for an MTree replication, that is, you can switch the destination and the source.
- Subdirectories within an MTree cannot be replicated, because the MTree, in its entirety, is replicated.
- The destination DD system must have available storage capacity of at least the post-compressed size of the expected maximum post-compressed size of the source directory or MTree.
- When replication is initialized, a destination directory is created automatically.
- A DD system can simultaneously be the source for one context and the destination for another context.

#### Procedure

1. In the Create Pair dialog, select **Directory**, **MTree** (default), or **Pool** from the **Replication Type** menu.
2. Select the source system hostname from the **Source System** menu.
3. Select the destination system hostname from the **Destination System** menu.
4. Enter the source path in the **Source Path** text box (notice the first part of the path is a constant that changes based on the type of replication chosen).
5. Enter the destination path in the **Destination Path** text box (notice the first part of the path is a constant that changes based on the type of replication chosen).
6. If you want to change any host connection settings, select the **Advanced** tab.
7. Select **OK**.

The Replication from the source to the destination begins.

Test results from returned the following guidelines for estimating the time needed for replication initialization.

These are guidelines *only* and may not be accurate in specific production environments.

- Using a T3 connection, 100ms WAN, performance is about 40 MiB/sec of pre-compressed data, which gives data transfer of:  
40 MiB/sec = 25 seconds/GiB = 3.456 TiB/day
- Using the base-2 equivalent of gigabit LAN, performance is about 80 MiB/sec of pre-compressed data, which gives data transfer of about double the rate for a T3 WAN.

#### Example 2 CLI Equivalent

Here is an example of creating MTree replication pairs at the CLI. In this example, the source system is `dd9900` and the destination system is `dlh5`. For details about usage in other scenarios, see the *DD OS Command Reference Guide*.

1. Create an MTree on the source system:

```
sysadmin@dd9900# mtree create /data/coll/Oracle2
MTree "/data/coll/Oracle2" created successfully.
```

2. Create the replication context in the destination system, using the full hostname.

```
sysadmin@dlh5# replication add source mtree://dd9900.chaos.local/data/coll/Oracle2
destination mtree://dlh5.chaos.local/data/coll/Oracle2
```

3. Create the replication context in the source, using the full hostname.

**Example 2 CLI Equivalent (continued)**

```
sysadmin@dd9900# replication add source mtree://dd9900.chaos.local/data/coll/
Oracle2 destination mtree://dlh5.chaos.local/data/coll/Oracle2
```

4. To verify that the MTree replication context has been created, use the `replication show config` command.

The output is horizontally truncated in this example.

```
sysadmin@dlh5# replication show config
CTX Source
Destination
-----
-----
1  dir://dd9900.chaos.local/backup/Oracle2      dir://dlh5.chaos.local/backup/
Oracle2
2  mtree://dd9900.chaos.local/data/coll/Oracle2 mtree://dlh5.chaos.local/data/
coll/Oracle2
-----
-----
* Used for recovery only.
```

5. To start replication between a source and destination, use the `replication initialize` command on the source. This command checks that the configuration and connections are correct and returns error messages if any problems occur.

```
sysadmin@dd9900# replication initialize mtree://dlh5.chaos.local/data/coll/Oracle2
(00:08) Waiting for initialize to start...
(00:10) Intialize started.
Use 'replication watch mtree://dlh5.chaos.local/data/coll/Oracle2' to monitor
progress.
```

**Configuring bi-directional replication**

To create a bi-directional replication pair, use the directory or MTree replication pair procedure (for example, using `mtree2`) from host A to host B. Use the same procedure to create a replication pair (for example, using `mtree1`) from host B to host A. For this configuration, destination pathnames cannot be the same.

**Configuring one-to-many replication**

To create a one-to-many replication pair, use the directory or MTree replication pair procedure (for example, using `mtree1`) on host A to: (1) `mtree1` on host B, (2) `mtree1` on host C, and (3) `mtree1` on host D. A replication recovery cannot be done to a source context whose path is the source path for other contexts; the other contexts must be broken and resynced after the recovery.

**Configuring many-to-one replication**

To create a many-to-one replication pair, use the directory or MTree replication pair procedure [for example, (1) `mtree1` from host A to `mtree1` on host C and (2) `mtree2` on host B to `mtree2` on host C.]

**Configuring cascaded replication**

To create a cascaded replication pair, use the directory or MTree replication pair procedure: (1) `mtree1` on host A to `mtree1` on host B, and (2) on host B, create a pair for `mtree1` to `mtree1` on host C. The final destination context (on host C in this example, but more than three hops are supported) can be a collection replica or a directory or MTree replica.

## Disabling and enabling a replication pair

Disabling a replication pair temporarily pauses the active replication of data between a source and a destination. The source stops sending data to the destination, and the destination stops serving as an active connection to the source.

### Procedure

1. Select one or more replication pairs in the Summary table, and select **Disable Pair**.
2. In the Display Pair dialog, select **Next** and then **OK**.
3. To resume operation of a disabled replication pair, select one or more replication pairs in the Summary table, and select **Enable Pair** to display the Enable Pair dialog.
4. Select **Next** and then **OK**. Replication of data is resumed.

### CLI Equivalent

```
# replication disable {destination | all}
# replication enable {destination | all}
```

## Deleting a replication pair

When a directory or MTree replication pair is deleted, the destination directory or MTree, respectively, becomes writable. When a collection replication pair is deleted, the destination DD system becomes a stand-alone read/write system, and the file system is disabled.

### Procedure

1. Select one or more replication pairs in the Summary table, and select **Delete Pair**.
2. In the Delete Pair dialog, select **Next** and then **OK**. The replication pairs are deleted.

### CLI Equivalent

Before running this command, always run the `filesys disable` command. Then, afterward, run the `filesys enable` command

```
# replication break {destination | all}
```

Certain situations may arise in which you must resynchronize replication to resolve an issue. For information about breaking and resynchronizing replication, see the KB article *Break and Resync Directory Replication*, available at <https://support.emc.com/kb/180668>.

## Changing host connection settings

To direct traffic out of a specific port, modify a current context by altering the connection host parameter using a host name previously defined in the local hosts file to address the alternate system. That host name will correspond to the destination. The host entry will indicate an alternate destination address for that host. This may be required on both the source and destination systems.

### Procedure

1. Select the replication pair in the Summary table, and select **Modify Settings**. You can also change these settings when you are performing Create Pair, Start Resync, or Start Recover by selecting the **Advanced** tab.
2. In the Modify Connection Settings dialog, modify any or all of these settings:
  - a. **Use Low Bandwidth Optimization** – For enterprises with small data sets and 6 Mb/s or less bandwidth networks, DD Replicator can further reduce the amount of data to be sent using *low bandwidth optimization*. This enables remote sites with limited bandwidth.



to use less bandwidth or to replicate and protect more of their data over existing networks. Low bandwidth optimization must be enabled on both the source and destination DD systems. If the source and destination have incompatible low bandwidth optimization settings, low bandwidth optimization will be inactive for that context. After enabling low bandwidth optimization on the source and destination, both systems must undergo a full cleaning cycle to prepare the existing data, so run `filesys clean start` on both systems. The duration of the cleaning cycle depends on the amount of data on the DD system, but takes longer than a normal cleaning. For more information on the `filesys` commands, see the *DD OS Command Reference Guide*.

**Important:** Low bandwidth optimization is not supported for Collection Replication.

- b. **Enable Encryption Over Wire** – DD Replicator supports encryption of data-in-flight by using standard SSL (Secure Socket Layer) protocol version 1.0.1, which uses the ADH-AES256-GCM-SHA384 and DHE-RSA-AES256-GCM-SHA384 cipher suites to establish secure replication connections. Both sides of the connection must enable this feature for encryption to proceed.
  - c. **Network Preference** – You may choose IPv4 or IPv6. An IPv6-enabled replication service can still accept connections from an IPv4 replication client if the service is reachable via IPv4. An IPv6-enabled replication client can still communicate with an IPv4 replication service if the service is reachable via IPv4.
  - d. **Use Non-default Connection Host** – The source system transmits data to a destination system listen port. Since a source system can have replication configured for many destination systems (each of which can have a different listen port), each context on the source can configure the connection port to the corresponding listen port of the destination.
3. Select **Next** and then **Close**.

The replication pair settings are updated, and replication resumes.

#### CLI Equivalent

```
#replication modify <destination> connection-host <new-host-name> [port <port>]
```

## Managing replication systems

You can add or delete protection systems to be used for replication using the Manage Systems dialog.

#### Procedure

1. Select **Manage Systems**.
2. In the Manage Systems dialog, add and/or delete systems, as required.
3. Select **Close**.

## Recovering data from a replication pair

If source replication data becomes inaccessible, it can be *recovered* from the replication pair destination. The source must be empty before recovery can proceed. Recovery can be performed for all replication topologies, except for MTree replication.

Recovery of data from a directory pool, as well as from directory and collection replication pairs, is described in the next sections.

### Recovering directory pool data

You can recover data from a directory-based pool, but not from an MTree-based pool.

#### Procedure

1. Select **More > Start Recover**.
2. In the Start Recover dialog, select **Pool** from the **Replication Type** menu.
3. Select the source system hostname from the **System to recover to** menu.
4. Select the destination system hostname from the **System to recover from** menu.
5. Select the context on the destination from which data is recovered.
6. If you want to change any host connection settings, select the **Advanced** tab.
7. Select **OK** to start the recovery.

### Recovering collection replication pair data

To successfully recover collection replication pair data, the source file system must be in a pristine state, and the destination context must be fully initialized.

#### Procedure

1. Select **More > Start Recover** to display the Start Recover dialog.
2. Select **Collection** from the **Replication Type** menu.
3. Select the source system host name from the **System to recover to** menu.
4. Select the destination system host name from the **System to recover from** menu.
5. Select the context on the destination from which data is recovered. Only one collection will exist on the destination.
6. To change any host connection settings, select the **Advanced** tab.
7. Select **OK** to start the recovery.

### Recovering directory replication pair data

To successfully recover directory replication pair data, the same directory used in the original context must be created (but left empty).

#### Procedure

1. Select **More > Start Recover** to display the Start Recover dialog.
2. Select **Directory** from the **Replication Type** menu.
3. Select the host name of the *system to which data needs to be restored* from the **System to recover to** menu.
4. Select the host name of the *system that will be the data source* from the **System to recover from** menu.
5. Select the context to restore from the context list.
6. To change any host connection settings, select the **Advanced** tab.
7. Select **OK** to start the recovery.

### Aborting a replication pair recovery

If a replication pair recovery fails or must be terminated, you can stop the replication recovery.

#### Procedure

1. Select the **More** menu, and select **Abort Recover** to display the Abort Recover dialog, which shows the contexts currently performing recovery.



2. Select the checkbox of one or more contexts to abort from the list.
3. Select **OK**.

#### After you finish

As soon as possible, you should restart recovery on the source.

## Resyncing an MTree, directory, or pool replication pair

*Resynchronization* is the process of recovering (or bringing back into sync) the data between a source and a destination replication pair after a manual break. The replication pair are resynchronized so both endpoints contain the same data. Resynchronization is available for MTree, directory, and pool replication, but not for collection replication.

#### About this task

A replication resynchronization can also be used:

- To recreate a context that has been deleted.
- When a destination runs out of space, but the source still has data to replicate.
- To convert a directory replication pair to an MTree replication pair.

#### Procedure

1. Delete the context on both the replication source and replication destination systems.
2. From either the replication source or replication destination system, select **More > Start Resync** to display the Start Resync dialog.
3. Select the Replication Type to be resynced: **Directory**, **MTree**, or **Pool**.
4. Select the replication source system host name from the **Source System** menu.
5. Select the replication destination system host name from the **Destination System** menu.
6. Enter the replication source path in the **Source Path** text box.
7. Enter the replication destination path in the **Destination Path** text box.
8. To change any host connection settings, select the **Advanced** tab.
9. Select **OK**.

#### CLI Equivalent

```
# replication resync destination
```

## Aborting a replication pair resynchronization

If a replication pair resynchronization fails or must be terminated, you can stop the resynchronization.

#### Procedure

1. From either the replication source or replication destination system, select **More > Abort Resync** to display the Abort Resync dialog, which lists all contexts currently performing resynchronization.
2. Select the checkboxes of one or more contexts to abort their resynchronization.
3. Select **OK**.

## DD Boost view

The DD Boost view provides configuration and troubleshooting information to NetBackup administrators who have configured DD systems to use DD Boost AIR (Automatic Image Replication) or any DD Boost application that uses managed file replication.

See the *DD Boost for OpenStorage Administration Guide* for DD Boost AIR configuration instructions.

The **File Replication** tab displays:

- **Currently Active File Replication:**
  - Direction (Out-Going and In-Coming) and the number of files in each.
  - Remaining data to be replicated (pre-compressed value in GiB) and the amount of data already replicated (pre-compressed value in GiB).
  - Total size: The amount of data to be replicated and the already replicated data (pre-compressed value in GiB).
- **Most Recent Status:** Total file replications and whether completed or failed
  - during the last hour
  - over the last 24 hours
- **Remote Systems:**
  - Select a replication from the list.
  - Select the time period to be covered from the menu.
  - Select **Show Details** for more information about these remote system files.

The **Storage Unit Associations** tab displays the following information, which you can use for audit purposes or to check the status of DD Boost AIR events used for the storage unit's image replications:

- A list of all storage unit **Associations** known to the system. The source is on the left, and the destination is on the right. This information shows the configuration of AIR on the protection system.
- The **Event Queue** is the pending event list. It shows the local storage unit, the event ID, and the status of the event.

An attempt is made to match both ends of a DD Boost path to form a pair and present this as one pair/record. If the match is impossible, for various reasons, the remote path will be listed as *Unresolved*.

### Remote system files

The Show Details button provides information for the selected remote file replication system. File Replications shows starting and ending information, as well as size and data amount, for the selected remote file replication system. The Performance Graph shows performance over time for the selected remote file replication system.

**Table 193** File Replications

Item	Description
Start	Starting point of time period.
End	Ending point of time period.
File Name	Name of specific replication file.

Table 193 File Replications (continued)

Item	Description
Status	Most recent status (Success, Failure).
Pre-Comp Size (MiB)	Amount of pre-compressed outbound and inbound data, as compared to network throughput or post-compressed data (in MiB).
Network Bytes (MiB)	Amount of network throughput data (in MiB).

Table 194 Performance Graph

Item	Description
Duration	Duration for replication (either 1d, 7d or 30d).
Interval	Interval for replication (either Daily or Weekly).
Pre-Comp Replicated	Amount of pre-compressed outbound and inbound data (in GiB).
Post-Comp Replicated	Amount of post-compressed data (in GiB).
Network Bytes	Amount of network throughput data (in GiB).
Files Succeeded	Number of files that were successfully replicated.
Files Failed	Number of files that failed to be replicated.
Show in new window	Brings up a separate window.
Print	Prints the graph.

## Performance view

The Performance view displays a graph that represents the fluctuation of data during replication. These are aggregated statistics of each replication pair for this DD system.

- **Duration** (x-axis) is 30 days by default.
- **Replication Performance** (y-axis) is in GibiBytes or MebiBytes (the binary equivalents of GigaBytes and MegaBytes).
- **Network In** is the total replication network bytes entering the system (all contexts).
- **Network Out** is the total replication network bytes leaving the system (all contexts).
- For a reading of a specific point in time, hover the cursor over a place on the graph.
- During times of inactivity (when no data is being transferred), the shape of the graph may display a gradually descending line, instead of an expected sharply descending line.

## Advanced Settings view

Advanced Settings lets you manage throttle and network settings.

### Throttle Settings

- **Throttle Override** – Displays throttle rate if configured, or 0 meaning all replication traffic is stopped.
- **Permanent Schedule** – Displays the time and days of the week on which scheduled throttling occurs.

### Network Settings

- **Bandwidth** – Displays the configured data stream rate if bandwidth has been configured, or Unlimited (default) if not. The average data stream to the replication destination is at least 98,304 bits per second (12 KiB).
- **Delay** – Displays the configured network delay setting (in milliseconds) if it has been configured, or None (default) if not.
- **Listen Port** – Displays the configured listen port value if it has been configured, or 2051 (default) if not.

### Adding throttle settings

To modify the amount of bandwidth used by a network for replication, you can set a *replication throttle* for replication traffic.

#### About this task

There are three types of replication throttle settings:

- **Scheduled throttle** – The throttle rate is set at a predetermined time or period.
- **Current throttle** – The throttle rate is set until the next scheduled change, or until a system reboot.
- **Override throttle** – The previous two types of throttle are overridden. This persists – even through reboot – until you select **Clear Throttle Override** or issue the `replication throttle reset override` command.

You can also set a default throttle or a throttle for specific destinations, as follows:

- **Default throttle** – When configured, all replication contexts are limited to this throttle, except for those destinations specified by destination throttles (see next item).
- **Destination throttle** – This throttle is used when only a few destinations need to be throttled, or when a destination requires a throttle setting different from the default throttle. When a default throttle already exists, this throttle takes precedence for the destination specified. For example, you can set the default replication throttle to *10 kbps*, but – using a destination throttle – you can set a single collection replication context to *unlimited*.

**i** Note: Currently, you can set and modify destination throttle only by using the command-line interface (CLI); this functionality is not available in the DD System Manager. For documentation on this feature, see the `replication throttle` command in the *DD OS Command Reference Guide*. If the DD System Manager detects that you have one or more destination throttles set, you will be given a warning, and you should use the CLI to continue.

Additional notes about replication throttling:

- Throttles are set only at the source. The only throttle that applies to a destination is the **0 Bps (Disabled)** option, which disables all replication traffic.
- The minimum value for a replication throttle is 98,304 bits per second.

#### Procedure

1. Select **Replication > Advanced Settings > Add Throttle Setting** to display the Add Throttle Setting dialog.
2. Set the days of the week for which throttling is to be active by selecting **Every Day** or by selecting checkbox(es) next to individual day(s).
3. Set the time that throttling is to start with the **Start Time** drop-down selectors for the hour:minute and AM/PM.
4. For **Throttle Rate**:

- Select **Unlimited** to set no limits.
- Enter a number in the text box (for example, 20000), and select the rate from the menu (bps, Kbps, Bps, or KBps).
- Select the **0 Bps (disabled)** option to disable all replication traffic.

5. Select **OK** to set the schedule. The new schedule is shown under **Permanent Schedule**.

#### Results

Replication runs at the given rate until the next scheduled change, or until a new throttle setting forces a change.

## Deleting Throttle Settings

You can delete a single throttle setting or all throttle settings at once.

#### Procedure

1. Select **Replication > Advanced Settings > Delete Throttle Setting** to display the Delete Throttle Setting dialog.
2. Select the checkbox for the throttle setting to delete, or select the heading checkbox to delete all settings. This list can include settings for the "disabled" state.
3. Select **OK** to remove the setting.
4. In the Delete Throttle Setting Status dialog, select **Close**.

## Temporarily overriding a throttle setting

A throttle override temporarily changes a throttle setting. The current setting is listed at the top of the window.

#### Procedure

1. Select **Replication > Advanced Settings > Set Throttle Override** to display the Throttle Override dialog.
2. Either set a new throttle override, or clear a previous override.
  - a. To set a new throttle override:
    - Select **Unlimited** to revert to the system-set throttle rate (no throttling performed), or
    - Set the throttling bit and rate in the text box (for example, 20000) and (bps, Kbps, Bps, or KBps), or
    - Select **0 Bps (Disabled)** to set the throttle rate to 0, effectively stopping all replication network traffic.
    - To enforce the change temporarily, select **Clear at next scheduled throttle event**.
  - b. To clear an override previously set, select **Clear Throttle Override**.
3. Select **OK**.

## Changing network settings

Using the bandwidth and network-delay settings together, replication calculates the proper TCP (transmission control protocol) buffer size for replication usage. These network settings are global to the DD system and should be set only once per system.

#### About this task

Note the following:

- You can determine the actual bandwidth and the actual network delay values for each server by using the `ping` command.
- The default network parameters in a restorer work well for replication in low latency configurations, such as a local 100Mbps or 1000Mbps Ethernet network, where the latency round-trip time (as measured by the `ping` command) is usually less than 1 millisecond. The defaults also work well for replication over low- to moderate-bandwidth WANs, where the latency may be as high as 50-100 milliseconds. However, for high-bandwidth high-latency networks, some tuning of the network parameters is necessary. The key number for tuning is the bandwidth-delay number produced by multiplying the bandwidth and round-trip latency of the network. This number is a measure of how much data can be transmitted over the network before any acknowledgments can return from the far end. If the bandwidth-delay number of a replication network is more than 100,000, then replication performance benefits from setting the network parameters in both restorers.

#### Procedure

1. Select **Replication > Advanced Settings > Change Network Settings** to display the Network Settings dialog.
2. In the Network Settings area, select **Custom Values**.
3. Enter **Delay** and **Bandwidth** values in the text boxes. The network delay setting is in milliseconds, and bandwidth is in bytes per second.
4. In the Listen Port area, enter a new value in the text box. The default IP Listen Port for a replication destination for receiving data streams from the replication source is 2051. This is a global setting for the DD system.
5. Select **OK**. The new settings appear in the Network Settings table.

## Monitoring replication

The DD System Manager provides many ways to track the status of replication – from checking replication pair status, to tracking backup jobs, to checking performance, to tracking a replication process.

### Viewing estimated completion time for backup jobs

You can use the Completion Predictor to see the estimated time for when a backup replication job will be completed.

#### Procedure

1. Select **Replication > Summary**.
2. Select a Replication context for which to display Detailed Information.
3. In the Completion Predictor area, select options from the **Source Time** drop-down list for a replication's completion time, and select **Track**.

The estimated time displays, in the Completion Time area, for when a particular backup job will finish its replication to the destination. If the replication is finished, the area shows **Completed**.



## Checking replication context performance

To check the performance of a replication context over time, select a Replication context in the Summary view, and select **Performance Graph** in the Detailed Information area.

## Tracking status of a replication process

To display the progress of a replication initialization, resynchronization, or recovery operation, use the **Replication > Summary** view to check the current state.

### CLI Equivalent

```
# replication show config all
```

CTX	Source	Destination	Connection
Host and Port	Enabled		
1	dir://host2/backup/dir2	dir://host3/backup/dir3	host3.company.com
Yes			
2	dir://host3/backup/dir3	dir://host2/backup/dir2	host3.company.com
Yes			

When specifying an IP version, use the following command to check its setting:

```
# replication show config rctx://2
```

```
CTX: 2
Source: ntree://ddbetal.dallasrdc.com/data/coll/EDM1
Destination: ntree://ddbeta2.dallasrdc.com/data/coll/EDM_ipv6
Connection Host: ddbeta2-ipv6.dallasrdc.com
Connection Port: (default)
Ipversion: ipv6
Low-bw-optim: disabled
Encryption: disabled
Enabled: yes
Propagate-retention-lock: enabled
```

## Replication lag

The amount of time between two copies of data is known as replication lag.

You can measure the replication lag between two contexts with the replication status command. For information about determining the cause of replication lag and mitigating its impact, see the KB article *Troubleshooting Replication Lag*, available at <https://support.emc.com/kb/180482>.

## Replication with HA

Floating IP addresses allow HA systems to specify a single IP address for replication configuration that will work regardless of which node of the HA pair is active.

Over IP networks, HA systems use a floating IP address to provide data access to the HA pair, regardless of which physical node is the active node. The net config command provides the `[type {fixed | floating}]` option to configure a floating IP address. The *DD OS Command Reference Guide* provides more information.

If a domain name is needed to access the floating IP address, specify the HA system name as the domain name. Run the `ha status` command to locate the HA system name.

**Note:** Run the `net show hostname type ha-system` command to display the HA system name, and if required, run the `net set hostname ha-system` command to change the HA system name.



All file system access should be through the floating IP address. When configuring backup and replication operations on an HA pair, always specify the floating IP address as the IP address for the protection system. Other system features such as DD Boost and replication will accept the floating IP address for the HA pair the same way as they accept the system IP address for a non-HA system.

#### Replication between HA and non-HA systems

Collection replication between HA and non-HA systems is not supported. Directory or MTree replication is required to replicate data between HA and non-HA systems.

## Replicating a system with quotas to one without

Replicate a system with a DD OS that supports quotas, to a system with a DD OS that does not have quotas.

- A reverse resync, which takes the data from the system without quotas and puts it back in an MTree on the system that has quotas enabled (and which continues to have quotas enabled).
- A reverse initialization from the system without quotas, which takes its data and creates a new MTree on the system that supports quotas, but does not have quotas enabled because it was created from data on a system without quotas.

## Replication Scaling Context

The Replication Scaling Context feature gives you more flexibility when configuring replication contexts.

In environments with more than 299 replication contexts that include both directory and MTree replication contexts, this feature allows you to configure the contexts in any order. Previously, you had to configure the directory replication contexts first, followed by the MTree replication contexts.

The total number of replication contexts cannot exceed 540.

## Directory-to-MTree replication migration

The directory-to-MTree (D2M) replication optimization feature allows you to migrate existing directory replication contexts to new replication contexts based on MTrees, which are logical partitions of the file system. This feature also lets you monitor the process as it unfolds and verify that has successfully completed.

Although you can use the graphical user interface (GUI) for this operation, it is recommended you use the Command Line Interface (CLI) for optimal performance.

## Performing migration from directory replication to MTree replication

#### About this task

Do not shut down or reboot your system during directory-to-MTree (D2M) migration.

#### Procedure

1. Stop all ingest operations to the directory replication source directory.
2. Create an MTree on the source DD system: `mtree create /data/coll/atree-name`

 Note: Do not create the MTree on the destination DD system.

- (Optional) Enable DD Retention Lock on the MTree.

**i** Note: If the source system contains retention-locked files, you might want to maintain DD Retention Lock on the new MTree.

See Enabling DD Retention Lock Compliance on an MTree.

- Create the MTree replication context on both the source and destination DD systems:  

```
replication add source mtree://source-system-name/source mtree replication
add destination mtree://destination-system-name/destination mtree
```
- Start the D2M migration: `replication dir-to-mtree start from rctx://1 to rctx://2`

In the previous example,

`rctx://1`

refers to the directory replication context, which replicates the directory `backup/backup/dir1` on the source system;

`rctx://2`

refers to the MTree replication context, which replicates the MTree `/data/coll/mtree1` on the source system.

**i** Note: This command might take longer than expected to complete. Do not press Ctrl-C during this process; if you do, you will cancel the D2M migration.

```
Phase 1 of 4 (precheck):
  Marking source directory /backup/dir1 as read-only...Done.

Phase 2 of 4 (sync):
  Syncing directory replication context...0 files flushed.
  current=45 sync_target=47 head=47
  current=45 sync_target=47 head=47
  Done. (00:09)

Phase 3 of 4 (fastcopy):
  Starting fastcopy from /backup/dir1 to /data/coll/mtree1...
  Waiting for fastcopy to complete...(00:00)
  Fastcopy status: fastcopy /backup/dir1 to /data/coll/mtree1: copied
  24
  files, 1 directory in 0.13 seconds
  Creating snapshot 'REPL-D2M-mtree1-2015-12-07-14-54-02'...Done

Phase 4 of 4 (initialize):
  Initializing MTree replication context...
  (00:08) Waiting for initialize to start...
  (00:11) Initialize started.

Use 'replication dir-to-mtree watch rctx://2' to monitor progress.
```

## Viewing directory-to-MTree migration progress

You can see which stage of the migration is currently in progress in the directory-to-MTree (D2M) replication.

### Procedure

- Enter `replication dir-to-mtree watch rctx://2` to see the progress.

`rctx://2`

specifies the replication context.

You should see the following output:

```
Use Control-C to stop monitoring.
Phase 4 of 4 (initialize).
<00:00> Replication initialize started...
<00:02> initializing:
<00:14>      100% complete, pre-comp: 0 KB/s, network: 0 KB/s
<00:14> Replication initialize completed.
Migration for ctx 2 successfully completed.
```

## Checking the status of directory-to-MTree replication migration

You can use the `replication dir-to-mtree status` command to check whether the directory-to-MTree migration (D2M) has successfully completed.

### Procedure

1. Enter the following command; here,

```
ctx://2
```

represents the MTree replication context on the source system: `replication dir-to-mtree status ctx://2`

The output should be similar to the following:

```
Directory Replication CTX:      1
MTree Replication CTX:        2
Directory Replication Source:   dir://127.0.0.2/backup/dir1
MTree Replication Source:      mtree://127.0.0.2/data/coll/mtree1
MTree Replication Destination: mtree://127.0.0.3/data/coll/mtree1
Migration Status:               completed
```

If there is no migration in progress, you should see the following:

```
# replication dir-to-mtree status ctx://2
No migration status for context 2.
```

2. Begin ingesting data to the MTree on the source DD system when the migration process is complete.
3. (Optional) Break the directory replication context on the source and target systems.

See the *DD OS Command Reference Guide* for more information about the `replication break` command.

## Aborting D2M replication

If necessary, you can abort the directory-to-MTree (D2M) migration procedure.

### About this task

The `replication dir-to-mtree abort` command aborts the ongoing migration process and reverts the directory from a read-only to a read-write state.

### Procedure

1. In the Command-Line Interface (CLI), enter the following command; here,

```
ctx://2
```

is the MTree replication context: `replication dir-to-mtree abort ctx://2`

You should see the following output:

```
Canceling directory to MTree migration for context dir-name.
Marking source directory dir-name as read-write...Done.
The migration is now aborted.
Remove the MTree replication context and MTree on both source and
destination
host by running 'replication break' and 'mtree delete' commands.
```

2. Break the MTree replication context: `replication break rctx://2`
3. Delete the MTree on the source system: `mtree delete mtree-path`

## Troubleshooting D2M

If you encounter a problem setting directory-to-MTree (D2M) replication, there is an operation you can perform to address several different issues.

### About this task

The `dir-to-mtree abort` procedure can help cleanly abort the D2M process. You should run this procedure in the following cases:

- The status of the D2M migration is listed as aborted.
- The system rebooted during D2M migration.
- An error occurred when running the `replication dir-to-mtree start` command.
- Ingest was not stopped before beginning migration.
- The MTree replication context was initialized before the `replication dir-to-mtree start` command was entered.

- ① Note: Do not run `replication break` on the MTree replication context before the D2M process finishes.
- Always run `replication dir-to-mtree abort` before running the `replication break` command on the `mrepl ctx`.
- Running the `replication break` command prematurely will permanently render the `drepl` source directory as read-only.
- If this occurs, please contact Support.

### Procedure

1. Enter `replication dir-to-mtree abort` to abort the process.
2. Break the newly created MTree replication context on both the source and destination systems.

In the following example, the MTree replication context is `rctx://2`

```
'
replication break rctx://2
```

3. Delete the corresponding MTrees on both the source and destination systems.

```
mtree delete mtree-path
```

- ① **Note:** MTree marked for deletion remain in the file system until the `filesys clean` command is run.

See the *DD OS Command Reference Guide* for more information.

4. Run the `filesys clean start` command on both the source and destination systems.  
For more information on the `filesys clean` commands, see the *DD OS Command Reference Guide*.
5. Restart the process.  
See Performing migration from directory replication to MTree replication.

## Additional D2M troubleshooting

There are solutions available if you forgot to enable DD Retention Lock for the new MTree or an error occurs after directory-to-MTree migration has been initialized.

### DD Retention Lock has not been enabled

If you forgot to enable DD Retention Lock for the new MTree and the source directory contains retention-locked files or directories, you have the following options:

- Let the D2M migration continue. However, you will not have DD Retention Lock information in the MTree after the migration.
- Abort the current D2M process as described in Aborting D2M replication on page 422 and restart the process with DD Retention Lock enabled on the source MTree.

### An error occurs after initialization

If the `replication dir-to-mtree start` process finishes without error but you detect an error during the MTree replication initialization (phase 4 of the D2M migration process), you can perform the following steps:

1. Make sure that there is no network issue.
2. Initialize the MTree replication context.

## Using collection replication for disaster recovery with SMT

To use the destination system of a collection replication pair configured with SMT as a replacement system for disaster recovery, additional SMT configuration steps must be performed in addition to the other configuration steps required to bring a replacement system online.

### Before you begin

Using the collection replication destination system in this manner requires autosupport reports to be configured and saved. The KB article *Collection replica with smt enabled*, available on <https://support.emc.com>, provides additional information.

### About this task

The replacement system will not have the following SMT details:

- Alert notification lists for each tenant-unit
- All users assigned to the DD Boost protocol for use by SMT tenants, if DD Boost is configured on the system
- The default-tenant-unit associated with each DD Boost user, if any, if DD Boost is configured on the system

Complete the following steps to configure SMT on the replacement system.

## Procedure

1. In the autosupport report, locate the output for the `smt tenant-unit show` detailed command.

```
Tenant-unit: "tul"
Summary:
Name      Self-Service  Number of Mtrees  Types          Pre-Comp (GiB)
-----
tul       Enabled      2                  DD Boost      2.0

Management-User:
User      Role
-----
tul_ta   tenant-admin
tul_tu   tenant-user
tum_ta   tenant-admin

Management-Group:
Group     Role
-----
qatest   tenant-admin

DDBoost:
Name      Pre-Comp (GiB)  Status  User  Tenant-Unit
-----
sul       2.0            RW/Q    ddbul tul

Q        : Quota Defined
RO       : Read Only
RW       : Read Write

Getting users with Default-tenant-unit tul
DD Boost user  Default tenant-unit
-----
ddbul         tul

Mtrees:
Name          Pre-Comp (GiB)  Status  Tenant-Unit
-----
/data/coll/ml  0.0            RW/Q    tul
/data/coll/sul 2.0            RW/Q    tul

D        : Deleted
Q        : Quota Defined
RO       : Read Only
RW       : Read Write
RD       : Replication Destination
RLGE     : Retention-Lock Governance Enabled
RLGD     : Retention-Lock Governance Disabled
RLCE     : Retention-Lock Compliance Enabled

Quota:
Tenant-unit: tul
Mtree      Pre-Comp (MiB)  Soft-Limit (MiB)  Hard-Limit (MiB)
-----
/data/coll/ml  0                71680             81920
/data/coll/sul 2048             30720             51200

Alerts:
Tenant-unit: "tul"
Notification list "tul_grp"
Members
-----
tom.tenant@abc.com
```



```
No such active alerts.
```

2. On the replacement system, enable SMT if it is not already enabled.
3. On the replacement system, license and enable DD Boost if it is required and not already enabled.
4. If DD Boost is configured, assign each user listed in the `DD Boost` section of the `smt tenant-unit show detailed` output as a DD Boost User.
 

```
# ddbboost user assign ddbul
```
5. If DD Boost is configured, assign each user listed in the `DD Boost` section of the `smt tenant-unit show detailed` output to the default tenant-unit shown, if any, in the output.
 

```
# ddbboost user option set ddbul default-tenant-unit tul
```
6. Create a new alert notification group with the same name as the alert notification group in the `Alerts` section of the `smt tenant-unit show detailed` output.
 

```
# alert notify-list create tul_grp tenant-unit tul
```
7. Assign each email address in the alert notification group in the `Alerts` section of the `smt tenant-unit show detailed` output to the new alert notification group.
 

```
# alert notify-list add tul_grp emails tom.tenant@abc.com
```



# CHAPTER 17

## DD Secure Multitenancy

This chapter includes:

- Secure Multi-Tenancy overview..... 428
- Provisioning a Tenant Unit..... 431
- Enabling Tenant Self-Service mode..... 435
- Data access by protocol..... 435
- Data management operations..... 437

## Secure Multi-Tenancy overview

*Secure Multi-Tenancy (SMT)* is the simultaneous hosting, by an internal IT department or an external provider, of an IT infrastructure for more than one consumer or workload (business unit, department, or Tenant).

SMT provides the ability to securely isolate many users and workloads in a shared infrastructure, so that the activities of one Tenant are not apparent or visible to the other Tenants.

A *Tenant* is a consumer (business unit, department, or customer) who maintains a persistent presence in a hosted environment.

Within an enterprise, a Tenant may consist of one or more business units or departments on a protection system that is configured and managed by IT staff.

- For a business unit (BU) use case, the Finance and Human Resources departments of a corporation could share the same system, but each department would be unaware of the presence of the other.
- For a service provider (SP) use case, the SP could deploy one or more systems to accommodate different Protection Storage services for multiple end-customers.

Both use cases emphasize the segregation of different customer data on the same physical system.

### SMT architecture basics

Secure Multitenancy (SMT) provides a simple approach to setting up Tenants and Tenant Units, using MTrees. SMT setup is performed using DD Management Center and/or the DD OS command line interface. This administration guide provides the theory of SMT and some general command line instructions.

The basic architecture of SMT is as follows.

- A Tenant is created on the DD Management Center and/or DD system.
- A Tenant Unit is created on a DD system for the Tenant.
- One or more MTrees are created to meet the storage requirements for the Tenant's various types of backups.
- The newly created MTrees are added to the Tenant Unit.
- Backup applications are configured to send each backup to its configured Tenant Unit MTree.

① **Note:** For more information about DD Management Center, see the *DD Management Center User Guide*. For more information about the DD OS command line interface, see the *DD OS Command Reference*.

### Terminology used in Secure Multi-Tenancy (SMT)

Understanding the terminology that is used in SMT will help you better understand this unique environment.

#### MTrees

*MTrees* are logical partitions of the file system and offer the highest degree of management granularity, meaning users can perform operations on a specific MTree without affecting the entire file system. MTrees are assigned to Tenant Units and contain that Tenant Unit's individualized settings for managing and monitoring SMT.

### Multi-Tenancy

*Multi-Tenancy* refers to the hosting of an IT infrastructure by an internal IT department, or an external service provider, for more than one consumer/workload (business unit/department/Tenant) simultaneously. DD SMT enables *Data Protection-as-a-Service*.

### RBAC (role-based access control)

*RBAC* offers multiple roles with different privilege levels, which combine to provide the administrative isolation on a multi-tenant protection system.

### Storage Unit

A *Storage Unit* is an MTree configured for the DD Boost protocol. Data isolation is achieved by creating a Storage Unit and assigning it to a DD Boost user. The DD Boost protocol permits access only to Storage Units assigned to DD Boost users connected to the system.

### Tenant

A *Tenant* is a consumer (business unit/department/customer) who maintains a persistent presence in a hosted environment.

### Tenant Self-Service

*Tenant Self-Service* is a method of letting a Tenant log in to a protection system to perform some basic services (add, edit, or delete local users, NIS groups, and/or AD groups). This reduces the bottleneck of always having to go through an administrator for these basic tasks. The Tenant can access only their assigned Tenant Units. Tenant Users and Tenant Admins will, of course, have different privileges.

### Tenant Unit

A *Tenant Unit* is the partition of a system that serves as the unit of administrative isolation between Tenants. Tenant units that are assigned to a tenant can be on the same or different systems and are secured and logically isolated from each other, which ensures security and isolation of the control path when running multiple Tenants simultaneously on the shared infrastructure. Tenant Units can contain one or more *MTrees*, which hold all configuration elements that are needed in a multi-tenancy setup. Users, management-groups, notification-groups, and other configuration elements are part of a Tenant Unit.

## Control path and network isolation

*Control path isolation* is achieved by providing the user roles of *tenant-admin* and *tenant-user* for a Tenant Unit. *Network isolation* for data and administrative access is achieved by associating a fixed set of *data access IP address(es)* and *management IP address(es)* with a Tenant Unit.

The *tenant-admin* and *tenant-user* roles are restricted in scope and capability to specific Tenant Units and to a restricted set of operations they can perform on those Tenant Units. To ensure a logically secure and isolated data path, a system administrator must configure one or more Tenant Unit MTrees for each protocol in an SMT environment. Supported protocols include DD Boost, NFS, CIFS, and DD VTL. Access is strictly regulated by the native access control mechanisms of each protocol.

*Tenant-self-service sessions* (through ssh) can be restricted to a fixed set of *management IP address(es)* on a DD system. Administrative access sessions (through ssh/http/https) can also be restricted to a fixed set of management IP address(es) on DD systems. By default, however, there are no management IP address(es) associated with a Tenant Unit, so the only standard restriction is through the use of the *tenant-admin* and *tenant-user* roles. You must use `smt tenant-unit management-ip` to add and maintain management IP address(es) for Tenant Units.

Similarly, data access and data flow (into and out of Tenant Units) can be restricted to a fixed set of local or remote *data access IP address(es)*. The use of assigned data access IP address(es)

enhances the security of the DD Boost and NFS protocols by adding SMT-related security checks. For example, the list of storage units returned over DD Boost RPC can be limited to those which belong to the Tenant Unit with the assigned local data access IP address. For NFS, access and visibility of exports can be filtered based on the local data access IP address(es) configured. For example, using `showmount -e` from the local data access IP address of a Tenant Unit will only display NFS exports belonging to that Tenant Unit.

The *sysadmin* must use `smt tenant-unit data-ip` to add and maintain data access IP address(es) for Tenant Units.

**i** Note: If you attempt to mount an MTree in an SMT using a non-SMT IP address, the operation will fail.

If multiple Tenant Units are belong to the same tenant, they can share a default gateway. However, if multiple Tenant Units that belong to different tenants are opevented from using the same default gateway.

Multiple Tenant Units belonging to the same tenant can share a default gateway. Tenant Units that belong to different tenants cannot use the same default gateway.

## Understanding RBAC in SMT

In Secure Multi-Tenancy (SMT), permission to perform a task depends on the role that is assigned to a user. DDMC uses role-based access control (RBAC) to control these permissions.

All DDMC users can:

- View all tenants
- Create, read, update, or delete tenant units belonging to any tenant if the user is an administrator on the protection system hosting the tenant unit
- Assign and unassign tenant units to and from a tenant if the user is an administrator on the system hosting the tenant unit
- View tenant units belonging to any tenant if the user has any assigned role on the system hosting the tenant unit

To perform more advanced tasks depends on the role of the user, as follows:

### admin role

A user with an *admin* role can perform all administrative operations on a protection system. An *admin* can also perform all SMT administrative operations on the system, including setting up SMT, assigning SMT user roles, enabling tenant self-service mode, creating a tenant, and so on. In the context of SMT, the *admin* is typically referred to as the *landlord*. In DD OS, the role is known as the *sysadmin*.

To have permission to edit or delete a tenant, you must be both a DDMC *admin* and a DD OS *sysadmin* on all systems that are associated with the tenant units of that tenant. If the tenant does not have any tenant units, you need only to be a DDMC *admin* to edit or delete that tenant.

### limited-admin role

A user with a *limited-admin* role can perform all administrative operations on a system as the *admin*. However, users with the *limited-admin* role cannot delete or destroy MTrees. In DD OS, there is an equivalent *limited-admin* role.

### tenant-admin role

A user with a *tenant-admin* role can perform certain tasks only when *tenant self-service* mode is enabled for a specific tenant unit. Responsibilities include scheduling and running a backup application for the tenant and monitoring resources and statistics within the assigned tenant unit. The *tenant-admin* can view audit logs, but RBAC ensures that only audit logs from the tenant units belonging to the *tenant-admin* are accessible. In addition, *tenant-admins* ensure administrative

separation when tenant self-service mode is enabled. In the context of SMT, the *tenant-admin* is referred to as the *backup admin*.

#### tenant-user role

A user with a *tenant-user* role can monitor the performance and usage of SMT components only on tenant unit(s) assigned to them and only when tenant self-service is enabled, but a user with this role cannot view audit logs for their assigned tenant units. Also, *tenant-users* may run the `show` and `list` commands.

#### none role

A user with a role of *none* is not allowed to perform any operations on a system other than changing their password and accessing data using DD Boost. However, after SMT is enabled, the *admin* can select a user with a *none* role from the system and assign them an SMT-specific role of *tenant-admin* or *tenant-user*. Then, that user can perform operations on SMT management objects.

#### management groups

BSPs (backup service providers) can use *management groups* defined in a single, external AD (active directory) or NIS (network information service) to simplify managing user roles on tenant units. Each BSP tenant may be a separate, external company and may use a name-service such as AD or NIS.

With SMT management groups, the AD and NIS servers are set up and configured by the *admin* in the same way as SMT local users. The *admin* can ask their AD or NIS administrator to create and populate the group. The *admin* then assigns an SMT role to the entire group. Any user within the group who logs in to the system is logged in with the role that is assigned to the group.

When users leave or join a tenant company, they can be removed or added to the group by the AD or NIS administrator. It is not necessary to modify the RBAC configuration on a system when users who are part of the group are added or removed.

## Provisioning a Tenant Unit

Launching the configuration wizard begins the initial provisioning procedure for Secure Multitenancy (SMT). During the procedure, the wizard creates and provisions a new Tenant Unit based on Tenant configuration requirements. Information is entered by the administrator, as prompted. After completing the procedure, the administrator proceeds to the next set of tasks, beginning with enabling Tenant Self-Service mode. Following the initial setup, manual procedures and configuration modifications can be performed as required.

#### Procedure

1. Start SMT.
 

```
# smt enable
SMT enabled.
```
2. Verify that SMT is enabled.
 

```
# smt status
SMT is enabled.
```
3. Launch the SMT configuration wizard.
 

```
# smt tenant-unit setup
No tenant-units.
```
4. Follow the configuration prompts.

```
SMT TENANT-UNIT Configuration
```

```
Configure SMT TENANT-UNIT at this time (yes|no) [no]: yes
```

```
Do you want to create new tenant-unit (yes/no)? : yes
```



```

Tenant-unit Name
  Enter tenant-unit name to be created
  : SMT_5.7_tenant_unit
Invalid tenant-unit name.
  Enter tenant-unit name to be created
  : SMT_57_tenant_unit

Pending Tenant-unit Settings
Create Tenant-unit  SMT_57_tenant_unit

Do you want to save these settings (Save|Cancel|Retry): save
SMT Tenant-unit Name Configurations saved.

SMT TENANT-UNIT MANAGEMENT-IP Configuration

  Configure SMT TENANT-UNIT MANAGEMENT-IP at this time (yes|no) [no]: yes

  Do you want to add a local management ip to this tenant-unit? (yes|no) [no]: yes

port  enabled  state  DHCP          IP address          netmask          type  additional
-----  -
ethMa  yes    running  no  192.168.10.57      255.255.255.0    n/a
      fe80::260:16ff:fe49:f4b0** /64
eth3a  yes    running  ipv4 192.168.10.236*   255.255.255.0*  n/a
      fe80::260:48ff:fe1c:60fc** /64
eth3b  yes    running  no  192.168.50.57      255.255.255.0    n/a
      fe80::260:48ff:fe1c:60fd** /64
eth4b  yes    running  no  192.168.60.57      255.255.255.0    n/a
      fe80::260:48ff:fe1f:5183** /64
-----  -
* Value from DHCP
** auto_generated IPv6 address

Choose an ip from above table or enter a new ip address. New ip addresses will need
to be created manually.

Ip Address
  Enter the local management ip address to be added to this tenant-unit
  : 192.168.10.57

  Do you want to add a remote management ip to this tenant-unit? (yes|no) [no]:

Pending Management-ip Settings

Add Local Management-ip  192.168.10.57
  Do you want to save these settings (Save|Cancel|Retry): yes
  unrecognized input, expecting one of Save|Cancel|Retry

  Do you want to save these settings (Save|Cancel|Retry): save
  Local management access ip "192.168.10.57" added to tenant-unit "SMT_57_tenant_unit".

SMT Tenant-unit Management-IP Configurations saved.

SMT TENANT-UNIT MANAGEMENT-IP Configuration

  Do you want to add another local management ip to this tenant-unit? (yes|no) [no]:

  Do you want to add another remote management ip to this tenant-unit? (yes|no) [no]:

SMT TENANT-UNIT DDBOOST Configuration
  Configure SMT TENANT-UNIT DDBOOST at this time (yes|no) [no]:

SMT TENANT-UNIT MTREE Configuration
  Configure SMT TENANT-UNIT MTREE at this time (yes|no) [no]: yes

Name          Pre-Comp (GiB)  Status  Tenant-Unit
-----
/data/coll/laptop_backup  4846.2  RO/RD  -

```

```

/data/coll/random          23469.9   RO/RD   -
/data/coll/software2      2003.7   RO/RD   -
/data/coll/tsm6           763704.9 RO/RD   -
-----
D   : Deleted
Q   : Quota Defined
RO  : Read Only
RW  : Read Write
RD  : Replication Destination
RLGE: Retention-Lock Governance Enabled
RLGD: Retention-Lock Governance Disabled
RLCE: Retention-Lock Compliance Enabled

Do you want to assign an existing MTree to this tenant-unit? (yes|no) [no]:
Do you want to create a mtree for this tenant-unit now? (yes|no) [no]: yes

MTree Name
Enter MTree name
: SMT_57_tenant_unit
Invalid mtree path name.
Enter MTree name
:
SMT_57_tenant_unit

Invalid mtree path name.
Enter MTree name
: /data/coll/SMT_57_tenant_unit

MTree Soft-Quota
Enter the quota soft-limit to be set on this MTree (<n> (MiB|GiB|TiB|PiB)|none)
:

MTree Hard-Quota
Enter the quota hard-limit to be set on this MTree (<n> (MiB|GiB|TiB|PiB)|none)
:

Pending MTree Settings
Create MTree      /data/coll/SMT_57_tenant_unit
MTree Soft Limit  none
MTree Hard Limit  none

Do you want to save these settings (Save|Cancel|Retry): save
MTree "/data/coll/SMT_57_tenant_unit" created successfully.
MTree "/data/coll/SMT_57_tenant_unit" assigned to tenant-unit "SMT_57_tenant_unit".

SMT Tenant-unit MTree Configurations saved.

SMT TENANT-UNIT MTREE Configuration

Name                Pre-Comp (GiB)   Status   Tenant-Unit
-----
/data/coll/laptop_backup  4846.2   RO/RD   -
/data/coll/random        23469.9   RO/RD   -
/data/coll/software2     2003.7   RO/RD   -
/data/coll/tsm6          763704.9   RO/RD   -
-----

D   : Deleted
Q   : Quota Defined
RO  : Read Only
RW  : Read Write
RD  : Replication Destination
RLGE: Retention-Lock Governance Enabled
RLGD: Retention-Lock Governance Disabled
RLCE: Retention-Lock Compliance Enabled

Do you want to assign another MTree to this tenant-unit? (yes|no) [no]: yes
Do you want to assign an existing MTree to this tenant-unit? (yes|no) [no]:

```



```

Do you want to create another mtree for this tenant-unit? (yes|no) [no]:
SMT TENANT-UNIT SELF-SERVICE Configuration
Configure SMT TENANT-UNIT SELF-SERVICE at this time (yes|no) [no]: yes
Self-service of this tenant-unit is disabled
Do you want to enable self-service of this tenant-unit? (yes|no) [no]: yes
Do you want to configure a management user for this tenant-unit? (yes|no) [no]:
Do you want to configure a management group for this tenant-unit (yes|no) [no]: yes
Management-Group Name
Enter the group name to be assigned to this tenant-unit
: SMT_57_tenant_unit_group
What role do you want to assign to this group (tenant-user|tenant-admin) [tenant-user]:
tenant-admin
Management-Group Type
What type do you want to assign to this group (nis|active-directory)?
: nis
Pending Self-Service Settings
Enable Self-Service      SMT_57_tenant_unit
Assign Management-group  SMT_57_tenant_unit_group
Management-group role   tenant-admin
Management-group type   nis
Do you want to save these settings (Save|Cancel|Retry): save
Tenant self-service enabled for tenant-unit "SMT_57_tenant_unit"
Management group "SMT_57_tenant_unit_group" with type "nis" is assigned to tenant-unit
"SMT_57_tenant_unit" as "tenant-admin".
SMT Tenant-unit Self-Service Configurations saved.
SMT TENANT-UNIT SELF-SERVICE Configuration
Do you want to configure another management user for this tenant-unit? (yes|no) [no]:
Do you want to configure another management group for this tenant-unit? (yes|no) [no]:
SMT TENANT-UNIT ALERT Configuration
Configure SMT TENANT-UNIT ALERT at this time (yes|no) [no]: yes
No notification lists.
Alert Configuration
Alert Group Name
Specify alert notify-list group name to be created
: SMT_57_tenant_unit_notify
Alert email addresses
Enter email address to receive alert for this tenant-unit
: dd_proserv@emc.com
Do you want to add more emails (yes/no)?
: no
Pending Alert Settings
Create Notify-list group  SMT_57_tenant_unit_notify
Add emails                dd_proserv@emc.com
Do you want to save these settings (Save|Cancel|Retry): save
Created notification list "SMT_57_tenant_unit_notify" for tenant "SMT_57_tenant_unit".
Added emails to notification list "SMT_57_tenant_unit_notify".

```

```
SMT Tenant-unit Alert Configurations saved.
```

```
Configuration complete.
```

## Enabling Tenant Self-Service mode

For administrative separation of duties and delegation of administrative/management tasks to implement Tenant Self-Service, which is required for control path isolation, the system administrator can enable this mode on a Tenant Unit and then assign users to manage the unit in the roles of tenant-admin or tenant-user. These roles allow users other than the administrator to perform specific tasks on the Tenant Unit to which they are assigned. In addition to administrative separation, Tenant Self-Service mode helps reduce the management burden on internal IT and service provider staff.

### Procedure

1. View Tenant Self-Service mode status for one or all Tenant Units.

```
# smt tenant-unit option show { tenant-unit | all }
```

2. Enable Tenant Self-Service mode on the selected Tenant Unit.

```
# smt tenant-unit option set tenant-unit self-service { enabled | disabled }
```

## Data access by protocol

Secure data paths, with protocol-specific access controls, enable security and isolation for Tenant Units. In a Secure Multitenancy (SMT) environment, data access protocol management commands are also enhanced with a Tenant Unit parameter to enable consolidated reporting.

DD systems support multiple data access protocols simultaneously, including DD Boost, NFS, CIFS, and DD VTL. A DD system can present itself as an application-specific interface, such as a file server offering NFS or CIFS access over the Ethernet, a DD VTL device, or a DD Boost device.

The native access control mechanisms of each supported protocol ensure that the data paths for each Tenant remain separate and isolated. Such mechanisms include access control lists (ACLs) for CIFS, exports for NFS, DD Boost credentials, and Multi-User Boost credential-aware access control.

## Multi-User DD Boost and Storage Units in SMT

When using Multi-User DD Boost with Secure Multi-Tenancy (SMT), user permissions are set by Storage Unit ownership.

*Multi-User DD Boost* refers to the use of multiple DD Boost user credentials for DD Boost Access Control, in which each user has a separate username and password.

A *Storage Unit* is an MTree configured for the DD Boost protocol. A user can be associated with, or "own," one or more Storage Units. Storage Units that are owned by one user cannot be owned by another user. Only the user owning the Storage Unit can access the Storage Unit for any type of data access, such as backup/restore. The number of DD Boost user names cannot exceed the maximum number of MTrees. (See the "MTrees" chapter in this book for the current maximum number of MTrees for each model.) Storage Units that are associated with SMT must have the *none* role that is assigned to them.

Each backup application must authenticate using its DD Boost username and password. After authentication, DD Boost verifies the authenticated credentials to confirm ownership of the Storage Unit. The backup application is granted access to the Storage Unit only if the user credentials that are presented by the backup application match the user names associated with

the Storage Unit. If user credentials and user names do not match, the job fails with a permission error.

## Configuring access for CIFS

Common Internet File System (CIFS) is a file-sharing protocol for remote file access. In a Secure Multitenancy (SMT) configuration, backup and restores require client access to the CIFS shares residing in the MTree of the associated Tenant Unit. Data isolation is achieved using CIFS shares and CIFS ACLs.

### Procedure

1. Create an MTree for CIFS and assign the MTree to the tenant unit.

```
# mtree create mtree-path tenant-unit tenant-unit
```

2. Set capacity soft and hard quotas for the MTree.

```
# mtree create mtree-path tenant-unit tenant-unit] [quota-soft-limit n(MiB|GiB|TiB|PiB) ] [quota-hard-limit n (MiB|GiB|TiB|PiB)
```

3. Create a CIFS share for *pathname* from the MTree.

```
# cifs share create share path pathname clients clients
```

## Configuring NFS access

NFS is a UNIX-based, file-sharing protocol for remote file access. In a Secure Multitenancy (SMT) environment, backup and restores require client access to the NFS exports residing in the MTree of the associated Tenant Unit. Data isolation is achieved using NFS exports and network isolation. NFS determines if an MTree is associated with a network-isolated Tenant Unit. If so, NFS verifies the connection properties associated with the Tenant Unit. Connection properties include the destination IP address and interface or client hostname.

### Procedure

1. Create an MTree for NFS and assign the MTree to the tenant unit.

```
# mtree create mtree-path tenant-unit tenant-unit
```

2. Set capacity soft and hard quotas for the MTree.

```
# mtree create mtree-path tenant-unit tenant-unit] [quota-soft-limit n(MiB|GiB|TiB|PiB) ] [quota-hard-limit n (MiB|GiB|TiB|PiB)
```

3. Create an NFS export by adding one or more clients to the MTree.

```
# nfs add path client-list
```

## Configuring access for DD VTL

DD VTL Tenant data isolation is achieved using DD VTL access groups that create a virtual access path between a host system and the DD VTL. (The physical Fibre Channel connection between the host system and DD VTL must already exist.)

Placing tapes in the DD VTL allows them to be written to, and read by, the backup application on the host system. DD VTL tapes are created in a DD VTL pool, which is an MTree. Because DD VTL pools are MTrees, the pools can be assigned to Tenant Units. This association enables SMT monitoring and reporting.

For example, if a tenant-admin is assigned a Tenant Unit that contains a DD VTL pool, the tenant-admin can run MTree commands to display read-only information. Commands can run only on the DD VTL pool assigned to the Tenant Unit.

These commands include:

- `mtree list` to view a list of MTrees in the Tenant Unit

- `mtree show compression` to view statistics on MTree compression
- `mtree show performance` to view statistics on performance

Output from most `list` and `show` commands include statistics that enable service providers to measure space usage and calculate chargeback fees.

DD VTL operations are unaffected and continue to function normally.

## Using DD VTL NDMP TapeServer

DD VTL Tenant data isolation is also achieved using NDMP. DD OS implements a NDMP (Network Data Management Protocol) tape server that allows NDMP-capable systems to send backup data to the DD system via a three-way NDMP backup.

The backup data is written to virtual tapes (which are in a pool) by a DD VTL assigned to the special DD VTL group *TapeServer*.

Because the backup data is written to tapes in a pool, information in the DD VTL topic regarding MTrees also applies to the DD NDMP TapeServer.

## Data management operations

Secure Multitenancy (SMT) management operations include monitoring Tenant Units and other objects, such as Storage Units and MTrees. For some SMT objects, additional configuration or modification may also be required.

### Collecting performance statistics

Each MTree can be measured for performance or “usage” statistics and other real-time information. Historical consumption rates are available for DD Boost Storage Units. Command output lets the tenant-admin collect usage statistics and compression ratios for an MTree associated with a Tenant Unit, or for all MTrees and associated Tenant Units. Output may be filtered to display usage in intervals ranging from minutes to months. Results are passed to the administrator, who uses the statistics as a chargeback metric. A similar method is used to gather usage statistics and compression ratios for Storage Units.

#### Procedure

1. Collect MTree real-time performance statistics.  
# `mtree show stats`
2. Collect performance statistics for MTrees associated with a Tenant Unit.  
# `mtree show performance`
3. Collect compression statistics for MTrees associated with a Tenant Unit.  
# `mtree show compression`

### Modifying quotas

To meet GoS criteria, a system administrator uses DD OS “knobs” to adjust the settings required by the Tenant configuration. For example, the administrator can set “soft” and “hard” quota limits on DD Boost Storage Units. Stream “soft” and “hard” quota limits can be allocated only to DD Boost Storage Units assigned to Tenant Units. After the administrator sets the quotas, the tenant-admin can monitor one or all Tenant Units to ensure no single object exceeds its allocated quotas and deprives others of system resources.

**About this task**

Quotas are set initially when prompted by the configuration wizard, but they can be adjusted or modified later. The example below shows how to modify quotas for DD Boost. (You can also use `quota capacity` and `quota streams` to deal with capacity and stream quotas and limits.)

**Procedure**

1. To modify soft and hard quota limits on DD Boost Storage Unit "su33":
 

```
ddboost storage-unit modify su33 quota-soft-limit 10 Gib quota-hard-limit 20 Gib
```
2. To modify stream soft and hard limits on DD Boost Storage Unit "su33":
 

```
ddboost storage-unit modify su33 write-stream-soft-limit 20 read-stream-soft-limit 6 repl -stream-soft-limit 20 combined-stream-soft-limit 20
```
3. To report physical size for DD Boost Storage Unit "su33":
 

```
ddboost storage-unit modify su33 report-physical-size 8 GiB
```

**SMT and replication**

In case of disaster, user roles dictate how a user can assist in data recovery operations. Several replication types are available in an SMT configuration. (See the *DD Replicator* chapter for more detail on how to perform replication.)

Here are some points to consider regarding user roles:

- The admin can recover MTrees from a replicated copy.
- The tenant-admin can replicate MTrees from one system to another, using DD Boost managed file replication.
- The tenant-admin can recover MTrees from a replicated copy, also by using DD Boost managed file replication.

**Collection replication**

Collection replication replicates core Tenant Unit configuration information.

**Secure replication over public internet**

To protect against man-in-the-middle (MITM) attacks when replicating over a public internet connection, authentication includes validating SSL certificate-related information at the replication source and destination.

**MTree replication (NFS/CIFS)**

MTree replication is supported on MTrees assigned to Tenant Units. During MTree replication, an MTree assigned to a Tenant Unit on one system can be replicated to an MTree assigned to a Tenant Unit on another system. MTree replication is not allowed between two different Tenants on the two DD systems. When security mode is set to *strict*, MTree replication is allowed only when the MTrees belong to same Tenants.

For backward compatibility, MTree replication from an MTree assigned to a Tenant Unit to an unassigned MTree is supported, but must be configured manually. Manual configuration ensures the destination MTree has the correct settings for the Tenant Unit. Conversely, MTree replication from an unassigned MTree to an MTree assigned to a Tenant Unit is also supported.

When setting up SMT-aware MTree replication, *security mode* defines how much checking is done on the Tenant. The *default* mode checks that the source and destination do not belong to different Tenants. The *strict* mode makes sure the source and destination belong to the same Tenant. Therefore, when you use strict mode, you must create a Tenant on the destination machine with the same UUID as the UUID of the Tenant on the source machine that is associated with the MTree being replicated.



### DD Boost managed file replication (also with DD Boost AIR)

DD Boost managed file replication is supported between Storage Units, regardless of whether one Storage Unit, or both, are assigned to Tenant Units.

During DD Boost managed file replication, Storage Units are not replicated in total. Instead, certain files within a Storage Unit are selected by the backup application for replication. The files selected in a Storage Unit and assigned to a Tenant Unit on one system can be replicated to a Storage Unit assigned to a Tenant Unit on another system.

For backward compatibility, selected files in a Storage Unit assigned to a Tenant Unit can be replicated to an unassigned Storage Unit. Conversely, selected files in an unassigned Storage Unit can be replicated to a Storage Unit assigned to a Tenant Unit.

DD Boost managed file replication can also be used in DD Boost AIR deployments.

#### Replication control for QoS

An upper limit on replication throughput (`repl-in`) can be specified for an MTree. Since MTrees for each tenant are assigned to a Tenant Unit, each tenant's replication resource usage can be capped by applying these limits. The relation of this feature to SMT is that MTree Replication is subject to this throughput limit.

## SMT Tenant alerts

A DD system generates *events* when it encounters potential problems with software or hardware. When an event is generated, an *alert* notification is sent immediately via email to members designated in the notification list and to the system administrator.

SMT alerts are specific to each Tenant Unit and differ from DD system alerts. When Tenant Self-Service mode is enabled, the tenant-admin can choose to receive alerts about the various system objects he or she is associated with and any critical events, such as an unexpected system shutdown. A tenant-admin may only view or modify notification lists to which he or she is associated.

The example below shows a sample alert. Notice that the two event messages at the bottom of the notification are specific to a Multi-Tenant environment (indicated by the word "Tenant"). For the entire list of DD OS and SMT alerts, see the *DD OS MIB Quick Reference Guide* or the SNMP MIB.

```
EVT-ENVIRONMENT-00021 - Description: The system has been shutdown by abnormal method; for example, not by one of the following: 1) Via IPMI chassis control command 2) Via power button 3) Via OS shutdown.
```

```
Action: This alert is expected after loss of AC (main power) event. If this shutdown is not expected and persists, contact your contracted support provider or visit us online at https://my.datadomain.com.
```

```
Tenant description: The system has experienced an unexpected power loss and has restarted.
```

```
Tenant action: This alert is generated when the system restarts after a power loss. If this alert repeats, contact your System Administrator.
```

## Managing snapshots

A *snapshot* is a read-only copy of an MTree captured at a specific point in time. A snapshot can be used for many things, for example, as a restore point in case of a system malfunction. The required role for using `snapshot` is `admin` or `tenant-admin`.

To view snapshot information for an MTree or a Tenant Unit:

```
# snapshot list mtree mtree-path | tenant-unit tenant-unit
```

To view a snapshot schedule for an MTree or a Tenant Unit:

```
# snapshot schedule show [name | strees stree-listmtree-list | tenant-unit  
tenant-unit]
```

## Performing a file system Fast Copy

A Fast Copy operation clones files and directory trees of a source directory to a target directory on a DD system. There are special circumstances regarding Fast Copy with Secure Multitenancy (SMT).

Here are some considerations when performing a file system Fast Copy with Tenant Self-Service mode enabled:

- A tenant-admin can Fast Copy files from one Tenant Unit to another when the tenant-admin is the tenant-admin for both Tenant Units, and the two Tenant Units belong to the same Tenant.
- A tenant-admin can Fast Copy files within the same Tenant Unit.
- A tenant-admin can Fast Copy files within the Tenant Units at source and destination.

To perform a file system Fast Copy:

```
# filesys fastcopy source <src> destination <dest>
```



# CHAPTER 18

## Cloud Tier

This chapter includes:

• Cloud Tier overview.....	442
• Configuring Cloud Tier.....	445
• Configuring cloud units.....	446
• Data movement.....	458
• Using the CLI to configure Cloud Tier.....	461
• Configuring encryption for DD cloud units.....	465
• Information needed in the event of system loss.....	465
• Using DD Replicator with Cloud Tier.....	466
• Using DD Virtual Tape Library (VTL) with Cloud Tier.....	466
• Displaying capacity consumption charts for Cloud Tier.....	466
• Cloud Tier logs.....	467
• Using the CLI to remove Cloud Tier.....	467

## Cloud Tier overview

Cloud Tier is a native feature of DD OS 6.0 (or later) for moving data from the active tier to low-cost, high-capacity object storage in the public, private, or hybrid cloud for long-term retention. Cloud Tier is best suited for long-term storage of infrequently accessed data that is being held for compliance, regulatory, and governance reasons. The ideal data for Cloud Tier is data that is past its normal recovery window.

Cloud Tier is managed using a single protection system namespace. There is no separate cloud gateway or virtual appliance required. Data movement is supported by the native policy management framework. Conceptually, the cloud storage is treated as an additional storage tier (Cloud Tier) attached to the system, and data is moved between tiers as needed. File system metadata associated with the data stored in the cloud is maintained in local storage, and also mirrored to the cloud. The metadata that resides in local storage facilitates operations such as deduplication, cleaning, Fast Copy, and replication. This local storage is divided into self-contained buckets, called cloud units, for ease of manageability.

## Supported platforms

Cloud Tier is supported on physical platforms that have the necessary memory, CPU, and storage connectivity to accommodate another storage tier.

Cloud Tier is supported on these systems:

**Table 195** Cloud Tier supported configurations

Model	Memory	Cloud capacity	Required number of SAS I/O modules	Supported disk shelf types for metadata storage	Number of ES30 shelves, ES40 shelves, or DS60 disk packs required	Required capacity for metadata storage
DD3300 4 TB	16 GB	8 TB	N/A	N/A	N/A	1 x 1 TB virtual disk = 1 TB
DD3300 8 TB	48 GB	16 TB	N/A	N/A	N/A	2 x 1 TB virtual disks = 2 TB
DDD3300 16 TB	48 GB	32 TB	N/A	N/A	N/A	2 x 1 TB virtual disks = 2 TB
DD3300 32 TB	64 GB	64 TB	N/A	N/A	N/A	4 x 1 TB virtual disks = 4 TB
DD6800	192 GB	576 TB	2	DS60 or ES30	2	30 x 4 TB HDDs = 120 TB
DD6900	288 GB	576 TB	2	DS60, ES40, or ES30 <sup>a</sup>	2	30 x 4 TB HDDs = 120 TB

Table 195 Cloud Tier supported configurations (continued)

Model	Memory	Cloud capacity	Required number of SAS I/O modules	Supported disk shelf types for metadata storage	Number of ES30 shelves, ES40 shelves, or DS60 disk packs required	Required capacity for metadata storage
DD9300	384 GB	1400 TB	2	DS60 or ES30	4	60 x 4 TB HDDs = 240 TB
DD9400	576 GB	1536 TB	2	DS60, ES40, or ES30 <sup>a</sup>	4	60 x 4 TB HDDs = 240 TB
DD9500	512 GB	1728 TB	4	DS60 or ES30	5	75 x 4 TB HDDs = 300 TB
DD9800	768 GB	2016 TB	4	DS60 or ES30	5	75 x 4 TB HDDs = 300 TB
DD9900	1152 GB	2016 TB	2	DS60, ES40, or ES30 <sup>a</sup>	5	75 x 4 TB HDDs = 300 TB
DDVE 16 TB	32 GB	32 TB	N/A	N/A	N/A	1 x 500 GB virtual disk = 500 GB <sup>b</sup>
DDVE 64 TB	60 GB	128 TB	N/A	N/A	N/A	1 x 500 GB virtual disk = 500 GB <sup>b</sup>
DDVE 96 TB	80 GB	192 TB	N/A	N/A	N/A	1 x 500 GB virtual disk = 500 GB <sup>b</sup>

- a. ES30 shelves are only supported after a controller upgrade from an older system model.
- b. The minimum metadata size is a hard limit. Dell EMC recommends that you start with 1 TB for metadata storage and expand in 1 TB increments. The *DDVE Installation and Administration Guide* provides more details about using Cloud Tier with DDVE.

- ⓘ Note: Cloud Tier is not supported on any system that is not listed and is configured with Collection Replication.
- ⓘ Note: The Cloud Tier feature may consume all available bandwidth in a shared WAN link, especially in a low bandwidth configuration (1 Gbps), and this may impact other applications sharing the WAN link. If there are shared applications on the WAN, the use of QoS or other network limiting is recommended to avoid congestion and ensure consistent performance over time.  
If bandwidth is constrained, the rate of data movement will be slow and you will not be able to move as much data to the cloud. It is best to use a dedicated link for data going to the Cloud Tier.

- ⓘ Note: Do not send traffic over onboard management network interface controllers (ethMx interfaces).

## Cloud Tier performance

The system uses internal optimizations to maximize Cloud Tier performance.

### Cloud seeding

The current migration engine to cloud is file based and an efficient de-duplication optimized engine is used for identifying and migrating only unique segments to cloud. This file based migration engine's efficiency is high when migrating higher generation data to Cloud Tier, which already has some data to de-duplicate against. However, when Cloud Tier is empty or nearly empty, there is no data to de-duplicate against. There is an overhead of compute cycles that are invested in deduplication. With seeding-based migration, the deduplication filtering is maintained on active tier storage and only unique data is migrated in bulk to Cloud Tier. In cloud seeding, the engine migrates the content from local storage to cloud storage without processing it for deduplication. When cloud seeding is active, files that are marked for migration to cloud storage are not cleaned (i.e. space is not freed-up) as part of the active tier file system cleaning until the migration of all identified files by seeding is complete. Active tier storage must be sized to account for this in environments where large amounts of data are migrated to cloud storage. If the Cloud Tier storage is less than five percent full and has post-comp data usage of 30 TiB (or more), as seen in `filesys show space` command, the system automatically uses cloud seeding when migrating data to cloud storage.

After five percent of the Cloud Tier capacity is consumed, cloud seeding automatically deactivates. Data is then processed for deduplication before migration to cloud storage.

Here are additional points to consider when using Seeding migration:

- Migration is supported in Seeding mode only when:
  - Active tier postcomp used size is 30 TiB or more as reported in `filesys show space` output.
  - Active tier is less than 70% full, when migration starts as reported in `filesys show space` output.
- ⓘ Note: While in seeding mode, if Active Tier usage during a migration cycle exceeds 90%, migration is halted and restarted in regular Filecopy mode.
- Migration in seeding mode is auto-suspended by cleaning on active tier, for the entire duration of the active tier cleaning. Once cleaning completes, seeding resumes automatically and restarts the migration to cloud.
- Migration in seeding mode auto-suspends if a cloud UNAVAIL event is received on the cloud-unit (cloud-unit is reported as "disconnected") to which it is migrating, and only resumes once the cloud-unit is available reports as active.
- Cleaning cannot start on a cloud-unit that is the destination of an in-progress migration operation in Seeding mode.
  - ⓘ Note: In two cloud-unit systems, to force cleaning to start on a second cloud-unit which is not being seeded, suspend migration in seeding mode using the `data-movement suspend` command and run the `cloud clean start` command on the second cloud-unit.
- Probabilistic File Verification in cloud does not run against cloud-units on which seeding mode migration is in progress, even if it is the default policy.
- If cleaning is in progress on Active Tier or Cloud Tier and scheduled data movement starts in seeding mode, the data movement operation suspends for the duration of the cleaning activity.
- Migration in seeding mode does not migrate files from MTrees which are replication destinations, even if the files are eligible for migration. Files from these replication destination

MTrees are migrated with the Filecopy engine once migration in seeding mode from all eligible MTree is complete.

- Seeding mode migration suspends physical capacity reporting for the duration of the migration activity.
- Migration in Seeding mode is only supported on all cloud enabled systems and configurations that have more than 80 Gb of RAM. Seeding based migration is disabled by default for DD VEs.

#### Large object size

Cloud Tier uses object sizes of 1 MB or 4 MB (depending on the cloud storage provider) to reduce the metadata overhead, and lower the number of objects to migrate to cloud storage.

## Configuring Cloud Tier

To configure Cloud Tier, add the license and enclosures, set a system passphrase, and create a file system with support for data movement to the cloud.

- For Cloud Tier, the cloud capacity license is required.
- To license Cloud Tier, refer to the applicable *DD OS Release Notes* for the most up-to-date information on product features, software updates, software compatibility guides, and information about protection products, licensing, and service.
- To set a system passphrase, use the **Administration > Access > Administrator Access** tab. If the system passphrase is not set, the **Set Passphrase** button appears in the Passphrase area. If a system passphrase is configured, the **Change Passphrase** button appears, and your only option is to change the passphrase.
- To create a file system, use the File System Create Wizard.

## Configuring storage for Cloud Tier

Cloud Tier storage is required for the DD system to support cloud-units. The Cloud Tier holds the metadata for the migrated files, while the actual data resides in the cloud.

#### Before you begin


The file system must be disabled to configure Cloud Tier.

#### Procedure

1. Select **Data Management > File System** and click **Disable** (at the bottom of the screen) to disable the file system.
2. Select **Hardware > Storage**.
3. In the Overview tab, expand **Cloud Tier**.
4. Click **Configure**.

The Configure Cloud Tier dialog box is displayed.

5. Select the checkbox for the shelf to be added from the Addable Storage section.

 **CAUTION** DD3300 systems require the use of 1 TB storage devices for Cloud Tier metadata storage.

6. Click the **Add to Tier** button.
7. Click **Save** to add the storage.
8. Select **Data Management > File System** and click **Enable Cloud Tier**.

To enable the cloud tier, you must meet the storage requirement for the licensed capacity. Configure the cloud tier of the file system. Click **Next**.

A cloud file system requires a local store for a local copy of the cloud metadata.

9. Click **Enable**.

The cloud tier is enabled with the designated storage.

10. Click **OK**.

You must create cloud units separately, after the file system is enabled.

11. Select **Enable file system**.

## Cleanable Space Estimation

The Cleanable Space Estimation tool assesses the amount of space that can be reclaimed on the Active Tier when the data-movement process migrates eligible files to the cloud and GC cleans the file system.

This tool can work with or without a cloud license present.

When there is no active CLOUDTIER-CAPACITY license, manually provide the age-threshold to use to assess total cleanable space on the active tier. If there is both an age-threshold and there is a policy set on MTrees, the preference is given to the user provided age-threshold.

There are three workflows:

- A system with cloud migration policies set: Files are identified as "eligible" based on the policy set on the respective MTrees and calculates the cleanable space.
- A system with cloud migration policies set but with a user provided age-threshold: Files are identified based on the user given age-threshold, overriding the system policies.
- A system with no cloud: Mandatory requirement for user to provide an age-threshold which would be used to determine total cleanable space.

Some additional points to consider:

- Data-movement cannot run in parallel with the data-movement eligibility-check process.
- Cleaning on Active Tier cannot be started if the eligibility-check is running.
- The eligibility-check cannot start if cleaning on the Active Tier is running.
- Cleaning on Cloud Tier cannot be started if the eligibility-check is running.
- The eligibility-check cannot start if cleaning on the Cloud Tier is running.
- If an UNAVAIL event is received, it should not have any impact on the eligibility-check operation.
- If the file system stops or crashes, eligibility-check stops and does not auto-resume once file system comes back up again.

- ① **Note:** There is no provision for initiating the eligibility-check from DD System Manager.

## Configuring cloud units

The cloud tier consists of a maximum of two cloud units, and each cloud unit is mapped to a cloud provider, enabling multiple cloud providers per protection system. The system must be connected to the cloud and have an account with a supported cloud provider.

Configuring cloud units includes these steps:

- Configuring the network, including firewall and proxy settings
- Importing CA certificates
- Adding cloud units



## Firewall and proxy settings

### Network firewall ports

- Port 443 (HTTPS) and/or Port 80 (HTTP) must be open to the cloud provider networks for both the endpoint IP and the provider authentication IP for bi-directional traffic. For example, for Amazon S3, both `s3-ap-southeast-1.amazonaws.com` and `s3.amazonaws.com` must have port 80 and/or port 443 unblocked and set to allow bi-directional IP traffic.
  - ① Note: Several public cloud providers use IP ranges for their endpoint and authentication addresses. In this situation, the IP ranges used by the provider need to be unblocked to accommodate potential IP changes.
- Remote cloud provider destination IP and access authentication IP address ranges must be allowed through the firewall.
- For ECS private cloud, local ECS authentication and web storage (S3) access IP ranges and ports 9020 (HTTP) and 9021 (HTTPS) must be allowed through local firewalls.
  - ① Note: ECS private cloud load balancer IP access and port rules must also be configured.

### Proxy settings

If there are any existing proxy settings that cause data above a certain size to be rejected, those settings must be changed to allow object sizes up to 4.5MB.

If customer traffic is being routed through a proxy, the self-signed/CA-signed proxy certificate must be imported. See "Importing CA certificates" for details.

### OpenSSL cipher suites

- Ciphers - ECDHE-RSA-AES256-SHA384, AES256-GCM-SHA384
- TLS Version: 1.2
- ① Note: Default communication with all cloud providers is initiated with strong cipher.

### Supported protocols

- HTTP
- HTTPS
- ① Note: Default communication with all public cloud providers occurs on secure HTTP (HTTPS), but you can overwrite the default setting to use HTTP.

## Importing CA certificates

Before you can add cloud units for Alibaba, Amazon Web Services S3 (AWS), Azure, Elastic Cloud Storage (ECS), and Google Cloud Provider (GCP), you must import CA certificates.

### Before you begin

For AWS and Azure public cloud providers, root CA certificates can be downloaded from <https://www.digicert.com/digicert-root-certificates.htm>.

- For an AWS cloud provider, download the Baltimore CyberTrust Root certificate.
- For an Azure cloud provider, download the Baltimore CyberTrust Root certificate.
- For ECS, the root certificate authority varies by customer. Implementing cloud storage on ECS requires a load balancer. If an HTTPS endpoint is used as an endpoint in the configuration, be sure to import the root CA certificate. Contact your load balancer provider for details.



- For an S3 Flexible provider, import the root CA certificate. Contact your S3 Flexible provider for details.

If your downloaded certificate has a .crt extension, it is likely that it will need to be converted to a PEM-encoded certificate. If so, use OpenSSL to convert the file from .crt format to .pem (for example, `openssl x509 -inform der -in BaltimoreCyberTrustRoot.crt -out BaltimoreCyberTrustRoot.pem`).

- For Alibaba:
  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 system.
- For GCP:
  1. Download the GlobalSign Root R2 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 system.

#### Procedure

1. Select **Data Management > File System > Cloud Units**.
2. In the tool bar, click **Manage Certificates**.  
The Manage Certificates for Cloud dialog is displayed.
3. Click **Add**.
4. Select one of these options:
  - **I want to upload the certificate as a .pem file.**  
Browse to and select the certificate file.
  - **I want to copy and paste the certificate text.**
    - Copy the contents of the .pem file to your copy buffer.
    - Paste the buffer into the dialog.
5. Click **Add**.

## Adding a cloud unit for Elastic Cloud Storage (ECS)

#### About this task

A protection system or DDVE instance requires a close time synchronization with the ECS system to configure a DD cloud unit. Configuring NTP on the protection system or DDVE instance, and the ECS system addresses this issue.

#### Procedure

1. Select **Data Management > File System > Cloud Units**.
2. Click **Add**.  
The Add Cloud Unit dialog box appears.

3. Enter a name for this cloud unit. Only alphanumeric characters are allowed.

The remaining fields in the Add Cloud Unit dialog pertain to the cloud provider account.

4. For **Cloud provider**, select **EMC Elastic Cloud Storage (ECS)** from the list.
5. Enter the provider **Access key** as password text.
6. Enter the provider **Secret key** as password text.
7. Enter the provider **Endpoint** in this format: `http://<ip/hostname>:<port>`. If you are using a secure endpoint, use `https` instead.

**i** | Note: Implementing cloud storage on ECS requires a load balancer.

By default, ECS runs the S3 protocol on port 9020 for HTTP and 9021 for HTTPS. With a load balancer, these ports are sometimes remapped to 80 for HTTP and 443 for HTTPS, respectively. Check with your network administrator for the correct ports.

8. If an HTTP proxy server is required to get around a firewall for this provider, click **Configure for HTTP Proxy Server**.

Enter the proxy hostname, port, user, and password.

**i** | Note: There is an optional step to run the cloud provider verify tool before adding the cloud unit. This tool performs pre-check tests to ensure that all requirements are met before to adding the actual cloud unit.

9. Click **Add**.

The File System main window displays summary information for the new cloud unit as well a control for enabling and disabling the cloud unit.

## Adding a cloud unit for Alibaba

### About this task

Regions are configured at bucket level instead of object level. Therefore, all objects contained in a bucket are stored in the same region. A region is specified when a bucket is created, and cannot be changed once it is created.

**Table 196** Alibaba regions

Regions	Location	Region Name
Mainland China regions	China East 1 (Hangzhou)	oss-cn-hangzhou
	China East 2 (Shanghai)	oss-cn-shanghai
	China North 1 (Qingdao)	oss-cn-qingdao
	China North 2 (Beijing)	oss-cn-beijing
	China North 3 (zhangjiakou)	oss-cn-zhangjiakou
	China North 5 (huhehaote)	oss-cn-huhehaote
	China South 1 (Shenzhen)	oss-cn-shenzhen
International Regions	Hong Kong	oss-cn-hongkong
	US West 1 (Silicon Valley)	oss-us-west-1
	US East 1 (Virginia)	oss-us-east-1

Table 196 Alibaba regions (continued)

Regions	Location	Region Name
	Asia Pacific SE 1 (Singapore)	oss-ap-southeast-1
	Asia Pacific SE 2 (Sydney)	oss-ap-southeast-2
	Asia Pacific SE 3 (Kuala Lumpur)	oss-ap-southeast-3
	Asia Pacific SE 5 (Jakarta)	oss-ap-southeast-5
	Asia Pacific NE 1 (Tokyo)	oss-ap-northeast-1
	Asia Pacific SOU 1 (Mumbai)	oss-ap-south-1
	EU Central 1 (Frankfurt)	oss-eu-central-1
	Middle East 1 (Dubai)	oss-me-east-1

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 these are the minimum requirements:

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

#### Procedure

1. Select **Data Management > File System > Cloud Units**.
2. Click **Add**.  
The Add Cloud Unit dialog is displayed.
3. Enter a name for this cloud unit. Only alphanumeric characters are allowed.  
The remaining fields in the **Add Cloud Unit** dialog pertain to the cloud provider account.
4. For **Cloud provider**, select **Alibaba Cloud** from the drop-down list.
5. Select **Standard** or **IA** from the **Storage class** drop-down list.
6. Select the region from the **Storage region** drop-down list.
7. Enter the provider **Access key** as password text.
8. Enter the provider **Secret key** as password text.
9. Ensure that port 443 (HTTPS) is not blocked in firewalls. Communication with the Alibaba cloud provider occurs on port 443.
10. If an HTTP proxy server is required to get around a firewall for this provider, click **Configure for HTTP Proxy Server**.  
Enter the proxy hostname, port, user, and password.

- ① **Note:** There is an optional step to run the cloud provider verify tool before adding the cloud unit. This tool performs pre-check tests to ensure that all requirements are met before to adding the actual cloud unit.

11. Click **Add**.

The file system main window now displays summary information for the new cloud unit as well a control for enabling and disabling the cloud unit.

## Adding a cloud unit for Amazon Web Services S3

AWS offers a range of storage classes. The *Cloud Providers Compatibility Matrix*, available from <http://compatibilityguide.emc.com:8080/CompGuideApp/> provides up-to-date information about the supported storage classes.

### About this task

For enhanced security, the Cloud Tier feature uses Signature Version 4 for all AWS requests. Signature Version 4 signing is enabled by default.

The following endpoints are used by the AWS cloud provider, depending on storage class and region. Be sure that DNS is able to resolve these hostnames before configuring cloud units.

- s3.amazonaws.com
- s3-us-west-1.amazonaws.com
- s3-us-west-2.amazonaws.com
- s3-eu-west-1.amazonaws.com
- s3-ap-northeast-1.amazonaws.com
- s3-ap-southeast-1.amazonaws.com
- s3-ap-southeast-2.amazonaws.com
- s3-sa-east-1.amazonaws.com
- ap-south-1
- ap-northeast-2
- eu-central-1

- ① **Note:** The China region is not supported.

- ① **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 these are the minimum requirements:

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

### Procedure

1. Select **Data Management > File System > Cloud Units**.

2. Click **Add**.  
The Add Cloud Unit dialog is displayed.
3. Enter a name for this cloud unit. Only alphanumeric characters are allowed.  
The remaining fields in the Add Cloud Unit dialog pertain to the cloud provider account.
4. For **Cloud provider**, select **Amazon Web Services S3** from the drop-down list.
5. Select the storage class from the drop-down list.
6. Select the appropriate **Storage region** from the drop-down list.
7. Enter the provider **Access key** as password text.
8. Enter the provider **Secret key** as password text.
9. Ensure that port 443 (HTTPS) is not blocked in firewalls. Communication with the AWS cloud provider occurs on port 443.
10. If an HTTP proxy server is required to get around a firewall for this provider, click **Configure for HTTP Proxy Server**.

Enter the proxy hostname, port, user, and password.

**i** Note: There is an optional step to run the cloud provider verify tool before adding the cloud unit. This tool performs pre-check tests to ensure that all requirements are met before to adding the actual cloud unit.

11. Click **Add**.  
The file system main window now displays summary information for the new cloud unit as well a control for enabling and disabling the cloud unit.

## Adding a cloud unit for Azure

Microsoft Azure offers a range of storage account types. The *Cloud Providers Compatibility Matrix*, available from <http://compatibilityguide.emc.com:8080/CompGuideApp/> provides up-to-date information about the supported storage classes.

### About this task

The following endpoints are used by the Azure cloud provider, depending on storage class and region. Be sure that DNS is able to resolve these hostnames before configuring cloud units.

- `<account-name>.blob.core.windows.net`  
**i** Note: Do not include the domain `blob.core.windows.net` as part of the account name.

The account name is obtained from the Azure cloud provider console.

### Procedure

1. Select **Data Management > File System > Cloud Units**.
2. Click **Add**.  
The Add Cloud Unit dialog is displayed.
3. Enter a name for this cloud unit. Only alphanumeric characters are allowed.  
The remaining fields in the Add Cloud Unit dialog pertain to the cloud provider account.
4. For **Cloud provider**, select **Microsoft Azure Storage** from the drop-down list.
5. For **Account type**, select **Government** or **Public**.
6. Select the storage class from the drop-down list.

7. Enter the provider **Account name**.
8. Enter the provider **Primary key** as password text.
9. Enter the provider **Secondary key** as password text.
10. Ensure that port 443 (HTTPS) is not blocked in firewalls. Communication with the Azure cloud provider occurs on port 443.
11. If an HTTP proxy server is required to get around a firewall for this provider, click **Configure for HTTP Proxy Server**.

Enter the proxy hostname, port, user, and password.

**i** Note: There is an optional step to run the cloud provider verify tool before adding the cloud unit. This tool performs pre-check tests to ensure that all requirements are met before to adding the actual cloud unit.

12. Click **Add**.

The file system main window now displays summary information for the new cloud unit as well a control for enabling and disabling the cloud unit.

## Adding a cloud unit for Google Cloud Provider

### About this task

The following tables list the Cloud Storage locations available for storing data.

**Table 197** Multi-regional locations

Multi-regional name	Multi-regional description
Asia	Data centers in Asia
US	Data centers in the United States
EU	Data centers in the European Union

**Table 198** Regional locations

Regional locations	Location	Region name
North America	northamerica-northeast1	Montréal
	us-central1	Iowa
	us-east1	South Carolina
	us-east4	Northern Virginia
	us-west1	Oregon
South America	southamerica-east1	São Paulo
Europe	europa-north1	Finland
	europa-west1	Belgium
	europa-west2	London
	europa-west3	Frankfurt
	europa-west4	Netherlands

Table 198 Regional locations (continued)

Regional locations	Location	Region name
Asia	asia-east1	Taiwan
	asia-northeast1	Tokyo
	asia-south1	Mumbai
	asia-southeast1	Singapore
Australia	australia-southeast1	Sydney

The Google Cloud Provider 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

① **Note:**  
Cloud Tier only supports Nearline and is selected automatically during setup.

#### Procedure

1. Select **Data Management > File System > Cloud Units**.
2. Click **Add**.  
The Add Cloud Unit dialog is displayed.
3. Enter a name for this cloud unit. Only alphanumeric characters are allowed.  
The remaining fields in the **Add Cloud Unit** dialog pertain to the cloud provider account.
4. For **Cloud provider**, select **Google Cloud Storage** from the drop-down list.
5. Enter the provider **Access key** as password text.
6. Enter the provider **Secret key** as password text.
7. **Storage class** is set as **Nearline** by default.  
If a multi-regional location is selected (Asia, EU or US), then the storage class and the location constraint is Nearline Multi-regional. All other regional locations have the storage class set as Nearline Regional.
8. Select the **Region**.
9. Ensure that port 443 (HTTPS) is not blocked in firewalls. Communication with Google Cloud Provider occurs on port 443.
10. If an HTTP proxy server is required to get around a firewall for this provider, click **Configure for HTTP Proxy Server**.  
Enter the proxy hostname, port, user, and password.



- Note:** There is an optional step to run the cloud provider verify tool before adding the cloud unit. This tool performs pre-check tests to ensure that all requirements are met before adding the actual cloud unit.

11. Click **Add**.

The file system main window now displays summary information for the new cloud unit as well a control for enabling and disabling the cloud unit.

## Adding an S3 Flexible provider cloud unit

The Cloud Tier feature supports additional qualified S3 cloud providers under an S3 Flexible provider configuration option.

### About this task

The S3 Flexible provider option supports the standard and standard-infrequent-access storage classes. The endpoints will vary depending on cloud provider, storage class and region. Be sure that DNS is able to resolve these hostnames before configuring cloud units.

### Procedure

1. Select **Data Management > File System > Cloud Units**.
2. Click **Add**.  
The Add Cloud Unit dialog is displayed.
3. Enter a name for this cloud unit. Only alphanumeric characters are allowed.  
The remaining fields in the Add Cloud Unit dialog pertain to the cloud provider account.
4. For **Cloud provider**, select **Flexible Cloud Tier Provider Framework for S3** from the drop-down list.
5. Enter the provider **Access key** as password text.
6. Enter the provider **Secret key** as password text.
7. Specify the appropriate **Storage region**.
8. Enter the provider **Endpoint** in this format: `http://<ip/hostname>:<port>`. If you are using a secure endpoint, use `https` instead.
9. For **Storage class**, select the appropriate storage class from the drop-down list.
10. Ensure that port 443 (HTTPS) is not blocked in firewalls. Communication with the S3 cloud provider occurs on port 443.
11. If an HTTP proxy server is required to get around a firewall for this provider, click **Configure for HTTP Proxy Server**.

Enter the proxy hostname, port, user, and password.

- Note:** There is an optional step to run the cloud provider verify tool before adding the cloud unit. This tool performs pre-check tests to ensure that all requirements are met before adding the actual cloud unit.

12. Click **Add**.

The File System main window now displays summary information for the new cloud unit as well a control for enabling and disabling the cloud unit.

## Modifying a cloud unit or cloud profile

### About this task

Modify cloud unit credentials, an S3 Flexible provider name, or details of a cloud profile.

### Modifying cloud unit credentials

#### Procedure

1. Select **Data Management > File System > Cloud Units**.
2. Click the pencil icon for the cloud unit whose credentials you want to modify.  
The Modify Cloud Unit dialog is displayed.
3. For **Account name**, enter the new account name.
4. For **Access key**, enter the new provider access key as password text.  
① | **Note:** Modifying the access key is not supported for ECS environments.
5. For **Secret key**, enter the new provider secret key as password text.
6. For **Primary key**, enter the new provider primary key as password text.  
① | **Note:** Modifying the primary key is only supported for Azure environments.
7. If an HTTP proxy server is required to get around a firewall for this provider, click **Configure for HTTP Proxy Server**.
8. Click **OK**.

### Modifying an S3 Flexible provider name

#### Procedure

1. Select **Data Management > File System > Cloud Units**.
2. Click the pencil icon for the S3 Flexible cloud unit whose name you want to modify.  
The Modify Cloud Unit dialog is displayed.
3. For **S3 Provider Name**, enter the new provider name.
4. Click **OK**.

### Using the CLI to modify a cloud profile

#### Procedure

1. Run the `cloud profile modify` command to modify the details of a cloud profile. The system prompts you to modify individual details of the cloud profile.  
For AWS S3, or Azure profiles, run this command to add a storage class to an existing cloud profile.  
  
The profile details that can be modified depend on the cloud provider:
  - Alibaba Cloud supports modification of the access key, and secret key.
  - AWS S3 supports modification of the access key, and secret key.
  - Azure supports modification of the access key, secret key, and primary key.

- ECS supports modification of the secret key.
- S3 Flexible supports modification of the access key, secret key, and provider name.

## Deleting a cloud unit

This operation results in the loss of all data in the cloud unit selected for deletion. Be sure to delete all files before deleting the cloud units.

### Before you begin

- Check if data movement to the cloud is running (CLI command: `data-movement status`). If it is, stop data movement using the `data-movement stop` CLI command.
- Check if cloud cleaning is running for this cloud unit (CLI command: `cloud clean status`). If it is, stop cloud cleaning using the `cloud clean` CLI command.
- Check if a data movement policy is configured for this cloud unit (CLI command: `data-movement policy show`). If it is, remove this policy using the `data-movement policy reset` CLI command.

### Procedure

1. Use the following CLI command to identify files in the cloud unit.

```
# fileys report generate file-location
```

2. Delete the files that are in the cloud unit to be deleted.
3. Use the following CLI command to run cloud cleaning.

```
# cloud clean start unit-name
```

Wait for cleaning to complete. The cleaning may take time depending on how much data is present in the cloud unit.

4. Disable the file system.
5. Use the following CLI command to delete the cloud unit.

```
# cloud unit del unit-name
```

Internally, this marks the cloud unit as `DELETE_PENDING`.

6. Use the following CLI command to validate that the cloud unit is in the `DELETE_PENDING` state.

```
# cloud unit list
```

7. Enable the file system.

The file system initiates the procedure in the background to delete any remaining objects from the buckets in the cloud for this cloud unit and then delete the buckets. This process can take a long time, depending on how many objects were remaining in these buckets. Until the bucket cleanup completes, this cloud unit continues to consume a slot on the protection system, which may prevent creation of a new cloud unit if both slots are occupied.

8. Periodically check the state using this CLI command:

```
# cloud unit list
```

The state remains `DELETE_PENDING` while the background cleanup is running.

9. Verify from the cloud provider S3 portal that all corresponding buckets have been deleted and the associated space has been freed up.

10. If needed, reconfigure data movement policies for affected MTrees and restart data movement.

#### Results

If you have difficulty completing this procedure, contact Support.

## Data movement

Data is moved from the active tier to the cloud tier as specified by your individual data movement policy. The policy is set on a per-MTree basis. Data movement can be initiated manually or automatically using a schedule.

### Adding data movement policies to MTrees

A file is moved from the Active to the Cloud Tier based on the date it was last modified. For data integrity, the entire file is moved at this time. The *Data Movement Policy* establishes the file age threshold, age range, and the destination.

#### About this task

- ① Note: A data movement policy cannot be configured for the /backup MTree.

#### Procedure

1. Select **Data Management > MTree**.
2. In the top panel, select the MTree to which you want to add a data movement policy.
3. Click the **Summary** tab.
4. Under **Data Movement Policy** click **Add**.
5. For **File Age in Days**, set the file age threshold (**Older than**) and optionally, the age range (**Younger than**).

- ① Note: The minimum number of days for **Older than** is 14. For nonintegrated backup applications, files moved to the cloud tier cannot be accessed directly and need to be recalled to the active tier before you can access them. So, choose the age threshold value as appropriate to minimize or avoid the need to access a file moved to the cloud tier.

6. For **Destination**, specify the destination cloud unit.
7. Click **Add**.

### Moving data manually

You can start and stop data movement manually. Any MTree that has a valid data movement policy has its files moved.

#### Procedure

1. Select **Data Management > File System**.
2. At the bottom of the page, click **Show Status of File System Services**.

These status items are displayed:

- File System
- Physical Capacity Measurement
- Data Movement

- Active Tier Cleaning
3. For **Data Movement**, click **Start**.

## Moving data automatically

You can move data automatically, using a schedule and a throttle. Schedules can be daily, weekly, or monthly.

### Procedure

1. Select **Data Management > File System > Settings**.
2. Click the **Data Movement** tab.
3. Set the throttle and schedule.
  - ① **Note:** The throttle is for adjusting resources for internal system processes; it does not affect network bandwidth.
  - ① **Note:** If a cloud unit is inaccessible when cloud tier data movement runs, the cloud unit is skipped in that run. Data movement on that cloud unit occurs in the next run if the cloud unit becomes available. The data movement schedule determines the duration between two runs. If the cloud unit becomes available and you cannot wait for the next scheduled run, you can start data movement manually.

## Recalling a file from the Cloud Tier

For nonintegrated backup applications, you must recall the data to the active tier before you can restore the data. Backup administrators must trigger a recall or backup applications must perform a recall before cloud-based backups can be restored. Once a file is recalled, its aging is reset and starts again from 0, and the file is eligible based on the age policy set. A file can be recalled on the same MTree only. Integrated applications can restore a file directly.

### About this task

- ① **Note:** In an MTree replication context, the file is read-only on the destination MTree.
- ① **Note:** If a file resides only in a snapshot, it cannot be recalled directly. To recall a file in a snapshot, use fastcopy to copy the file from the snapshot back to the active MTree, then recall the file from the cloud. A file can only be recalled from the cloud to an active MTree.

### Procedure

1. Select **Data Management > File System > Summary**.
2. Do one of the following:
  - In the Cloud Tier section of the Space Usage panel, click **Recall**.
  - Expand the File System status panel at the bottom of the screen and click **Recall**.
    - ① **Note:** The **Recall** link is available only if a cloud unit is created and has data.
3. In the Recall File from Cloud dialog, enter the exact file name (no wildcards) and full path of the file to be recalled, for example: `/data/coll/mt11/file1.txt`. Click **Recall**.
4. To check the status of the recall, do one of the following:
  - In the Cloud Tier section of the Space Usage panel, click **Details**.
  - Expand the File System status panel at the bottom of the screen and click **Details**.

The Cloud File Recall Details dialog is displayed, showing the file path, cloud provider, recall progress, and amount of data transferred. If there are unrecoverable errors during the recall,

an error message is displayed. Hover the cursor over the error message to display a tool tip with more details and possible corrective actions.

### Results

Once the file has been recalled to the active tier, you can restore the data.

- ① **Note:** For nonintegrated applications, once a file has been recalled from the cloud tier to the active tier, a minimum of 14 days must elapse before the file is eligible for data movement. After 14 days, normal data movement processing will occur for the file. The file now has to wait the age-threshold or age-range to move back to the cloud as this time the ptime will be examined rather than the mtime. This restriction does not apply to integrated applications.
- ① **Note:** For data-movement, nonintegrated applications configure an age-based data movement policy on the protection system to specify which files get migrated to the cloud tier, and this policy applies uniformly to all files in an MTree. Integrated applications use an application-managed data movement policy, which lets you identify specific files to be migrated to the cloud tier.

## Using the CLI to recall a file from the cloud tier

For nonintegrated backup applications, you must recall the data to the active tier before you can restore the data. Backup administrators must trigger a recall or backup applications must perform a recall before cloud-based backups can be restored. Once a file is recalled, its aging is reset and will start again from 0, and the file will be eligible based on the age policy set. A file can be recalled on the source MTree only. Integrated applications can recall a file directly.

### About this task

- ① **Note:** If a file resides only in a snapshot, it cannot be recalled directly. To recall a file in a snapshot, use `fastcopy` to copy the file from the snapshot back to the active MTree, then recall the file from the cloud. A file can only be recalled from the cloud to an active MTree.

### Procedure

1. Check the location of the file using:

```
filesys report generate file-location [path {<path-name> / all}]
[output-file <filename>]
```

The pathname can be a file or directory; if it is a directory, all files in the directory are listed.

Filename	Location
/data/coll/mt11/file1.txt	Cloud Unit 1

2. Recall the file using:

```
data-movement recall path <path-name>
```

This command is asynchronous, and it starts the recall.

```
data-movement recall path /data/coll/mt11/file1.txt
Recall started for "/data/coll/mt11/file1.txt".
```

3. Monitor the status of the recall using

```
data-movement status [path {pathname | all | [queued] [running]
[completed] [failed]} | to-tier cloud | all]
```

```
data-movement status path /data/coll/mt11/file1.txt
Data-movement recall:
```

```
-----
Data-movement for "/data/coll/mt11/file1.txt": phase 2 of 3 (Verifying)
80% complete; time: phase XX:XX:XX total XX:XX:XX
Copied (post-comp): XX XX, [pre-comp] XX XX
```



If the status shows that the recall isn't running for a given path, the recall may have finished, or it may have failed.

4. Verify the location of the file using

```
filesystem report generate file-location [path (<path-name> | all)]
[output-file <filename>]
```

Filename	Location
-----	-----
/data/coll/mt11/file1.txt	Active

### Results

Once the file has been recalled to the active tier, you can restore the data.

- ① **Note:** For nonintegrated applications, once a file has been recalled from the cloud tier to the active tier, a minimum of 14 days must elapse before the file is eligible for data movement. After 14 days, normal data movement processing will occur for the file. This restriction does not apply to integrated applications.
- ① **Note:** For data-movement, nonintegrated applications configure an age-based data movement policy on the protection system to specify which files get migrated to the cloud tier, and this policy applies uniformly to all files in an MTree. Integrated applications use an application-managed data movement policy, which lets you identify specific files to be migrated to the cloud tier.

## Direct restore from the cloud tier

Direct restore lets nonintegrated applications read files directly from the cloud tier without going through the active tier.

Key considerations in choosing to use direct restore include:

- Direct restore does not require an integrated application and is transparent for nonintegrated applications.
- Reading from the cloud tier does not require copying first into the active tier.
- Histograms and statistics are available for tracking direct reads from the cloud tier.
- Direct restore is supported only for ECS cloud providers.
- Applications do experience cloud tier latency.
- Reading directly from the cloud tier is not bandwidth optimized.
- Direct restore supports a small number of jobs.

Direct restore is useful with nonintegrated applications that do not need to know about the cloud tier and won't need to restore cloud files frequently.

## Using the CLI to configure Cloud Tier

You can use the CLI to configure Cloud Tier.

### Procedure

1. Configure storage for both active and cloud tier. As a prerequisite, the appropriate capacity licenses for both the active and cloud tiers must be installed.
  - a. Ensure licenses for the features CLOUDTIER-CAPACITY and CAPACITY-ACTIVE are installed. To check the ELMS license:

```
# elicense show
```

If the license is not installed, use the `elicense update` command to install the license. Enter the command and paste the contents of the license file after this prompt. After



pastings, ensure there is a carriage return, then press Control-D to save. You are prompted to replace licenses, and after answering yes, the licenses are applied and displayed.

```
# elicense update
Enter the content of license file and then press Control-D, or press
Control-C to cancel.
```

b. Display available storage:

```
# storage show all
# disk show state
```

c. Add storage to the active tier:

```
# storage add enclosures <enclosure no> tier active
```

d. Add storage to the cloud tier:

```
# storage add enclosures <enclosure no> tier cloud
```

2. Install certificates.

Before you can create a cloud profile, you must install the associated certificates.

For AWS and Azure public cloud providers, root CA certificates can be downloaded from <https://www.digicert.com/digicert-root-certificates.htm>.

- For an AWS or Azure cloud provider, download the Baltimore CyberTrust Root certificate.
- For Alibaba, Alibaba download the GlobalSign Root R1 certificate from <https://support.globalsign.com/customer/portal/articles/1426602-globalsign-rootcertificates>.
- For ECS, the root certificate authority will vary by customer. Contact your load balancer provider for details.

Downloaded certificate files have a .crt extension. Use openssl on any Linux or Unix system where it is installed to convert the file from .crt format to .pem.

```
$openssl x509 -inform der -in DigiCertHighAssuranceEVRootCA.crt -out
DigiCertHighAssuranceEVRootCA.pem
```

```
$openssl x509 -inform der -in BaltimoreCyberTrustRoot.crt -out
BaltimoreCyberTrustRoot.pem
```

```
# adminaccess certificate import ca application cloud
Enter the certificate and then press Control-D, or press Control-C to
cancel.
```

3. To configure the system for data-movement to the cloud, you must first enable the "cloud" feature and set the system passphrase if it has not already been set.

```
# cloud enable
Cloud feature requires that passphrase be set on the system.
Enter new passphrase:
Re-enter new passphrase:
Passphrases matched.
The passphrase is set.
Encryption is recommended on the cloud tier.
Do you want to enable encryption? [yes|no] [yes]:
Encryption feature is enabled on the cloud tier.
Cloud feature is enabled.
```

4. Configure the cloud profile using the cloud provider credentials. The prompts and variables vary by provider.

```
# cloud profile add <profilename>
```

- ① **Note:** For security reasons, this command does not display the access/secret keys you enter.

Select the provider:

Enter provider name (alibabacloud|aws|azure|ecs|google|s3\_flexible)

- Alibaba Cloud requires access key, secret key, storage class and region.
- AWS S3 requires access key, secret key, storage class, and region.
- Azure requires account name, whether or not the account is an Azure Government account, primary key, secondary key, and storage class.
- ECS requires entry of access key, secret key and endpoint.
- Google Cloud Platform requires access key, secret key, and region. (Storage class is Nearline.)
- S3 Flexible providers require the provider name, access key, secret key, region, endpoint, and storage class.

At the end of each profile addition you are asked if you want to set up a proxy. If you do, these values are required: *proxy hostname*, *proxy port*, *proxy username*, and *proxy password*.

5. Verify the cloud profile configuration:

```
# cloud profile show
```

6. Create the active tier file system if it is not already created:

```
# fileysys create
```

7. Enable the file system:

```
# fileysys enable
```

8. Configure the cloud unit:

```
# cloud unit add unitname profile profilename
```

Use the `cloud unit list` command to list the cloud units.

9. Optionally, configure encryption for the cloud unit.

- a. Verify that the ENCRYPTION license is installed:

```
# elicence show
```

- b. Enable encryption for the cloud unit:

```
# fileysys encryption enable cloud-unit unitname
```

- c. Check encryption status:

```
# fileysys encryption status
```

10. Create one or more MTrees:

```
# mtree create /data/coll/nt11
```

11. Verify the Cloud Tier configuration:

```
# cloud provider verify
```

This operation will perform test data movement after creating a temporary profile and bucket.

Do you want to continue? (yes|no) [yes]:

```

Enter provider name (aws|azure|ecs|s3_generic): aws
Enter the access key:
Enter the secret key:
Enter the region (us-east-1|us-west-1|us-west-2|eu-west-1|ap-northeast-1|ap-southeast-1|ap-
southeast-2|
sa-east-1|ap-south-1|ap-northeast-2|eu-central-1):

Verifying cloud provider ..
This process may take a few minutes.
Cloud Enablement Check:
  Checking Cloud feature enabled: PASSED
  Checking Cloud volume: PASSED

Connectivity Check:
  Checking firewall access: PASSED
  Validating certificate PASSED

Account Validation:
  Creating temporary profiler: PASSED
  Creating temporary bucket: PASSED

S3 API Validation:
  Validating Put Bucket: PASSED
  Validating List Bucket: PASSED
  Validating Put Object: PASSED
  Validating Get Object: PASSED
  Validating List Object: PASSED
  Validating Delete Object: PASSED
  Validating Bulk Delete: PASSED

Cleaning Up:
  Deleting temporary bucket: PASSED
  Deleting temporary profile: PASSED

Provider verification passed.

```

12. Configure the file migration policy for this MTree. You can specify multiple MTrees in this command. The policy can be based on the age threshold or the range.

- a. To configure the age-threshold (migrating files older than the specified age to cloud):

```
# data-movement policy set age-threshold age_in_days to-tier cloud
cloud-unit unitname mtree mtreename
```

- b. To configure the age-range (migrating only those files that are in the specified age-range):

```
# data-movement policy set age-range min-age age_in_days max-age
age_in_days to-tier cloud cloud-unit unitname mtree mtreename
```

13. Export the file system, and from the client, mount the file system and ingest data into the active tier. Change the modification date on the ingested files such that they now qualify for data migration. (Set the date to older than the age-threshold value specified when configuring the data-movement policy.)
14. Initiate file migration of the aged files. Again, you can specify multiple MTrees with this command.

```
# data-movement start mtree mtreename
```

To check the status of data-movement:

```
# data-movement status
```

You can also watch the progress of data-movement:

```
# data-movement watch
```

- Verify that file migration worked and the files are now in the cloud tier:

```
# fileSYS report generate file-location path all
```

- Once you have migrated a file to the cloud tier, you cannot directly read from the file (attempting to do so results in an error). The file can only be recalled back to the active tier. To recall a file to the active tier:

```
# data-movement recall path pathname
```

## Configuring encryption for DD cloud units

Encryption can be enabled at three levels: System, Active Tier, and cloud unit. Encryption of the Active Tier is only applicable if encryption is enabled for the system. Cloud units have separate controls for enabling encryption.

### Procedure

- Select **Data Management > File System > DD Encryption**.
  - Note:** If no encryption license is present on the system, the Add Licenses page is displayed.
- In the DD Encryption panel, do one of the following:
  - To enable encryption for **Cloud Unit x**, click **Enable**.
  - To disable encryption for **Cloud Unit x**, click **Disable**.
  - Note:** You are prompted to enter security officer credentials to enable encryption.
- Enter the security officer **Username** and **Password**. Optionally, check **Restart file system now**.
- Click **Enable** or **Disable**, as appropriate.
- In the File System Lock panel, lock or unlock the file system.
- In the Key Management panel, click **Configure**.
- In the Change Key Manager dialog, configure security officer credentials and the key manager.
  - Note:** Cloud encryption is allowed only through the Embedded Key Manager. External key managers are not supported.
- Click **OK**.
- Use the DD Encryption Keys panel to configure encryption keys.

## Information needed in the event of system loss

Once Cloud Tier is configured, record the following information about the system and store it in a safe location apart from the system. This information will be needed to recover the Cloud Tier data in case the system is lost.

- Note:** This process is designed for emergency situations only and will involve significant time and effort from the Dell EMC engineering staff.
- Serial number of the original system

- System passphrase of the original system
- DD OS version number of the original system
- Cloud Tier profile and configuration information

## Using DD Replicator with Cloud Tier

Collection replication is not supported on systems with Cloud Tier enabled.

Directory replication only works on the /backup MTree, and this MTree cannot be assigned to the Cloud Tier. So, directory replication is not affected by Cloud Tier.

Managed file replication and MTree replication are supported on Cloud Tier enabled systems. One or both systems can have Cloud Tier enabled. If the source system is Cloud Tier enabled, data may need to be read from the cloud if the file was already migrated to the Cloud Tier. A replicated file is always placed first in the Active Tier on the destination system even when Cloud Tier is enabled. A file can be recalled from the Cloud Tier back to the Active Tier on the source MTree only. Recall of a file on the destination MTree is not allowed.

- i Note: If the source system is running DD OS 5.6 or 5.7 and replicating into a Cloud Tier enabled system using MTree replication, the source system must be upgraded to a release that can replicate to a Cloud Tier enabled system. Please see the *DD OS Release Notes* system requirements.
- i Note: Files in the Cloud Tier cannot be used as base files for virtual synthetic operations. The incremental forever or synthetic full backups need to ensure that the files remain in the Active Tier if they will be used in virtual synthesis of new backups.

## Using DD Virtual Tape Library (VTL) with Cloud Tier

On systems configured with Cloud Tier and DD VTL, the cloud storage is supported for use as the VTL vault. To use DD VTL tape out to cloud, license and configure the cloud storage first, and then select it as the vault location for the VTL.

DD VTL tape out to cloud on page 342 provides additional information about using VTL with Cloud Tier.

## Displaying capacity consumption charts for Cloud Tier

Three charts are available for displaying Cloud Tier consumption statistics—Space Usage, Consumption, and Daily Written.

### Procedure

1. Select **Data Management > File System > Charts**.
2. For **Chart**, select one of the following:
  - Space Usage
  - Consumption
  - Daily Written
3. For **Scope**, select **Cloud Tier**.
  - The Space Usage Tab displays space usage over time, in MiB. You can select a duration (one week, one month, three months, one year, or All). The data is presented (color-

coded) as pre-compression used (blue), post-compression used (red), and the compression factor (green).

- The Consumption Tab displays the amount of post-compression storage used and the compression ratio over time, which enables you to analyze consumption trends. You can select a duration (one week, one month, three months, one year, or All). The data is presented (color-coded) as capacity (blue), post-compression used (red), compression factor (green), cleaning (orange) and data movement (violet).
- The Daily Written Tab displays the amount of data written per day. You can select a duration (one week, one month, three months, one year, or All). The data is presented (color-coded) as pre-compression written (blue), post-compression used (red), and the total compression factor (green).

## Cloud Tier logs

If Cloud Tier suffers a failure of any kind, in configuration or operation, the system automatically creates a folder with a timestamp that is associated with the time of the failure.

Mount the `/ddvar/log/debug` directory to access the logs.

**Note:** The output of the `log list view` command does not list all the detailed log files that are created for the Cloud Tier failure.

## Using the CLI to remove Cloud Tier

You can use the CLI to remove the Cloud Tier configuration.

### Before you begin

Delete all files in the cloud units before removing the Cloud Tier configuration from the system. Run the `filesys report generate file-location path all output-file file_loc` command to identify the files in the cloud units, and delete them from the NFS mount points of the MTrees.

**Note:** The command above creates the report `file_loc` in the `/ddr/var/` directory.

### Procedure

1. Disable the file system.

```
# filesys disable

This action will disable the file system.
Applications may experience interruptions
while the file system is disabled.
Are you sure? (yes/no) [no]: yes

ok, proceeding.

Please wait.....
The filesystem is now disabled.
```

2. List the cloud units on the system.

```
# cloud unit list
Name           Profile        Status
-----
cloud_unit-1   cloudProfile   Active
cloud_unit-2   cloudProfile2  Active
-----
```



### 3. Delete the cloud units individually.

```
# cloud unit del cloud_unit-1

This command irrevocably destroys all data
in the cloud unit "cloud_unit-1".
Are you sure? (yes|no) [no]: yes

ok, proceeding.

Enter sysadmin password to confirm:

Destroying cloud unit "cloud_unit-1"
Cloud unit 'cloud_unit-1' deleted. The data in the cloud will be deleted asynchronously on
the filesystem startup.

# cloud unit del cloud_unit-2

This command irrevocably destroys all data
in the cloud unit "cloud_unit-2".
Are you sure? (yes|no) [no]: yes

ok, proceeding.

Enter sysadmin password to confirm:

Destroying cloud unit "cloud_unit-2"
Cloud unit 'cloud_unit-2' deleted. The data in the cloud will be deleted asynchronously on
the filesystem startup.
```

### 4. Verify the delete operations are in progress.

```
# cloud unit list
Name           Profile           Status
-----
cloud_unit-1   cloudProfile      Delete-Pending
cloud_unit-2   cloudProfile2     Delete-Pending
-----
```

### 5. Restart the file system.

```
# fileysys enable
Please wait.....
The filesystem is now enabled.
```

### 6. Run the cloud unit list command to verify that neither cloud unit appears.

Contact Support if one or both cloud units still display with the status Delete-Pending.

### 7. Identify the disk enclosures that are assigned to Cloud Tier.

```
# storage show tier cloud

Cloud tier details:
Disk  Disks           Count  Disk  Additional
Group -----
dgX   2.1-2.15, 3.1-3.15  30     3.6 TiB
-----
Current cloud tier size: 0.0 TiB
Cloud tier maximum capacity: 108.0 TiB
```

### 8. Remove the disk enclosures from Cloud Tier.

```
# storage remove enclosures 2, 3

Removing enclosure 2...Enclosure 2 successfully removed.

Updating system information...done
```



```
Successfully removed: 2 done  
Removing enclosure 3...Enclosure 3 successfully removed.  
Updating system information...done  
Successfully removed: 3 done
```



# CHAPTER 19

## DD Retention Lock

This chapter includes:

- DD Retention Lock overview..... 472
- Supported data access protocols..... 474
- Compliance mode on iDRAC..... 475
- Enabling DD Retention Lock on an MTree..... 476
- Client-Side Retention Lock file control..... 480
- System behavior with DD Retention Lock..... 485

## DD Retention Lock overview

When data is locked on an MTree that is enabled with DD Retention Lock, DD Retention Lock helps ensure that data integrity is maintained. Any data that is locked cannot be overwritten, modified, or deleted for a user-defined retention period of up to 70 years.

There are two DD Retention Lock editions:

- *DD Retention Lock Governance Edition* retains the functionality of DD Retention Lock prior to DD OS 5.2. You can use DD Retention Lock Governance to define retention policies on data that is to be retained for a specific period of time to meet internal IT governance policies implemented by the system administrator.
- *DD Retention Lock Compliance Edition* enables you to meet the strictest data permanence requirements of regulatory standards, such as those of SEC 17a-4(f). The full list of regulatory standards includes:
  - CFTC Rule 1.31b
  - FDA 21 CFR Part 11
  - Sarbanes-Oxley Act
  - IRS 98025 and 97-22
  - ISO Standard 15489-1
  - MoREQ2010

For certification information, see *Compliance Assessments - Summary and Conclusions - EMC Data Domain Retention Lock Compliance Edition* at <https://www.dellemc.com/en-us/index.htm>. Login is required.

Compliance with these standards ensures that files locked on a Data Domain or PowerProtect system using DD Retention Lock Compliance Edition software cannot be altered or destroyed before the retention period expires. DD Retention Lock Compliance Edition requires a security officer for implementation of policies. An audit log file is accessible by the administrator or security officer.

Each edition requires a separate, add-on license, and either or both can be used on a single system.

The retention-locking protocol is the same for both the DD Retention Lock Governance and Compliance Editions. The differences in use stem from the system behavior for the DD Retention Lock Compliance Edition, since it places strict restrictions to meet compliance requirements. For an overview, see the *EMC Data Domain Retention Lock Software - A Detailed Review* (a white paper) available at <https://www.dellemc.com/en-us/index.htm>. Login is required.

The DD Retention Lock Governance Edition does not require a security officer and provides a higher degree of flexibility for archive data retention.


For archive compliance storage requirements, SEC rules require that a separate copy of retention-locked data must be stored with the same retention requirements as the original. Retention-locked files can be replicated using DD Replicator to another Data Domain or PowerProtect system. If a retention-locked file is replicated, it remains retention locked on the destination system, with the same level of protection as the source file.

DD Retention Lock Governance Edition is supported for on-premises, cloud-based, and DD3300 DD VE instances. DD Retention Lock Compliance Edition is not supported for on-premises, cloud-based, or DD3300 DD VE instances.

The topics that follow provide additional information on DD Retention Lock.

## DD Retention Lock protocol

Only files that are explicitly committed to be retention-locked files are retention locked on the protection system. Files are committed to be retention-locked files through client-side file commands issued while DD Retention Lock Governance or Compliance is enabled on the MTree containing the files.

 **Note:** Linux, Unix, and Windows client environments are supported.

Files that are written to shares or exports that are not committed to be retained (even if DD Retention Lock Governance or Compliance is enabled on the MTree containing the files) can be modified or deleted at any time.

Retention locking prevents any modification or deletion of files under retention from occurring directly from CIFS shares or NFS exports during the retention period specified by a client-side *atime* update command. Some archive applications and backup applications can issue this command when appropriately configured. Applications or utilities that do not issue this command cannot lock files using DD Retention Lock.

Retention-locked files are always protected from modification and premature deletion, even if retention locking is subsequently disabled or if the retention-lock license is no longer valid.

You cannot rename or delete non-empty folders or directories within an MTree that is retention-lock enabled. However, you can rename or delete empty folders or directories and create new ones.


The retention period of a retention-locked file can be extended (but not reduced) by updating the file's *atime*.

For both DD Retention Lock Governance and Compliance, once the retention period for a file expires, the file can be deleted using a client-side command, script, or application. However, the file cannot be modified even after the retention period for the file expires. The system never automatically deletes a file when its retention period expires.

## DD Retention Lock flow

The general flow of activities with DD Retention Lock.

1. Enable MTrees for DD Retention Lock Governance or Compliance retention locking using the DD System Manager or DD OS commands issued from the system console.
2. Commit files to be retention locked on the protection system using client-side commands issued by an appropriately configured archiving or backup application, manually, or via scripts.
 

 **Note:** Windows clients may need to download utility programs for DD OS compatibility.
3. Optionally, extend file retention times using client-side commands.
4. Optionally, delete files with expired retention periods using client-side commands.

## Automatic retention lock

The automatic retention lock functionality allows you to set automatic values for the retention period, and the lock delay (the time before a file becomes locked) on a per MTree basis. The automatic retention lock settings apply to new files created on the MTree after the retention lock settings are configured. Existing files are not impacted.

Set the automatic retention period to ensure that every new file created on the MTree will be automatically locked and retained for the specified amount of time.

Set the automatic lock delay on the MTree to allow a period of time where a new file can be modified before it gets locked.

Automatic retention lock is subject to the following limitations:

- Retention lock must be re-applied manually to any files reverted when automatic retention lock is in use.
- MTree replication of an MTree with automatic retention lock enabled to a system with an earlier version of DD OS that does not support automatic retention lock, results in the locked files replicating to the target system as regular files.
- In Automatic Retention Lock, for the files which are being ingested, the `mtree retention-lock report generate` command may incorrectly report those files as locked as well report an incorrect cooling off period.

## Supported data access protocols

DD Retention Lock is compatible with industry-standard, NAS-based Write-Once-Read-Many (WORM) protocols, and integration is qualified with archive applications such as Symantec Enterprise Vault, SourceOne, Cloud Tiering Appliance, or DiskXtender. Customers using backup applications such as CommVault can also develop custom scripts to use DD Retention Lock.

The protocol support of DD Retention Lock is as follows:

- NFS is supported with both DD Retention Lock Governance and Compliance.
- CIFS is supported with both DD Retention Lock Governance and Compliance.
- Automatic retention lock is supported on NFS and CIFS with both Retention Lock Governance and Compliance.
- DD VTL is supported with DD Retention Lock Governance, but not with DD Retention Lock Compliance. Automatic retention lock is not supported on DD VTL.

Virtual tapes, here referred to as *tapes*, are represented as files on the file system.

- You can retention-lock one or more tapes using the `vtl tape modify` command, described in the *DD OS Command Reference Guide*.  
The `mtree retention-lock revert path` command can be used to revert the retention-locked state of tapes that are locked with the `vtl tape modify` command. After the tape is unlocked, updates can be made to it. The unlocked state will not be visible via the DD System Manager or CLI until the DD VTL service is disabled then enabled. However, updates are applied to the unlocked tape. This capability is only for the DD Retention Lock Governance Edition.
- The retention time for tapes can be displayed using the `vtl tape show` command with the `time-display retention` argument.
- You can retention-lock an individual tape using the DD System Manager.
- DD Boost is supported with both DD Retention Lock Governance and Compliance. Automatic retention lock is not supported on DD Boost.  
If client-side scripts are used to retention-lock backup files or backup images, and if a backup application (Veritas NetBackup, for example) is also used on the system via DD Boost, be aware that the backup application may not share the context of the client-side scripts. Thus, when a backup application attempts to expire or delete files that were retention locked via the client-side scripts, space is not released on the Data Domain or PowerProtect system.

Dell EMC recommends that administrators change their retention period policy to align with the retention lock time. This applies to many of the backup applications that are integrated with DD Boost, including Veritas NetBackup, Veritas Backup Exec, and NetWorker.

Setting retention lock during data ingest to a DD BOOST file in DSP mode is not allowed, and the client setting the RL receives an error. Retention lock should be set after the data ingest is complete.

Setting retention lock during data ingest to a DD BOOST file in OST mode, or to an NFS file is not allowed and the client writing the data receives error as soon as RL is set. The partial file written before RL is set and committed to disk as a worm file.

## Compliance mode on iDRAC

DD6900, DD9400, and DD9900 systems require that compliance mode be enabled on iDRAC before Retention Lock Compliance can be configured on the system.

Navigate to **Administration > Compliance** to view, and enable or disable iDRAC compliance access for DD6900, DD9400, and DD9900 systems.

The **Enabled Administrators** table displays the iDRAC administrator users currently enabled on the PowerProtect system, and the amount of time those users will be allowed to access the system.

The **iDRAC Users** table displays the iDRAC users currently configured on the system, the role for each user, and whether access for that user is enabled or disabled.

## Create an iDRAC user account

Enable compliance mode on iDRAC for DD6900, DD9400, and DD9900 systems to use DD Retention Lock Compliance.

### Before you begin

This task is only for DD6900, DD9400, and DD9900 systems.

Configure a security officer authorization policy on the system, and run the `system retention-lock configure` command to configure Retention Lock Compliance Edition on the system.

### Procedure

1. Select **Administration > Compliance**.
2. Click **Enable Retention Lock Compliance**.
 

① **Note:** This button is only available if Retention Lock Compliance Edition has been configured.
3. Specify the security officer credentials, and click **Enable**.
4. Create one or more iDRAC user accounts.
  - a. In the **Role** list box, select **Administrator (Disabled)** or **Operator (Enabled)**.
  - b. In the **Username** field, specify a username for the iDRAC user account.
  - c. In the **Password** and **Confirm Password** fields, specify a password for the iDRAC user account.
  - d. Click **Add User** to add the user.
  - e. Specify details for another user account, or click **Save** to proceed.

## Request PowerProtect access for iDRAC administrators

Request PowerProtect access for iDRAC administrator users for DD6900, DD9400, and DD9900 systems to use DD Retention Lock Compliance.

### Before you begin

This task is only for DD6900, DD9400, and DD9900 systems.



#### Procedure

1. Select **Administration > Compliance**.
2. Select an iDRAC administrator from the **iDRAC Users** table.
3. Click **Enable**.
4. Specify the security officer credentials, and click **OK**.
5. In the **Duration** list box, select the amount of time to allow access and click **OK**.

## Extend PowerProtect access for iDRAC administrators

Extend PowerProtect access for iDRAC administrator users for DD6900, DD9400, and DD9900 systems when access is required for a longer period of time.

#### Before you begin

This task is only for DD6900, DD9400, and DD9900 systems.

#### Procedure

1. Select **Administration > Compliance**.
2. Select an iDRAC administrator from the **Enabled Administrators** table.
3. Click **Enable** and select the duration from the list box.
4. Specify the security officer credentials, and click **Authorize**.
5. In the **Duration** list box, select the amount of time to allow access and click **Save**.
6. Click **Yes** at the confirmation prompt.

## Disable PowerProtect access for iDRAC administrators

Disable PowerProtect access for iDRAC administrator users for DD6900, DD9400, and DD9900 systems when access is no longer required.

#### Before you begin

This task is only for DD6900, DD9400, and DD9900 systems.

#### Procedure

1. Select **Administration > Compliance**.
2. Select an iDRAC administrator from the **iDRAC Users** table.
3. Click **Disable**.
4. Specify the security officer credentials, and click **OK**.

## Enabling DD Retention Lock on an MTree

Only files within DD Retention Lock Governance or Compliance enabled MTrees can be retention-locked.

MTrees enabled for DD Retention Lock Compliance cannot be converted to DD Retention Lock Governance MTrees and vice versa.

The procedures that follow show how to enable MTrees for either DD Retention Lock Governance or DD Retention Lock Compliance.

## Enabling DD Retention Lock Governance on an MTree

Add a DD Retention Lock Governance license to a system, and then enable DD Retention Lock Governance on one or more MTrees.

### Procedure

1. Add the DD Retention Lock Governance license, if it is not listed under Feature Licenses.
  - a. Select **Administration > Licenses**
  - b. In the Licenses area click **Add Licenses**.
  - c. In the License Key text box, type the license key.
 

① **Note:** License keys are case-insensitive. Include the hyphens when typing keys.
  - d. Click **Add**.
2. Select an MTree for retention locking.
  - a. Select **Data Management > MTree**.
  - b. Select the MTree you want to use for retention locking. You can also create an empty MTree and add files to it later.
3. Click the MTree Summary tab to display information for the selected MTree.
4. Scroll down to Retention Lock area and click **Edit** to the right of Retention Lock.
5. Enable DD Retention Lock Governance on the MTree and change the default minimum and maximum retention lock periods for the MTree, if required.

Perform the following actions in the Modify Retention Lock dialog box:

- a. Select **Enabled** to enable DD Retention Lock Governance on the MTree.
- b. In the **Use** drop-down list, select **Manual** or **Automatic**.
  - For manual retention lock, to change the minimum or maximum retention period for the MTree:
    - a. Type a number for the interval in the text box (for example, 5 or 14).
    - b. From the drop-down list, select an interval (minutes, hours, days, years).
 

① **Note:** Specifying a minimum retention period of less than 12 hours, or a maximum retention period longer than 70 years, results in an error.
  - For automatic retention lock, to change the minimum, maximum, or automatic retention period, or the automatic lock delay for the MTree:
    - a. Type a number for the interval in the text box (for example, 5 or 14).
    - b. From the drop-down list, select an interval (minutes, hours, days, years).
 

① **Note:** Specifying a minimum retention period of less than 12 hours, a maximum retention period longer than 70 years, an automatic retention period that does not fall between the minimum and maximum values, or an automatic lock delay less than 5 minutes or more than 7 days results in an error.
    - ① **Note:** If a file is modified before the automatic lock delay has elapsed, the lock delay time starts over when the file modification is complete. For example, if the lock delay is 120 minutes and the file is modified after 60 minutes, the lock delay will start again at 120 minutes after the file is modified.

- c. Click **OK** to save the settings.

After you close the Modify Retention Lock dialog box, which is updated MTree information appears in the Retention Lock area.

6. Check retention lock information for the MTree.

Note the following retention lock fields:

- **Top:**
  - The Status field indicates the read/write access for the MTree, the type of retention locking on the MTree, and whether retention locking is enabled or disabled.
- **Bottom:**
  - The Status field indicates whether retention locking is enabled for the MTree.
  - The Retention Period field indicates minimum and maximum retention periods for the MTree. The retention period that is specified for a file in the MTree must be equal to or greater than the minimum retention period and equal to or less than the maximum retention period.
  - The UUID field is a unique identification number that is generated for the MTree.

- ① **Note:** To check retention lock configuration settings for any MTree, select the MTree in the Navigation Panel, then click the Summary tab.

#### After you finish

Retention-lock files in a retention-lock-enabled MTree.

## Enabling DD Retention Lock Compliance on an MTree

Add a DD Retention Lock Compliance license to a system, set up a system administrator and one or more security officers, configure and enable the system to use DD Retention Lock Compliance software, and then enable DD Retention Lock Compliance on one or more MTrees.

#### About this task

Enabling Retention Lock Compliance on a DD6900, DD9400, or DD9900 system locks down the iDRAC GUI and SSH interfaces. Do not use the iDRAC interfaces to create additional iDRAC users because DD OS automatically disables those new users and reboots the system. Use the `user iDRAC create` command to create new iDRAC users after enabling Retention Lock Compliance.

#### Procedure

1. Add the DD Retention Lock Compliance license on the system, if it is not present.
  - a. First, check whether the license is already installed.
 

```
elicense show
```
  - b. If the RETENTION-LOCK-COMPLIANCE feature is not displayed, install the license.
 

```
elicense update license-file
```
2. Set up one or more security officer users accounts according to Role-Based Access Control (RBAC) rules.
  - a. In the system administrator role, add a security officer account.
 

```
user add user role security
```
  - b. Enable the security officer authorization.
 

```
authorization policy set security-officer enabled
```

3. Configure and enable the system to use DD Retention Lock Compliance.

- ⓘ Note: Enabling DD Retention Lock Compliance enforces many restrictions on low-level access to system functions used during troubleshooting. Once enabled, the only way to disable DD Retention Lock Compliance is to initialize and reload the system, which results in destroying all data on the system.

⚠ CAUTION When setting the lock period for Retention Lock Compliance MTree, users cannot set the period to be less than the current minimum or maximum period allowed. Doing so generates a message notifying the user that the entry was invalid and stating the minimum or maximum retention period allowed. To set the minimum retention period to a value less than 720 minutes or a maximum retention period of less than 1827 days, run the `mtree retention-lock set min-retention-period` or `mtree retention-lock set max-retention-period` commands before enabling DD Retention Lock.

a. Configure the system to use DD Retention Lock Compliance.

```
system retention-lock compliance configure
```

The system automatically reboots.

b. After the restart process is complete, enable DD Retention Lock Compliance on the system.

```
system retention-lock compliance enable
```

4. Enable compliance on an MTree that will contain retention-locked files.

```
mtree retention-lock enable mode compliance mtree mtree-path
```

- ⓘ Note: Compliance cannot be enabled on `/backup` or pool MTrees.

5. To change the default minimum and maximum retention lock periods for a compliance-enabled MTree, type the following commands with security officer authorization.

- `mtree retention-lock set min-retention-period period mtree mtree-path`
- `mtree retention-lock set max-retention-period period mtree mtree-path`

- ⓘ Note: The retention *period* is specified in the format `[number] [unit]`. For example: 1 min, 1 hr, 1 day, 1 mo, or 1 year. Specifying a minimum retention period of less than 12 hours, or a maximum retention period longer than 70 years, results in an error.

6. To change the automatic retention period and automatic lock delay for a compliance-enabled MTree, type the following commands with security officer authorization.

- `mtree retention-lock set automatic-retention-period period mtree mtree-path`

ⓘ Note: The automatic retention *period* is specified in the format `[number] [unit]`. For example: 1 min, 1 hr, 1 day, 1 mo, or 1 year. The value must be between the minimum and maximum retention periods.

- `mtree retention-lock set automatic-lock-delay time mtree mtree-path`

ⓘ Note: The automatic lock delay *time* is specified in the format `[number] [unit]`. For example: 5 min, 2 hr, or 1 day. The value must be between five minutes and seven days. The default is 120 minutes. If a file is modified before the automatic lock delay has elapsed, the lock delay time starts over when the file modification is complete.

For example, if the lock delay is 120 minutes and the file is modified after 60 minutes, the lock delay will start again at 120 minutes after the file is modified.

Repeat steps 4 through 6 to enable additional MTrees.

#### After you finish

Retention lock files reside in a retention-lock-enabled MTree.

## Client-Side Retention Lock file control

This section describes the DD Retention Lock client command interface for locking files stored on the protection system. Client commands are the same for DD Retention Lock Governance and Compliance. Linux, Unix, and Windows client environments are supported; however, Windows clients may need to download utility programs with commands to lock files.

- ① **Note:** If your application already supports industry-standard WORM, writing a WORM file to a DD Retention Lock Governance or Compliance enabled MTree will lock the file on the system. The retention time in the application should agree with the DD Retention Lock settings. You do not need to use the commands described in this section. To check whether an application is tested and certified for the DD Retention Lock, refer to the *Data Domain Archive Application Compatibility Guide*.
- ① **Note:** Some client machines using NFS, but running a legacy OS, cannot set retention time later than 2038. The NFS protocol doesn't impose the 2038 limit and allows to specifying times until 2106. Further, DD OS doesn't impose the 2038 limit.

Client-side commands are used to manage the retention locking of individual files. These commands apply to all retention-lock-capable systems and must be issued in addition to the setup and configuration of DD Retention Lock on the system.

#### Required Tools for Windows Clients

You need the `touch.exe` command to perform retention-locking from a Windows-based client.

To obtain this command, download and install utilities for Linux/Unix-based applications according to your Windows version. These utilities are best recommendations from Dell EMC and should be used per customer environment.

- For Windows 8, Windows 7, Windows Server 2008, Windows Vista, Windows Server 2003, and Windows XP:  
<http://sourceforge.net/projects/unxutils/files/latest>
- For Windows Server 2008, Windows Vista Enterprise, Windows Vista Enterprise 64-bit edition, Windows Vista SP1, Windows Vista Ultimate, and Windows Vista Ultimate 64-bit edition:  
<http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=23754>
- For Windows Server 2003 SP1 and Windows Server 2003 R2:  
<http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=20983>

- ① **Note:** The `touch` command for Windows may have a different format than the Linux examples in this chapter.

Follow the installation instructions provided and set the search path as needed on the client machine.

#### Client Access to System Files

After an MTree is enabled for DD Retention Lock Governance or Compliance, you can:

- Create a CIFS share based on the MTree. This CIFS share can be used on a client machine.



- Create an NFS mount for the MTree and access its files from the NFS mount point on a client machine.
- ① **Note:** The commands listed in this section are to be used only on the client. They cannot be issued through the DD System Manager or CLI. Command syntax may vary slightly, depending on the utility you are using.

The topics that follow describe how to manage client-side retention lock file control.

## Setting Retention Locking on a file

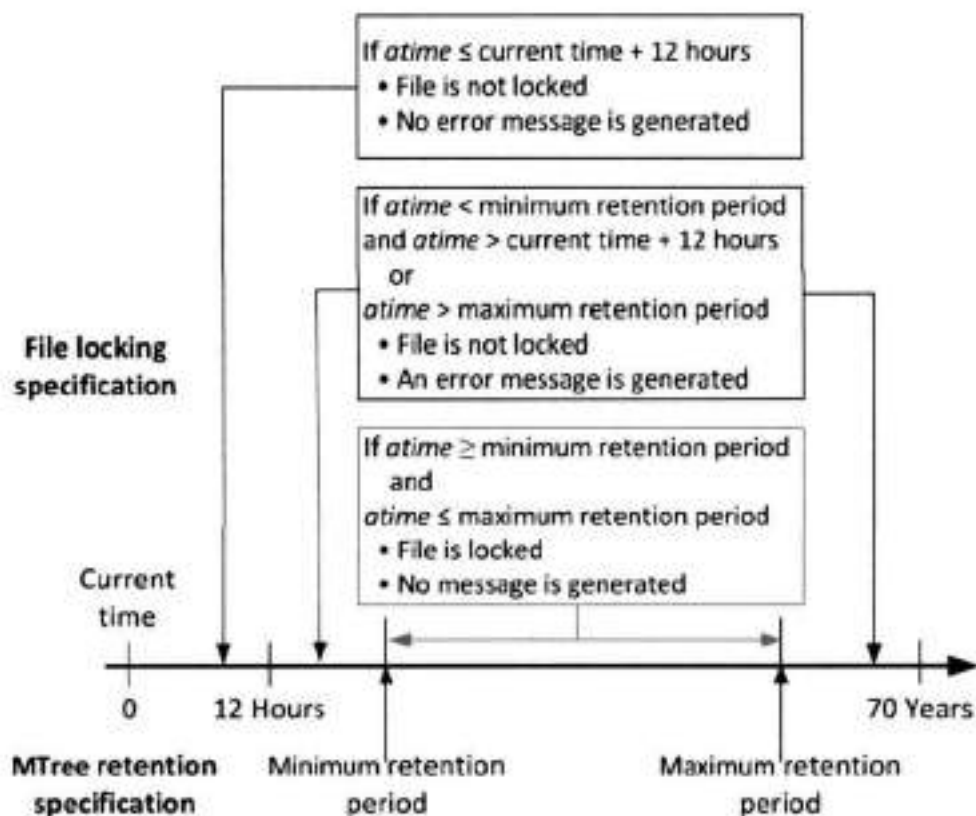
To perform retention locking on a file, change the last access time (*atime*) of the file to the desired retention time of the file, that is, the time when the file can be deleted.

This action is usually performed using the archive application, and all the archive applications that are qualified on the protection system today (per the *Data Domain Archive Application Compatibility Guide*) follow the basic locking protocol outlined here.

The future *atime* you specify must respect the minimum and maximum retention periods of the file's MTree (as offsets from the current time), as shown in the next figure.

Figure 21 Valid and invalid *atimes* for retention locking files

### For DD Retention Lock Governance and Compliance



- ① **Note:** Some client machines using NFS, but running a legacy OS, cannot set retention time later than 2038. The NFS protocol doesn't impose the 2038 limit and allows to specifying times until 2106. Further, DD OS doesn't impose the 2038 limit.

Errors are permission-denied errors (referred to as EACCESS, a standard POSIX error). These are returned to the script or archive application setting the *atime*.

- ⓘ Note: A file must be completely written to the system before it is committed to be a retention-locked file.

The following command can be used on clients to set the *atime*

```
touch -a -t [atime] [filename]
```

The format of *atime* is:

```
[[YY]YY] MMDDhhmm[.ss]
```

For example, suppose the current date and time is 1 p.m. on January 18, 2012 (that is, 201201181300), and the minimum retention period is 12 hours. Adding the minimum retention period of 12 hours to that date and time results in a value of 201201190100. Therefore, if the *atime* for a file is set to a value greater than 201201190100, that file becomes retention locked.

The following command:

```
ClientOS# touch -a -t 201412312230 SavedData.dat
```

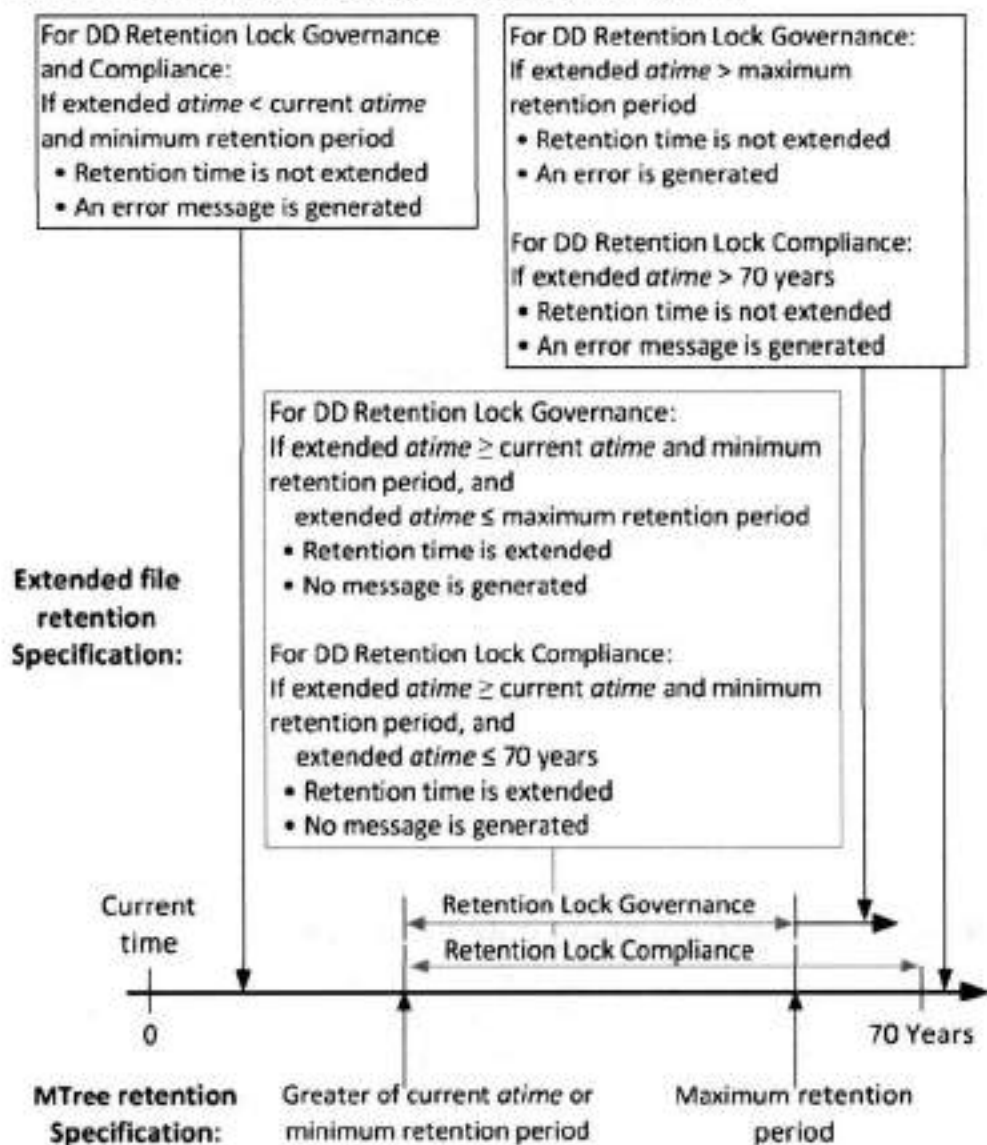
will lock file `SavedData.dat` until 10:30 p.m. December 31, 2014.



## Extending Retention Locking on a file

To extend the retention time of a retention-locked file, set the file's *atime* to a value greater than the file's current *atime* but less than the maximum retention period of the file's MTree (as an offset from the current time), as shown in the next figure.

Figure 22 Valid and invalid *atime*s for extending retention locking on files



For example, changing the *atime* from 201412312230 to 202012121230 using the following command:

```
ClientOS# touch -a -t 202012121230 SavedData.dat
```

will cause the file to be locked until 12:30 p.m. December 12, 2020.

① Note: Some client machines using NFS, but running a very old OS, cannot set retention time later than 2038. The NFS protocol doesn't impose the 2038 limit and allows to specifying times until 2106. Further, DD OS doesn't impose the 2038 limit.

Errors are permission-denied errors (referred to as EACCESS, a standard POSIX error). These are returned to the script or archive application setting the *atime*.

## Identifying a Retention-Locked file

The *atime* value for a retention-locked file is its retention time. To determine whether a file is retention locked, try to set the *atime* of the file to a value earlier than its current *atime*. This action will fail with a permission-denied error if and only if the file is a retention-locked file.

First, list the current *atime* value, and then execute the `touch` command with an earlier *atime* using these commands:

```
ls -li --time=atime [filename]
touch -a -t [atime] [filename]
```

The following example shows the command sequence:

```
ClientOS# ls -li --time=atime SavedData.dat
202012121230
ClientOS# touch -a -t 202012111230 SavedData.dat
```

If the *atime* of `SavedData.dat` is 202012121230 (12:30 p.m. December 12, 2020) and the `touch` command specifies an earlier *atime*, 202012111230 (12:30 p.m. December 11, 2020), the `touch` command fails, indicating that `SavedData.dat` is retention-locked.

 **Note:** The `--time=atime` option is not supported in all versions of Unix.

## Specifying a directory and touching only those files

Use the command line to create a root directory containing the files for which access times will change.

In this routine, *root directory to start from* contains the files on which you want to change access times using this client system command:

```
find [root directory to start from] -exec touch -a -t [expiration time] {} \;
```

For example:

```
ClientOS# find [/backup/datal/] -exec touch -a -t 202012121230 {} \;
```

## Reading a list of files and touching only those files

In this routine, *name of file list* is the name of a text file that contains the names of the files on which you want to change access times. Each line contains the name of one file.

Here is the client system command syntax:

```
touch -a -t [expiration time] `cat [name of file list]`
```

For example:

```
ClientOS# touch -a -t 202012121230 `cat /backup/datal/filelist.txt`
```

## Deleting or expiring a file

Delete or expire a file with an expired retention lock using a client application, or delete a file using a standard file-delete command.

Expiring a file using an application makes the file inaccessible to the application. The file may or may not actually be removed from the protection system by the expiration operation. If it is not removed, the application often provides a separate delete operation. You must have the appropriate access rights to delete the file, independent of DD Retention Lock.

- ① **Note:** If the retention period of the retention-locked file has not expired, the delete operation results in a permission-denied error.
- ① **Note:** For more information, refer to KB article 516962 Data Domain: How to delete data.

### Privileged delete

For DD Retention Lock Governance (only), you can delete retention locked files using this two step process.

#### Procedure

1. Use the `mtree retention-lock revert path` command to revert the retention locked file.
2. Delete the file on the client system using the `rm filename` command.

### Using ctime or mtime on Retention-Locked files

*ctime* is the last-metadata-change time of a file.

#### ctime

*ctime* gets set to the current time when any of the follow events occur:

- A non-retention-locked file is retention locked.
- The retention time of a retention-locked file is extended.
- A retention-locked file is reverted.

- ① **Note:** User access permissions for a retention-locked file are updated using the Linux command line tool `chmod`.

#### mtime

*mtime* is the last-modified time of a file. It changes only when the contents of the file change. So, the *mtime* of a retention-locked file cannot change.

## System behavior with DD Retention Lock

System behavior topics are discussed separately for DD Retention Lock Governance and DD Retention Lock Compliance in the sections that follow.

### DD Retention Lock governance

Certain DD OS commands behave differently when using DD Retention Lock Governance. The following sections describe the differences for each.

#### Replication

Collection replication, MTree replication, and directory replication replicate the locked or unlocked state of files.

Files that are governance retention locked on the source are governance retention locked on the destination and have the same level of protection. For replication, the source system must have a DD Retention Lock Governance license installed—a license is not required on the destination system.

Replication is supported between systems that are:

- Running the same major DD OS version (for example, both systems are running DD OS 5.5.x.x).

- Running DD OS versions within the next two consecutive higher or lower major releases (for example, 5.3.x.x to 5.5.x.x or 5.5.x.x to 5.3.x.x). Cross-release replication is supported only for directory and MTree replication.

① Note: MTree replication is not supported for DD OS 5.0 and earlier.

Be aware that:

- Collection replication and MTree replication replicate the minimum and maximum retention periods configured on MTrees to the destination system.
- Directory replication does not replicate the minimum and maximum retention periods to the destination system.

The procedure for configuring and using collection, MTree, and directory replication is the same as for protection systems that do not have a DD Retention Lock Governance license.

#### Replication Resync

The `replication resync destination` command tries to bring the destination into sync with the source when the MTree or directory replication context is broken between destination and source systems. This command cannot be used with collection replication. Note that:

- If files are migrated to the cloud tier before the context is broken, the MTree replication resync overwrites all the data on the destination, so you will need to migrate the files to the cloud tier again.
- If the destination directory has DD Retention Lock enabled, but the source directory does not have DD Retention Lock enabled, then a resync of a directory replication will fail.
- With Mtree replication, resync will fail if the source MTree does not have retention lock enabled and the destination MTree has retention lock enabled.
- With Mtree replication, resync will fail if the source and destination MTrees are retention lock enabled but the propagate retention lock option is set to FALSE.

## Fastcopy

When the `filesystems fastcopy [retention-lock] source src destination dest` command is run on a system with a DD Retention Lock Governance enabled MTree, the command preserves the retention lock attribute during the fastcopy operation.

① Note: If the destination MTree is not retention lock enabled, the retention-lock file attribute is not preserved.

## Filesys destroy

Effects of the `filesystems destroy` command when it is run on a system with a DD Retention Lock Governance enabled MTree.

- All data is destroyed, including retention-locked data.
- All `filesystems` options are returned to their defaults. This means that retention locking is disabled and the minimum and maximum retention periods are set back to their default values on the newly created file system.

① Note: This command is not allowed if DD Retention Lock Compliance is enabled on the system.

## MTree delete

When the `mtree delete mtree-path` command attempts to delete a DD Retention Lock Governance enabled (or previously enabled) MTree that currently contains data, the command returns an error.

① **Note:** The behavior of `mtree delete` is similar to a command to delete a directory—an MTree with retention lock enabled (or previously enabled) can be deleted only if the MTree is empty.

## DD Retention Lock compliance

Certain DD OS commands behave differently when using DD Retention Lock Compliance. The following sections describe the differences for each.

### Replication

An MTree enabled with DD Retention Lock Compliance can be replicated via MTree and collection replication only. Directory replication is not supported.

MTree and collection replication replicate the locked or unlocked state of files. Files that are compliance retention locked on the source are compliance retention locked on the destination and have the same level of protection. Minimum and maximum retention periods configured on MTrees are replicated to the destination system.

To perform collection replication, the same security officer user must be present on both the source and destination systems before starting replication to the destination system and afterward for the lifetime of the source/replica pair.

#### Replication Resync

The `replication resync destination` command can be used with MTree replication, but not with collection replication.

- If the destination MTree contains retention-locked files that do not exist on the source, then resync will fail.
- Both source and destination MTrees must be enabled for DD Retention Lock Compliance, or resync will fail.

### Replication procedures

The topics in this section describe MTree and collection replication procedures supported for DD Retention Lock Compliance.

① **Note:** For full descriptions of the commands referenced in the following topics, see the *DD OS Command Reference Guide*.

#### Replicating an MTree: One-to-one topology

Replicate a DD Retention Lock Compliance enabled MTree from a source system to a destination system.

##### Before you begin

Enable DD Retention Lock on an MTree and configure client-side retention lock file control before replication.

##### Procedure

1. Until instructed otherwise, perform the following steps on the destination system only.



2. Add the DD Retention Lock Compliance license on the system, if it is not present.
  - a. First, check whether the license is already installed.
 

```
elicense show
```
  - b. If the RETENTION-LOCK-COMPLIANCE feature is not displayed, install the license.
 

```
elicense update license-file
```
3. Set up one or more security officer users accounts according to Role-Base Access Control (RBAC) rules.

- a. In the system administrator role, add a security officer account.

```
user add user role security
```

- b. Enable the security officer authorization.

```
authorization policy set security-officer enabled
```

4. Configure and enable the system to use DD Retention Lock Compliance.

**ⓘ** Note: Enabling DD Retention Lock Compliance enforces many restrictions on low-level access to system functions used during troubleshooting. Once enabled, the only way to disable DD Retention Lock Compliance is to initialize and reload the system, which results in destroying all data on the system.

**⚠** CAUTION When setting the lock period for Retention Lock Compliance MTree, users cannot set the period to be less than the current minimum or maximum period allowed. Doing so generates a message notifying the user that the entry was invalid and stating the minimum or maximum retention period allowed. To set the minimum retention period to a value less than 720 minutes or a maximum retention period of less than 1827 days, run the `mtree retention-lock set min-retention-period` or `mtree retention-lock set max-retention-period` commands before enabling DD Retention Lock.

- a. Configure the system to use DD Retention Lock Compliance.

```
system retention-lock compliance configure
```

The system automatically reboots.

- b. After the restart process is complete, enable DD Retention Lock Compliance on the system.

```
system retention-lock compliance enable
```

5. Create a replication context.

```
replication add source mtree://source-system-name/data/coll/mtree-name destination mtree://destination-system-name/data/coll/mtree-name
```

6. Perform the following steps on the source system only.

7. Create a replication context.

```
replication add source mtree://source-system-name/data/coll/mtree-name destination mtree://destination-system-name/data/coll/mtree-name
```

8. Initialize the replication context.

```
replication initialize mtree://destination-system-name/data/coll/mtree-name
```

9. Confirm that replication is complete.

```
replication status mtree://destination-system-name/data/coll/mtree-
name detailed
```

This command reports 0 pre-compressed bytes remaining when replication is finished.

## Replicating an MTree: One-to-many topology

Replicate a DD Retention Lock Compliance enabled MTree from a source system to multiple destination systems.

### Before you begin

Enable DD Retention Lock compliance on an MTree and configure client-side retention lock file control before replication.

### Procedure

1. Until instructed otherwise, perform the following steps on the destination system only.
2. Add the DD Retention Lock Compliance license on the system, if it is not present.
  - a. First, check whether the license is already installed.
 

```
elicense show
```
  - b. If the RETENTION-LOCK-COMPLIANCE feature is not displayed, install the license.
 

```
elicense update license-file
```
3. Set up one or more security officer users accounts according to Role-Base Access Control (RBAC) rules.
  - a. In the system administrator role, add a security officer account.
 

```
user add user role security
```
  - b. Enable the security officer authorization.
 

```
authorization policy set security-officer enabled
```
4. Configure and enable the system to use DD Retention Lock Compliance.

ⓘ **Note:** Enabling DD Retention Lock Compliance enforces many restrictions on low-level access to system functions used during troubleshooting. Once enabled, the only way to disable DD Retention Lock Compliance is to initialize and reload the system, which results in destroying all data on the system.

⚠ **CAUTION** When setting the lock period for Retention Lock Compliance MTrees, users cannot set the period to be less than the current minimum or maximum period allowed. Doing so generates a message notifying the user that the entry was invalid and stating the minimum or maximum retention period allowed. To set the minimum retention period to a value less than 720 minutes or a maximum retention period of less than 1827 days, run the `mtree retention-lock set min-retention-period` or `mtree retention-lock set max-retention-period` commands before enabling DD Retention Lock.

- a. Configure the system to use DD Retention Lock Compliance.

```
system retention-lock compliance configure
```

The system automatically reboots.

- b. After the restart process is complete, enable DD Retention Lock Compliance on the system.



```
system retention-lock compliance enable
```

5. Create a replication context.

```
replication add source mtree://source-system-name/data/coll/mtree-name
destination mtree://destination-system-name/data/coll/mtree-name
```

6. Perform the following steps on the source system only.

7. Create a replication context for each destination system.

```
replication add source mtree://source-system-name/data/coll/mtree-name
destination mtree://destination-system-name/data/coll/mtree-name
```

8. Initialize the replication context for each destination system MTree.

```
replication initialize mtree://destination-system-name/data/coll/mtree-name
```

9. Confirm that replication is complete for each destination system.

```
replication status mtree://destination-system-name/data/coll/mtree-name
detailed
```

This command reports 0 pre-compressed bytes remaining when replication is finished.

### Adding DD Retention Lock Compliance protection to an existing MTree replication pair

Add DD Retention Lock Compliance protection to an existing MTree replication pair that is not enabled for retention locking.

#### Procedure

1. Until instructed otherwise, perform the following steps on both the source and destination systems.

2. Log in to the DD System Manager.

The DD System Manager window appears with **DD Network** in the Navigation panel.

3. Select a protection system.

In the Navigation panel, expand **DD Network** and select a system

4. Add the DD Retention Lock Governance license, if it is not listed under Feature Licenses.

- a. Select **Administration > Licenses**

- b. In the Licenses area click **Add Licenses**.

- c. In the License Key text box, type the license key.

 **Note:** License keys are case-insensitive. Include the hyphens when typing keys.

- d. Click **Add**.

5. Break the current MTree context on the replication pair.

```
replication break mtree://destination-system-name/data/coll/mtree-name
```

6. Create the new replication context.

```
replication add source mtree://source-system-name/data/coll/mtree-name
destination mtree://destination-system-name/data/coll/mtree-name
```

7. Perform the following steps on the source system only.
8. Select an MTree for retention locking.  
Click the **Data Management > MTree** tab, then the checkbox for the MTree you want to use for retention locking. (You can also create an empty MTree and add files to it later.)
9. Click the MTree Summary tab to display information for the selected MTree.
10. Lock files in the compliance-enabled MTree.
11. Ensure that both source and destination (replica) MTrees are the same.  

```
replication resync mtree://destination-system-name/data/coll/mtree-name
```
12. Check the progress of resync.  

```
replication watch mtree://destination-system-name/data/coll/mtree-name
```
13. Confirm that replication is complete.  

```
replication status mtree://destination-system-name/data/coll/mtree-name detailed
```

  
This command reports 0 pre-compressed bytes remaining when replication is finished.

### Converting a collection replication pair to MTree replication pairs

A procedure for customers who used collection replication under DD Retention Lock Compliance in DD OS 5.2 and want to convert compliance-enabled MTrees in the collection replication pair to MTree replication pairs.

#### Procedure

1. On the source system only:
  - a. Create a snapshot for each DD Retention Lock Compliance enabled MTree.  

```
snapshot create snapshot-name /data/coll/mtree-name
```
  - b. Synchronize the collection replication pair.  

```
replication sync col://destination-system-name
```
  - c. Confirm that replication is complete.  

```
replication status col://destination-system-name detailed
```

  
This command reports 0 pre-compressed bytes remaining when replication is finished.
  - d. View snapshot information for each DD Retention Lock Compliance enabled MTree.  

```
snapshot list mtree /data/coll/mtree-name
```

  
Note the snapshot names for use later.
2. On the destination system only:
  - a. Confirm that the replication is complete.  

```
replication status mtree://destination-system-name/data/coll/mtree-name detailed
```

  
This command reports 0 pre-compressed bytes remaining when replication is finished.
  - b. View each MTree snapshot replicated to the destination system.  

```
snapshot list mtree /data/coll/mtree-name
```
  - c. Ensure that all DD Retention Lock Compliance MTree snapshots have been replicated by comparing the snapshot names generated here with those generated on the source system.

```
snapshot list mtree /data/coll/mtree-name
```

3. On the both the source and destinations systems:

- a. Disable the file system.

```
filesystems disable
```

- b. Break the collection replication context.

```
replication break col://destination-system-name
```

- c. Enable the file system. (Security officer authorization may be required.)

```
filesystems enable
```

- d. Add a replication context for each DD Retention Lock Compliance enabled MTree.

```
replication add source mtree://source-system-name/data/coll/mtree-name
destination mtree://destination-system-name/data/coll/mtree-name
```

ⓘ Note: Source and destination MTree names must be the same.

4. On the source system only:

- a. Ensure that both source and destination MTrees are the same.

```
replication resync mtree://destination-system-name
```

- b. Check the progress of resync.

```
replication watch destination
```

- c. Confirm that replication is complete.

```
replication status mtree://destination-system-name/data/coll/mtree-name
detailed
```

This command reports 0 pre-compressed bytes remaining when replication is finished.

## Performing collection replication

Replicate /data/coll from a compliance-enabled source system to a compliance-enabled destination system.

### About this task

ⓘ Note: For collection replication the same security officer account must be used on both the source and destination systems.

### Procedure

- Until instructed to do differently, perform the following steps on the source system only.
- Log in to the DD System Manager.  
The DD System Manager window appears with **DD Network** in the Navigation Panel.
- Select a protection system.  
In the Navigation Panel, expand **DD Network** and select a system.
- Add the DD Retention Lock Governance license, if it is not listed under Feature Licenses.
  - Select **Administration > Licenses**
  - In the Licenses area click **Add Licenses**.
  - In the License Key text box, type the license key.

① | Note: License keys are case-insensitive. Include the hyphens when typing keys.

d. Click **Add**.

5. Create the replication context.

```
replication add source col://source-system-name destination col://
destination-system-name
```

6. Until instructed to do differently, perform the following steps on the destination system only.

7. Destroy the file system.

```
filesys destroy
```

8. Log in to the DD System Manager.

The DD System Manager window appears with **DD Network** in the Navigation Panel.

9. Select a protection system.

In the Navigation Panel, expand **DD Network** and select a system.

10. Create a file system, but do not enable it.

```
filesys create
```

11. Create the replication context.

```
replication add source col://source-system-name destination col://
destination-system-name
```

12. Configure and enable the system to use DD Retention Lock Compliance.

```
system retention-lock compliance configure
```

(The system automatically reboots and executes the `system retention-lock compliance enable` command.)

13. Perform the following steps on the source system only.

14. Initialize the replication context.

```
replication initialize source col://source-system-name destination
col://destination-system-name
```

15. Confirm that replication is complete.

```
replication status col://destination-system-name detailed
```

This command reports 0 pre-compressed bytes remaining when replication is finished.

### Adding DD Retention Lock Compliance protection to an existing collection replication pair

Add DD Retention Lock Compliance protection to a collection replication pair that was created without DD Retention Lock Compliance enabled on the source and destination systems.

#### Procedure

1. Until instructed otherwise, perform the following steps on both the source and destination systems.
2. Disable the replication.

```
replication disable col://destination-system-name
```

3. Log in to the DD System Manager.

The DD System Manager window appears with **DD Network** in the Navigation Panel.

4. Select a protection system.

In the Navigation Panel, expand **DD Network** and select a system.

5. Until instructed otherwise, perform the following steps on the source system.
6. Configure and enable the system to use DD Retention Lock Compliance.

```
system retention-lock compliance configure
```

(The system automatically reboots by executing the `system retention-lock compliance enable` command.)

7. Enable the replication context.

```
replication enable col://destination-system-name
```

8. Until instructed otherwise, perform the following steps on the destination system.
9. Configure and enable the system to use DD Retention Lock Compliance.

```
system retention-lock compliance configure
```

(The system automatically reboots by executing the `system retention-lock compliance enable` command.)

10. Enable the replication context.

```
replication enable col://destination-system-name
```

## Fastcopy

When the `filesys fastcopy [retention-lock] source src destination dest` command is run on a system with a DD Retention Lock Compliance enabled MTree, the command preserves the retention lock attribute during the fastcopy operation.

- ① Note: If the destination MTree is not retention lock enabled, the retention-lock file attribute is not preserved.

## CLI usage

Considerations for a protection system with DD Retention Lock Compliance.

- Commands that break compliance cannot be run. The following commands are disallowed:
  - `filesys destroy`
  - `mtree delete mtree-path`
  - `mtree retention-lock reset {min-retention-period period | max-retention-period period} mtree mtree-path`
  - `mtree retention-lock disable mtree mtree-path`
  - `mtree retention-lock revert`
  - `user reset`
- The following command requires security officer authorization if the license being deleted is for DD Retention Lock Compliance:
  - `elicense reset`
  - `elicense update`
- The following commands require security officer authorization if DD Retention Lock Compliance is enabled on an MTree specified in the command:
  - `mtree retention-lock set {min-retention-period period | max-retention-period period} mtree mtree-path`

- `mtree rename mtree-path new-mtree-path`
- The following commands require security officer authorization if DD Retention Lock Compliance is enabled on the system:
  - ① **Note:** These commands must be run in interactive mode.
  - `alerts notify-list reset`
  - `config set timezone zonename`
  - `config reset timezone`
  - `cifs set authentication active-directory realm [ [dc1 [dc2 ...]]`
  - `ntp add timeserver time server list`
  - `ntp del timeserver time server list`
  - `ntp disable`
  - `ntp enable`
  - `ntp reset`
  - `ntp reset timeservers`
  - `replication break {destination | all}`
  - `replication disable {destination | all}`
  - `system set date MMDDhhmm[[CC]YY]`

## 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 file system is disabled and can be resumed only by a security officer.

### Finding the System Clock Skew

You can run the DD OS command `system retention-lock compliance status` (security officer authorization required) to get system and security clock information, including the last recorded security clock value, and the accumulated system clock variance. This value is updated every 10 minutes.

### Removing the system clock skew

Clock skew is updated every time the security clock records a new value for the system clock. After 1 year, it is reset to 0.

#### About this task

At any time, you can run the DD OS command `system set date MMDDhhmm[[CC]YY]` to set the time of the system clock (security officer authorization required). If the clock skew becomes larger than the preset value (2 weeks), the file system is disabled. Complete these steps to restart the file system and remove the skew between security and system clocks.

#### Procedure

1. At the system console, enable the file system.
 

```
fileSYS enable
```
2. At the prompt, confirm that you want to quit the `fileSYS enable` command and check whether the system date is right.



3. Display the system date.

```
system show date
```

4. If the system date is not correct, set the correct date (security officer authorization is required) and confirm it.

```
system set date MMDDhhmm[[CC]YY]
system show date
```

5. Enable the file system again.

```
filesystem enable
```

6. At the prompt, continue to the enabling procedure.

7. A security officer prompt appears. Complete the security officer authorization to start the file system. The security clock will automatically be updated to the current system date.

# CHAPTER 20

## DD Encryption

This chapter includes:


- DD Encryption overview..... 498
- Configuring encryption..... 498
- About key management..... 499
- Key manager setup..... 507
- Changing key managers after setup..... 509
- Checking DD Encryption settings..... 509
- Enabling and disabling DD Encryption..... 510
- Locking and unlocking the file system..... 511

## DD Encryption overview

Data encryption protects user data if the protection system is stolen or if the physical storage media is lost during transit, and it eliminates accidental exposure of a failed drive if it is replaced.

When data enters the protection system using any of the supported protocols (NFS, CIFS, DD VTL, DD Boost, and NDMP Tape Server), the stream is segmented, fingerprinted, and de-duplicated (global compression). It is then grouped into multi-segment compression regions, locally compressed, and encrypted before being stored to disk.

Once enabled, the DD Encryption feature encrypts all data entering the system. You cannot enable encryption at a more granular level.

 **CAUTION** Data that has been stored before the DD Encryption feature is enabled does not automatically get encrypted. To protect all of the data on the system, be sure to enable the option to encrypt existing data when you configure encryption.

### Additional Notes:

The `filesys encryption apply-changes` command applies any encryption configuration changes to all data present in the file system during the next cleaning cycle. For more information about this command, see the *DD OS Command Reference Guide*.

DD Encryption supports all of the currently supported backup applications described in the Backup Compatibility Guides available through Online Support at <http://support.emc.com>.

DD Replicator can be used with encryption, enabling encrypted data to be replicated using collection, directory, MTree, or application-specific managed file replication with the various topologies. Each replication form works uniquely with encryption and offers the same level of security. For more information, see the section on using DD Encryption with replication.

Files locked using DD Retention Lock can be stored, encrypted, and replicated.

The autosupport feature includes information about the state of encryption on the system:

- Whether or not encryption is enabled
- The Key Manager in effect and which keys are used
- The encryption algorithm that is configured
- The state of the file system

## Configuring encryption

This procedure includes configuring a key manager.

If the Encryption Status on the **Data Management > File System > Encryption** tab shows Not Configured, click **Configure** to set up encryption on the protection system.

 **Note:** The system passphrase must be set in order to enable encryption.

Provide the following information:

- Algorithm
  - Select an encryption algorithm from the drop-down list or accept the default AES 256-bit (CBC).  
The AES 256-bit Galois/Counter Mode (GCM) is the most secure algorithm but it is significantly slower than the Cipher Block Chaining (CBC) mode.
  - Determine what data is to be encrypted: existing and new or only new. Existing data will be encrypted during the first cleaning cycle after the file system is restarted. Encryption of existing data can take longer than a standard file system cleaning operation.

- Key Manager (select one of the three)
  - Embedded Key Manager
 

By default, the protection system Embedded Key Manager is in effect after you restart the file system.

You can enable or disable key rotation. If enabled, type a rotation interval between 1-12 months.
  - SafeNet KeySecure Key Manager
 

**i** Note: See the section about key management for an explanation about how the Embedded Key Manager and SafeNet KeySecure Key Manager work.

The Summary shows the selected configuration values. Review them for correctness. To change a value, click **Back** to browse to the page where it was entered and modify it.

A system restart is necessary to enable encryption. To apply the new configuration, select the option to restart the file system.

- i** Note: Applications may experience an interruption while the file system is restarted.

## About key management

Encryption keys determine the output of the cryptographic algorithm. They are protected by a passphrase, which encrypts the encryption key before it is stored in multiple locations on disk. The passphrase is generated by the user and requires both an administrator and a security officer to change it.

A key manager controls the generation, distribution, and lifecycle management of multiple encryption keys. A protection system can use either the Embedded Key Manager or SafeNet KeySecure Key Manager.

Only one can be in effect at a time. When encryption is enabled on a protection system, the Embedded Key Manager is in effect by default. If you configure the SafeNet KeySecure Key Manager, it replaces the Embedded Key Manager and remains in effect until you disable it. A file system restart is required for a new key manager to be operational.

The Embedded Key Manager provides and generates multiple keys internally, although the system uses only one key at a time to encrypt data coming into the system.

The Embedded Key Manager rotates keys and supports a maximum of 254 keys, and allows you to specify how many months a key is in effect before being replaced (after the file system is restarted). The Embedded Key Manager key rotation is managed on the protection system.

### KeySecure

KeySecure 8.5 and 8.9 supported, which is a KMIP compliant key manager product from Safenet Inc/Gemalto Keysecure. To be able to use KMIP key manager, users have to configure both the key manager and the protection system/DDVE, to trust each other. Users have to pre-create keys on the key manager. A protection system will retrieve these keys and their states from KeySecure after establishing a secure TLS connection. See the *DD OS and Gemalto KeySecure Integration Guide* for more information on how to create keys and use them on a protection system.

## Rectifying lost or corrupted keys

Create a file that contains all of your system's current encryption keys. Your support provider can use this file to import keys back to your system should they become lost or corrupted. It is recommended that you create an export file on a regular basis.

You are prompted for the Security Officer's credential to export the keys. For additional key file protection, you can use a passphrase that differs from the one used in a protection system. After exporting, it is recommended that you save the key file in a secure file server accessible only by

authorized users. You must remember the passphrase used for the key file. If the passphrase is lost or forgotten, the protection system cannot import and restore the keys. Enter:

```
# filesystem encryption keys export
```

## Key manager support

All Key Managers support all DD OS file system protocols.

### Replication

When configuring protection systems for directory or MTree replication, configure each system separately. The two systems can use either the same or a different key class, and the same or different key managers.

For collection replication configuration, the protection system must be configured on the source. All replicated data is encrypted with the key set on the source. New data written to the destination after a replication break will either use the last active key set on the source, or a new key if the key manager is configured.

## Working with the Embedded Key Manager

When the Embedded Key Manager is selected, the protection system creates its own keys.

After the key rotation policy is configured, a new key is automatically created at the next rotation. An alert informs you of the creation of a new key. You must perform a file system restart to activate the new key and deactivate the old key. You can disable the key rotation policy by clicking the disable button associated with the Embedded Key Manager Key's rotation status.

### Creating a key (Embedded Key Manager)

Create an encryption key for the Embedded Key Manager.

#### Procedure

1. Select **Data Management > File System > DD Encryption**.
2. In the Encryption Keys section, click **Create...**
3. Type your security officer user name and password.
4. Click **Restart the filesystem now** if you want to restart the file system.

A new protection system key will be created. After the file system is restarted, the previous key will become deactivated and the new key will become activated.

5. Click **Create**.

### Destroying a key (Embedded Key Manager)

Destroy an encryption key for the Embedded Key Manager.

#### Procedure

1. Select **Data Management > File System > Encryption**.
2. In the Encryption Keys section, select the key in the list to be destroyed.
3. Click **Destroy....**

The system displays the Destroy dialog that includes the tier and state for the key.

4. Type your security officer user name and password.
5. Confirm that you want to destroy the key by clicking **Destroy**.

 Note: After a file system clean has run, the key state changes to Destroyed.

## Deleting a key

You can delete Key Manager keys that are in the **Destroyed** or **Compromised-Destroyed** states. However, you only need to delete a key when the number of keys has reached the maximum 254 limit. This procedure requires security officer credentials.

### About this task

- ① **Note:** To reach the **Destroyed** state, the **Destroying a Key** procedure must be performed on the key and a system cleaning must be run.

### Procedure

1. Select **Data Management > File System > Encryption**.
2. In the **Encryption Keys** section, select the key or keys in the list to be deleted.
3. Click **Delete....**  
The system displays the key to be deleted, and the tier and state for the key.
4. Type your security officer user name and password.
5. Confirm that you want to delete the key or keys by clicking **Delete**.

## 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.

## Using DD System Manager to set up and manage the KeySecure Key Manager

This section describes how to use DD System Manager to manage the KeySecure Key Manager.

### Creating a key for the KeySecure Key Manager

Create an encryption key for the KeySecure Key Manager (KMIP).

#### About this task

#### Procedure

1. Scroll down to the **Key Manager Encryption Keys** table.
2. Click **Add** to create a new Key Manager encryption key.
  - a. Enter the Security Officer username and password.
  - b. Click **Restart the file system now**.
  - c. Click **Create**.
3. Click **Restart the file system now** to make the changes take effect.

A new KIMP key is created. After the file system is restarted, the previous key is deactivated and the new key is activated.



## Modifying the state of an existing key in KeySecure Key Manager

Use DD SM to modify the state of an existing KIMP encryption key.

### Before you begin

Review the conditions for changing a key state:

- When a key already exists (is active) and a new key is created, the new key will change to the **Pending-Activated** state until the user restarts the file system.
- Users can deactivate a key in an **Activated-RW** state only if there is a **Pending-Activated** key to take its place.
- A key in a **Pending-Activated** state is deactivated only if there is another **Pending-Activated** key to take its place.
- A key in an **Activated-RO** key requires no conditions. Deactivate at any time.

### Procedure

1. Select **Data Management > File System > DD Encryption**.
2. Scroll down to view the **Key Manager Encryption Keys** table.
3. Select the appropriate key from the **Key Manager Encryption Keys** table.
4. To deactivate a key:
  - a. Click on any key that shows an **Activated** state.
  - b. Enter the security officer username and password.
  - c. Click **DEACTIVATE**.

Figure 23 Change KIMP key to a Deactivated state



5. Click **Restart the filesystem now**.

### Results

The state of an existing key is changed.

## Configuring the KeySecure Key Manager

Use DD SM to set the key rotation policy from the protection system.

### Before you begin

Confirm the desired Key rotation period (weeks or months), the Key rotation start date, and the Next key rotation date.

### Procedure

1. Select **Data Management > File System > DD Encryption**.
2. In the **Key Management** section, click **Configure**. The **Change Key Manager** dialog box opens.
3. Enter your security officer user name and password.
4. Select **KeySecure Key Manager** from the **Key Manager Type** drop down menu. The **Change Key Manager** information appears.
5. Set the key rotation policy:
  - (i) **Note:** The rotation policy is specified in weeks and months. The minimum key rotation policy increment is one week, and the maximum key rotation policy increment is 52 weeks (or 12 months).
  - a. Enable the Key Rotation policy. Set the **Enable Key rotation policy** button to enable.
  - b. Enter the appropriate dates in the Key rotation schedule field.
  - c. Select the appropriate number of weeks or months from the **Weeks** or **Months** drop down menu.
  - d. Click **OK**.
  - e. Click **Restart the filesystem now** if you want to restart the file system to make the changes take effect immediately, per Fig 3

### Results

The key rotation policy is set or changed.

## Using the DD CLI to manage the KeySecure Key Manager

This section describes how to use the CLI to manage the KeySecure Key Manager.

### Create a new active key on the KeySecure Key Manager

Use the protection system CLI to create a new active key.

#### Before you begin

Ensure that you have the appropriate user credentials. The security role is required to run these commands.

#### Procedure

1. Log into the protection system using the security role:
 

```
Username:<security office user>
Password:<security officer password>
```
2. Create a new active key:

```
# fileys encryption key-manager keys create
```

3. Output that is similar to the following appears:

```
New encryption key was successfully created.
The filesystem must be restarted to activate the new key.
```

**Results**

A new active key is created.

## Modify the state of an existing key in the KeySecure Key Manager

Use the protection system CLI to modify the state of an existing key to a deactivated state.

### Before you begin

Ensure that you have the appropriate user credentials. The security role is required to run these commands.

### Procedure

1. Log into the protection system using the security role:

```
Username: sec
```

```
Password: <security officer password>
```

2. Modify the state of an existing key:

```
# filesys encryption key-manager keys modify{<key-id> | muid <key-  
muid>}state deactivated
```

For example:

```
# filesys encryption key-manager keys modify muid  
740E711374A8C964A62817B4AD193C8DC44374A6ED534C85642782014F2E9D41 state  
deactivated
```

3. Output that is similar to the following appears:

```
Key state modified.
```

### Results

The state of an existing key is modified.

## Set or reset a key rotation policy in the KeySecure Key Manager

Use the Data Domain CLI to set the key rotation policy on the Data Domain system to periodically rotate keys. Note that the rotation policy is specified in weeks and months. The minimum key rotation policy increment is one week, and the maximum key rotation policy increment is 52 weeks (or 12 months).

### Before you begin

Ensure that you have the appropriate user credentials. The security role is required to run these commands.

### Procedure

1. Log into the Data Domain system using the security role:

```
Username: sec
```

```
Password: <security officer password>
```

2. Set a key rotation policy for the first time. In our example, we will set the rotation policy to **three weeks**:

```
# filesystem encryption key-manager set key-rotation-policy
  (every <n> (weeks | months) | none)
```

For example:

```
# filesystem encryption key-manager set key-rotation-policy every 3 weeks
```

Output that is similar to the following appears:

```
Key-rotation-policy is set. Encryption key will be rotated every 3
weeks.
```

3. Subsequently, run this command if you choose to change the existing key rotation policy. In our example, we will change the rotation policy from **three weeks** to **four months**:

① Note: Log into the Data Domain system using the security role (where Username is `sec`, and the password is the `<security officer password>`).

```
# filesystem encryption key-manager reset [key-rotation-policy]
```

For example:

```
filesystem encryption key-manager set key-rotation-policy every 4 months
```

Output that is similar to the following appears:

```
Key-rotation-policy is set. Encryption key will be rotated every 4
months.
```

4. Display the current key rotation policy, or verify that the policy is set correctly:

```
# filesystem encryption key-manager show
```

Output that is similar to the following appears:

```
The current key-manager configuration is:
Key Manager: Enabled
Server Type: KeySecure
Server: <IP address of KMIP server>
Port: 5696
Fips-mode: enabled
```

```

Status: Online
Key-class: <key-class>
KMIP-user: <KMIP username>
Key rotation period: 2 months
Last key rotation date: 03:14:17 03/19 2018
Next key rotation date: 01:01:00 05/17 2018

```

### Results

The key rotation policy is set or changed.

## How the cleaning operation works

Encryption affects the performance of cleaning operations when data encrypted with the Compromised or Marked-For-Destroyed keys is re-keyed using the Activated-RW key.

At the end of the cleaning operation, there will be no data that is encrypted with the Compromised or Marked-For-Destroyed keys. Also, any data written by the cleaning operation is encrypted with the Activated-RW key.

## Key manager setup

Follow the instructions for the type of key manager you are using.

For more information about SafeNet KeySecure Key Manager setup, see the *DD OS and Gemalto KeySecure Integration Guide*.

## Setting up KMIP key manager

With KMIP support, a protection appliance can retrieve symmetric key objects that are used for data at rest encryption from KMIP key managers.

### Procedure

1. Set up a KeySecure instance with IP address <IP1>.
2. Create and install an SSL server certificate on the KeySecure.
3. Enable KMIP by navigating to **Device > Key Server**.  
Ensure <IP1> is the address that is used and Port is <Port1> and the server certificate from Step 2 is used.
4. Create a certificate signing request (CSR) for the system on the protection system/DD VE or Linux computer.
  - a. Log in to the protection system.
  - b. Issue the command `adminaccess certificate cert-signing-request generate`.

If the command is successful, it generates the file `CertificateSigningRequest.csr`, which is located in `/ddvar/certificates/`.

By default, NFS exports do not have permissions to access the certificates folder, even to a root user.

```

# mount 16tbddve:/ddvar /mnt/DDVE
# cd /mnt/DDVE/certificates/
bash: cd: /mnt/DDVE/certificates/: Permission denied
# ls -al /mnt/DDVE/
total 800292
drwxr-xr-x 25 root staff 4096 Apr 10 08:32 .

```



```

drwxr-xr-x 26 root root          4096 Oct 24 12:11 ..
-rwxr-xr-x  1 root staff         180 Apr 10 08:36 .bashrc
drwxrwsr-x  2 root staff        4096 Aug 18  2016 benchmark
drwxr-sr-x  3 root staff        4096 Apr  4 15:49 cacerts
drwxrwsr-x  2 root staff        4096 Apr  4 12:50 cdes
drwxrws---  2 root staff        4096 Apr 11  2017 certificates
drwxrwsr-x  3 root staff        4096 Jul  1  2016 core

```

5. Take this CSR and have it issued/signed by the CA on the KeySecure.
 

If the command is successful, it generates the file `CertificateSigningRequest.csr`, which is located in `/ddvar/certificates/`.
6. Download that signed certificate (x.509 pem file) on to the protection system and use the private key of the CSR to create a `pkcs#12` file.
 

Rename `csr` to `pem` in the file name.
7. Download the root CA certificate from the CA of the KeySecure (**Security > Local CAs**).
8. On the protection system/DD VE, use `adminaccess` CLI to install the `pkcs#12` client certificate and the CA certificate. Use application type as **keysecure**.
9. On the KeySecure, create a symmetric key with AES-256 as the algorithm and key length.
  - a. Set the owner to the user that will use as KMIP on the protection system/DD VE.
  - b. Select the `Exportable` option.
  - c. Under **Security > Keys > Attributes** for the key, ensure to set **Application Namespace** to `DD_DARE_KEYS`. Ensure to set **Application Data** to key-class that you are planning to use on the protection system/DD VE.
10. Use `filesys encryption key-manager set` command to configure ALL the parameters to access the keysecure key manager.
11. Enable the external key-manager by using the command `filesys encryption key-manager enable`.
12. Enable encryption by using the commands `filesys encryption enable` and `filesys restart`.
 

This action restarts the file system.
13. Keys should be automatically retrieved from the keysecure key-manager should be seen in the local key table.

Sample output of local key table for `filesys encryption keys show`:

```

Active Tier:
Key Id      Key #/112                                     State      Size
-----
0.1 #56                                           Deactivated 0
0.2 953C694E2128FV77FC2B1027F8A51E44F8847A9D171B088C8C01576FF3DE1D5 Activated-RV 0
-----

```

\* Post-comp size is based on last cleaning of Tue Feb 14 10:02:02 2017.

The current active key is used to encrypt any data being ingested.

14. Sync the key states.
  - a. On the keysecure web interface, create a new active key as previously described.
  - b. On the keysecure web interface, deactivate the old key by clicking the key and going under the **Life Cycle** tab. Click **Edit State**. Set the **Cryptographic State** to **Deactivated**. Click **Save**.
15. On the protection system, sync the local key table by running the `filesys encryption keys sync` command.

Sample output of local key table for filesys encryption keys show:

Active Tier:

Key ID	Key MUIE	State	Size post-comp
0_1	*56	Deactivated	0
0_2	9530694E2128F977FC9B18D7F8A51E44F8047A8D171D08EDC8C01576FF5D61B5	Deactivated	0
0_3	851431E574D4F03886CA1F2795896D4C4D1EBC57A0997EFE04A148E584E9A99A	Activated-3W	0

• Post-comp size is based on last cleaning of Tue Feb 14 10:12:05 2017.

**Note:** Keys can be marked as versioned keys. When 2nd and 3rd versions of a specific key are generated, KMIP queries currently don't pick up these keys and may be an issue if that key is being used by a protection system or DD VE.

## Changing key managers after setup

Modify settings for the Embedded Key Manager.

**Before you begin**

To manage certificates for a system, you must start DD System Manager on that system.

**Procedure**

1. Select **Data Management > File System > Encryption**.
2. Under Key Management, click **Configure**.
3. Type your security officer username and password.
4. Select to enable or disable key rotation. If enabled, enter a rotation interval between 1-to-12 months. Select **Restart the file system now**, and click **OK**.
5. Click **Manage Certificates** to add certificates.

## Deleting certificates

Select a certificate with the correct fingerprint.

**Procedure**

1. Select a certificate to delete.
2. Click **Delete**.

The system displays a Delete Certificate dialog with the fingerprint of the certificate to be deleted.

3. Click **OK**.

## Checking DD Encryption settings

Check the settings for the DD Encryption feature.

Click the **Data Management > File System > Encryption** tabs. The currently used Key Manager is shown as Enabled. For a description of the DD Encryption settings, see the section about the encryption view.

## Enabling and disabling DD Encryption

After configuring DD Encryption, the status is enabled and the Disabled button is active. When DD Encryption is disabled, the Enabled button is active.

### Enabling DD Encryption

Use the DD System Manager to enable the DD Encryption feature.

#### Procedure

1. Using the DD System Manager, select the protection system you are working with in the Navigation panel.
2. In the Encryption view, click the **Enable** button.
3. Both of the following options are available:
  - Select **Apply to existing data** and click **OK**. Encryption of existing data will occur during the first cleaning cycle after the file system is restarted.
  - Select **Restart the file system now** and click **OK**. DD Encryption will be enabled after the file system is restarted.

#### After you finish

 Note: Applications may experience an interruption while the file system is restarted.


### Disabling DD Encryption

Use the DD System Manager to disable the DD Encryption feature.

#### Procedure

1. Using the DD System Manager, select the protection system you are working with in the Navigation panel.
2. In the Encryption view, click the **Disable** button.  
The Disable Encryption dialog box is displayed.
3. In the Security Officer Credentials area, enter the user name and password of a security officer.
4. Select one of the following:
  - Select **Apply to existing data** and click **OK**. Decryption of existing data will occur during the first cleaning cycle after the file system is restarted.
  - Select **Restart the file system now** and click **OK**. DD Encryption will be disabled after the file system is restarted.

#### After you finish

 Note: Applications may experience an interruption while the file system is restarted.

## Locking and unlocking the file system

Use this procedure when an DD Encryption-enabled protection system (and its external storage devices) are being transported, or if you want to lock a disk that is being replaced. The procedure requires two accounts: Security Officer and System Administration roles.

### Procedure

1. Select **Data Management > File System > Encryption** .  
In the File System Lock area, the Status shows whether the file system is Locked or Unlocked.
2. Disable the file system by clicking **Disabled** in the File System status area.
3. Use the procedure to lock or unlock the file system.


## Locking the file system


To lock the file system, DD Encryption must be enabled and the file system must be disabled.

### Procedure


1. Select **Data Management > File System > Encryption** and click **Lock File System**.
2. In the text fields of the Lock File System dialog box, provide:
  - The username and password of a Security Officer account (an authorized user in the Security User group on that protection system).
  - The current and a new passphrase.
3. Click **OK**.

This procedure re-encrypts the encryption keys with the new passphrase. This process destroys the cached copy of the current passphrase (both in-memory and on-disk).

 **Note:** Changing the passphrase requires two-user authentication to protect against the possibility of a rogue employee's shredding the data.

 **CAUTION** Be sure to take care of the passphrase. If the passphrase is lost, you will never be able to unlock the file system and access the data. The data will be irrevocably lost.

4. Shut down the system:

 **CAUTION** Do not use the chassis power switch to power off the system. Type the following command at the command prompt instead.

```
# system poweroff The 'system poweroff' command shuts down the
system and turns off the power. Continue? (yes|no|?) [no]:
```

5. Transport the system or remove the disk being replaced.
6. Power on the system and use the procedure to unlock the file system.

## Unlocking the file system

This procedure prepares an encrypted file system for use after it has arrived at its destination.

### Procedure

1. Select **Data Management > File System > Encryption** and click **Unlock File System**.
2. In the text fields, type the passphrase that was used to lock the file system.
3. Click **OK**.
4. Click **Close** to exit.

If the passphrase is incorrect, the file system does not start and the system reports the error. Type the correct passphrase, as directed in the previous step.

## Changing the encryption algorithm

Reset the encryption algorithm if necessary, or select options to encrypt new and existing data or just new data.

### Procedure

1. Select **Data Management > File System > Encryption**
2. To change the Encryption Algorithm used to encrypt the protection system, click **Change Algorithm**.

The Change Algorithm dialog box is displayed. Supported encryption algorithms are:

- AES-128 CBC
- AES-256 CBC
- AES-128 GCM
- AES-256 GCM

3. Select an encryption algorithm from the drop-down list or accept the default AES 256-bit (CBC).

The AES 256-bit Galois/Counter Mode (GCM) is the most secure algorithm but it is significantly slower than the Cipher Block Chaining (CBC) mode.

**Note:** To reset the algorithm to the default AES 256-bit (CBC), click **Reset to default**.

4. Determine what data will be encrypted:
  - To encrypt existing and new data on the system, select **Apply to Existing data, Restart file system now**, and click **OK**. Existing data will be encrypted during the first cleaning cycle after the file system is restarted.

**Note:** Encryption of existing data can take longer than a standard file system clean operation.

- To encrypt only new data, select **Restart file system now** and click **OK**.

5. The status is displayed. Click **Close** when the process is complete.

**Note:** Applications may experience an interruption while the file system is restarted.

**DECISION**

SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO S/A

# Item 1 - DD6900

## (Cont...)

DECISION

**Brasília (Sede)**

Sector Hotelero Sul - Quadra 06 - Conjunto W  
Bloco A - Sala 1001 - Asa Sul - Brasília/DF  
Cep. 70.220-910 - Tel. (61) 3045-0050

**Salvador**

Avenida Tancredi Neves, 620 - Salas 2010 e 2011  
20º andar - Torre Empresarial do Ed. Mundo Plaza  
Caminho das Árvoreas - Salvador/BA - Cep. 41.820-020  
Tel. (71) 3565.7007

**São Paulo**

Rua Arizona, 1.422 - Conjunto 76 - Ed. Platinium  
Building Bemri - Bemri - São Paulo/SP - Cep. 04.507-000  
Tel. (11) 5583.0044







# EQUIPAMENTOS DELL EMC POWERPROTECT SÉRIE DD

A série DD tem os melhores equipamentos de armazenamento de proteção, que são a última geração dos modelos Dell EMC Data Domain.

A série DD oferece uma solução rápida, segura e eficiente otimizada para a proteção de dados multicloud e demandas futuras.

A série DD compreende os DD9900, DD9400, DD6900, DD6400, DD3300 e um equipamento definido por software com PowerProtect DD Virtual Edition (DDVE).

	DD3300	DD6400	DD6900	DD9400	DD9900
<b>Throughput máx.</b>	Até 4,2 TB/h	Até 12,7 TB/h	Até 15 TB/h	Até 25 TB/h	Até 41 TB/h
<b>Throughput máximo (DD Boost)</b>	Até 7,0 TB/h	Até 27,7 TB/h	Até 33 TB/h	Até 57 TB/h	Até 94 TB/h
<b>Capacidade lógica<sup>1</sup></b>	Até 1,8 PB	Até 11,2 PB	Até 18,7 PB	Até 49,9 PB	Até 97,5 PB
<b>Capacidade lógica com o Cloud Tier</b>	Até 4,8 PB	Até 33,5 PB	Até 56,1 PB	Até 149,8 PB	Até 293 PB
<b>Capacidade útil</b>	4 TB a 32 TB	8 TB a 172 TB	24 TB a 288 TB	192 TB a 768 TB	576 TB a 1,5 PB
<b>Capacidade útil com o Cloud Tier</b>	Até 96 TB	Até 516 TB	Até 864 TB	Até 2,3 PB	Até 4,5 PB
<b>Gaveta ES40</b>	N/A	SAS de 8 TB e 7.200 RPM	SAS de 4 TB e 7.200 RPM	SAS de 8 TB e 7.200 RPM <sup>2</sup>	SAS de 8 TB e 7.200 RPM <sup>3</sup>
<b>Gaveta DS60</b>	N/A	N/A	SAS de 4 TB e 7.200 RPM <sup>2</sup>	SAS de 8 TB e 7.200 RPM	SAS de 8 TB e 7.200 RPM
<b>Gaveta FS25</b>	N/A	N/A	SSD de 3,8 TB <sup>2</sup>	SSD de 3,8 TB <sup>2</sup>	SSD de 3,8 TB <sup>2</sup>

<sup>1</sup> Capacidade lógica baseada em deduplicação de até 50 vezes (DD3300) e, normalmente, deduplicação em 65 vezes (dd6400, DD6900, DD9400 e DD9900) com base na compactação de dados extra assistida por hardware, normalmente 30% a mais por TB em comparação com a geração anterior. A capacidade e o throughput de fato dependem da carga de trabalho de aplicativos, da deduplicação e de outras configurações.

<sup>2</sup> Somente na configuração de alta disponibilidade. Em uma configuração padrão, as SSDs estão no controlador. Estes sistemas são compatíveis com uma configuração ativa/em espera de alta disponibilidade: DD9900, DD9400 e DD6900

<sup>3</sup> Suportado, mas não para pedidos em rack de fábrica.

	DD3300	DD6400	DD6900	DD9400	DD9900
<b>Sistema de rede integrado</b>	1 porta de gerenc.  4x 10G Base-T	1 porta de gerenc.  4x 10G BASE-T ou 4 SFP+ 10G	1 porta de gerenc.  4x 10G BASE-T ou 4 SFP+ 10G	1 porta de gerenc.  4x 10G BASE-T ou 4 SFP+ 10G	1 porta de gerenc.  4x 10G BASE-T ou 4 SFP+ 10G
<b>Sistema de rede opcional com placas de E/S</b>	A placa 10GBase-T pode ter negociação automática para dar suporte a 1 GbE  SLIC única com duas portas de até 10 GbE: óptica  HBA FC único com quatro portas de 16 Gbps	Até 3 entradas de quatro portas 10G Base-T, que podem passar por negociação automática para serem compatíveis com 1 GbE  Até três entradas de quatro portas 10G SFP+ (inclusive integradas)  Até três SFP+ 25G de duas portas  Até uma porta dupla Fibre Channel com HBA de 16 Gbit/s	Até quatro 10G base-T de quatro portas, que podem ser autonegociadas para dar suporte a 1 GbE  Até quatro SFP+ 10G de 4 portas (inclusive integradas)  Até três SFP+ 25G de duas portas  Até três HBA FC de 16 Gb de quatro portas	Até quatro 10G base-T de quatro portas, que podem ser autonegociadas para dar suporte a 1 GbE  Até quatro SFP+ 10G de 4 portas (inclusive integradas)  Até três SFP+ 25G de duas portas  Até três HBA FC de 16 Gb de quatro portas	Até quatro 10G base-T de quatro portas (inclusive integradas), que podem ser autonegociadas para dar suporte a 1 GbE  Até quatro SFP+ 10G de quatro portas  Até quatro SFP+ 25G de duas portas  Até quatro 100G de duas portas  Até quatro HBA FC de 16 Gb de quatro portas
	DD3300	DD6400	DD6900	DD9400	DD9900
<b>Peso (libras)</b>	16 HDDs: 73 lb	4 SSDs/8 discos rígidos: 73 lb	6 SSDs: 73 lb	9 SSDs: 73 lb	4 SSDs: 110 lb
<b>Dimensões</b>	17,1" x 29,8" x 3,5" Unidades de rack EIA de 2 U	17,1" x 29,8" x 3,5" Unidades de rack EIA de 2 U	17,1" x 29,8" x 3,5" Unidades de rack EIA de 2 U	17,1" x 29,8" x 3,5" Unidades de rack EIA de 2 U	17,1" x 32,0" x 5,2" 3 unidades de rack EIA
<b>Energia 100 a 120/200 a 240 V~, 50/60 Hz</b>	16 HDDs: 429 VA	4 SSDs/8 discos rígidos: 524 VA	6 SSDs: 364 VA	9 SSDs: 647 VA	4 SSDs: 1.117 VA
<b>Classificação térmica (watts)</b>	16 HDDs: 425 Watts	4 SSDs/8 discos rígidos: 516 watts	6 SSDs: 352 Watts	9 SSDs: 635 Watts	4 SSDs: 1.111 Watts
<b>Classificação térmica (btu/h)</b>	16 HDDs: 1.450	4 SSDs/8 discos rígidos: 1.760 BTU/h	6 SSDs: 1.201 btu/h	9 SSDs: 2.167 BTU/h	4 SSDs: 3.791 BTU/h
<b>Temperatura/altitude operacionais<sup>3</sup></b>	10°C a 35 C, 35°C a 3.117 pés	10°C a 35 C, 35°C a 3.117 pés	10°C a 35 C, 35°C a 3.117 pés	10°C a 35 C, 35°C a 3.117 pés	10°C a 35 C, 35°C a 3.117 pés
<b>Temperatura não operacional (de transporte)</b>	-40 °C a +65 °C (-40 F a +149 F)	-40 °C a +65 °C (-40 F a +149 F)	-40 °C a +65 °C (-40 F a +149 F)	-40 °C a +65 °C (-40 F a +149 F)	-40 °C a +65 °C (-40 F a +149 F)
<b>Umidade operacional</b>	10% a 80% com ponto de condensação máxima a 29 °C (84,2 °F)	10% a 80% com ponto de condensação máxima a 29 °C (84,2 °F)	10% a 80% com ponto de condensação máxima a 29 °C (84,2 °F)	10% a 80% com ponto de condensação máxima a 29 °C (84,2 °F)	10% a 80% com ponto de condensação máxima a 29 °C (84,2 °F)
<b>Ruído acústico operacional (capacidade de som)</b>	LWAd: 7,8 bels	7,2 bels	7,2 bels	7,6 bels	8,8 bels
<b>Ruído acústico operacional (pressão sonora)</b>	LpAm: 67 db	61 db	52 db	58 db	70 db

## **Declaração de conformidade**

O equipamento de tecnologia da informação da Dell EMC está em conformidade com todos os requisitos regulamentares atualmente aplicáveis de compatibilidade eletromagnética, segurança do produto e normas ambientais, quando colocados no mercado.

Informações regulamentares detalhadas e a verificação de conformidade estão disponíveis no site de conformidade com normas da Dell. [http://dell.com/regulatory\\_compliance](http://dell.com/regulatory_compliance)

## **Software**

### **Recursos do software**

Global Compression™, Data Inviolability Architecture, abrangendo verificação em linha e RAID 6 com paridade de disco dual integrada, snapshots, comunicação por Telnet, FTP, SSH, alertas por e-mail, recuperação agendada de capacidade, failover e agregação de Ethernet, Link Aggregation Control Protocol (LACP), marcação da VLAN, aliases de IP, DD Boost, DD Encryption, DD Extended Retention, DD Retention Lock, DD Virtual Tape Library (VTL) (para ambientes operacionais IBM e de sistemas abertos). Os complementos disponíveis incluem: DD Boost, Cloud Tier para retenção em longo prazo, Cloud Disaster Recovery e DD Replicator.

### **Gerenciamento de sistema**

PowerProtect DD Management Center, DD System Manager, SNMP (Simple Network Management Protocol) e interface de gerenciamento de linha de comando.

### **Gerenciamento de dados**

NFS v3 sobre TCP, CIFS e DD Boost sobre 1GbE ou 10GbE ou Fibre Channel, emulação de biblioteca de fitas (VTL) sobre Fibre Channel e servidor de fitas NDMP.

## Gaveta de SSD FS25

### Interface externa (host/expansão)

Duas portas SAS (Serial Attached SCSI II, SCSI com conexão serial II) de 4 vias e 12Gb/s por LCC (Link Control Card, placa de controle de link) — uma porta para o host e outra para expansão

### Tipo de conector

Conectores SFF-8088 (mini-SAS)

### Comprimento do cabo SAS

Até 5 metros

### Unidades de disco

gabinets com 25 unidades, suportes, unidades SSD com formato de 2,5 polegadas de 3,84 TB

### Dimensões

Altura: 8,46 cm (3,40 pol.)

Largura: 44,45 cm (17,5 pol.)

Profundidade: 33,02 cm (13,0 pol.)

Peso: 10,0 kg (22,0 lb)

### Operacional

Alimentação (VA): 187 VA ou 136 W, (100-240 V ~, 47 a 63 Hz)

Classificação térmica: 464 btu/h

### Ambiental

Temperatura ambiente: 10 °C a 35 °C (50 °F a 95 °F)

Gradiente de temperatura: 20 °C/h (36 °F/h)

Extremos de umidade relativa: 20 a 80% sem condensação

Elevação: -16 a 3.050 m (-50 a 10.000 pés)

Temperatura não operacional (de transporte):

Temperatura ambiente: -40 °C a 65 °C (-40 °F a 149 °F)

Gradiente de temperatura: 20 °C/h (36 °F/h)

Umidade relativa: 10% a 90% sem condensação

Altura: -16 a 10.600 m (-50 a 35.000 pés)

## Gaveta de expansão DS60

### Interface externa (host/expansão)

Portas quádruplas SCSI II (SAS) x8 com conexão serial de 12 Gb/s por Placa de controle de link (LCC) — Metade de cada porta está bloqueada, permitindo o uso de conectores mini-SAS-HD padrão — uma porta é usada para a conexão de host e a outra é usada para expansão.

### Tipo de conector

Conectores SFF-8088 (mini-SAS)

### Comprimento do cabo SAS

Até 5 metros

### Unidades de disco

Gabinets de 60 unidades por gaveta de expansão DS60, com suporte a unidades de baixo perfil com 1 pol. de altura e modelo de 3,5 pol.

Opções de unidade: SAS (12 Gbit/s), 4 TB ou 8 TB

### Dimensões

Altura: 22,23 cm (8,75 pol.) 5U (bandeja de gerenciamento de cabos de 4U mais 1U)

Largura incluindo rails: 44,45 cm (17,50 pol.)

Profundidade (somente chassi): 87,63 cm (34,5 pol.)

Profundidade máxima (totalmente configurado): 92,46 cm (36,4 pol.)

Peso: 90,7 kg (225,0 lb) (com FRUs instalados)

### Operacional

Alimentação: 785 VA ou 770 W (200-240 V ~, 47 a 63 Hz)

Classificação térmica: 2.627 btu/h

### Ambiental

Temperatura ambiente: 5 °C to 40 °C (41 °F a 104 °F)

Gradiente de temperatura: 10 °C/h (18 °F/h)

Extremos de umidade relativa: 20 a 80% sem condensação

Elevação: -16 a 2.300 m (-50 a 7.500 pés)

Temperatura não operacional (de transporte):

Temperatura ambiente: -40 °C a 65 °C (-40 °F a 149 °F)

Gradiente de temperatura: 25 °C/h (45 °F/h)

Umidade relativa: 10% a 90% sem condensação

Altura: -16 a 10.600 m (-50 a 35.000 pés)

## Gaveta de expansão ES40

### Interface externa (host/expansão)

Duas portas SAS (Serial Attached SCSI II, SCSI com conexão serial II) de 4 vias e 12Gb/s por LCC (Link Control Card, placa de controle de link) — uma porta para o host e outra para expansão

### Tipo de conector

Conectores SFF-8088 (mini-SAS)

### Comprimento do cabo SAS

Até 5 metros

### Unidades de disco

gabinets de 15 unidades, suportes, unidades SAS de formato de 3,5 polegadas, 4 TB e 7.200 rpm

### Dimensões

Altura: 13,33 cm (5,25 pol.)

Largura: 44,45 cm (17,5 pol.)

Profundidade: 35,56 cm (14 pol.)

Peso: 30,8 kg (68 lb)

### Operacional

Alimentação (VA): 272 VA ou 232 W, (100-240 V ~, 47 a 63 Hz)

Classificação térmica: 792 btu/h

### Ambiental

Temperatura ambiente: 10 °C a 35 °C (50 °F a 95 °F)

Gradiente de temperatura: 20 °C/h (36 °F/h)

Extremos de umidade relativa: 20 a 80% sem condensação

Elevação: -16 a 3.050 m (-50 a 10.000 pés)

Temperatura não operacional (de transporte):

Temperatura ambiente: -40 °C a 65 °C (-40 °F a 149 °F)

Gradiente de temperatura: 20 °C/h (36 °F/h)

Umidade relativa: 10% a 90% sem condensação

Altura: -16 a 10.600 m (-50 a 35.000 pés)

## Rack série DD

### Configuração de energia

A alimentação padrão é monofásica, e a opcional é trifásica.

Dois domínios de alimentação (base e estendido), ambos redundantes.

### Número de entradas de AC

Duas ou quatro (DD9900 monofásica de alta disponibilidade com 4 DS60 ou DD9900/DD9900 de alta disponibilidade com 5 DS60)

### Tipos de plugue

L6-30P, 56PA322, 332P6W, 3750DP, L7-30, 60309, CS-8365C, 9P54U2T, 3 pontos em estrela ou 3 pontos em estrela com condutores móveis

### Capacidade de alimentação da PDU

monofásica, 24 A, 200-240 V~, 50/60 Hz  
trifásica, 3 W + G, 40 A, 200 a 240 V~, 50/60 Hz (3P-Delta)

trifásica, 3 W + N + PE, 24 A, 200 a 240 V~, 50/60 Hz (3P-Wye)

### Dimensões

Capacidade de rack disponível de 40U

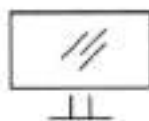
Altura: 190,8 cm (75 pol.)

Largura: 61,1 cm (24,0 pol.)

Profundidade: 99,2 cm (39,0 pol.)

Peso (vazio): 173 kg (380 lb)

Um rack 42U de 60 cm x 1.200 cm também está disponível



Saiba mais sobre a série DD



Entre em contato com um especialista da Dell Technologies





# DELL POWERPROTECT DD SERIES APPLIANCES

The ultimate protection storage appliance

DD series enables organizations to protect, manage and recover data at scale across their diverse environments. DD series is the next generation of Data Domain appliances, that are now setting the bar for data protection from edge to core to cloud. DD series provides the ecosystem support, efficiency, powerful data protection and cloud-enabled capabilities that customers have come to expect and appreciate from Data Domain and takes it to the next level.

The DD Operating System (DDOS) is the intelligence that powers DD series. It provides the agility, security and reliability that enables DD series to deliver high-speed, scalable, and industry-leading multicloud protection storage for backup, archive, and disaster recovery. DDOS integrates seamlessly with existing infrastructures, enabling ease-of-use with leading backup and archiving applications, and offers superior performance in conjunction with Dell PowerProtect Data Manager and Data Protection Suite. When purchasing a new DD series appliance, you can now consume DDOS as a subscription providing flexibility for deployment while minimizing upfront costs.

Fast, secure and efficient data protection

DD series minimizes the risk of data loss and leverages the value of protected data, while meeting ever more demanding SLAs and increasing ROI. DDOS drives DD series to deliver up to 38% faster backups and up to 45% faster restores at higher compression levels.\*\* This improved level of compression efficiency typically increases the logical capacity by up to 30% per TB\*.

DD series can now scale up to a physical capacity of 1.5PB in a single rack, thereby utilizing minimal floor space and lowering power and cooling by up to 41%.\*\*\* By employing denser disk drives, DD series has lowered the required rack space by up to 39%.

DD series provides up to an additional 3PB of cloud capacity for long-term retention, with Cloud Tier.

DD series supports high availability within the single rack. By doing so, DD series can further reduce the total cost of ownership by reducing downtime in the unlikely event of a hardware failure. DD series delivers high speed networking connectivity with support for 25GbE and 100GbE network adapters.

## Key benefits

### Fast, secure, and efficient

- 1.5PB usable capacity in a single rack
- Up to 3PB capacity for long-term retention
- Improved logical capacity of up to 30%\*
- Instant access and instant restore of up to 64VMs and 100k IOPS\*\*\*\*
- High speed network connectivity – 10GbE, 25GbE and 100GbE
- Seamless integration and superior performance with PowerProtect Data Manager and Data Protection Suite
- Supports leading enterprise backup and archive applications

### Industry-leading multicloud protection

- Software-defined protection storage on-premises with PowerProtect DD Virtual Edition (DDVE) and in-cloud with APEX Protection Storage for Public Cloud
- DDVE scales up to 96TB and APEX Protection Storage up to 258TB in-cloud
- Improves in-cloud restore performance by up to 10x\*\*\*\*
- Cloud Tier delivers simple and efficient long-term retention to a public, private or hybrid cloud
- Low-cost disaster recovery to the cloud

### Operational simplicity

- Enhanced DD System Manager provides complete chassis view
- Single point of management for all DD series by DD Management Center
- Support for Smart Scale making managing data at scale less complex

### Energy efficiency on Dell Storage

- Dell is committed to improving energy efficiency in our storage portfolio with each generation

Based on Dell internal testing and field telemetry data, January 2023. Actual results may vary.

\* Based on Dell internal testing compared to the previous generation, January 2023. Actual results may vary.

When comparing 1 petabyte of data on a DD9800 with Cloud Tier and PowerProtect DD9900 with Cloud Tier. Actual results may vary, March 2023.

\*\*\*\* Based on Dell internal testing when comparing DDVE 7.7 to DDVE 7.1. Actual results may vary, March 2023.

\*\* When using DDOS 7.7 and later on the DD9900. Based on Dell internal testing. Actual results may vary, January 2023.



## Smart Scale for PowerProtect appliances

Organizations must often manage multiple data centers and cloud environments, add, upgrade, and retire protection storage infrastructure, accommodate new evolving applications and optimize capacity and performance. Not an easy task but one that Dell is helping companies overcome with Smart Scale. Smart Scale allows you to manage up to 32 DD series appliances in a single system pool under a unified name space driving down management complexity while increasing storage efficiency. Smart Scale is deployed free of charge through our single pane of glass management console, PowerProtect DD Management Center. Smart Scale is supported on the DD9900, DD9400, DD6900, DD6400 and DDVE on-prem. For software integration we support Dell PowerProtect Data Manager, Dell NetWorker, and third-party backup applications. Smart Scale introduces mobile storage units providing flexibility and transparent mobility of backup data in each pool.

## Instant access and instant restore

Instant access and instant restore delivers high performance of VMs with up to 100K IOPS with the ability to instantly access up to 64 VMs simultaneously.\*\*\*\*\*

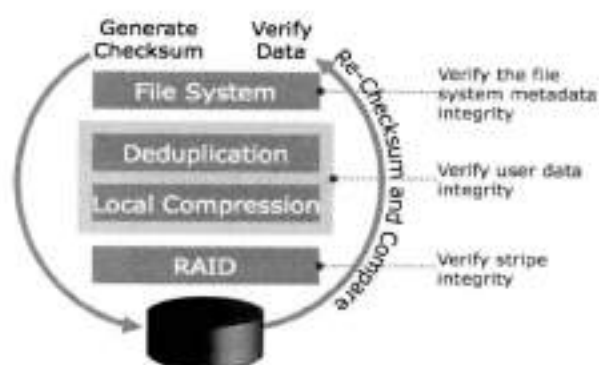
Instant access and instant recovery save time, minimizing mean time to repair (MTTR), by enabling instant access to data from the backup image on the included DD series SSD drives. It also saves primary storage space with the ability to manage data on the appliance itself and lowers cost by better utilizing the physical resources in both the data protection as well as the production environments.

In case of a failure or disaster recovery in a virtualized environment, DD series can spin-up production-oriented VMs immediately within the appliance itself. By doing so, the customer can continue their daily routine without experiencing any downtime, while the failed VMs are restored to the production environment.

## Data Invulnerability Architecture

DD series is designed as the storage of last resort – providing you with the confidence that you can always reliably recover your data. The Data Invulnerability Architecture is built into DDOS and DD series to provide the industry's best defense against data loss. Inline write and read verification protects against and automatically recovers from data integrity issues during data ingest and retrieval while RAID-6 and hot spares protect against disk failure.

Capturing and correcting I/O errors inline during the backup process eliminates the need to repeat backup jobs, ensuring backups complete on time and satisfy service-level agreements. In addition, unlike other enterprise arrays or file systems, continuous fault detection and self-healing ensures data remains recoverable throughout its lifecycle on DD series.



End-to-end data verification

## End-to-end data verification

End-to-end data verifications reads data after it is written and compares it to what was sent to disk, proving that it is reachable through the file system to disk and that the data is not corrupted. Specifically, when DDOS receives a write request from backup software, it computes a checksum over the data. After analysing the data for redundancy, it stores the new data segments and all the checksums. After all the data is written to disk, DDOS verifies that it can read the entire file from the disk platter and through PowerProtect DD, and that the checksums of the data read back match the checksums of the written data. This confirms the data is correct and recoverable from every level of the system.

## Comprehensive DD series portfolio

	DDVE - 96TB	DD3300	DD6400	DD6900	DD9400	DD9900
Backup Ingest (w/DD Boost)	Up to 11.2TB/hr	Up to 7.0TB/hr	Up to 27.7 TB/hr	Up to 33TB/hr	Up to 57TB/hr	Up to 94TB/hr
Logical Capacity (w/Active Tier)	Up to 4.8PB	Up to 1.6PB	Up to 11.2PB	Up to 18.7PB	Up to 49.9PB	Up to 97.5PB
Usable Capacity (w/Active Tier)	1TB-96TB	4TB-32TB	8TB-172TB	24TB-288TB	192TB-768TB	576TB-1.5PB

Logical capacity based on up to 50x deduplication (DD3300) and up to 65x deduplication (DD6400, DD6900, DD9400, DD9900) based on additional hardware-assisted data compression of up to 30% better than previous generation. Actual capacity & throughput depends on application workload, deduplication, and other settings.

### Seamless integration

DD series integrates easily with existing infrastructures, enabling ease-of-use with leading backup and archiving applications, and offers superior performance in conjunction with PowerProtect Data Manager and Data Protection Suite.

DD series can simultaneously support multiple access methods including NFS and/or CIFS, VTL, NDMP and DD Boost™ all applications and utilities can be supported in the same DD series at the same time to enable greater protection storage consolidation. A system can present itself as a file server, offering NFS, CIFS access over Ethernet; as a virtual tape library (VTL) over Fibre Channel; as an NDMP tape server over Ethernet; or as a disk target using application specific interfaces like DD Boost. DD VTL is qualified with leading open systems and IBMi enterprise backup applications.

### Industry-leading multi-cloud protection

DD series simplifies and obtains operational efficiencies including resiliency and scale as you grow in any cloud environment – private, public and hybrid. DD series supports the most extensive cloud ecosystem – AWS, Azure, VMware Cloud, Google Cloud, Alibaba Cloud, and Dell ECS to deliver excellent in-cloud data protection at reduced costs. DD series can natively tier deduplicated data to any supported cloud environment for long-term retention with Cloud Tier. DD series provides fast disaster recovery with orchestrated DR and provides an efficient architecture to extend on-premises data protection with lowered costs.

### PowerProtect DD Virtual Edition and APEX Protection Storage for Public Cloud

PowerProtect DD Virtual Edition (DDVE) and APEX Protection Storage for Public Cloud leverage the power of DDOS to deliver software-defined protection storage on-premises and in-cloud. DDVE and APEX Protection Storage are fast and simple to download, deploy and configure – and can be up and running in minutes.

DDVE can be deployed on-premises on any standard hardware, converged or hyper-converged, and runs in VMware vSphere, Microsoft Hyper-V, and KVM. DDVE is also certified with VxRail and Dell PowerEdge servers. An assessment tool can be run during deployment to check the underlying infrastructure and ensure it meets recommended requirements. A single DDVE instance can scale up to 96TB.

APEX Protection Storage runs in-cloud with AWS, AWS GovCloud, VMware Cloud, Azure, Azure Government Cloud, Alibaba Cloud, and Google Cloud. APEX Protection Storage can scale up to 256TB.

Within DDVE and APEX Protection Storage, capacity can easily be distributed between virtual systems and/or locations and can scale in increments of 1TB allowing you to grow capacity as the business demands. DDVE and APEX Protection Storage maintain the core DDOS features and include DD Boost, DD Encryption and DD Replicator. DDVE and APEX Protection Storage can be configured and managed using DD System Manager and centrally manage multiple instances, on-premises and in-cloud, through PowerProtect DD Management Center.

## Long-term retention and disaster recovery in-cloud

With Cloud Tier DDOS can natively tier data to a public, private or hybrid cloud for long-term retention. Only unique data is sent directly from DD series to the cloud and data lands on the cloud object storage already deduplicated. It supports AWS, AWS Gov Cloud, Azure, Google Cloud, IBM Cloud, Alibaba Cloud, Seagate Lyve Cloud, and Dell Elastic Cloud Storage (ECS). With deduplication ratios of up to 65x, storage footprint is greatly reduced lowering overall TCO. Cloud Tier can scale up to 3PB of usable capacity. With DD Encryption, data in the cloud remains secure. Cloud Tier works with DDVE for on-prem deployments.

Cloud Disaster Recovery (Cloud DR) allows enterprises to copy backed-up VMs from their on-premises DD series environments to the public cloud (AWS, VMware Cloud on AWS, Azure) and to orchestrate DR testing and failover of workloads to the cloud in a disaster scenario with end-to-end orchestration.

## Operational simplicity

DD series is very simple to install and manage resulting in lower administrative and operational costs. Administrators can access DDOS through command line over SSH or through DD System Manager, a browser-based graphical user interface.

Multiple DD series appliances can be managed and monitored through a single interface, PowerProtect DD Management Center, or DDMC. Customizable dashboards provide visibility into aggregate status, status by geo, and the ability to drill-down to system-level details. DDMC can now provide insights into current and projected capacities at the system level for DD series and legacy Data Domain systems allowing for enhanced forecasting and capacity management. Role-based access allows different levels of access via assigned user roles for various levels of expertise within the organization. Simple programmability as well as SNMP monitoring provides additional management flexibility. DDMC offers a pre check option before scheduling a DDOS upgrade to make sure your environment is compatible with the update. Once the pre check is complete you can schedule a one-to-many upgrade allowing you to schedule multiple DDOS upgrades as opposed to one to one updates. Configuring multiple DD series appliances is simple with DDMC by allowing you to create and apply configuration templates to your appliances. With cyber-attacks and threats on the rise, DDMC can provide compliance alerts when a system's configuration is out of compliance. In the event of a DDOS upgrade failure the appliance will automatically default back to the previous OS release minimizing system downtime and allowing for continuous backup operations.

In addition, DD series has an automatic call-home system reporting called auto-support, which provides email notification of complete system status to Dell support and a selected list of administrators. This non-intrusive alerting and data collection capability enables proactive support and service without administrator intervention, further simplifying ongoing management.

DD series appliances are now integrated with Dell CloudIQ. CloudIQ provides proactive insights and performance analytics across supported storage, data protection, and hyper-converged products through one UI.

## DD series software add-ons

### DD Boost

DD Boost software delivers an advanced level of integration with backup applications and data base utilities, enhancing performance and ease of use. Dell also provides a DD Boost File System Plug-In (BoostFS) with DD Boost for even greater application support, which enables all the benefits of DD Boost for applications that use NFS for data protection. Rather than sending all data to the system for deduplication processes, DD Boost enables the backup server or application client to send only unique data segments across the network to the system.

### DD Replicator

DD Replicator software provides automated, policy-based, network-efficient, and encrypted replication for disaster recovery and multi-site backup and archive consolidation. DD Replicator software asynchronously replicates only compressed, deduplicated data over the WAN. Cross-site deduplication further reduces bandwidth requirements when multiple sites are replicating to the same destination system. This improves network efficiency across all sites and reduces daily network bandwidth requirements making network-based replication fast, reliable and cost effective. To meet a broad set of DR requirements, DD Replicator provides flexible replication topologies, such as full system mirroring, bi-directional, many-to-one, one-to-many, and cascaded.

## Future-Proof Program and Dell Technologies APEX

The Future-Proof Program is a customer facing program that gives our customers additional peace of mind with guaranteed satisfaction and investment protection through a comprehensive set of world class technology capabilities and programs for future technology changes. DD series participates in this Future-Proof Program. DD series is part of the Dell Technologies APEX program allowing for flexible payment options including pay as you go, pay as you use, and provided as-a-Service offerings.



Learn more about  
[DD series](#)



[Contact a Dell Technologies Expert](#)



# Dell EMC PowerProtect DD Series Appliances: Encryption Software

## Abstract

This document describes the Dell EMC™ PowerProtect DD series appliance encryption software and its capabilities with the Dell EMC Data Domain™ Operating System (DDOS).

October 2020

## Revisions

# Revisions

Date	Description
June 2013	Initial release
October 2020	Updated for DDOS 7.3 release

# Acknowledgments

Author: Vinod Kumar Kumaresan

The information in this publication is provided "as is." Dell Inc. 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 software described in this publication requires an applicable software license.

Copyright © 2020 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. [10/20/2020] [Technical White Paper] |H18559



## Table of contents

Revisions.....	2
Acknowledgments.....	2
Table of contents.....	3
Executive summary.....	4
Audience.....	4
1 DD series encryption software overview.....	5
1.1 Encryption types offered by DD series encryption software.....	6
1.1.1 Inline encryption of data at rest using DD Encryption.....	6
1.1.2 Encryption of data in-flight using DD Replicator.....	7
1.1.3 Encryption of data in-flight with DD Boost.....	8
2 DD Encryption configuration.....	9
2.1 Enabling and disabling DD Encryption.....	14
2.1.1 Enabling DD Encryption.....	14
2.1.2 Disabling DD Encryption.....	15
3 Key management.....	16
3.1 Embedded key manager.....	16
3.2 KMIP-compliant external key managers: KeySecure and Data Security Manager.....	16
3.3 Key manager support.....	16
3.3.1 Replication.....	16
3.3.2 Embedded key manager setup.....	17
3.3.3 Setting up a KMIP-compliant external key manager (KeySecure and DSM).....	18
3.4 Key manager setup.....	18
4 File system lock.....	19
5 Changing the encryption algorithm.....	20
6 DD Encryption with DD Replicator.....	21
6.1 Collection replication.....	21
6.2 MTree or directory replication.....	21
6.3 Cascaded replication.....	21
7 DD Encryption and Cloud Tier.....	22
8 Conclusion.....	23
A Technical support and resources.....	24
A.1 Related resources.....	24



## Executive summary

The Dell EMC™ Data Domain™ Operating System (DDOS) is the intelligence that powers Dell EMC PowerProtect DD series appliances. DD series encryption software enables organizations to enhance the security of the data that resides on DD series appliances using industry-standard encryption algorithms. DD series encryption software protects backup and archive data that is stored on DD series appliances with data encryption that is performed inline before the data is written to disk. The Encryption at Rest feature satisfies internal governance rules and compliance regulations. It also protects against the reading of customer data on individual disks or disk shelves that are removed from the system due to theft.

DD Replicator with encryption enables encrypted data to be replicated using collection, directory, MTree, or application-specific managed file replication with the various topologies.

This document details DD series data encryption features which provide the following benefits:

- Protect against unauthorized access if disks are stolen from the system
- Protect the system during transport from unauthorized access
- Meet IT governance and compliance

## Audience

This technical white paper is intended for Dell Technologies customers, partners, and employees. It describes the DD series encryption features of DDOS, and details how they can be used to securely manage, protect, and recover data.

## 1 DD series encryption software overview

Data encryption protects user data if the protection system is stolen or if the physical storage media is lost during transit. It also eliminates accidental exposure of a failed drive if it is replaced. When data enters the protection system using any of the supported protocols (NFS, CIFS, DDVTL, DD Boost, and NDMP tape server), the stream is segmented, fingerprinted, and deduplicated (global compression). It is then grouped into multi-segment compression regions, locally compressed, and encrypted before being stored to disk. Once data encryption is enabled, the DD Encryption feature encrypts all data entering the appliance.



Figure 1 DD series encryption software overview

DD series encryption software provides the following benefits:

- Secure data management:
  - Encrypt all data stored on a DD series deduplication storage system
  - Protect data from theft or loss of the system, disk shelves, disks, or factory returned disks
  - Easily implement encryption to satisfy internal governance rules and compliance regulations
  - Meet compliance needs using industry-standard AES-128 or AES-256 encryption algorithms
  - Use RSA BSAFE FIPS 140-2 compliant cryptographic libraries
- Inline encryption:
  - Real-time, immediate data encryption with compression
  - Stream-Informed Segment Layout (SISL) architecture used for optimized encryption
  - Software-based approach requires no extra hardware
- Key management and data integrity:
  - Robust protection against accidental key loss
  - Passphrase protection of encryption keys
  - Data Invulnerability Architecture (DIA) with dual-disk parity RAID 6

- Easy integration:
  - Supports leading backup and archive applications
  - Supports leading enterprise applications for database and virtual environments
  - Allows simultaneous use of VTL, NAS, NDMP, and DD Boost

## 1.1 Encryption types offered by DD series encryption software

There are three types of encryption offered with DD series appliances:

- Inline encryption of data at rest using the DD Encryption feature
- Encryption of data in-flight using DD Replicator software, which is used for replicating data between sites over the WAN
- Encryption of data in-flight using DD Boost software, using Transport Layer Security (TLS)

### 1.1.1 Inline encryption of data at rest using DD Encryption

DD Encryption provides inline encryption. As data is ingested, the stream is deduplicated, compressed, and encrypted using an encryption key before it is written to the RAID group. DD Encryption uses RSA BSAFE libraries, which are validated according to the Federal Information Processing Standards (FIPS) 140-2.

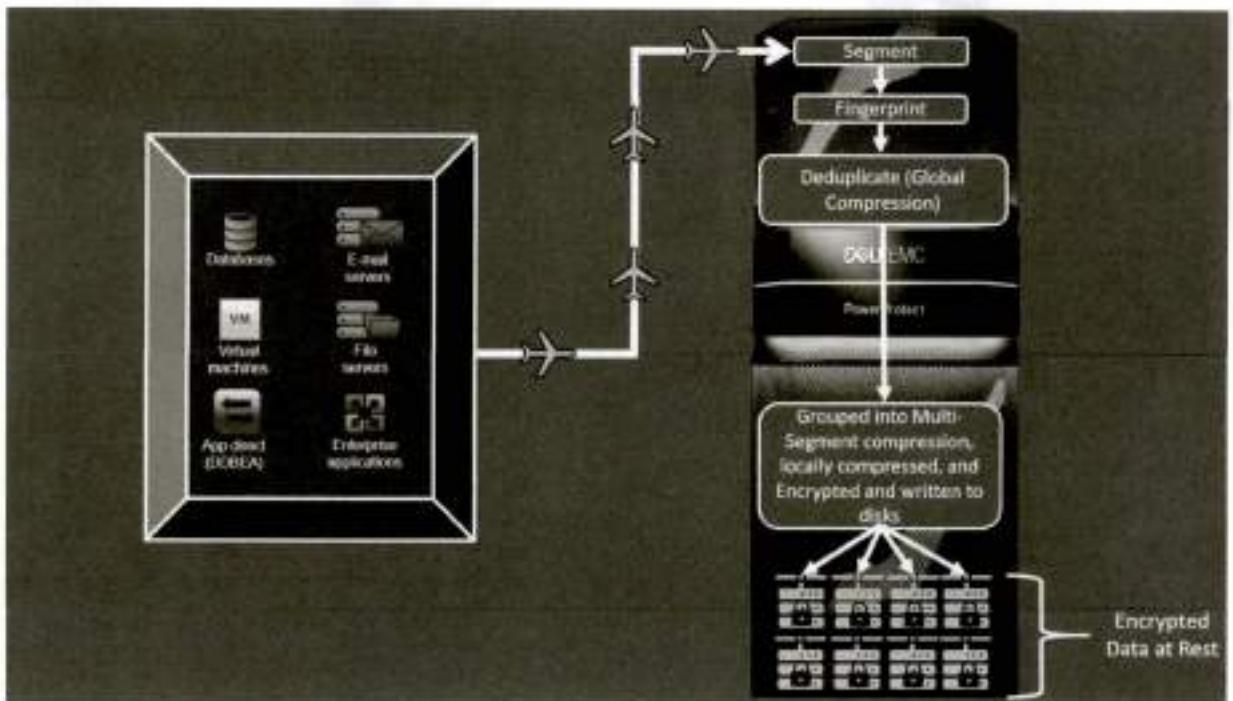


Figure 2 DD Encryption overview

Encryption is not enabled by default. When enabled, the Embedded Key Manager (EKM) is in effect. DD series appliances also support external key managers (SafeNet KeySecure and Vormetric Data Security Manager) that are compliant with the Key Management Interoperability Protocol (KMIP). External Certificate Authority (CA) and host certificates are required to set up SafeNet KeySecure Key Manager (KMIP). You can request these certificates from third-party certificate authorities or create them using the appropriate OpenSSL utility. If encryption is enabled on Cloud Tier, only EKM is supported.



You can select one of two cipher modes, Cipher Block Chaining (CBC) mode or Galois/Counter mode (GCM), to best fit your security and performance requirements. GCM is the most secure algorithm, but it is slower than the CBC mode. The system also uses 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 accessible to a user. Without the passphrase, the file system cannot be unlocked, and data is not accessible. For more information, see the document [Dell EMC DD OS Version 7.3 Administration Guide](#) (may require login).

### 1.1.2 Encryption of data in-flight using DD Replicator

Encryption of data in flight encrypts data that is being transferred using DD Replicator between two DD series appliances. It uses AES 256-bit encryption to encapsulate the replicated data over the wire. The encryption-encapsulation layer is immediately removed when it transfers to the destination system. Data within the payload can also be encrypted using DD Encryption.

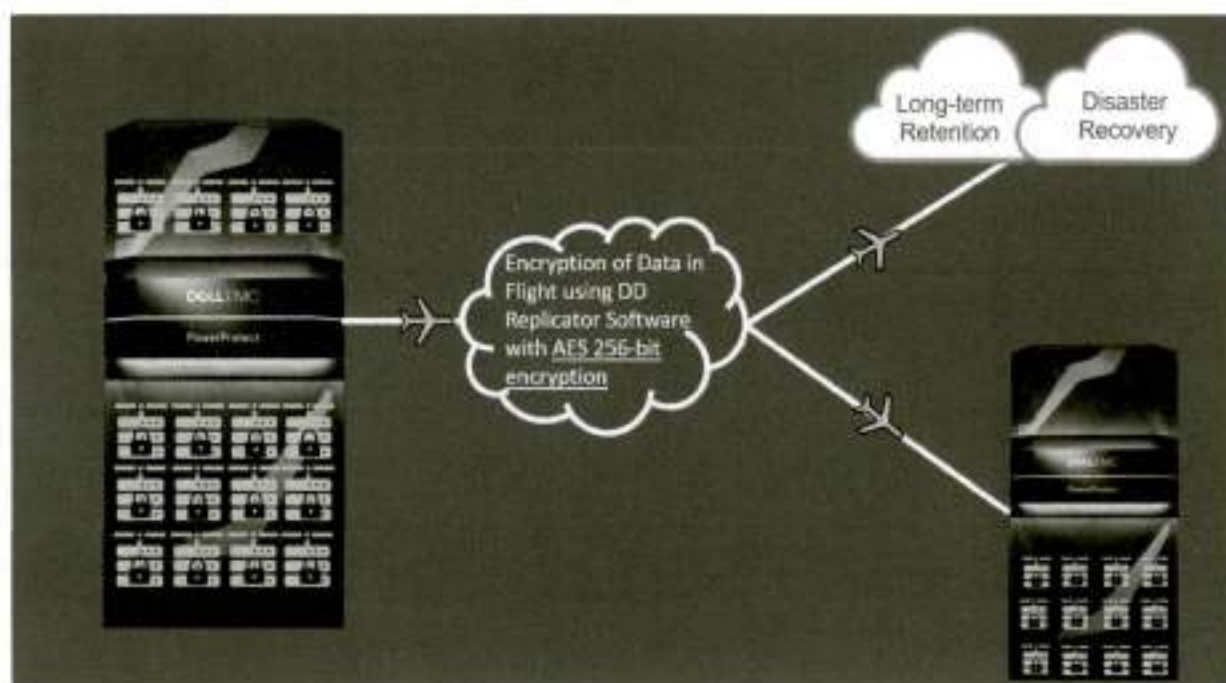


Figure 3 DD Replicator overview

#### 1.1.2.1 DD Replicator

DD Replicator provides automated, policy-based, network-efficient replication for disaster recovery, remote-office data protection, and multisite tape consolidation. DD 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 use a VPN for secure connections between sites, DD Replicator can securely encapsulate its replication payload over SSL with AES 256-bit encryption. This ability enables secure transmission over the wire, a process also known as encrypting data in flight.

#### 1.1.2.2 Encryption of data in-flight over NFS

NFSv3 and NFSv4 support Kerberos v5 protocol with integrity checking using checksums (krb5i) and Kerberos v5 protocol with privacy service (krb5p) for integrity and privacy, respectively. However, there are performance penalties for encryption.

### 1.1.3 Encryption of data in-flight with 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 system. When it is configured, the client can use TLS to encrypt the session between the client and the system. If TLS with certificates is used, 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, either of these options is used: ADH-AES256-SHA for the HIGH encryption option, or ADH-AES128-SHA for the MEDIUM encryption option.

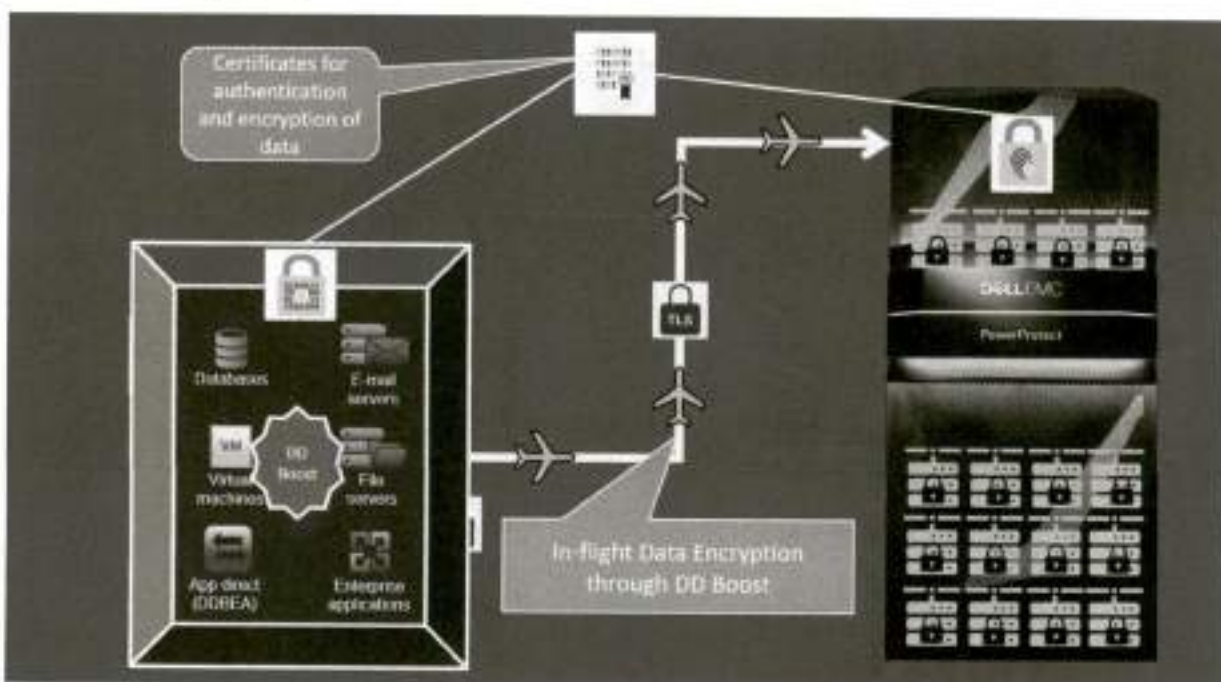


Figure 4 DD Boost overview

## 2 DD Encryption configuration

Use the following steps to configure DD Encryption.

1. To enable data encryption, in DD System Manager, click **Data Management > File System > DD ENCRYPTION** and click **Configure**.

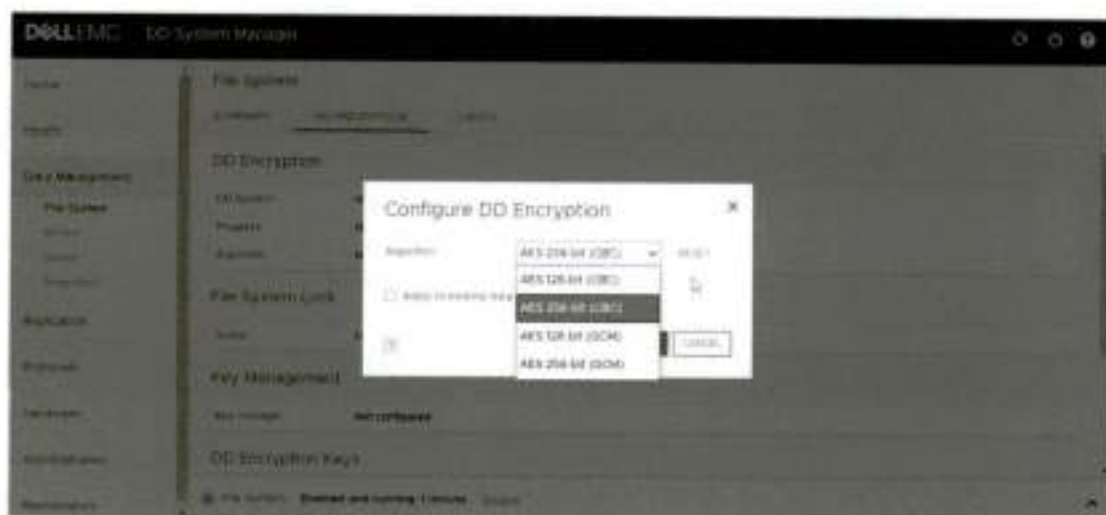


2. Enter the system passphrase to enable encryption.



## DD Encryption configuration

3. In the **Configure DD Encryption** window, use the **Algorithm** drop-down menu to select an encryption algorithm or accept the default **AES 256-bit (CBC)**. The AES 256-bit GCM is the most secure algorithm, but it is slower than CBC mode.



By checking the **Apply to existing data** option, the existing data will be encrypted during the first cleaning cycle after the file system is restarted. Encryption of existing data can take longer than a standard file-system-cleaning operation.



## DD Encryption configuration

4. In the **Change Key Manager** window > **Key Manager** section, select one of the following options in the **Type** drop-down menu:

- Embedded Key Manager
- KeySecure Key Manager (SafeNet KeySecure Key Manager)
- DSM Key Manager (Data Security Manager Key Manager)

**Change Key Manager** [X]

**Warning:** If you are using a Cloud Tier, you must obtain the encryption key from DD in order to encrypt your data.

**Security Officer Credentials**

User Name:

Password:

**Key Manager**

Type: **Embedded Key Manager** (dropdown menu showing: Embedded Key Manager, KeySecure Key Manager, DSM Key Manager)

Key rotation policy:

Key rotation schedule:  Monthly

Restart file system now  
The configuration will take effect after the file system is restarted.

[F] **OK** **CANCEL**

## DD Encryption configuration

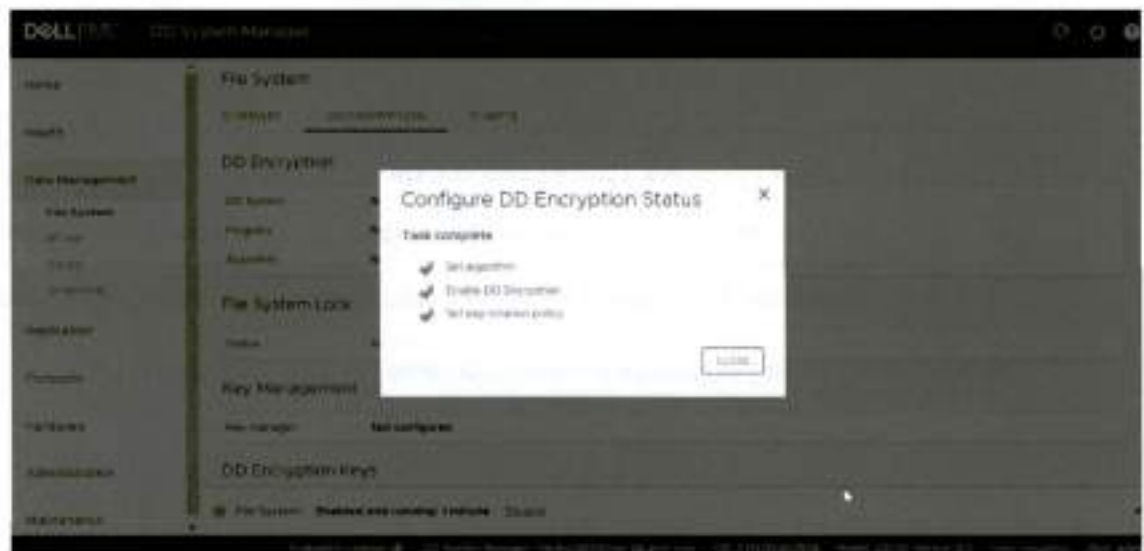
- When the encryption is enabled, by default the Embedded Key Manager is in effect after the file system is restarted. You can enable or disable key rotation. If enabled, enter a rotation interval between 1 month and 12 months.



- Review the configuration confirmation page, and click **Finish**.



- DD Encryption is now successfully configured with Embedded Key Manager.



## 2.1 Enabling and disabling DD Encryption

### 2.1.1 Enabling DD Encryption

Follow this procedure to enable the DD Encryption feature:

1. In DD System Manager, use the **Navigation** panel to select the protection system.
2. In the **DD Encryption** view, click **ENABLE**.



3. Select one of the following options and click **OK**.
  - **Apply to existing data:** Encryption of existing data occurs during the first cleaning cycle after the file system is restarted.
  - **Restart the file system now:** DD Encryption is only enabled after the file system is restarted.

---

**Note:** Applications may experience an interruption while the file system is restarted.

---

## 2.1.2 Disabling DD Encryption

Follow this procedure to disable the DD Encryption feature:

1. In DD System Manager, use the **Navigation** panel to select the protection system.
2. In the **DD Encryption** view, click **DISABLE**.



The **Disable Encryption** window displays.

3. In the **Security Officer Credentials** area, enter the username and password of a security officer.
4. Select one of the following and click **OK**.
  - **Apply to existing data:** Decryption of existing data occurs during the first cleaning cycle after the file system is restarted.
  - **Restart the file system now:** DD Encryption is only disabled after the file system is restarted.



## 3 Key management

Encryption keys determine the output of the cryptographic algorithm. They are protected by a passphrase, which encrypts the encryption key before it is stored in multiple locations on disk. The user generates the passphrase which requires both an administrator and a security officer to change it.

A key manager controls the generation, distribution, and life-cycle management of multiple encryption keys. A protection system can use either the embedded key manager or KMIP-complaint key manager such as SafeNet KeySecure or NextGen or Vormetric Data Security Manager. Only one key manager can be in effect at a time. When encryption is enabled on a protection system, the Embedded Key Manager is in effect by default. If the SafeNet KeySecure Key Manager is configured, it replaces the embedded key manager and remains in effect until it is disabled manually.

### 3.1 Embedded key manager

The embedded key manager provides and generates multiple keys internally, although the system uses only one key at a time to encrypt data coming into the system.

The embedded key manager rotates keys, supports a maximum of 254 keys, and allows you to specify how long a key will be in effect before it is replaced. The key rotation of the embedded key manager is managed on the protection system.

### 3.2 KMIP-compliant external key managers: KeySecure and Data Security Manager

DD series appliances support a KMIP-compliant key manager: KeySecure v8.5, v8.9, v8.10 and v8.12.1; NextGen v1.9.1 and v.10 from SafeNet or Gemalto; or Data Security Manager (DSM) 6.3 from Thales/Vormetric. To use a KMIP key manager, users must configure both the key manager and the protection system or DDVE to trust each other. A protection system retrieves these keys and their states from the key manager after establishing a secure TLS connection.

You can encrypt file-system data (active tier only) by configuring KeySecure, NextGen, or DSM as the key manager. You may manage keys from DD series appliances and configure a key-rotation policy for weekly or monthly automatic key rotation. You cannot enable external key managers (which include KeySecure, NextGen, and DSM) on systems that have encryption enabled on one or more cloud units, similar to Key Secure.

See the document [KMIP Integration Guide for DD OS](#) for more information about how to create keys and use them on a protection system.

### 3.3 Key manager support

All key managers support all DDOS file-system protocols.

#### 3.3.1 Replication

When configuring protection systems for directory or MTree replication, configure each system separately. The two systems can use either the same or a different key class, and the same or different key managers. For collection-replication configuration, you must configure the protection system on the source. All replicated



data is encrypted with the key set on the source. New data that is written to the destination after a replication break uses either the last active key set on the source or a new key if the key manager is configured.

### 3.3.2 Embedded key manager setup

When the embedded key manager is selected, the protection system creates its own keys. After the key-rotation policy is configured, a new key is automatically created at the next rotation. To disable the key-rotation policy, click the **Disable** button that is associated with the key-rotation status of the embedded key manager.

#### Create an encryption key:

1. Click Data Management > File System > DD Encryption.
2. In the **Encryption Keys** section, click **Create**.
3. Enter the security officer username and password.

A new protection system key is created and activated immediately.

4. Click **Create**.

#### Destroy an encryption key:

1. Click Data Management > File System > Encryption.
2. In the **Encryption Keys** section, click the key in the list to be destroyed.
3. Click **Destroy**.

The system displays the **Destroy** window that includes the tier and state for the key.

4. Enter the security officer username and password.
5. To confirm destroying the key, click **Destroy**.

You can delete key manager keys that are in the Destroyed or Compromised-Destroyed states. However, you can delete a key only when the number of keys has reached the maximum limit of 254 limit. This procedure requires security officer credentials.

#### Delete an encryption key:

1. Click Data Management > File System > Encryption.
2. In the **Encryption Keys** section, click the key or keys in the list to be deleted.
3. Click **Delete**.

The system displays the key to be deleted, and the tier and state for the key.

4. Enter the security officer username and password.
5. To confirm deleting the key or keys, click **Delete**.

### 3.3.3 Setting up a KMIP-complaint external key manager (KeySecure and DSM)

DD series appliances support external key managers by using KMIP, and centrally manage encryption keys in a single, centralized platform. Note the following:

- When applicable, you can precreate keys on the Key Manager.
- You cannot enable a KMIP key manager on systems that have encryption enabled on one or more cloud units.

#### 3.3.3.1 Using DD System Manager to set up and manage a KMIP-complaint key manager

Follow this procedure to create a key for the KMIP-complaint key manager:

1. In DD System Manager, scroll down to the **Key Manager Encryption Keys** table.
2. Click **Add** to create a new key manager encryption key.
  - a. Enter the security officer username and password.
  - b. Click **Create**.

A new KMIP key is created and activated immediately.

#### 3.3.3.2 Configuring the KMIP-complaint key manager

Follow this procedure to configure a KMIP-complaint key manager:

1. Click **Data Management > File System > DD Encryption**.
2. In the **Key Management** section, click **Configure**. The **Change Key Manager** dialog box opens.
3. Enter the security officer username and password.
4. In the **Key Manager Type** drop-down menu, click **KeySecure** or **DSM**. The **Change Key Manager** information appears.
5. Set the key rotation policy:
  - a. To enable the key-rotation policy, click the **Enable Key rotation policy** button.
  - b. Enter the appropriate dates in the **Key rotation schedule** field.
  - c. In the **Weeks** or **Months** drop-down menu, select the duration for the policy and click **OK**.

## 3.4 Key manager setup

For more information about setting up SafeNet KeySecure or the Thales/Vormetric DSM Key Manager, see the section "Setting up KMIP key manager" in the document [Dell EMC DD OS Version 7.3 Administration Guide](#).

## 4 File system lock

You can enable the file system lock when the DD-Encryption-enabled protection system and its external storage devices are being transported, or to lock a disk that is being replaced. This procedure requires two roles: security officer and system administration.

Follow this procedure to lock the file system:

1. Click **Data Management > File System > DD Encryption**.
2. In the **File System Lock** area, click **Lock**.



3. In the **Lock File System** window, enter the following and click **OK**.
  - The username and password of a security officer account (an authorized user in the Security User group on that protection system)
  - The current and a new passphrase

This procedure re-encrypts the encryption keys with the new passphrase. This process destroys the cached copy of the current passphrase (both in memory and on disk).

4. Shut down the system.
5. Transport the system or remove the disk being replaced.
6. Power on the system and use the following procedure to unlock the file system.

Follow this procedure to unlock the file system:

1. Select **Data Management > File System > Encryption** and click **Unlock**.
2. In the text fields, type the passphrase that was used to lock the file system.
3. Click **OK**, and click **Close** to exit.

**Note:** If the passphrase is incorrect, the file system does not start, and the system reports the error. Enter the correct passphrase as directed in the previous step.

## 5 Changing the encryption algorithm

If necessary, you can reset the encryption algorithm. Also, you can select options to encrypt new and existing data, or encrypt only new data.

Follow this procedure to change the encryption algorithm:

1. Click **Data Management > File System > Encryption**.
2. To change the Encryption Algorithm used to encrypt the protection system, click **Change Algorithm**.

The **Change Algorithm** window displays the supported encryption algorithms:

- AES-128 CBC
  - AES-256 CBC
  - AES-128 GCM
  - AES-256 GCM
3. Select an encryption algorithm from the drop-down box, or accept the default option of **AES 256-bit (CBC)**.

The AES 256-bit GCM is the most secure algorithm, but it is slower than CBC mode.

---

**Note:** To reset the algorithm to the default AES 256-bit (CBC), click **Reset to default**.

---

4. Determine what data will be encrypted:
  - To encrypt existing and new data on the system:
    - i. Click **Apply to Existing data**,
    - ii. Restart the file system.
    - iii. Click **OK**.
    - iv. Existing data will be encrypted during the first cleaning cycle after the file system is restarted.

---

**Note:** Encryption of existing data can take longer than a standard file-system-clean operation.

---

- To encrypt only new data, click **Restart file system now** and click **OK**.
5. The status is displayed. Click **Close** when the process is complete.

---

**Note:** Applications may experience an interruption while the file system is restarted.

---



## 6 DD Encryption with DD Replicator

DD Replicator can be used with the optional DD Encryption feature, enabling encrypted data to be replicated using collection, directory, or MTree replication.

Replication contexts are always authenticated with a shared secret. That shared secret is used to establish a session key using a Diffie-Hellman key exchange protocol. That session key is also used to encrypt and decrypt the protection system encryption key when appropriate.

### 6.1 Collection replication

In collection replication, the source and destination must have the same encryption configuration because the destination data is expected to be an exact replica of the source data. In particular, the encryption feature must be turned on or off at both the source and destination. If the feature is turned on, the encryption algorithm and the system passphrases must also match. The parameters are checked during the replication-association phase.

During collection replication, the source transmits the data in encrypted form, and transmits the encryption keys to the destination. The data can be recovered at the destination because the destination has the same passphrase and the same system encryption key.

---

**Note:** Collection replication is not supported for cloud-tier-enabled systems.

---

### 6.2 MTree or directory replication

In MTree or directory replication, encryption configuration does not have to be the same at both the source and destination. Instead, the source and destination securely exchange the destination's encryption key during the replication-association phase. The data is re-encrypted at the source using the destination's encryption key before transmission to the destination.

If the destination has a different encryption configuration, the data transmitted is prepared appropriately. For example, if the feature is turned off at the destination, the source decrypts the data, and it is sent to the destination as unencrypted.

### 6.3 Cascaded replication

In a cascaded-replication topology, a replica is chained among three systems. The last system in the chain can be configured as a collection, MTree, or directory. If the last system is a collection-replication destination, it uses the same encryption keys and encrypted data as its source. If the last system is an MTree or directory-replication destination, it uses its own key, and the data is encrypted at its source. The encryption key for the destination at each link is used for encryption. Encryption for systems in the chain works the same as in a replication pair.

## 7 DD Encryption and Cloud Tier

DD Encryption can be enabled at three levels: system, active tier, and cloud unit. Encryption of the active tier is only applicable if encryption is enabled for the system. Cloud units have separate controls for enabling encryption. Follow these steps to enable DD encryption for cloud units:

1. Click **Data Management > File System > DD Encryption**.

---

**Note:** If no encryption license is present on the system, the **Add Licenses** page is displayed.

---

2. In the **DD Encryption** panel, perform one of the following actions:
  - To enable encryption for **Cloud Unit X**, click **Enable**.
  - To disable encryption for **Cloud Unit X**, click **Disable**.

---

**Note:** You are prompted to enter security officer credentials to enable encryption.

---

3. Enter the security officer **Username** and **Password**.
4. Optionally, check **Restart file system now**.
5. Click **Enable** or **Disable**, as appropriate.
6. In the **File System Lock** panel, lock or unlock the file system.
7. In the **Key Management** panel, click **Configure**.
8. In the **Change Key Manager** window, configure the security officer credentials and the key manager.

---

**Note:** Cloud encryption is allowed only through the Embedded Key Manager. External key managers are not supported.

---

9. Click **OK**.
10. Use the **DD Encryption Keys** panel to configure the encryption keys.

If encryption is enabled for the cloud tier, any data written to the cloud or buckets is encrypted using the Embedded Key Manager (eKM) keys. The data is encrypted on the DD series appliance before it is written to the cloud. There is no end-to-end encryption, but data is always encrypted throughout the data movement.

If the encryption is disabled on the cloud tier, data is decrypted on the DD series appliance before it is sent over a TLS connection to the cloud. If the encryption is enabled on the cloud-provider side (for example, using ECS native encryption), the data is encrypted when it reaches that end point. Similarly, the data is decrypted at the endpoint and is transmitted over TLS when it is recalled or read from the DD series appliance.

---

**Note:** When using an embedded key manager, only the newly ingested data is encrypted. For example, encryption occurs for data that is ingested after embedded encryption is enabled, unless you run the **Apply changes** command. This command converts or encrypts all the existing unencrypted data.

---



## 8 Conclusion

DD series encryption software provides a robust, secure, data-management solution that can encrypt all user data stored on a DD series deduplication storage appliance. It protects user data from theft or loss of system, disk shelves, or disks, or for disks returned to factory. The DD series encryption software can help satisfy internal governance rules and helps with meeting compliance regulations.

DD Encryption helps meet compliance regulations by using industry standard AES- 128 or AES-256 encryption algorithms and the RSA BSAFE FIPS 140-2 validated cryptographic libraries. It also supports standard CBC and the stronger cipher mode GCM for additional security.

DD Encryption is transparent to all ingest protocols and backup or archiving applications, works with all DD series replication types.

## A Technical support and resources

[Dell.com/support](http://Dell.com/support) is focused on meeting customer needs with proven services and support.

[Storage and data protection technical white papers and videos](#) provide expertise that helps to ensure customer success with Dell EMC storage and data protection products.

### A.1 Related resources

- [Dell EMC PowerProtect DDOS Admin Guide](#)
- [Dell EMC DD OS Version 7.3 Administration Guide](#)
- [KMIP Integration Guide for DDOS](#)
- [DD OS 7.3 KMIP Integration Guide](#)



# Dell PowerProtect Cyber Recovery: Reference Architecture

October 2022

H18661.3

## Reference Architecture

### Abstract

This document describes the features and reference architecture of Dell PowerProtect Cyber Recovery—another layer of protection to customers' data protection infrastructure.

Dell Technologies

## Copyright

The information in this publication is provided as is. Dell Inc. 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 software described in this publication requires an applicable software license.

Copyright © 2022 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Intel, the Intel logo, the Intel Inside logo and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries. Other trademarks may be trademarks of their respective owners. Published in the USA October 2022 H18661.3.

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

## Contents

<b>Executive summary .....</b>	<b>4</b>
<b>Introduction .....</b>	<b>5</b>
<b>Cyber Recovery architecture .....</b>	<b>15</b>
<b>Integrating vault storage and applications with Cyber Recovery .....</b>	<b>23</b>
<b>MTree replication .....</b>	<b>28</b>
<b>Infrastructure service recommendations.....</b>	<b>31</b>
<b>Technical support and resources.....</b>	<b>33</b>



## Executive summary

### Overview

As organizations become increasingly aware of the cybersecurity risks that threaten their mission-critical operations and their reputation, IT security has become an essential part of enterprise digital strategy. According to the Gartner 2020 Board of Directors Survey, cybersecurity-related risk is rated as the second-highest source of risk for the enterprise, following regulatory compliance risk.

According to Gartner, 40 percent of boards of directors will have a dedicated cybersecurity committee overseen by a qualified board member by 2025. Currently, only 10 percent of companies have this type of committee. This is one example of many organizational changes that Gartner expects to see at the board, management, and security team level in response to greater risk created by the expanded digital footprint of organizations.

Global business relies on the constant flow of data across interconnected networks, and digital transformation has increased the transfer of sensitive data. This increased data flow presents ample opportunity for cyber threats, exposure of data for ransom, corporate espionage, or even cyber warfare.

Dell Technologies and Dell PowerProtect Cyber Recovery protect business-critical data and minimize the impact of a cyberattack. The PowerProtect Cyber Recovery solution offers a higher likelihood of success in the recovery of business-critical systems.

Cyber Recovery provides proven, modern, and intelligent protection to isolate critical data, identify suspicious activity, and accelerate data recovery. This protection allows normal business operations to resume quickly after a cyber-attack.

### Audience

This white paper is intended for Dell Technologies' customers, partners, and employees who would like to understand the PowerProtect Cyber Recovery solution.

### Revisions

Date	Description
June 2021	Initial release
April 2022	Updated white paper content with Cyber Recovery 19.10 version
August 2022	Updated white paper content with Cyber Recovery 19.11 version
October 2022	Updated white paper content with Cyber Recovery 19.12 version

### We value your feedback

Dell Technologies and the authors of this document welcome your feedback on this document. Contact the Dell Technologies team by [email](#).

**Author:** Vinod Kumar

---

**Note:** For links to other documentation for this topic, see the [PowerProtect Cyber Recovery Info Hub](#).

---

## Introduction

### Dell PowerProtect Cyber Recovery

PowerProtect Cyber Recovery enables automated workflows to augment data protection infrastructure with true data isolation, data forensics, analytics, and, most importantly, data recovery for increased business resiliency. Cyber Recovery combines multiple layers of protection and security into a turnkey solution to provide maximum protection for critical data.

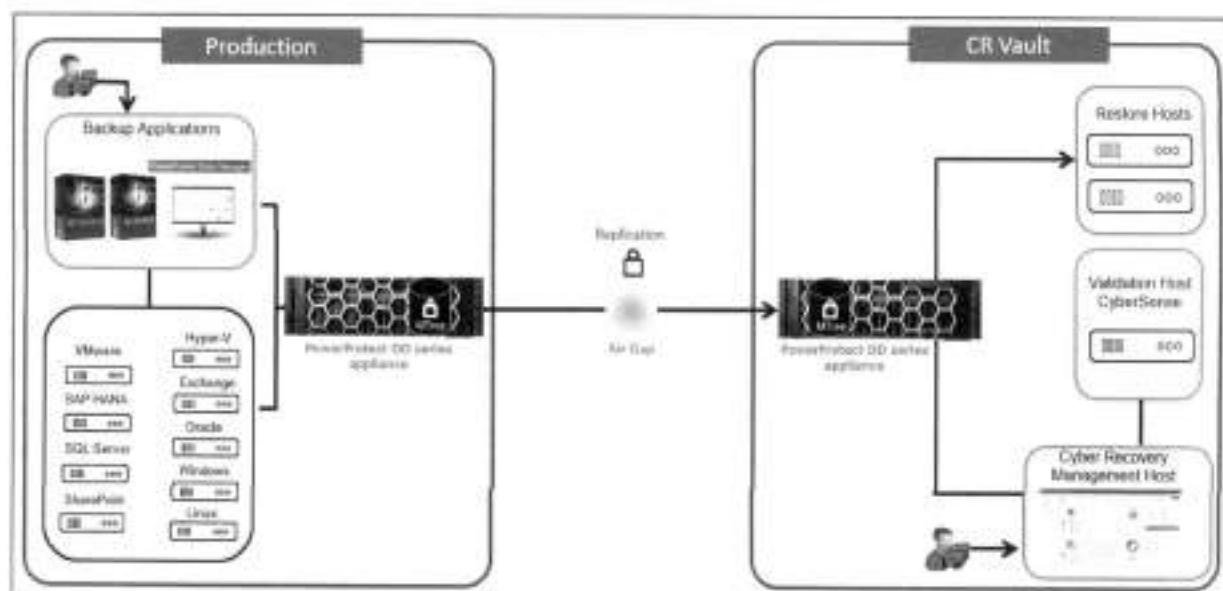
**Proven and modern  
Cyber Recovery  
solution:**

PowerProtect Cyber Recovery

- ✓ Data Isolation and Governance
- ✓ Automated Data Copy and Air Gap
- ✓ Intelligent Analytics and Tools
- ✓ Recovery and Remediation
- ✓ Solution Planning and Design

The Cyber Recovery solution protects the backed-up mission-critical business data and technology configurations in a secure vault environment that can be used for data recovery. The management software also enables creation of writable sandbox copies for data validation and analytics.

The Cyber Recovery vault is disconnected from the production network through an automated air gap. The vault stores all critical data off-network to isolate it from attack. Cyber Recovery automates data synchronization between production systems and the vault by creating immutable copies with locked retention policies.



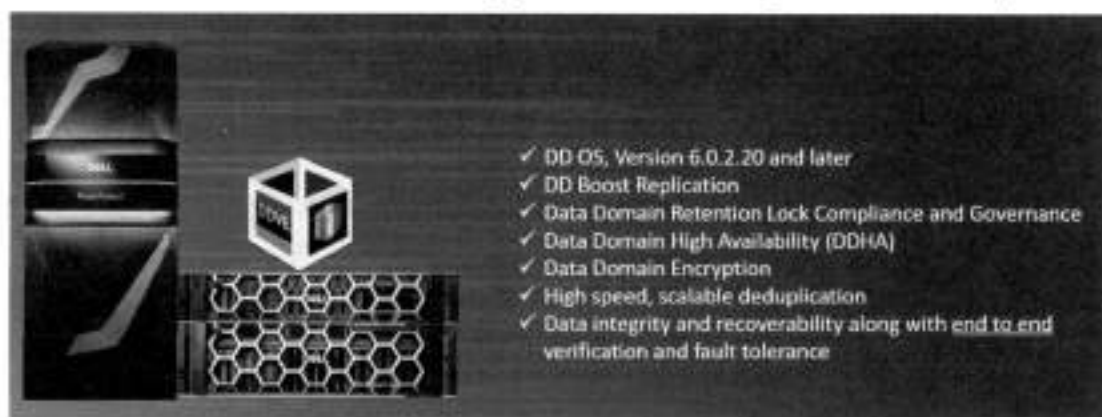
If a security breach occurs, the Security Officer or an admin user can manually secure the Cyber Recovery vault. During this time, the Cyber Recovery software does not perform any replication operations, even if they are scheduled. This action promotes business resiliency, provides assurance following extreme data loss or destruction, and includes both business and technology configuration data to enable rapid recovery of the environment and resumption of normal business operations.

#### Dell PowerProtect DD series appliances for Cyber Recovery

PowerProtect DD series appliances are fast, secure, and efficient data protection appliances that support the Cyber Recovery solution and accommodate a unique Cyber Recovery vault.

Cyber Recovery works with DD series MTree replication technology to move and retain the protected copies of critical data in the Cyber Recovery vault. Cyber Recovery supports up to five DD series in the Cyber Recovery vault.

### Dell PowerProtect series appliances for Cyber Recovery



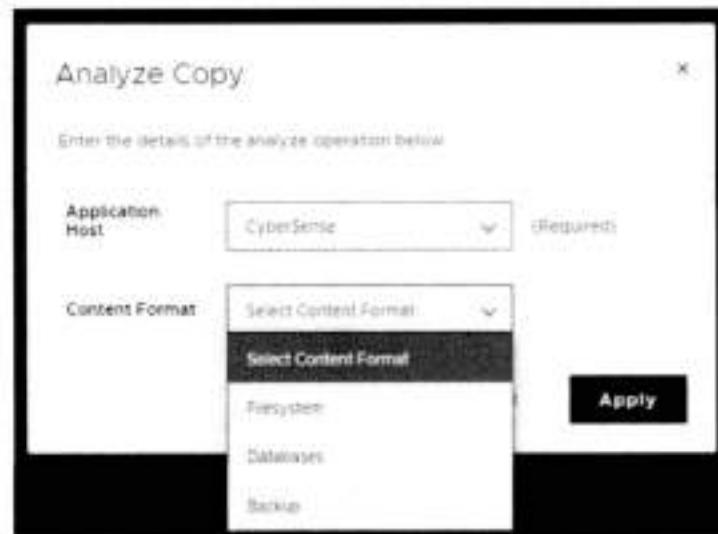
Required DD series licenses for Cyber Recovery include DD Boost, Replication, Retention Lock Governance, and Retention Lock Compliance.

## Cyber Recovery features

The Cyber Recovery solution key features include:

- Secure data in an isolated network with an automated operational air gap
- Policy-based secure copy creation, management, and scheduling
- Integration with Index Engine CyberSense software to detect if the backup data has been compromised
- Robust REST API framework that enables analytics with artificial intelligence (AI) and machine learning (ML) for malware (including ransomware). Cyber Recovery REST API availability on [Dell Marketplace](#) and [Stoplight](#)
- Recovery assistance and the ability to export data to a recovery host easily
- Automated recovery options for the NetWorker and PowerProtect Data Manager applications
- Optional multifactor authentication enabled from the UI or command-line interface (CLI) to provide added protection for the Cyber Recovery software and its resources
- Informative dashboards that show system alerts, the state of the Cyber Recovery vault, and critical details
- Ability to transmit alerts through SMTP outside the Cyber Recovery vault
- Support for high availability (HA) on DD series in the Cyber Recovery vault
- Replication window enforcement that stops a sync operation if it runs longer than the replication window
- Automatic retention locking feature that allows setting of retention lock with no additional operation. Cyber Recovery deployments running DDOS 7.8 support replicating a Retention Lock Compliance replication on the production system to the Cyber Recovery vault
- Ability to create a Cyber Recovery policy by selecting multiple MTree replication contexts (multiple MTrees are only supported for a PowerProtect Data Manager policy)
- Cyber Recovery supports subscription licensing model along with evaluation or proof-of-concept license that is valid for 90 days
- Sheltered Harbor endorsement for achieving compliance with financial institution data vaulting standards and certification, planning for operational resilience and recovery, and protecting financial critical data
- On-demand cleanup from the Cyber Recovery UI by clicking the **Maintenance** tab under the gear icon in the masthead navigation
- A maximum of three simultaneous login sessions for the Security Office (crso) for enhanced security
- Notification if a user's email address is modified or if multifactor authentication is disabled

- Option to add a virtual Ethernet adapter to configure a separate IP address for SMTP communication from the Cyber Recovery vault if the Postfix mail transfer agent is used
- Support for recovery of PowerProtect Data Manager with Oracle, SQL, and file system workloads
- Option to provide the location of the latest bootstrap backup for a faster automated NetWorker recovery
- Support for the Cyber Recovery vault on Amazon Web Services (AWS), available from Amazon Marketplace using custom pricing
- Support for the Cyber Recovery software on a supported Linux operating system in a Microsoft Hyper-V environment
- Support for the analyze operation for PowerProtect Data Manager backups (Filesystem, VMware, and Oracle) is enabled
- Addition of REST API V6, which is backwards compatible with REST API V5 and V4. REST API V3 and earlier versions are no longer supported
- The `crsetup.sh` script to perform a readiness check before upgrading the Cyber Recovery software
- Support for multiple DDVE appliances for the Cyber Recovery vault on AWS—up to 5 DDVEs are supported
- CyberSense analysis report can be sent to additional email addresses
- Cyber Recovery telemetry feature sends telemetry information using one-way email to Dell Technologies for troubleshooting purposes. Telemetry can be run on demand using CRCLI or scheduled to run with frequency of minimum of one day and maximum of 30 days
- Cyber Recovery custom certificate support: users can generate a Certificate Signed Request (CSR), submit the CSR to Certificate Authority (CA) to apply for a CA signed certificate, and can add it to the Cyber Recovery system
- Secure reset option to regenerate the Cyber Recovery certificates – Starting with Cyber Recovery version 19.11, the `crsetup.sh` script includes an option that allows you to reset the Cyber Recovery root certificates and encryption keys when your deployment is compromised.
- From CRCLI and API, users have the option to:
  - Include or exclude files and file path from the analyze action
  - The content format of the MTree to be analyzed can be specified optionally, which is included as part of the CyberSense report for informational purposes



- Password expiration is set to 90 days by default; the value can be changed to a minimum of 30 days and a maximum of 180 days for all UI users

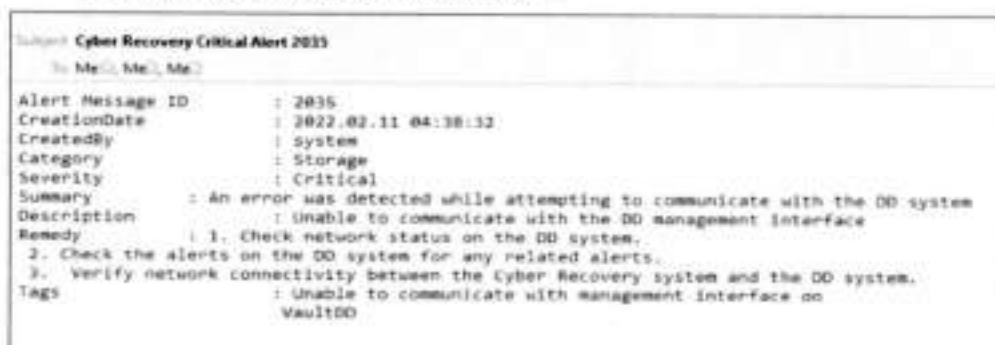
#### Cyber Recovery alert services

- DD series capacity alert
  - Cyber Recovery notifies a user if the Secure Copy/Sync operation fails due to space issues in Vault Data Domain. If the DD system in the Cyber Recovery vault generates a capacity alert, the Cyber Recovery software displays it as warning or critical alert on the dashboard and on the Alerts tab. The threshold capacity can be set on the DD system.



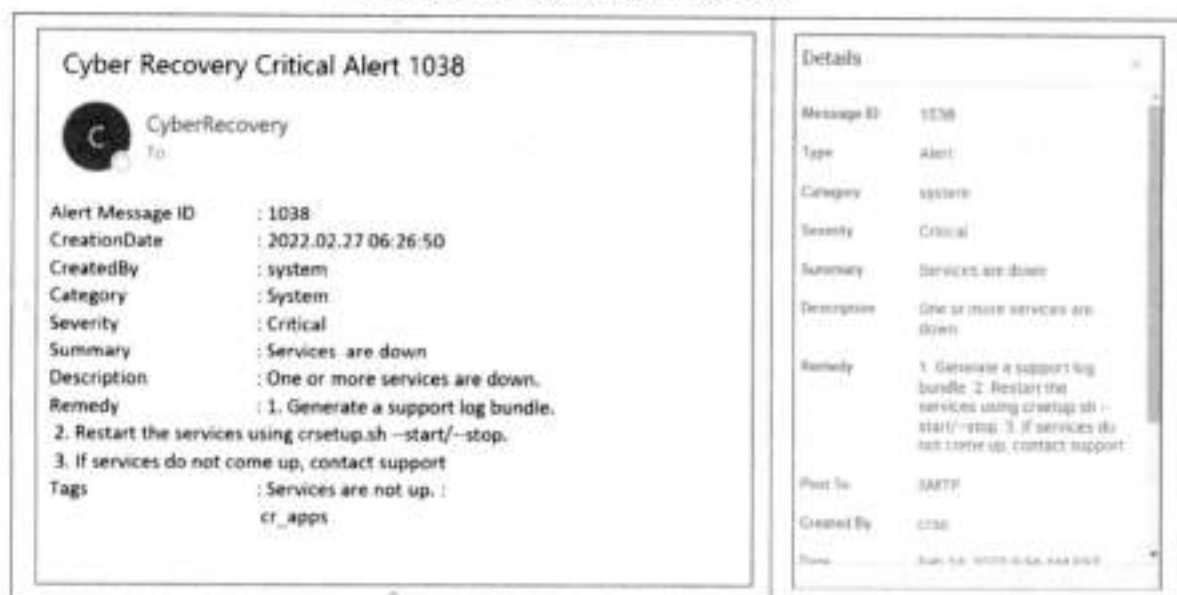


- Alert when one or more DD series is down:



When a DD series in the Cyber Recovery vault is down, the Cyber Recovery software generates a critical alert that is displayed on the dashboard and on the Alerts tab. It also sends an email message to user accounts that are configured to receive email messages. The vault status is displayed as Degraded (orange icon) until the DD system is up and running again.

- Monitor Cyber Recovery services
  - Cyber Recovery 19.10 monitors its services in the background and alerts every hour after initial critical alert if one or more Cyber Recovery service is down. If a Cyber Recovery service stops, the Cyber Recovery software displays a critical alert on the dashboard and the Alerts tab. Use the `crsetup.sh` script to restart the service.



### Cyber Recovery UI support menu

Cyber Recovery 19.10 provides a new support menu for users in Cyber Recovery UI. Users can generate and download the support bundle from Cyber Recovery UI.



### CyberSense host information in copy details

Cyber Recovery provides information about the analysis host which analyzed the copy in the copy details. This information helps users to identify the Cyber Sense details for environments with more than one CyberSense host.



### Policy network interfaces

Users can use eth V1 for analysis or for Cyber Recovery policy but cannot use both at the same time. For example, only ethV0 is listed in the following figure because ethV1 is being used for the Cyber Recovery policy.

### Analyze Copy

Select analyze options.

**Application Host**  (Required)

**Advanced Options**    
 If Storage Data interface is not selected, the default is used in analyze operation. To include and exclude files, select a file or specify a file or directory name in the text box. Each file name or directory name must be on a separate line.

**Content Format**

**Storage Data Interface**

**Files/Directories to Include**

**Files/Directories to Exclude**

### CyberSense analyze dashboard link from Cyber Recovery jobs

Starting with Cyber Recovery version 19.12, the job details section and policies/copies section have links that open the CyberSense analyze dashboard when a copy is found to be suspicious.

The screenshot shows the 'Protection Jobs' section of the Dell PowerProtect Cyber Recovery console. A summary bar indicates 6 Total jobs, 1 Failed, 0 Completion/Exposure, 5 Successful, and 0 Cancelled. Below this is a table of jobs with columns for Name, Status, Policy Name, Request, Run Time, and Exposed Time. The 'Details' column for each job contains a link to the CyberSense analyze dashboard. The details panel on the right shows the selected job's information, including the job name and a link to the analyze dashboard.

Name	Status	Policy Name	Request	Run Time	Exposed Time	Details
policy 01740	Failed	01740	analyze	04/15/2022 1:00:00L	04/15/2022 1:00:00L	<a href="#">Details</a>
policy 01741	Successful	01741	analyze	04/15/2022 1:00:00L	04/15/2022 1:00:00L	<a href="#">Details</a>
policy 01742	Successful	01742	analyze	04/15/2022 1:00:00L	04/15/2022 1:00:00L	<a href="#">Details</a>
policy 01743	Successful	01743	analyze	04/15/2022 1:00:00L	04/15/2022 1:00:00L	<a href="#">Details</a>
policy 01744	Successful	01744	analyze	04/15/2022 1:00:00L	04/15/2022 1:00:00L	<a href="#">Details</a>
policy 01745	Successful	01745	analyze	04/15/2022 1:00:00L	04/15/2022 1:00:00L	<a href="#">Details</a>

### CyberSense analyze dashboard

CyberSense analyze dashboard is a UI that was designed specifically for CyberSense workflow. It provides the ability to scope and analyze a potential attack in a single dashboard.



### Links to the Alerts and Events page

Starting with Cyber Recovery version 19.12, any failed jobs that generated alerts have links to the "Alerts and Events" page and show the alert details.



## Cyber Recovery users and access management

**Multiple security officer roles:** Starting with Cyber Recovery version 19.12, the Cyber Recovery security officer (crso) can create multiple security officer roles and manage those accounts. The security officer has the same permissions as the crso but cannot manage the crso account.



**Note:** Security officer users cannot create other security officer users. The "Admin" role will no longer be able to create users.

**Users' deletion:** Starting with Cyber Recovery version 19.12, the crso and security officer can delete security officer, admin, and dashboard users from the Cyber Recovery UI.



**Note:** One cannot add a user with the same username of a previously deleted user. Instead, add a user that has a different username.

## Cyber Recovery support matrix

For details about compatibility, see the [Dell PowerProtect Cyber Recovery Simple Support Matrix](#).

## Cyber Recovery architecture

**Production environment**— For the production side of the solution, it is taken that the data to be protected as part of the Cyber Recovery solution is available in a format supported by the DD series and CyberSense. The data must be stored on a DD series MTree in the production environment.

**Vault environment**—The Cyber Recovery vault environment contains a DD series and the Cyber Recovery management host that runs the Cyber Recovery software. Data from the production environment enters the Cyber Recovery vault environment through DD series MTree replication. This environment can also contain various recovery and analytics/indexing physical or virtual hosts that integrate with the solution.

Cyber Recovery integrates with the Integrated Data Protection backup solution to maintain mission-critical business data in a secure vault environment for data recovery.

Server infrastructure is installed in the vault environment and is not shared with or connected to the production environment. Keeping vault server equipment separate from the production environment ensures that any ongoing issues (cyberattacks, operational issues, and so on) do not propagate into the vault environment.

Additional safeguards include an automated operational air gap that provides network isolation and eliminates management interfaces.

The server infrastructure in the Cyber Recovery vault can be deployed in multiple ways:

- Discrete physical servers
- Hyper-V, VMware ESXi with or without VSAN
- Dell VxRail appliance

### Cyber Recovery solution components

The Cyber Recovery solution includes the following components:

**Production DD series**—The source DD series contains the production data that the Cyber Recovery solution protects.

**Vault DD series**—The DD series system in the Cyber Recovery vault is the replication target for the source DD series.

**Cyber Recovery software**—The Cyber Recovery software orchestrates synchronization, manages, locks the multiple data copies that are stored on the DD series in the Cyber Recovery vault, and orchestrates recovery. The software also governs the optional process of performing analytics on data that is stored on the DD series in the Cyber Recovery vault using the CyberSense feature.

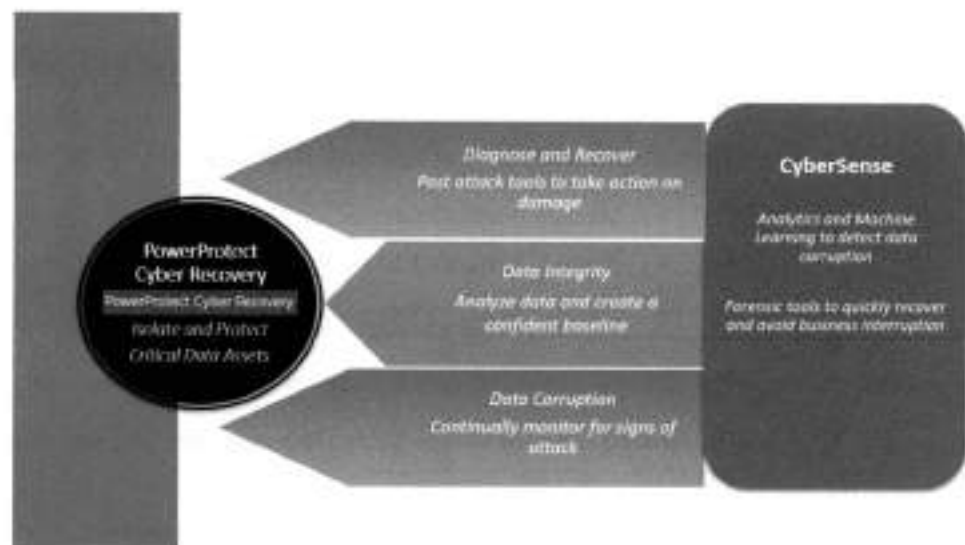
**Retention Lock (governance or compliance) software**—Data Domain Retention Lock technology provides data immutability for a specified time. Retention Lock functionality is enabled based on Cyber Recovery policy configuration.

**Cyber Recovery management host**—Cyber Recovery software is installed on the management host. This server is installed in the vault environment.



**Recovery hosts**—The backup application recovery server is a designated server to which the backup application (NetWorker, Avamar, PowerProtect Data Manager, or other applications or combination of applications) and backup application catalog are recovered. Multiple servers can be deployed, depending on the recovery requirements of the solution. The backup application recovery server is sized so that all backup applications that are being protected by the Cyber Recovery solution can be recovered. If the Cyber Recovery solution is protecting a physical, single-node Avamar system in a production environment, a single-node Avamar system must also reside in the vault for recovery purposes.

**Analytics/indexing host (CyberSense)**—Cyber Recovery is the first solution to fully integrate with CyberSense. CyberSense adds an intelligent layer of protection to help find data corruption when an attack penetrates the data center. CyberSense is deployed on the Cyber Recovery vault environment. This innovative approach provides full content indexing. It uses machine learning (ML) to analyze the backup copies in the vault with over 100 content-based statistics and detects signs of corruption due to ransomware. CyberSense detects corruption with up to 99.5 percent confidence, identifies threats, and diagnoses attack vectors while protecting the business-critical content – all within the security of the vault.



#### Enhancements with CyberSense Version 7.9:

- Improved performance when indexing Dell Technologies backups on the PowerProtect DD server by using the DD Boost delta block API. CyberSense supports both performance Optimized and Capacity Optimized backups.
- Improved performance for the following workloads:
  - For Avamar - VMDK
  - For NetWorker - VMDK and file system Block Based Backup (BBB)
  - For PowerProtect Data Manager - VMDK, file system BBB, and Exchange

#### Enhancements with CyberSense Version 8.0:

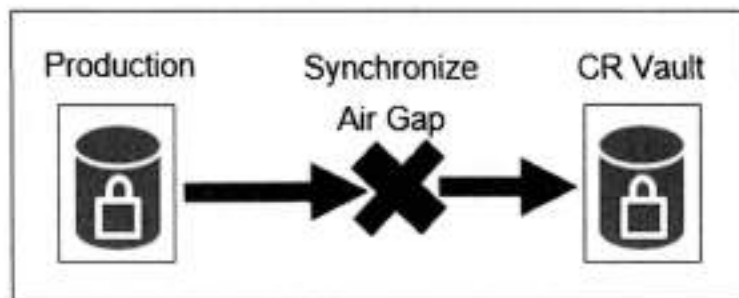
- An OVA deployment option is available.

- CyberSense support for SELinux Linux - SELinux can be set to "active" and "Enforcing" to meet STIGs requirement
- CyberSense can be deployed on AWS using an AMI which will be shared with customers' AWS accounts by Dell Technologies
- Support for CyberSense migration from RHEL to SLES - Migrate data from a RHEL server to a SLES server
- CyberSense analyze dashboard - Provide a UI that was designed specifically for CyberSense workflow

#### Logical air gap

The term "air gap" implies physical isolation from an unsecure system or network. Logical air gap describes a physical connection but logical isolation from the network. The logical air gap provides another layer of defense by reducing the surface of attack.

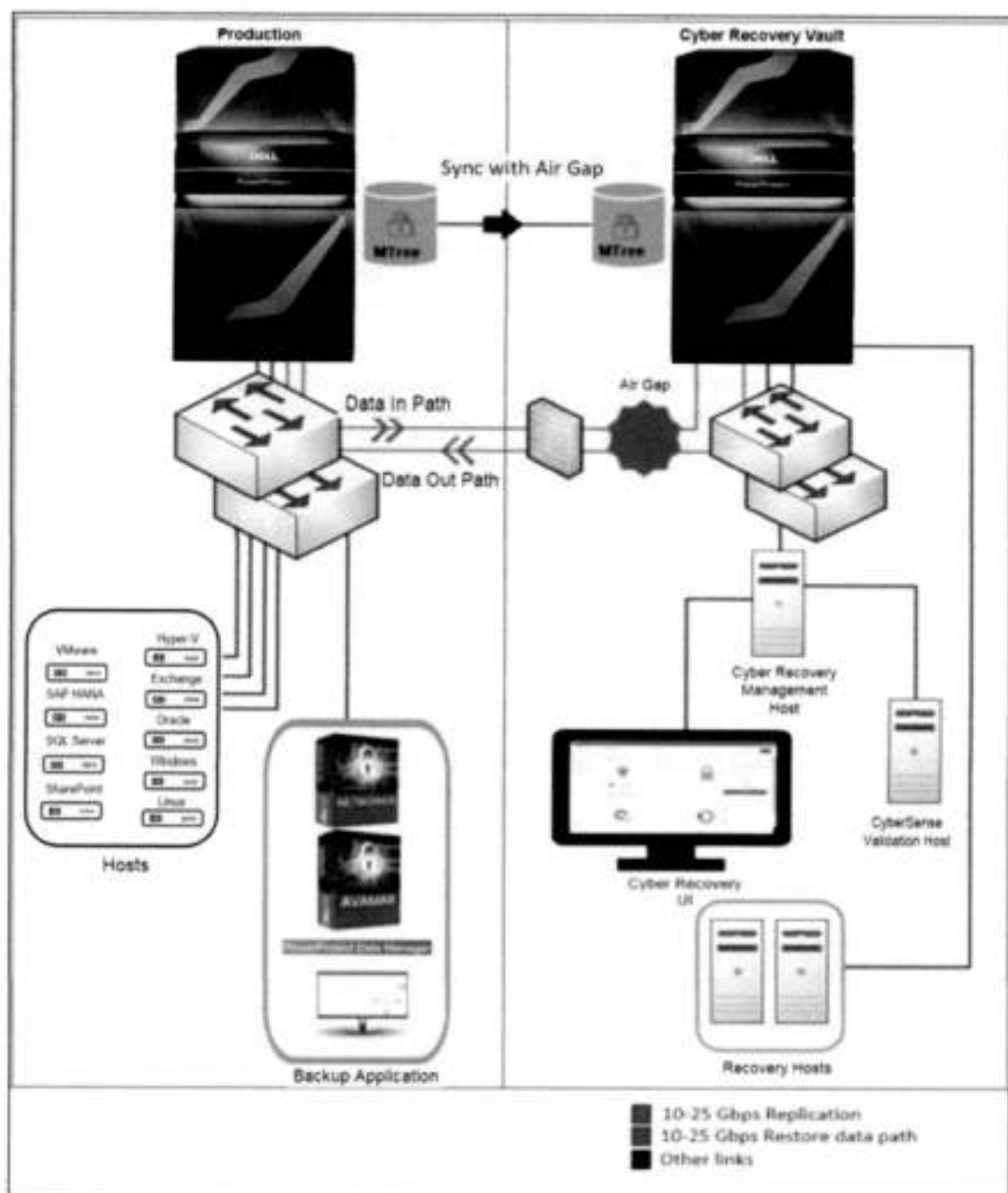
Cyber Recovery provides the air-gapped feature to keep the Cyber Recovery vault disconnected from the production network. The DD series in the Cyber Recovery vault is disconnected (air-gapped) from the production network most of the time and is only connected when Cyber Recovery triggers replication.



The DD series in the Cyber Recovery vault is connected to the production DD series only during the data synchronization operation.

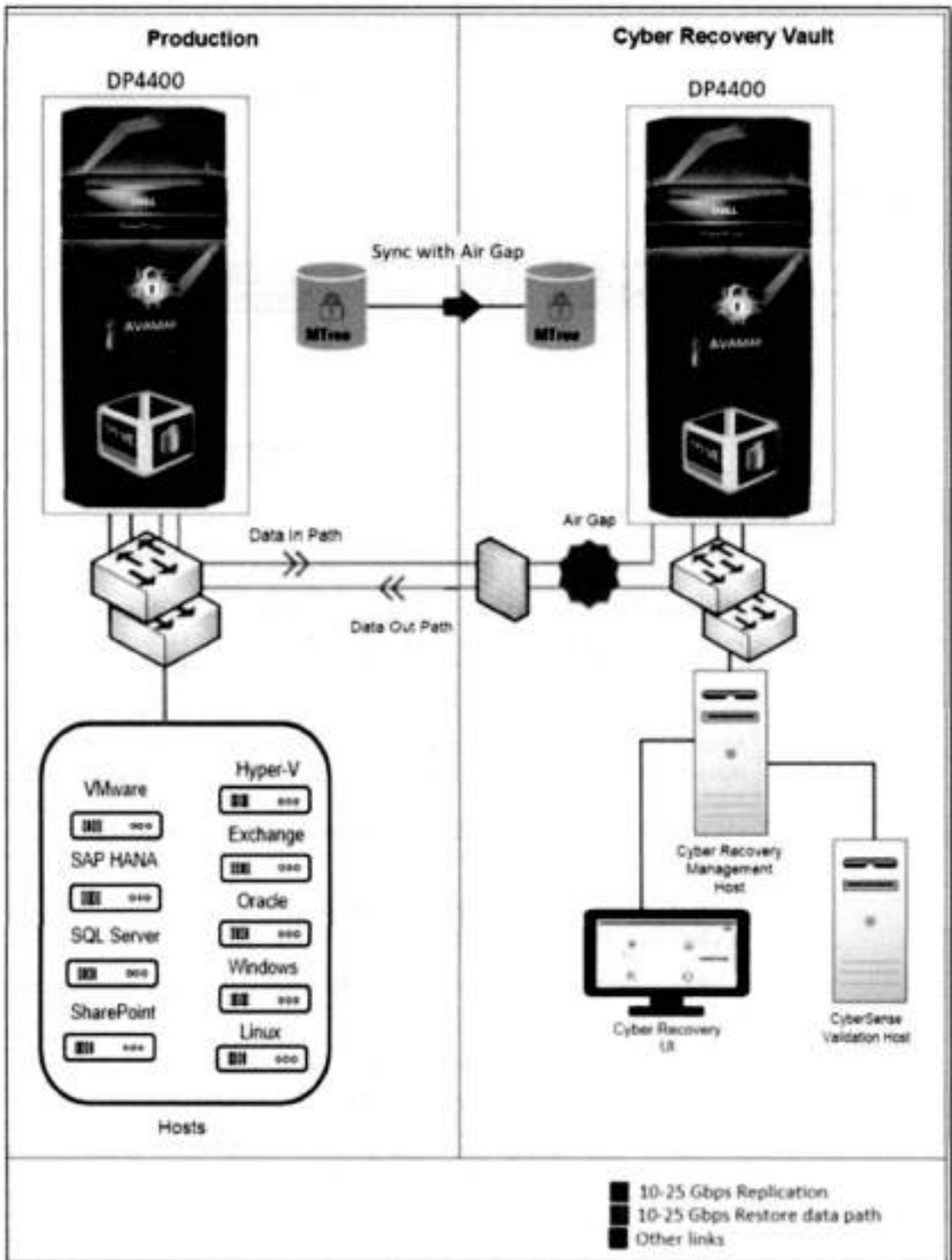
**Cyber Recovery integration with DD series**

The reference architecture below represents Cyber Recovery solution integration with DD series. The Cyber Recovery solution uses DD series to replicate data from the production system to the Cyber Recovery vault through a dedicated replication data link.



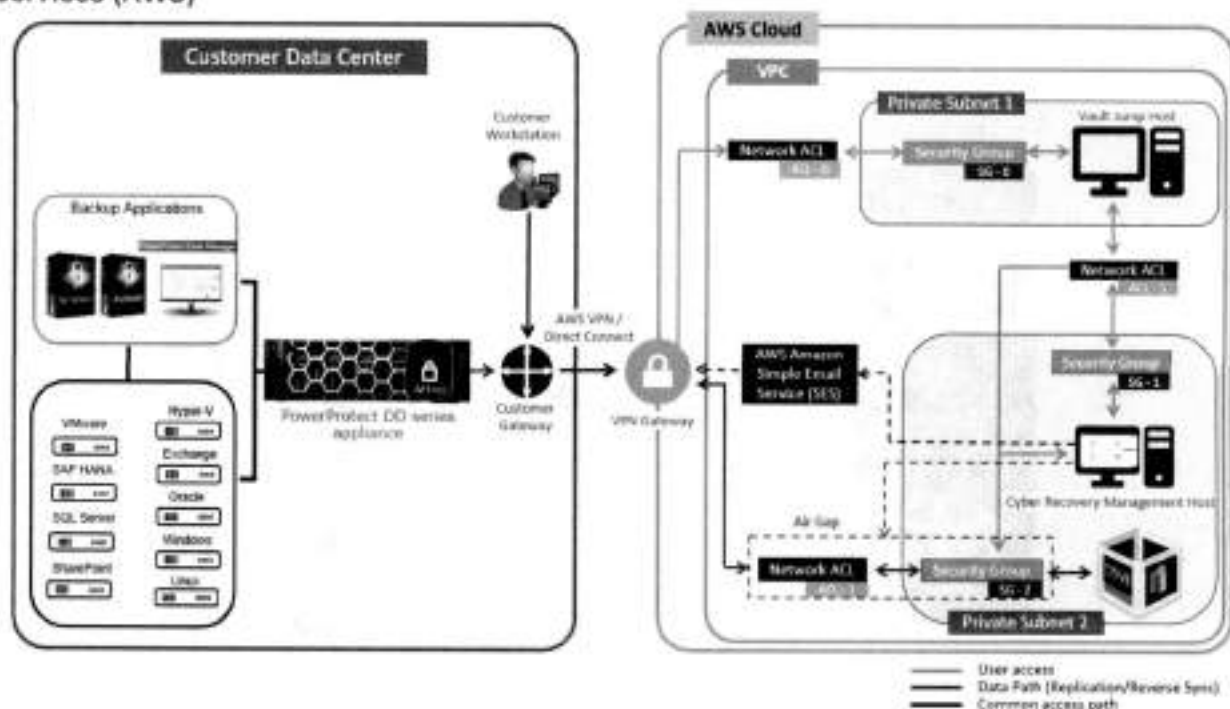
Cyber Recovery integration with the IDPA (DP4400)

The reference architecture below represents Cyber Recovery solution integration with IDPA.



**Cyber Recovery on Amazon Web Services (AWS)**

The Cyber Recovery vault is supported on AWS starting with Cyber Recovery 19.7 and later versions. The Cyber Recovery solution is also supported in AWS GovCloud.



The Cyber Recovery software is available as an Amazon Machine Image (AMI). To deploy the Cyber Recovery software to an Elastic Compute Cloud (EC2) instance in a Virtual Private Cloud (VPC), use an AWS CloudFormation template.

The CloudFormation template deploys all the components that the Cyber Recovery solution requires in the VPC on AWS. The template creates two private subnets: A private subnet that includes the jump host and a private subnet that includes the Cyber Recovery management host and DDVE. It also configures security groups, Access Control Lists (ACLs), inbound and outbound rules. The vault jump host can be accessed using a VPN gateway or an AWS Direct Connect.

Cyber Recovery software is also available as additional purchase option through AWS Marketplace using custom pricing.

AWS provides VPC security mechanisms for additional security measures for the Cyber Recovery vault:

- Security groups, which protect the instances deployed in the VPC
- Network access control list (ACL)

The Cyber Recovery software enables and disables access to a private subnet through a network access control list (network ACL) and enables and disables access to an instance through security groups.

## CyberSense on AWS

Starting with Cyber Recovery version 19.12, Cyber Recovery vault on AWS supports the CyberSense software. With CyberSense version 8.0, CyberSense software can be integrated with Cyber Recovery vault on AWS to analyze your data.

CyberSense 8.0 can be deployed on AWS using an AMI. On request, Dell Technologies provides access to the AMI that is required to deploy the CyberSense software on AWS. The AMI must be deployed in the same subnet with the Cyber Recovery management host and the vault DDVE. The jump host, deployed by the CloudFormation template as part of the Cyber Recovery vault deployment on AWS, enables access to the CyberSense host.

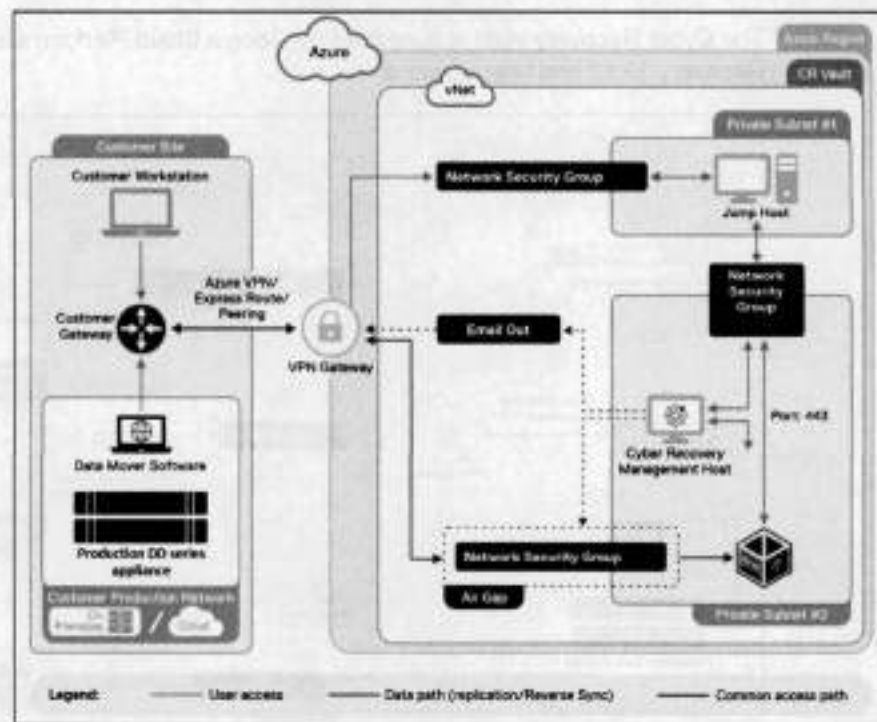
**Note:** Contact Dell Technologies team to deploy CyberSense on AWS.

For more details, see the [Dell PowerProtect Cyber Recovery AWS Deployment Guide](#).

## Cyber Recovery on Microsoft Azure

The Cyber Recovery solution is available on Microsoft Azure. The Cyber Recovery vault is deployed using the Azure Resource Manager (ARM) template.

The Cyber Recovery vault deployment is fully automated based on the template provided by Dell Technologies. On request, Dell Technologies provides access to the ARM template and VM Image that are required to deploy the Cyber Recovery solution. The ARM template deploys all the necessary Cyber Recovery vault components.



The ARM template creates:

- The Resource Group—The Resource Group includes all the components required for the Cyber Recovery solution.



## Cyber Recovery architecture

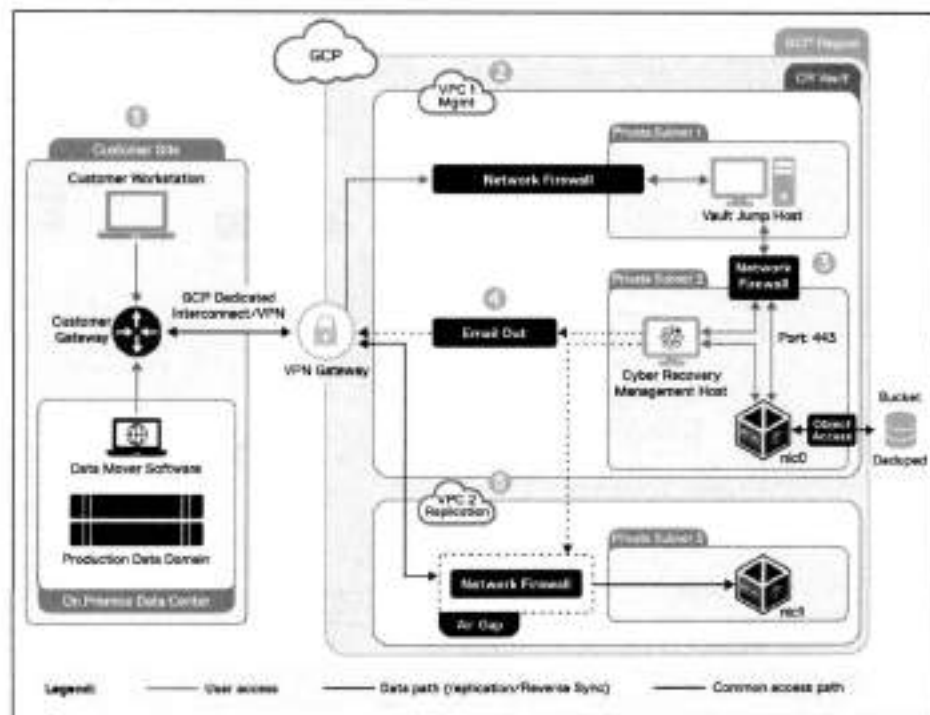
- The Virtual Network (VNet)—The network that the various components use to communicate with each other.
- Two subnets—The two private subnets include:
  - An Azure jump host on one subnet
  - The Cyber Recovery management host and DDVE on the other subnet
- Network Security Groups—The Network Security Groups and VMs provide a layer of security for the VNet that acts as a virtual firewall for controlling traffic in and out of the subnets.
- VNet endpoints—The VNet endpoints enable private connections between the VNet and supported Azure services.
- Identity and Access Management (IAM) roles—Along with the VNet endpoints, the roles provide access to Azure services for specific VMs.
- A storage account—The storage account includes a container for the DDVE storage.

The Cyber Recovery management host and vault DDVE are deployed on an isolated subnet and the jump host is deployed on a separate subnet. The Cyber Recovery management host and vault DDVE can be accessed only through the jump host.

For more details on how to deploy the Cyber Recovery solution on Azure, see the [Dell PowerProtect Cyber Recovery Azure Deployment Guide](#).

## Cyber Recovery on Google Cloud Platform

The Cyber Recovery vault is supported on Google Cloud Platform starting with Cyber Recovery 19.12 and later versions.



The Cyber Recovery software is made available as a VM image. The basic Cyber Recovery solution on Google Cloud Platform architecture includes a single region, two Virtual Private Clouds (VPCs), and a single availability zone (AZ).

To deploy the Cyber Recovery software in Google Cloud Platform, use a Terraform template.

The Terraform template creates:

- Two Cyber Recovery VPCs: The VPCs include all the components required for the Cyber Recovery solution.
- Three subnets: The three private subnets include:
  - A subnet with the Google Cloud Platform jump host
  - A subnet with the Cyber Recovery management host and DDVE
  - A subnet with a second DDVE network interface that is used for replication

---

**Note:** The production workstation cannot access the Cyber Recovery management host directly. The Windows-based jump host is available in the VPC to access the Cyber Recovery and DDVE instances. The management path is through the jump host.

---

- Firewall rules

The Terraform template also deploys a Google Cloud Platform jump host. The Windows-based jump host is available in the VPC to access the Cyber Recovery and DDVE instances. The management path is through the jump host.

Back up data is stored in a storage bucket with a high level of deduplication.

The Cyber Recovery deployment using Terraform does not include a VPN. We strongly recommend that you:

- Set up a VPN.
- Use a VPN gateway or Google Cloud Interconnect to access the jump host.

For more details on how to deploy the Cyber Recovery solution on Google Cloud Platform, see [Dell PowerProtect Cyber Recovery on Google Cloud Platform Deployment Guide](#).

## Integrating vault storage and applications with Cyber Recovery

### Adding vault storage with Cyber Recovery

1. From the Main Menu, select Infrastructure > Assets.
2. Click VAULT STORAGE at the top of the Assets content pane.
3. Click Add.
4. Complete the following fields in the dialog box:

**Add Vault Storage**

Enter the details of the Storage resource below.

Nickname: GOVERN

FQDN or IP Address: 11000010002.hqs.fab.emc.com

Storage Username: cradmtr

Storage Password: .....

SSH Port Number: 22

Tags: Add Tag +

Cancel Save

5. Click **Save**.

The Vault Storage table lists the storage object:

Dell Technologies | PowerProtect Cyber Recovery

Assets

Vault Storage Applications VCenters

Add Edit Delete

Details	Nickname	FQDN or IP Address	SSH Port Number	Storage Username
	GOVERN	11000010002.hqs.fab.emc.com	22	cradmtr

### Adding CyberSense with Cyber Recovery

1. From the Main Menu, select **Infrastructure > Assets**.
2. Click **APPLICATIONS** at the top of the **Assets** content pane.
3. Click **Add**.
4. Complete the following fields in the dialog box:

**Add Vault Application**

Enter the details of the Application resource below

Nickname: CyberSense

FQDN or IP Address: [Empty]

Host Username: root

Host Password: [Masked]

SSH Port Number: 22

Application Type: CyberSense

Tags: Add Tag

Buttons: Cancel, Save

5. Click **Save**.

The Applications table lists the CyberSense application:

Details	Nickname	FQDN or IP Address	Type
[Icon]	CyberSense	192.168.1.100	CyberSense

### Adding PowerProtect Data Manager with Cyber Recovery

### Adding vCenter

1. From the Main Menu, select **Infrastructure > Assets**.
2. Click **vCenters** at the top of the **Assets** content pane.
3. Click **Add**.
4. Complete the following fields in the dialog box and click **Save**.

**Add vCenter Asset**

Enter the details of the vCenter resource below

Nickname: vCenter

FQDN or IP Address:

Username: administrator@igphers.local

Password:

Tags: Add Tag+

Cancel Save

### Adding PowerProtect Data Manager

1. From the Main Menu, select **Infrastructure > Assets**.
2. Click **APPLICATIONS** at the top of the Assets content pane.
3. Click **Add**.
4. Complete the following fields in the dialog box and click **Save**.

**Add Vault Application**

Enter the details of the Application resource below

Nickname: PDDM

FQDN or IP Address:

Host Username: admin

Host Password:

SAN Port Number: 33

Application Type: PDDM

Application Username: admin

Application Password:

vCenter Name: vCenter

Tags: Add Tag+

Cancel Save

### Adding NetWorker with Cyber Recovery

1. From the Main Menu, select **Infrastructure > Assets**.
2. Click **APPLICATIONS** at the top of the Assets content pane.

3. Click **Add**.
4. Complete the following fields in the dialog box and click **Save**.

**Add Vault Application**

Enter the details of the application resource below.

Nickname:  ●

FQDN or IP Address:

Host Username:

Host Password:

SMI Port Number:

Application Type:

Application Username:  ●

Application Password:

Tags:

Cancel **Save**

### Adding Avamar with Cyber Recovery

1. From the Main Menu, select **Infrastructure > Assets**.
2. Click **APPLICATIONS** at the top of the Assets content pane.
3. Click **Add**.
4. Complete the following fields in the dialog box and click **Save**.

**Add Vault Application**

Enter the details of the application resource below.

Nickname:  ●

FQDN or IP Address:

Host Username:

Host Password:

SMI Port Number:

Application Type:

Tags:

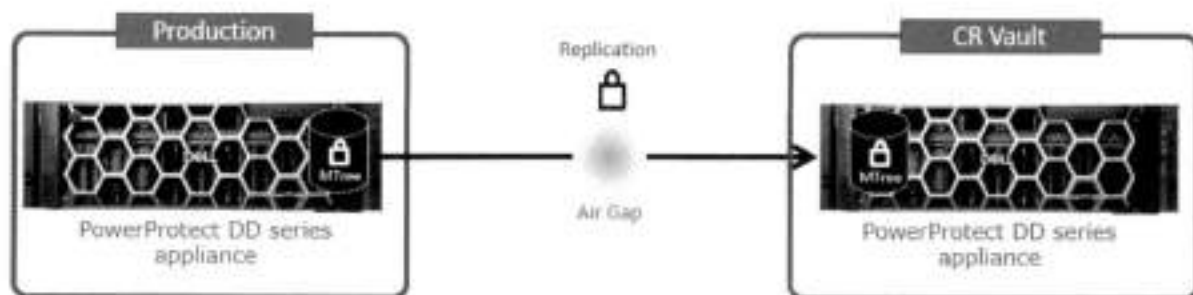
Cancel **Save**



## MTree replication

MTree replication is a DD series feature that copies unique data from the production DD series MTree to the DD series MTree in the Cyber Recovery vault.

MTree replication synchronizes data between the production environment and the air-gapped Cyber Recovery vault. Immutable protection points are created in the Cyber Recovery vault. They can be used for recovery and analytics after being copied to a read/write DD series MTree.



The Cyber Recovery software controls data synchronization from the production environment to the vault environment by DD series MTree replication. After the datasets and associated MTrees to be protected by the Cyber Recovery solution are determined, replication contexts are set up between the production and vault DD series.

MTree replication is designed so that all data within an MTree is replicated securely between two DD series appliances. After the initial synchronization is completed and all data is copied to the vault DD series, each subsequent synchronization operation copies only new and changed data segments.

### Creating the MTree replication context on DD series

Replication contexts must be created and initialized between DD series. The policy for the replication is created on the Cyber Recovery management host.



## Cyber Recovery policies and actions

The UI displays the available policy types: Standard and PPDM.

The screenshot shows a 'Add Policy' dialog box with a 'Policy Information' section. The 'Name' field is empty. The 'Type' dropdown menu is open, showing 'Select Type', 'Select Type', 'PPDM', and 'Standard'. The 'Storage' field is empty. The dialog box has a 'Cancel' button and a 'Next' button. The status bar at the bottom indicates 'Step 1 of 4'.

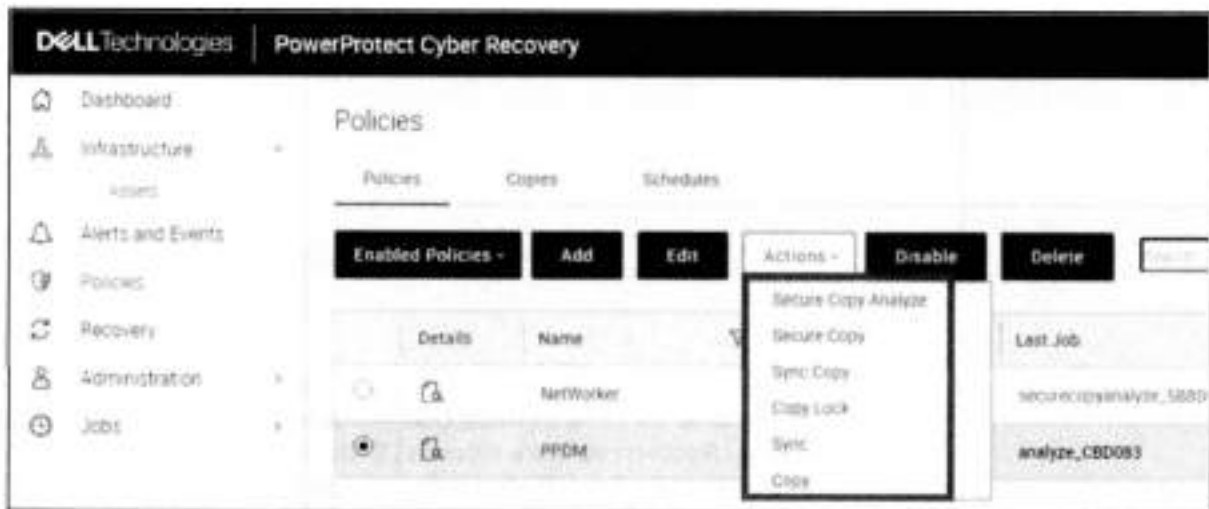
For backup software other than PowerProtect Data Manager, select the policy **Type** as **Standard**. The Cyber Recovery software supports DD Boost backup recovery, in addition to NFS backup recoveries, for PowerProtect Data Manager Version 19.10. Starting with Cyber Recovery version 19.12, Cyber Recovery software supports up to 32 Cyber Recovery policies.

**Note:** Backup and Recovery Design Center (BRDC) will help in assisting with the number of supported Cyber Recovery policies in your environment. Contact [DPADBRDC@emc.com](mailto:DPADBRDC@emc.com) for information about the actual number of policies supported for your environment.

In the policy type menu, Sheltered Harbor is not enabled by default. When Sheltered Harbor is enabled on the system, it is then displayed in the menu.



The following actions are available for all policy types except for the Sheltered Harbor policy type:



- **Sync Copy** (Sync the data and create a fast copy)
- **Secure Copy** (Performs a replication, creates a PIT copy, and then retention locks all files in the PIT copy)
- **Secure Copy Analyze** (Performs a replication, creates a PIT copy, retention locks all files in the PIT copy and runs an analysis on the resulting PIT copy)

**Note:** The "Secure Copy Analyze" action is available only if a CyberSense application is configured. If the "Analyze" operation of the schedule still runs when the next schedule starts and gets to the "Analyze" operation, it will fail because there can only be a single active "Analyze" operation for each Cyber Recovery policy.

- **Sync** (Sync the data)
- **Copy** (Create a fast copy of data that is already on PowerProtect DD series appliance in the vault environment)
- **Copy Lock** (Locks all files in the PIT copy)

For a Sheltered Harbor policy type, the only action available is Sheltered Harbor Copy (Sync, Verify, Copy, Certify, Lock, Report).

## Infrastructure service recommendations

The following table shows infrastructure service recommendations:

**Table 1. Infrastructure service recommendations**

Service	Scope	Required	Notes
AD/LDAP	In-vault	Recommended	Stores Credentials. Can provide access controls and other functions.
DNS	In-vault	Recommended	Highly recommended when multiple hosts are in the vault.
Cyber Recovery UI	In-vault	Recommended	
Extended CR UI	Inbound/ outbound	Recommended	A firewall, jump-server or other techniques can be used for further hardening.
Jump server	Inbound/ outbound	Recommended	<ul style="list-style-type: none"> <li>Allows software and other critical maintenance.</li> <li>Allows remote access for testers.</li> </ul>
NTP	In-vault/ inbound	Required	A reliable time source is required to prevent clock skew. In-vault NTP can be provided.
Physical lockbox/vault	In-vault	Recommended	Use a two-key lockbox to store a written copy of Data Domain system password. Open only in an emergency.
SMTP	Outbound	Required for some services	Allows vault services to send information out of the vault.
SMTP relay server	Outbound		Software packages are available from Microsoft and others.
SNMP	Outbound	Not recommended	Consider using SYSLOG. Data Domain supports both SNMP and SYSLOG, both are disabled by default.
Syslog	Outbound		Also consider Rsyslog.

### Recommended network speed for DD series interfaces

The Cyber Recovery software enables and disables the replication Ethernet interface and the replication context on the DD series in the Cyber Recovery vault to control the flow of data from the production environment to the vault environment. The Cyber Recovery software manages the replication link, and the connection is only enabled when new data must be ingested by the DD series in the Cyber Recovery vault.

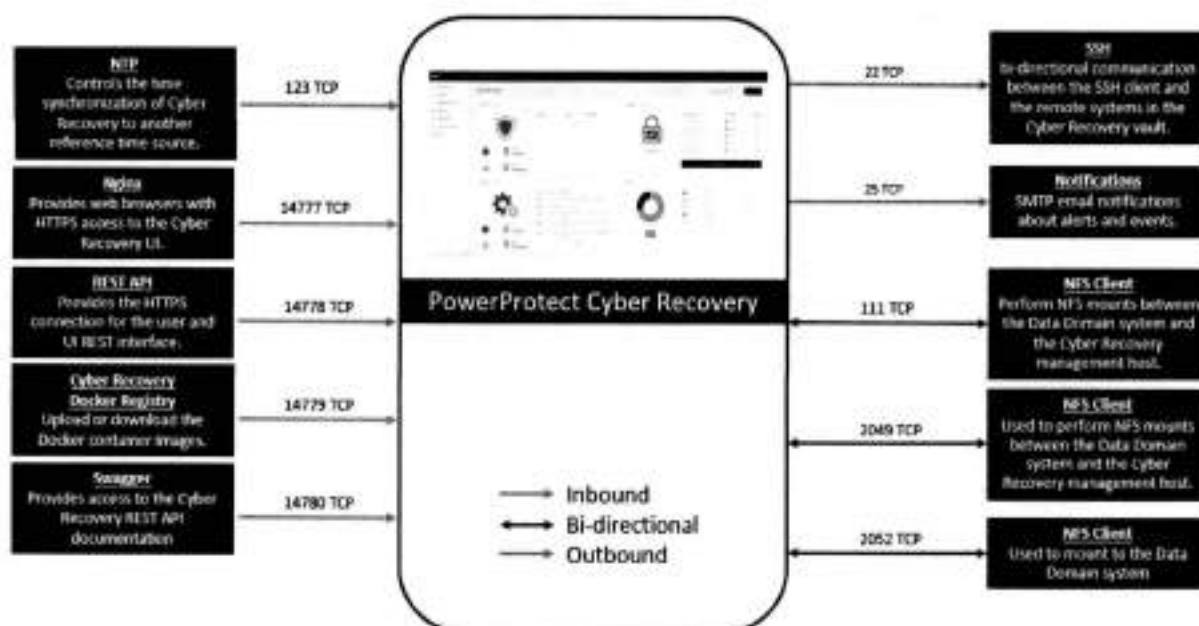
The replication link on the DD series in the Cyber Recovery vault uses its own unique Ethernet interface. For the replication link that connects the production DD series to the DD series in the Cyber Recovery vault, using the fastest link speed possible, preferably 10 Gb/s Ethernet (GbE) is recommended and supported up to 25 Gb/s.

To secure the network links that connect the vault environment to the production environment, or any other network, installing a firewall or other packet inspection tool on both the DD series replication link and the SMTP link is recommended. It is recommended not to make use of packet inspection if a firewall is placed in the replication path. The cost of firewall will be very high, and the deep packet inspection would slow the process down.

If a hyperconverged VMware appliance is installed in the Cyber Recovery vault, the VMware NSX Distributed Firewall (DFW) is a satisfactory firewall option to reduce complexity in the vault environment and protect VMware-based infrastructure. Additionally, the DFW is a potential software-defined option for protecting the Data Domain replication link between production and vault DD series at near wire speed.

The Cyber Recovery software does not support adding Ethernet interfaces to a Cyber Recovery virtual appliance deployment.

**Cyber Recovery network ports** The following figure lists the network ports that Cyber Recovery functions require:



**Recommended connections between DD series**

The Cyber Recovery software works with a replication data link between the vault-environment and production-environment DD series. The Cyber Recovery software communicates with all DD series appliances using SSH.

The production and vault environment networks are not directly connected to each other, except for a replication data link between the DD series in the two environments. The replication data link can be connected directly or through a dedicated switch to the DD series in the vault environment. We recommend using the dedicated replication switches.

## Technical support and resources

The [Dell Technologies support page](#) is focused on meeting customer needs with proven services and support.

The [Dell Technologies Info Hub](#) provides expertise that helps to ensure customer success on Dell Technologies data protection platforms.

### Related resources

The Cyber Recovery product documentation set includes:

- [PowerProtect Cyber Recovery Info Hub](#)
- [Dell PowerProtect Cyber Recovery Product Guide](#)
- [Dell PowerProtect Cyber Recovery Installation Guide](#)
- [Dell PowerProtect Cyber Recovery Solutions Guide](#)
- [Dell PowerProtect Cyber Recovery AWS Deployment Guide](#)
- [Dell PowerProtect Cyber Recovery Azure Deployment Guide](#)
- [Dell PowerProtect Cyber Recovery Google Cloud Platform](#)
- [Dell PowerProtect Cyber Recovery Solution Brief](#)
- [Dell PowerProtect Cyber Recovery Simple Support Matrix](#)

---

**Note:** Access to these documents might depend on your login credentials.

---





# Dell Data Domain Boost File System: Deployment and Configuration

June 2023

H18833.1

## White Paper

### Abstract

This document describes the deployment and configuration of Dell DD Boost File System (BoostFS) for Windows and Linux application hosts.

## Copyright

The information in this publication is provided as is. Dell Inc. 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 software described in this publication requires an applicable software license.

Copyright © 2021–2023 Dell Inc. or its subsidiaries. Published in the USA June 2023 H18833.1.

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

## Contents

<b>Executive summary .....</b>	<b>4</b>
<b>Introduction .....</b>	<b>5</b>
<b>Preparing PowerProtect DD system for BoostFS .....</b>	<b>8</b>
<b>Creating BoostFS user and storage unit on PowerProtect DD.....</b>	<b>9</b>
<b>Installing and configuring BoostFS agent on Windows application host .....</b>	<b>13</b>
<b>Mounting and unmounting the BoostFS file system (Windows host) .....</b>	<b>22</b>
<b>Installing and configuring BoostFS agent on Linux application host .....</b>	<b>24</b>
<b>Mounting and unmounting the BoostFS file system (Linux host).....</b>	<b>28</b>
<b>Conclusion.....</b>	<b>29</b>
<b>References.....</b>	<b>30</b>

## Executive summary

**Overview** Dell Data Domain Boost File System (BoostFS) provides a general file system interface to the DD Boost library, allowing standard backup applications to take advantage of DD Boost features.

The BoostFS plug-in resides on the application system and presents a standard file system mount point to the application. With direct access to a BoostFS mount point, the application can leverage the storage and network efficiencies of the DD Boost protocol for backup and recovery. Only simple qualifications are needed for the application to support BoostFS. The file system interface makes BoostFS easy to deploy so that it can be up and running in minutes.

**Audience** This white paper is intended for Dell Technologies customers, partners, and employees who are interested in learning about the BoostFS plug-in technology and the unique benefits that it provides.

**Revisions**

Date	Part number/ revision	Description
June 2021	H18833	Initial release
June 2023	H18833.1	Updated for DDOS 7.11

**We value your feedback** Dell Technologies and the authors of this document welcome your feedback on this document. Contact the Dell Technologies team by [email](#).

**Author:** Vinod Kumaresan

**Contributors:** Dhananjay Hiremath and Vikas Chaudhary

---

**Note:** For links to other documentation for this topic, see the [Data Protection Info Hub](#).

---

## Introduction

### BoostFS overview

DD Boost software delivers an advanced level of integration with backup applications and database utilities, enhancing performance and ease of use. The BoostFS plug-in with DD Boost provides even greater application support, which enables all the benefits of DD Boost for data protection. BoostFS is supported and available for Linux and Windows hosts.



Figure 1. DD Boost and BoostFS features

DD Boost enables the backup server or application client to send only unique data segments, rather than all data, across the network to the PowerProtect DD appliance. This process reduces the amount of data transferred over the network by 80 to 98 percent.

BoostFS licenses are not included with the DD Boost licensing option available on all PowerProtect DD series appliances (including DDVE). BoostFS is a separate software product that must be purchased and licensed for the clients that it is deployed on.

### Advantages of BoostFS

By leveraging DD Boost technology, BoostFS helps reduce bandwidth, can improve backup times, offers load-balancing, allows in-flight encryption, and supports the DD multitenancy feature set.

In-flight encryption supported through DD Boost allows applications to encrypt in-flight backup or restore data over LAN from the protection system. When it is configured, the client can use TLS to encrypt the session between the client and the protection system. DD 7.6.0.5 and later versions support GCM-based ciphers in both Boost client and DD.

As a file server system implementation, the BoostFS workflow is similar to NFS but leverages the DD Boost protocol. In addition, BoostFS improves backup times compared to NFS and various copy-based solutions.

BoostFS supports single-node PowerProtect DD systems, high-availability (HA) systems, Extended Retention systems, PowerProtect DD Virtual Edition (DDVE), and Extended Distance Protection.



## Features of BoostFS

BoostFS features include:

- **Faster, more efficient backup:** BoostFS distributes parts of the deduplication process to backup server or application client, offering 50 percent faster backups and requiring up to 98 percent less network bandwidth.
- **Simplified disaster recovery:** Applications can control the PowerProtect DD replication process with full catalog awareness.
- **Advanced load balancing and failover:** Transport links are aggregated for transparent load balancing and automatic link failover.
- **DD Boost everywhere:** The Boost File System plug-in expands application support.
- **Concurrent connections:** The maximum number of connections that can be used simultaneously is 256. The minimum value is 64, and the default value is 128.
- **Compressed restore:** This feature reduces bandwidth usage during the sending and receiving of data but increases CPU usage. When the mount option `ddboost-read-compression` is set to `true`, data is compressed on the server before being sent to the client. When the client receives the data, it must decompress the data. Sending and receiving compressed data uses less network bandwidth, but compressing and decompressing the data requires a significant amount of CPU power. By default, the `ddboost-read-compression` option is set to `false`.

```
# ddboost-read-compression=<true|false>
```

- **Multithreaded Boost Mode:** You can specify the number of threads to use in multithreaded Boost mode for writing each file (the default is 2). The setting does not have any significance if `mtboost-enabled=false`. The minimum value is 0, and the maximum value is 16.

```
# Enable Boost multithreading (default: true)
mtboost-enabled=true|false
```

- **Improved Microsoft SQL backup performance:** Starting with BoostFS 7.2.0.5, BoostFS for Windows provides improved Microsoft SQL backup performance. By default, this feature is disabled. This feature can be enabled by using the `data-cache-enable` mount option.
- **File security:** BoostFS for Windows supports access control lists (ACLs) on files and directories within the BoostFS mount point.
- **Linux automounter:** To mount file systems dynamically, use the Linux automounter with the `autofs` command. Mounts created with the `automount` command are automatically unmounted when not in use.

### DD Boost features supported by BoostFS

BoostFS supports the following DD Boost features:

- Distributed Segment Processing
- Load balancing and failover
- Hard stream limits

- User authentication (Kerberos)
- Data encryption
- Replication Cloud Tier
- Transport Layer Security (TLS) anonymous authentication, which is supported to provide encryption

### Supported environments

#### BoostFS for Windows

BoostFS for Windows requires:

- DDOS version 6.2 or later
- Windows Server 2016, Windows Server 2019, or Windows Server 2022

#### BoostFS for Linux

BoostFS for Linux requires:

- DDOS version 6.2 or later
- FUSE 2.8 or later

Boost FS for Linux supports the following Linux distributions:

- Red Hat Enterprise Linux versions 7, 8, and 9
- CentOS 7 and 8
- SUSE Linux Enterprise Server versions 11, 12, and 15
- Ubuntu 14.04, 15, 20, and 22
- Oracle Linux versions 7, 8, and 9

### Supported applications

The Dell DD BoostFS support matrix, available from E-Lab Navigator at <https://elabnavigator.emc.com/eln/elnhome>, lists the supported applications. On the E-Lab Navigator home page, select **Data Protection and Availability Solutions > PowerProtect DD series appliances**.

### Configuring the BoostFS plug-in

The following figure shows the steps for configuring the BoostFS plug-in. The remaining sections of this paper provide the details.

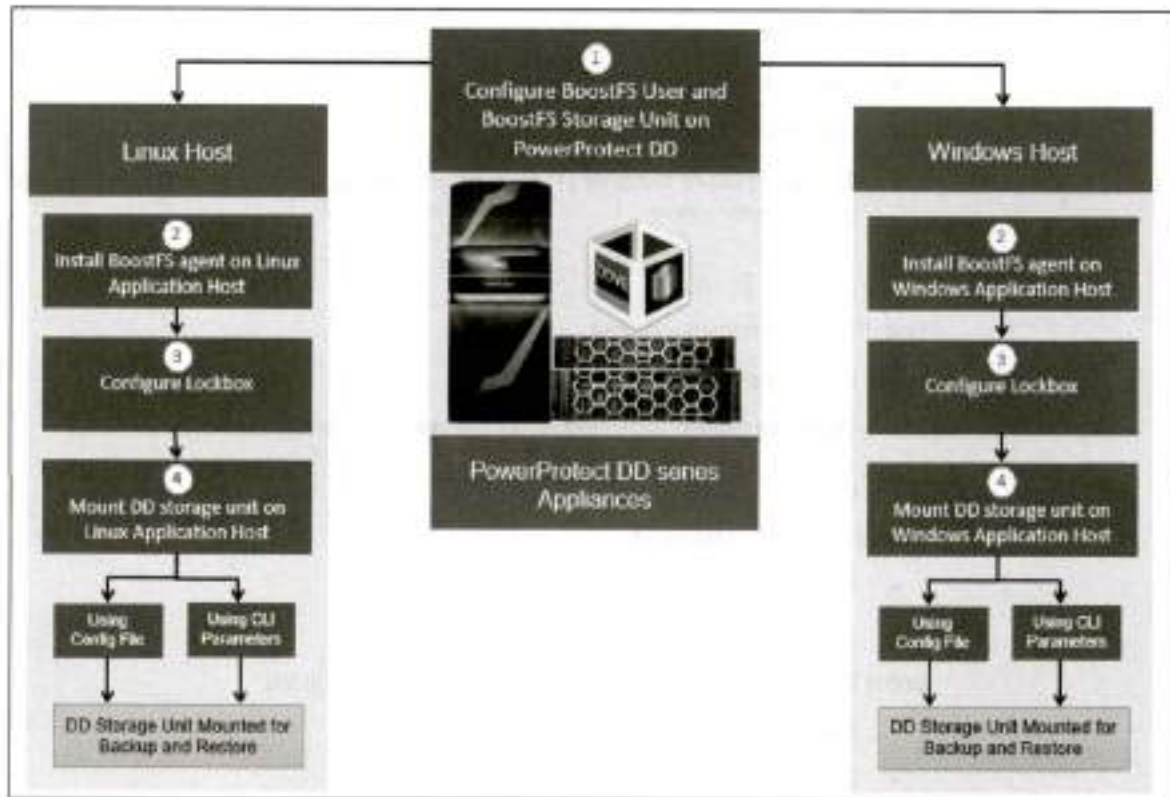


Figure 2. Steps to configure BoostFS plug-in

## Preparing PowerProtect DD system for BoostFS

### Prerequisites

Ensure that your environment meets the following prerequisites:

- PowerProtect DD enabled for DD Boost deduplication must have a unique name. You can use the DNS name of the PowerProtect DD system, which is always unique.
- All application host systems must be able to access the Key Distribution Center (KDC). In a Windows environment, the Windows server that hosts the Microsoft Active Directory service acts as the KDC and the domain name system (DNS). If the systems cannot reach the KDC, check the DNS settings at `/etc/resolv.conf`.

### Preparing for BoostFS

Prepare the environment for BoostFS as follows:

1. On the PowerProtect DD system, log in as an administrative user.
2. Verify that the file system is enabled and running by entering `filesys status`.

```
sysadmin@lldpvd003# filesys status
The filesystem is enabled and running.
sysadmin@lldpvd003#
```

3. Verify that DD Boost is enabled by entering `ddbost status`.



```
sysadmin@lldpdvcl083# ddbboost status
DD Boost status: enabled
sysadmin@lldpdvcl083#
```

If the DD Boost is reported as disabled, enable it by entering `ddbboost enable`.

```
sysadmin@lldpdvcl083# ddbboost enable
DD Boost enabled.
sysadmin@lldpdvcl083#
```

4. Verify that distributed segment processing is enabled by entering `ddbboost option show`.

```
sysadmin@lldpdvcl083# ddbboost option show
Option                               Value
-----                               -
distributed-segment-processing       enabled
virtual-synthetics                   enabled
global-authentication-mode           none
global-encryption-strength           none
sysadmin@lldpdvcl083#
```

If distributed segment processing is shown as disabled, enable it by entering `ddbboost option set distributed-segment-processing enabled`.

```
sysadmin@lldpdvcl083# ddbboost option set distributed-segment-processing enabled
DD Boost option "distributed-segment-processing" set to enabled.
sysadmin@lldpdvcl083#
```

You can set the hostname and the domain name on the PowerProtect DD system by using the `net set` CLI command:

```
# net set hostname {host}
# net set {domain name [local-domain-name]}
```

## Creating BoostFS user and storage unit on PowerProtect DD

### Introduction to BoostFS user and storage unit

One or more storage units must be created on each PowerProtect DD system that is enabled for BoostFS. Storage units are accessible only to applications with the username that owns the storage unit. One username owns each storage unit, and the same username can own multiple storage units. PowerProtect DD administrators can also use existing DD Operating System (DDOS) CLI commands to create and manage storage units used by BoostFS.

The application passes the username and password to BoostFS, and DD Boost passes them to the PowerProtect DD system when attempting to connect to the PowerProtect DD system. The PowerProtect DD system then authenticates the username and password. The username and password can be shared by different applications.

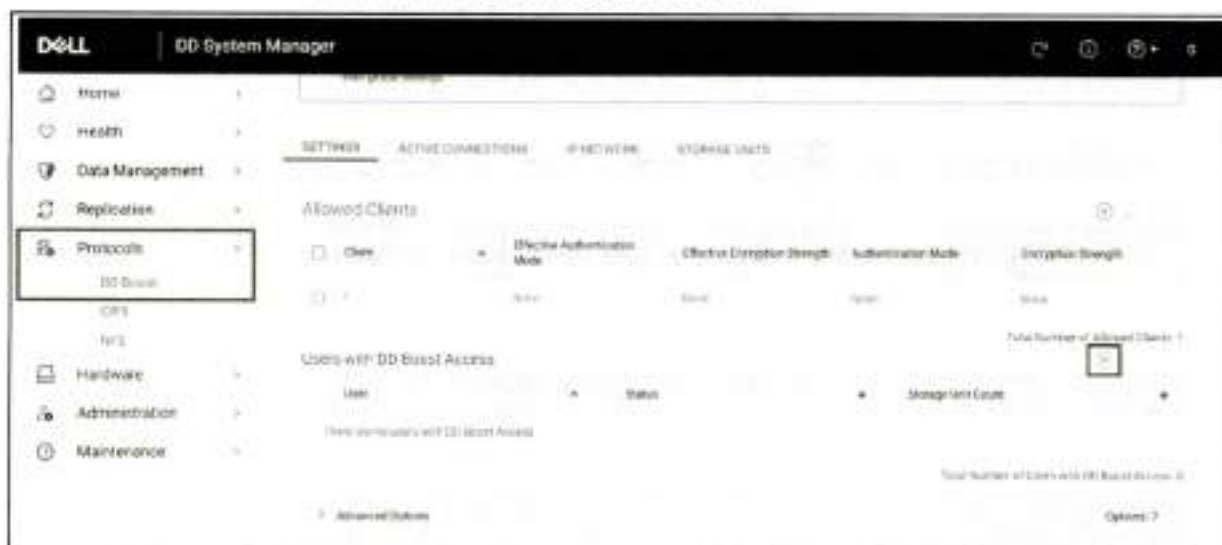
## Creating a BoostFS user

Create a BoostFS user on the PowerProtect DD system as follows:

1. Log in to DD System Manager.



2. Go to **Protocols > DD Boost** and create a BoostFS user under **Users with DD Boost Access** by selecting the add icon.



3. Select **Create a new Local User**.



4. Enter the required details and click **ADD**.

### Add User ✕

Select or Create User: Create a new Local Us ▾

User: boostuser

Password: \*\*\*\*\*

Verify Password: \*\*\*\*\*

Management Role: none

**i** The user will be added to the DD Boost access list.

ADD
CANCEL

### Add User Status ✕

**Task complete**

- ✔ Create a new user
- ✔ Adding user to DD Boost access list

CLOSE

The new BoostFS user, boostuser, has been created:

The screenshot shows the Dell DD System Manager interface. The left sidebar contains navigation options: HOME, Health, Data Management, Replication, Protocols (with sub-items DC Boost, DFS, NFS), Hardware, Administration, and Maintenance. The main content area is titled 'DD System Manager' and has tabs for SETTINGS, ACTIVE CONNECTIONS, IP NETWORKS, and STORAGE UNITS. Under the 'SETTINGS' tab, there are two sections: 'Allowed Clients' and 'Users with DD-Boost Access'. The 'Users with DD-Boost Access' section contains a table with the following data:

User	Status	Storage Unit Count
boostuser	enabled	0

Below the table, there is an 'Advanced Options' section with an 'Options 1' button.



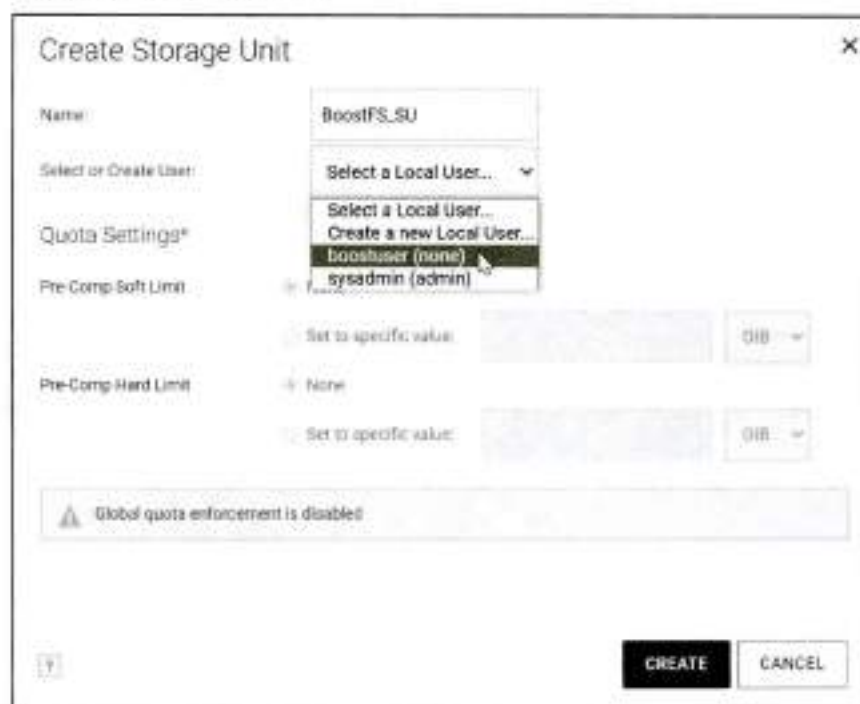
## Creating a storage unit

Create a storage unit on the PowerProtect DD system as follows:

1. Go to **Protocols > DD Boost**, select the **STORAGE UNITS** tab, and then select the add icon to create a storage unit.



2. Enter a name for the storage unit and select **boostuser**, which is the BoostFS user that you previously created.



3. Click **CREATE** to create the BoostFS storage unit for the BoostFS user boostuser.



The BoostFS storage unit BoostFS\_SU has been created successfully for the BoostFS user boostuser.



## Installing and configuring BoostFS agent on Windows application host

### Prerequisites

You can install or upgrade BoostFS for Windows by using the MSI installer.

When installing or upgrading BoostFS for Windows:

- Use an account with administrator rights to run the installer.
- Ensure that there is enough free space to complete the installation, which requires approximately 7 MB of disk space.
- Deactivate all BoostFS mount points. If any mount points are active, the upgrade and removal processes will fail.

### CBFS driver

The MSI installer includes several binary files as well as a device driver from EidoS Corporation. BoostFS for Windows uses CBFS, a software interface from EidoS that

enables file systems to exist in user space and not only within a driver in kernel space. This functionality is similar to that of FUSE on UNIX operating systems. To install BoostFS for Windows, the CBFS driver from EldoS Corporation must be installed.



## BoostFS for Windows components

### Installation location components

The BoostFS for Windows installation includes the following files at the installed location:

- `boostfs.exe`—An executable that supports various commands including establishing a BoostFS mount
- Shared libraries that enable `boostfs.exe`
- RSA Lockbox libraries
- Universal C Runtime Library (UCRT)  
If the UCRT is already installed on the system, `boostfs.exe` uses the system version of the UCRT.
- HTML files that provide basic guidance about the use and configuration of `boostfs.exe`
- If not already installed, the 2012 and 2015 Visual C++ redistributables are installed

### Start Menu entries

Three links are added to the Start Menu under **Programs > BoostFS**. These links open:

- A command prompt at the installed location of BoostFS
- The BoostFS help file
- The BoostFS configuration help file

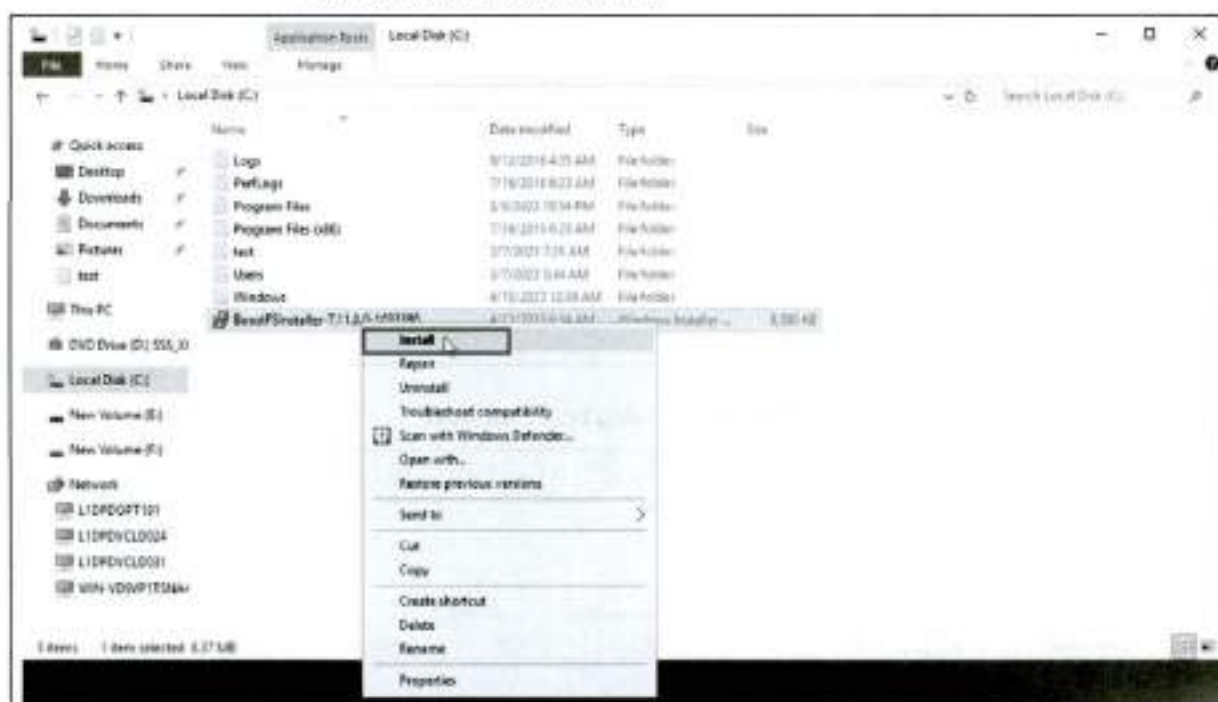
## Files in C:\BoostFS

A directory is created at `C:\BoostFS`. This directory is the default location for BoostFS logs and lockbox containers, and it is the sole location of the configuration file `C:\BoostFS\boostfs.conf`. The lockbox and logs directories may be configured to be placed elsewhere after installation, but the configuration file must exist in this location.

## Installing BoostFS agent

Install BoostFS agent as follows:

1. Log in to Windows host and download the BoostFS agent package for Windows from Dell Support: <https://www.dell.com/support/home/en-us/product-support/product/data-domain-boost-file-system/drivers>.
2. Right-click the installer file and select **Install** to proceed with the BoostFS agent installation on the Windows host.



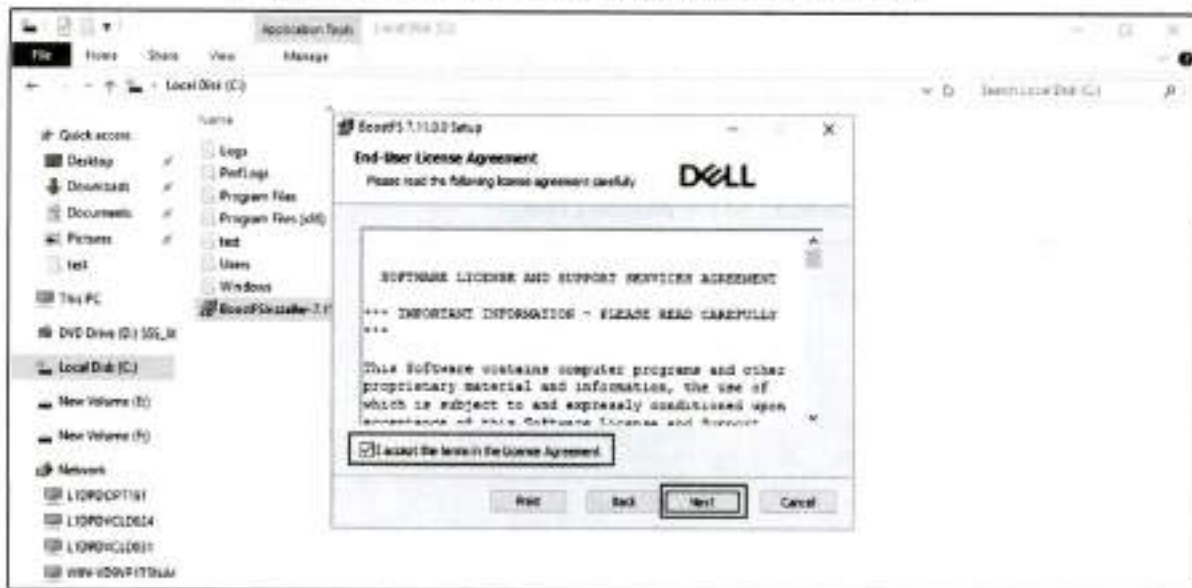
3. Click **Next** to proceed with installation.



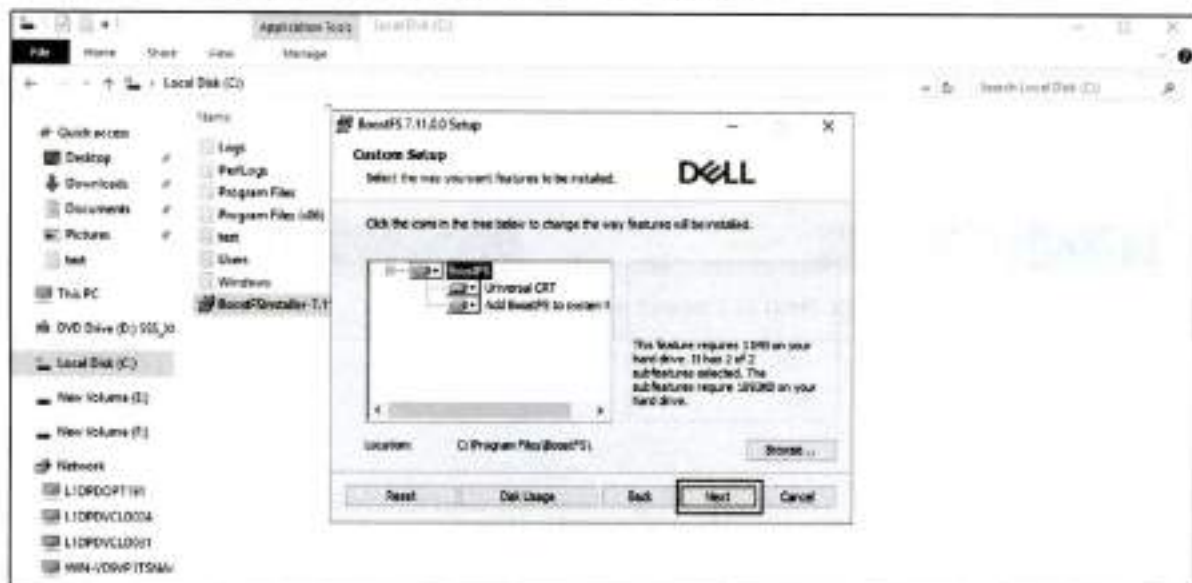


Installing and configuring BoostFS agent on Windows application host

4. Accept the End-User License Agreement and click Next.



5. At the Custom Setup dialog box, click Next.

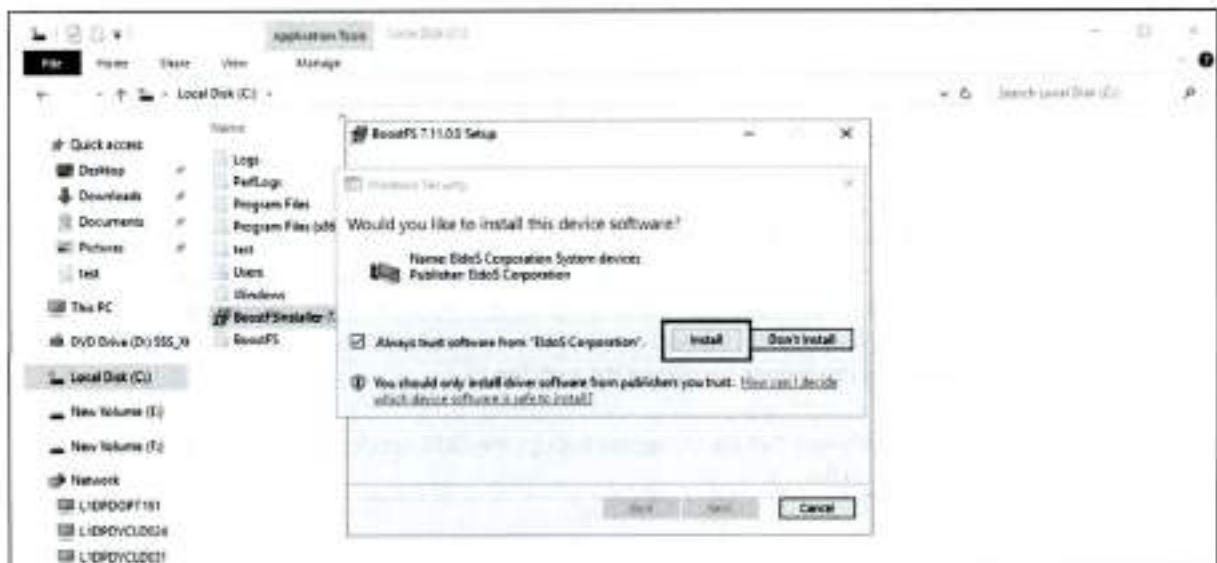


installing and configuring BoostFS agent on Windows application host

6. Click **Install** to proceed with BoostFS installation.



7. Click **Install** to install the device driver.



BoostFS agent installation on the Windows host has been completed successfully.



Installing and configuring BoostFS agent on Windows application host

8. Click **Finish** to exit the installation.



## Configuring BoostFS for Windows

BoostFS configuration parameters can be specified by using the CLI, the configuration file, or both.

### BoostFS for Windows configuration file

The BoostFS configuration file is at `C:\BoostFS\boostfs.conf`. The configuration file has sections for global and mount-point-specific parameters. Mount-point-specific parameter values override global parameter values. If the global section does not define `data-domain-system` and `storage-unit` parameters, those parameters must be passed to the mount command through the CLI.

---

**Note:** Parameters that are configured through the CLI override conflicting values in the configuration file.

---

```

BoostFS - Notepad
File Edit Format View Help
BoostFS 3.3 example config file for Windows
#
# The configuration file is divided into sections, delimited by brackets [].
# Options that are to apply to all mount points are in the [global] section.
# More details on the various configuration options can be found in the
# BoostFS manual. Command line options override what is in this file.
#
# Format:
# # - Identifies a comment line, and must be at the start. Configuration
# parameters can be disabled by adding a '#' to the start of the line.
#
# Values which contain spaces should use double quotations around the
# entire value.
#
# No whitespace is allowed between the option and the value, i.e.
# log_dir = /path is not allowed.
#
# Comments are not allowed after the option value pair.
#
#####

[global]
# Data Domain hostname or IP address
# data_domain=system02195-1.yourdomain.com

# Storage unit
# storage-unit=rae

# Security option used for authentication (Default: lockbox)
# security=lockbox

# Storage unit username (should only be used in conjunction with Kerberos authentication)
# storage-unit-username=qtadain

# Lockbox path (Default: C:\BoostFS\lockbox\boostfs.lockbox)
# lockbox-path=C:\lockbox-name

# Enable logging (Default: true)
# log-enabled=true/false

# Log level (Default: info)
# log-level=debug/info/warning/critical

# Directory for log files (Default: C:\BoostFS\logs)

```

### BoostFS for Windows command overview

The Windows command prompt or PowerShell can be used to issue BoostFS commands.

The BoostFS installation includes a shortcut on the Start menu to open the command prompt in the directory containing the executable. During the installation process, the installer can automatically add the location of the executable to the PATH environment variable so that there is no need to specify the path when issuing BoostFS commands. If this option is not chosen during installation, the location can be manually added later.

### BoostFS authentication methods

BoostFS has two authentication options:

- RSA Lockbox
- Kerberos

#### RSA Lockbox-based authentication

RSA Lockbox is the default password manager for BoostFS for Windows. To use RSA Lockbox, the lockbox must be configured by using the `boostfs lockbox set` command.

#### Sharing a BoostFS lockbox file on multiple clients

Sharing a common lockbox file enables you to create a single management point for BoostFS clients to access BoostFS mount points on PowerProtect or Data Domain systems.

A common lockbox file can be created for all BoostFS clients from a primary client. By using this feature, you can avoid creating a separate lockbox file for each unique BoostFS client.

The primary client is the client from which the shared lockbox is initially created. Because some operations can be performed only from the primary client, record which client is the primary.

The easiest way to share a lockbox file is to store it in a network share that is accessible by all clients that use it.

#### **Kerberos-based authentication**

BoostFS for Windows supports the MIT implementation of Kerberos authentication as an alternative to RSA Lockbox authentication.

The primary entities involved with Kerberos authentication are:

- BoostFS client
- An Active Directory server acting as the Kerberos Key Distribution Center (KDC)
- PowerProtect DD systems running DDOS version 6.0 or later

The Kerberos file contains a "shared secret" (a password, passphrase, or other unique identifier) between the KDC server and the PowerProtect DD appliance.

In an Active Directory environment, the Windows server that hosts the Active Directory service also acts as the KDC and Domain Name Server (DNS).

#### ***Kerberos tickets***

To authenticate using Kerberos, a Ticket Granting Ticket (TGT) must be acquired for two types of user accounts:

- A Kerberos TGT
- A Kerberos ticket for various services (service tickets) that the client will use (BoostFS, DNS, CIFS, NFS)

Each user has access to only the tickets they create with the BoostFS Kerberos commands. Users cannot access tickets that others have created.

For more detailed information about using RSA Lockbox-based and Kerberos-based authentication with BoostFS for Windows, see the [\*DD BoostFS for Windows Configuration Guide\*](#).

#### **Creating lockbox entry using command line**

To create a lockbox entry by using the command line:

1. Open the BoostFS command prompt.



2. Enter `boostfs lockbox -h` for lockbox configuration options.

```

Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Program Files\BoostFS>boostfs lockbox -h

Usage:
  boostfs lockbox set
    -u <storage-unit-username>
    -d <data-domain-system>
    -s <storage-unit>
    [-l <lockbox-path>]

  boostfs lockbox {remove | query}
    -d <data-domain-system>
    -s <storage-unit>
    [-l <lockbox-path>]

  boostfs lockbox {add-hosts | delete-hosts}
    [-l <lockbox-path>]
    <hostname[.hostname]...>

  boostfs lockbox show-hosts
    [-l <lockbox-path>]
  
```

3. Enter the parameters in the following format to set the lockbox entry:

```

boostfs lockbox set -u <storage-unit-username> -d <data-domain system> -s <storage-unit>
  
```

```

C:\Program Files\BoostFS>boostfs lockbox set -u boostuser -d lldpdc10003.hop.lab.emc.com -s BoostFS_SU
Enter storage unit user password:
Enter storage unit user password again to confirm:
Lockbox entry set

C:\Program Files\BoostFS>
  
```



## Mounting and unmounting the BoostFS file system (Windows host)

### Mounting options

Mount the BoostFS file system by running the `boostfs mount` command in either of the following ways:

- Using a UNC mount path

```
boostfs mount [-l <lockbox-path>] [[-o <param>=<value>] ...]  
<UNC-mount-path> [<drive-letter>]
```

- Using the PowerProtect DD system and storage unit names

```
boostfs mount -d <data-domain-system> -s <storage-unit> -o  
security=kerb5 -u <storage-unit-username> <mount-point>
```

Where `-d` specifies the PowerProtect DD system and `-s` specifies the storage unit.

### Mounting the BoostFS file system

Mount the BoostFS file system as follows:

- From the Windows host CLI, go to the path where BoostFS is installed and enter `boostfs mount -h` for mount options.

```
Administrator: BoostFS CMD Prompt  
C:\Program Files\BoostFS>boostfs mount -h  
usage:  
  boostfs mount  
  
  All property values are taken from the configuration file [global] section. Mandatory  
  parameters data-domain-system and storage-unit must exist in the config file.  
  
  or  
  
  boostfs mount  
  [[-o | --option <param>=<value>] ...]  
  <UNC mount path>  
  [mapped drive letter]  
  
  or  
  
  boostfs mount  
  -d <data-domain-system>  
  -s <storage-unit>  
  [-l <lockbox-path>]  
  [[-o | --option <param>=<value>] ...]  
  [mapped drive letter]
```

2. Enter the parameters in the following format to mount the BoostFS file system:

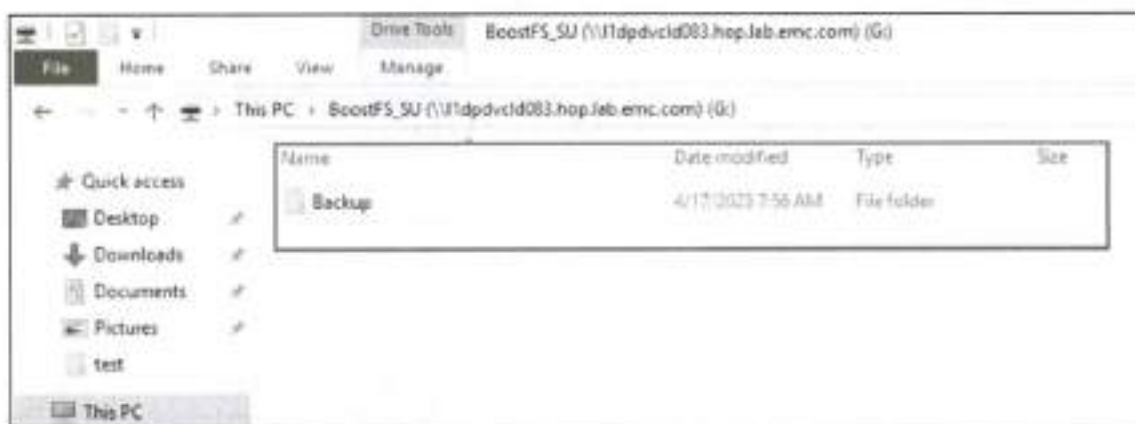
```
boostfs mount -d <data-domain-system> -s <storage-unit>
<drive-letter>
```

```
C:\Program Files\BoostFS>boostfs mount -d l1dpdvcl083.hop.lab.emc.com -s BoostFS_SU g:
mount: Mounting l1dpdvcl083.hop.lab.emc.com:BoostFS_SU on g:
C:\Program Files\BoostFS>
```

The BoostFS storage unit has been mounted as a file system on the Windows host for performing backup and restore operations:



For example, sample folder **Backup** is created on the DD storage unit mounted on the Windows host.





### Unmounting the BoostFS file system

You can unmount the BoostFS file system by running the `boostfs umount/unmount` command in one of the following formats:

- `boostfs umount/unmount <UNC-mount-path>`
- `boostfs umount/unmount <drive-letter>`

```
C:\Program Files\BoostFS>boostfs unmount g:  
umount: unmounting //11dpcvcl0883.hop.lab.emc.com/BoostFS_5U  
C:\Program Files\BoostFS>
```

## Installing and configuring BoostFS agent on Linux application host

### BoostFS agent for Linux—introduction and prerequisites

BoostFS agent for Linux is available as a single RPM installation package that both enterprise and small-scale users can download. It is available in both RPM and .deb formats. The RPM package includes the `boostfs` executable.

Before beginning the process, ensure that:

- The FUSE version on the client is 2.8 or later.

While the BoostFS process is running:

- BoostFS mount points must be deactivated.
- BoostFS cannot be upgraded.
- BoostFS cannot be uninstalled.

### BoostFS for Linux components

The BoostFS for Linux client is composed of the following:

- A daemon process that supports various commands
- Two shared libraries: `libDDBoost.so` and `libDDBoostFS.so`
- `rsalib`: A hidden directory that contains redistributable RSA libraries
- A configuration file
- A manual page

`libDDBoost.so`, a FUSE-agnostic library built on the DD Boost library, provides such services as connection management, a retry mechanism, and client logging. The packaging defaults to the Red Hat Package Manager (RPM) format, but the native packaging for other operating systems is also supported.

---

**Note:** Verify that the appropriate package is used for the client operating system.

---

**Role of FUSE in BoostFS for Linux**

BoostFS for Linux uses FUSE, an open-source software interface that enables nonprivileged users to securely create and mount their own file-system implementations.

FUSE allows the export of a virtual file system to the Linux kernel. Write operations through BoostFS and FUSE benefit from PowerProtect DD distributed segment processing.

Using FUSE and the DD Boost plug-in, BoostFS exports a storage unit on a PowerProtect DD system to a mount point on a client. On the client, file system operations conducted on the mount point are captured by the kernel before being passed through FUSE to BoostFS.

BoostFS runs as a daemon on a client. As a software module, BoostFS serves as a layer between FUSE and DD Boost.

**Installing the BoostFS agent**

Install the BoostFS agent for Linux as follows:

1. Download and place the BoostFS agent for Linux host to the `/tmp` directory.

```
root@l1dpdvc1d091/tmp
login as: root
root@l1dpdvc1d091:hop.lab.cmc.com's password:
Last login: Sun Apr 16 09:16:46 2023 from 10.107.71.92
[root@l1dpdvc1d091 ~]#
[root@l1dpdvc1d091 ~]#
[root@l1dpdvc1d091 ~]#
[root@l1dpdvc1d091 ~]#
[root@l1dpdvc1d091 ~]#
[root@l1dpdvc1d091 ~]#
[root@l1dpdvc1d091 ~]# cd /tmp
[root@l1dpdvc1d091 tmp]# ls
DDBoostFS-7.11.0.0-1033390.rhel.x86_64.rpm  ks-script-52a652 yum.log
[root@l1dpdvc1d091 tmp]#
```

2. Install the BoostFS agent package by running the following command:

```
rpm -ivh DDBoostFS-7.11.0.0-1033390.rhel.x86_64.rpm
```

```
[root@l1dpdvc1d091 tmp]# ls
DDBoostFS-7.11.0.0-1033390.rhel.x86_64.rpm  ks-script-52a652 yum.log
[root@l1dpdvc1d091 tmp]# rpm -ivh DDBoostFS-7.11.0.0-1033390.rhel.x86_64.rpm
```

BoostFS agent has been installed successfully on the Linux host:

```
[root@l1dpdvc1d091 tmp]# ls
DDBoostFS-7.11.0.0-1033390.rhel.x86_64.rpm  ks-script-52a652 yum.log
[root@l1dpdvc1d091 tmp]# rpm -ivh DDBoostFS-7.11.0.0-1033390.rhel.x86_64.rpm
warning: DDBoostFS-7.11.0.0-1033390.rhel.x86_64.rpm: Header V3-DSA/SHA1 Signature, key ID 70
f374bc: NOKEY
Preparing... [100%]
Updating / installing...
 1:ddboostfs-7.11.0.0-1033390 [100%]
[root@l1dpdvc1d091 tmp]#
```

## Configuring BoostFS for Linux

You can configure BoostFS by using either of the following options:

- CLI
- Configuration file: `boostfs.conf`

### BoostFS for Linux command overview

The `boostfs` command is used to establish the FUSE mount, create the lockbox (optional), and set up Kerberos credentials if Kerberos is chosen as the authentication method.

### BoostFS for Linux configuration file

The configuration file is in `/opt/emc/boostfs/etc` and can be edited by the root user or a user with sudo privileges. Parameters can be specified either in the configuration file or on the command line, or both.

The configuration file has a global section and a mount-point-specific section. Configuration parameters that are configured through the command line take the highest priority and override any values in the configuration file. Mount-specific parameter values override global parameter values.

## BoostFS authentication methods

BoostFS has two authentication options:

- RSA Lockbox (default)
- Kerberos

### RSA Lockbox-based authentication

RSA Lockbox is the default password manager for BoostFS for Linux. To use RSA Lockbox, you must run the `boostfs lockbox set` command to configure the lockbox. Starting with BoostFS 1.1, a shared BoostFS lockbox file can also be configured.

#### Shared lockbox files

Beginning with BoostFS 1.1, a common lockbox file can be created for all BoostFS clients. By using this feature, you can avoid creating a separate lockbox file for each unique BoostFS client.

Sharing a common lockbox file enables you to create a single management point for BoostFS clients to access BoostFS mount points on PowerProtect DD systems.

### Kerberos-based authentication

BoostFS Linux supports the MIT implementation of Kerberos authentication as an alternative to RSA Lockbox authentication.

The primary entities involved with Kerberos authentication are:

- BoostFS client
- Kerberos Key Distribution Center (KDC), which can be on either one of the following:
  - An Active Directory server on a domain controller in a Windows environment
  - A POSIX-based operating system with optional NIS lookups



- PowerProtect DD system running DD OS version 6.0 or later

The Kerberos file contains a "shared secret" (a password, passphrase, or other unique identifier) between the KDC server and the PowerProtect DD appliance.

In an Active Directory environment, the Windows server that hosts the Active Directory service also acts as the KDC and a Domain Name Server (DNS). When you use a UNIX KDC, the DNS server does not have to be the KDC server; it can be a separate server.

---

**Note:** Before using Kerberos for BoostFS, verify that the Kerberos client libraries for Linux distribution are installed on the machine.

---

#### *Kerberos tickets*

To authenticate using Kerberos, Ticket Granting Ticket (TGT) must be acquired for two types of user accounts:

- A Kerberos TGT
- A Kerberos ticket for various services (service tickets) that the client will use (BoostFS, DNS, CIFS, NFS)

Each user has access to only the tickets that they create with the BoostFS Kerberos commands. Users cannot access tickets that others have created.

For more detailed information about using RSA Lockbox-based and Kerberos-based authentication with BoostFS for Linux, see the [DD BoostFS for Linux Configuration Guide](#).

#### Creating lockbox entry using the command line

To create a lockbox entry by using the command line:

1. From the `/opt/emc/ddboost/bin` directory, enter the following command:

```
./boostfs lockbox -h
```

```
[root@lldpvc1d091 /]# cd /opt/emc/boostfs/bin/
[root@lldpvc1d091 bin]# ls
boostfs boostfs mount enabler
[root@lldpvc1d091 bin]# ./boostfs lockbox -h
Usage:
  boostfs lockbox set
    -u <storage-unit> <username>
    -d <data-domain-system>
    -s <storage-unit>
    [-l <lockbox-path>]
    -v
  boostfs lockbox [remove | query]
    -d <data-domain-system>
    -s <storage-unit>
    [-l <lockbox-path>]
  boostfs lockbox [add-hosts | delete-hosts]
    [-l <lockbox-path>]
    <hostname [ ,hostname ]...>
  boostfs lockbox show-hosts
    [-l <lockbox-path>]
```

## Mounting and unmounting the BoostFS file system (Linux host)

2. Enter parameters in the following format to set the lockbox entry:

```
./boostfs lockbox set -u <storage-unit-username> -d <data-domain-system> -s <storage-unit>
```

```
(root@lldpdcvcl091 bin) # ./boostfs lockbox set -u boostuser -d lldpdcvcl091.lap.lab.csc.com -s BoostFS_01
Enter storage unit user password:
Enter storage unit user password again to confirm:
lockbox entry set
```

The lockbox entry has been set successfully.

## Mounting and unmounting the BoostFS file system (Linux host)

**Prerequisites** The `boostfs mount` command establishes the BoostFS FUSE mount:

```
boostfs mount [-d|--data-domain-system] <data-domain-system> [-s|--storage-unit] <storage-unit> [[-o|--option <param>=<value>] ...] <mount-point>
```

Before mounting the BoostFS Storage Unit, a mount point must be created.

From the command line, create a directory by running the `mkdir /mnt/boostfs_SU` command, and validate the mount point by running the `ls -ltr /mnt` command.

```
(root@lldpdcvcl091 ~) # mkdir /mnt/boostfs_SU
(root@lldpdcvcl091 ~) # ls -ltr /mnt
total 0
drwxr-xr-x  2 root root  6 Apr 17 12:58 boostfs_SU
(root@lldpdcvcl091 ~) #
```

### Mounting the BoostFS file system

Mount the BoostFS file system as follows:

1. From the command line, go to the path where BoostFS is installed and enter `./boostfs mount -h` for mount options.

```
(root@lldpdcvcl091 bin) # ./boostfs mount -h
Usage:
  boostfs mount <mount-point>

Property values from the configuration file apply. Mandatory options
data-domain-system and storage-unit must be present

      -d <data-domain-system>
      -s <storage-unit>
      [-l <lockbox-path>]
      [[-o | --option <param>=<value>] ...]
  <mount-point>

(root@lldpdcvcl091 bin) #
```

2. Enter the parameters in the following format to mount the BoostFS file system:

```
./boostfs mount -d <data-domain-system> -s <storage-unit>
<mount-point>
```

```
[root@lldpdcvcl091 bin]# ./boostfs mount -d lldpdcvcl003.lhop.lab.emc.com -s BoostFS_SU /mnt/boostfs_SU
mount: Mounting lldpdcvcl003.lhop.lab.emc.com:BoostFS_SU on /mnt/boostfs_SU
[root@lldpdcvcl091 bin]#
```

The BoostFS storage unit has been mounted as a file system on the Linux host for performing backup and restore operations:

```
[root@lldpdcvcl091 bin]# cd /mnt/boostfs_SU
[root@lldpdcvcl091 boostfs_SU]# ls
backup
[root@lldpdcvcl091 boostfs_SU]#
[root@lldpdcvcl091 boostfs_SU]#
[root@lldpdcvcl091 boostfs_SU]#
[root@lldpdcvcl091 boostfs_SU]#
[root@lldpdcvcl091 boostfs_SU]#
[root@lldpdcvcl091 boostfs_SU]# df -h
Filesystem              Size  Used Avail Use% Mounted on
devtmpfs                 1.9G   0  1.9G   0% /dev
tmpfs                    1.9G   0  1.9G   0% /dev/shm
tmpfs                    1.9G  8.5M  1.9G   1% /run
tmpfs                    1.9G   0  1.9G   0% /sys/fs/cgroup
/dev/mapper/rhel-root    46G   2.2G   44G   5% /
/dev/sda1                 497M  154M  343M  31% /boot
tmpfs                    380M   0  380M   0% /run/user/0
boostfs                  304G  268M  304G   1% /mnt/boostfs_SU
[root@lldpdcvcl091 boostfs_SU]#
```

### Unmounting the BoostFS file system

Run the following command to unmount the BoostFS file system:

```
./boostfs unmount <mount-point>
```

```
[root@lldpdcvcl091 bin]# ./boostfs unmount /mnt/boostfs_SU
[root@lldpdcvcl091 bin]#
```

## Conclusion

The BoostFS plug-in leverages the DD Boost protocol and provides improved backup times compared to various copy-based solutions. BoostFS, the DD Boost file system interface for backup and recovery:

- Expands the benefits of DD Boost to even more applications
- Can be deployed in minutes to reduce backup window and storage capacity
- Provides key advanced DD Boost features in a file system format



## References

### Dell Technologies support and documentation

[Dell.com/support](https://dell.com/support) is focused on meeting customer needs with proven services and support.

The following documents provide additional information related to this white paper. Access to documents depends on your login credentials. If you do not have access to a document, contact your Dell Technologies representative.

- [Dell DD BoostFS for Windows Configuration Guide](#)
- [Dell DD BoostFS for Linux Configuration Guide](#)
- [Dell DDOS Administration Guide](#)

The [Dell PowerProtect DD Series Appliances](#) web page provides more information about PowerProtect DD series appliances.

The [Data Protection Info Hub](#) provides expertise to ensure customer success with Dell Technologies data protection products.



7.11.0

Search

POWERPROTECT  
DD SERIES  
APPLIANCES  
7.12.0 REST API

Introduction

What's New

Getting Start... &gt;

Tasks &gt;

APIS

POWERPROTECT  
DD API  
DOCUMENTATION

Overview

Activities &gt;

Admin Acce... &gt;

Alerts &gt;

Alerts Notifyl... &gt;

Analytics Ca... &gt;

Auth &gt;

Authorizatio... &gt;

Cifs Auth &gt;

Cifs Options &gt;

Cifs Shares &gt;

Cifs Status &gt;

Cifs Status D... &gt;

Cifs Status E... &gt;

Cloud &gt;

Cloud Profiles &gt;

Cloud Provider &gt;

Cloud Provid... &gt;

Cloud Unit &gt;

Cloud Unit Id... &gt;

Cloud Unit Id... &gt;

## PowerProtect DD Series Appliances

Inline deduplication for data protection and disaster recovery in enterprise environments.

Version	Category Name
7.11.0	Data Protection

API Documentation

## Introduction

### Introduction to Dell EMC PowerProtect DD Appliance REST API

Dell EMC PowerProtect DD Series Appliances and older Data Domain systems are disk-based appliances that run PowerProtect DD OS to provide inline deduplication for data protection and disaster recovery (DR) in the enterprise environment.

**Note:** In this guide, "DD system," "the protection system," or "the system" refers to PowerProtect DD Series Appliances that are running DD OS 7.0 or later as well as earlier Data Domain systems.

## Basic concepts

### REST API endpoint

The PowerProtect DD system REST API endpoint:

- Earlier than DD OS 7.2:

```
https://<DD-SYSTEM-IP/FQDN>:3889/rest/<API-VERSION>/<RESOURCE>
```

The API version can be v1.0, v2.0, v3.0, and so on.

- DD OS 7.2 or later:

```
https://<DD-SYSTEM-IP/FQDN>:3889/api/<API-VERSION>/<RESOURCE>
```

The current API version is v1.

The old REST API endpoint is still supported.

### Template, query parameters and object IDs

The resource URI can contain template or query parameters.

A template parameter indicates the resource on which the operation is performed. Replace template parameters with object IDs, which are unique identifiers that are associated with DD objects. Object IDs are URL-encoded and are returned as part of a RESTful response. API users must use object IDs in GET details, and PUT and DELETE URIs to refer to a specific object.

For example, the **SYSTEM-ID** template parameter in the following request should be replaced by the URL-encoded ID of the PowerProtect DD system for which you want to fetch a list of users.

```
GET https://<DD-SYSTEM-IP/FQDN>:3889/rest/v1.0/dd-systems/{SYSTEM-ID}/users
```

**Note:** On a PowerProtect DD system, a SYSTEM-ID of 0 can be used to indicate the local PowerProtect DD system ID in place of the actual URL-encoded SYSTEM-ID.

For example, the following request retrieves the list of users on the local PowerProtect DD system:

```
GET https://<DD-SYSTEM-IP/FQDN>:3809/rest/v1.0/dd-systems/0/users
```

The **ID** in the GET `https://<DD-SYSTEM-IP>:3809/rest/v1.0/dd-systems/{SYSTEMID}/users/{ID}` request is also a template parameter and represents the URL-encoded unique ID of the user for whom to fetch detailed information.

The following list provides examples of URL-encoded IDs:

- Data Domain system ID, URL encoded system UUID:

```
d853debd0ef9406a21a9e7f877761e85d3d
```

- MTree ID, URL encoded MTree name:

```
%2Fdata%2Fcol1%2Fnas-archive
```

- Export ID, URL encoded export path:

```
%2Fdata%2Fcol1%2Fengineering%2Fsantaciara
```

- CIFS share, URL-encoded share name:

```
nas-archive
```

Query parameters provide additional criteria to which the response data must conform. Query parameters are part of the URL query string and must contain URL-encoded values. For example, the following query fetches a list of users on a specific PowerProtect DD system starting at page one, and assuming that each page has five users:

```
GET https://<DD-SYSTEM-IP/FQDN>:3809/rest/v1.0/dd-systems/0/users?page=1&size=5
```

If a request is sent with an incomplete URI, a list of related links may be returned for the client to correct itself. For example, if client sends a GET `/rest/v1.0/dd-systems/0/protocols` request, it returns the following response:

```

{
  "code": 0,
  "link": [
    {
      "href": "/rest/v1.0/dd-systems/0",
      "rel": "parent"
    },
    {
      "href": "/rest/v1.0/dd-systems/0/protocols/nfs",
      "rel": "nfs"
    },
    {
      "href": "/rest/v1.0/dd-systems/0/protocols/cifs",
      "rel": "cifs"
    },
    {
      "href": "/rest/v1.0/dd-systems/0/protocols/vdisk",
      "rel": "vdisk"
    },
    {
      "href": "/rest/v1.0/dd-systems/0/protocols/ddboost",
      "rel": "ddboost"
    }
  ],
  "details": "success"
}

```

## Data formats

The PowerProtect DD system REST API supports XML and JSON data formats. The client can choose the data format in its request and response. In the HTTP header, use **Content-Type** header to specify the request format, and use **Accept** header to specify the expected response format.

```

Content-type: application/xml or application/json
Accept: application/xml or application/json

```

The PowerProtect DD system, as the server, uses the following rules to determine the format of requests and responses:

- If **Content-Type** is set, the server expects the input data to be in the specified format. If the **Accept** header is specified, the server response must be in the specified data type format.
- If the **Content-Type** header is specified but the **Accept** is not, the format of response data is the same as the request data.
- If neither the **Content-Type** nor the **Accept** headers is specified, the default format for both request and response types is assumed to be *application/json*.

## Backward and forward compatibility

As additional features are added to the product, APIs may change. Observe these common practices when dealing with API changes:

- **Deprecated APIs and fields:** Do not use them. Deprecated APIs and fields are removed when the infrastructure no longer supports them.
- **Handling requests and responses in JSON:** Exercise flexibility and tolerance with unrecognized fields and enumerations. New fields and enumerations might be added in support of new features such as a new asset type or new protection type. If you do not use them, ignore these fields and enumerations when they are not recognized.

## Contact

Contact support here: <https://www.dell.com/support/home/us/en/04/product-support/product/data-domain>

© 2023 Dell Technologies | [Privacy](#) | [Terms of Use](#)





## PowerProtect Série DP: Armazenamento de proteção: Data Domain: Limpeza automática

Resumo: A limpeza automática habilitada para previsão é executada somente quando seu mecanismo de previsão determina que a capacidade utilizada excede uma porcentagem configurada dentro de um tempo definido.

### Conteúdo do artigo

#### Instruções

##### O que é limpeza automática?

A limpeza automática com previsão ativada complementa o mecanismo de limpeza existente prevendo a capacidade do sistema e permitindo que a limpeza seja iniciada de maneira automática quando o sistema prevê que atingirá determinados níveis de uso de capacidade em determinado período, em vez de depender apenas de agendamentos de limpeza baseados em tempo, independentemente do uso da capacidade ou da atividade do sistema.

##### Em qual versão do sistema operacional a limpeza automática foi introduzida?

A limpeza automática habilitada para previsão foi introduzida no DD OS 7.6.x incorporado ao Integration Data Protection Appliance 2.7.x.

A limpeza automática está disponível somente para o nível ativo.

**NOTA: Esse recurso está desabilitado por padrão. Ele pode ser configurado de acordo com o requisito.**

##### Quais são os desafios do processo de limpeza tradicional ou regular?

- A limpeza do DD ou coleta de lixo (GC) é um processo de longa execução que também atrasa o processo mutuamente exclusivo, como a limpeza da nuvem.
- Ele exige muitos recursos. O desempenho de ingestão ou REPL pode ser afetado.
- A GC leva à fragmentação de dados, que internamente costuma degradar a localidade dos dados e afeta o desempenho de leitura ao longo do tempo, afetando, assim, o desempenho da restauração.
- A GC é executada conforme o agendamento, mesmo quando não há necessidade (cenários como: O sistema não está próximo do total, os backups têm retenção mais longa, alguns dos backups expiram dentro de uma semana).
- A GC pode fazer uso intenso de E/S e pode competir com a ingestão.
- A vida útil do disco pode ser afetada pela repetição de E/S.

##### Quais são os benefícios da limpeza automática?

- Com a limpeza automática, a GC é executada somente quando necessário, portanto, é eficiente em termos de recursos.
- Reduzir o número de ciclos de limpeza, por sua vez, reduz a fragmentação de dados e melhora o desempenho de leitura ou restauração.
- Se a previsão indicar que a capacidade utilizada pelo sistema não excede x quantidade de uso nos próximos n dias, a limpeza agendada do nível ativo será ignorada, mas, internamente, será marcada como bem-sucedida para que, se a limpeza da nuvem estiver agendada para execução, ela possa ser ativada.

##### Qual é o conceito por trás da limpeza automática?

- A limpeza automática usa um Mecanismo de previsão.
- O Mecanismo de previsão é um segmento dentro do file system do Data Domain e é executado a cada hora.

- Coleta bytes físicos gravados e armazena esses registros de capacidade.
- A previsão de capacidade pode ser feita após a coleta de 10 registros de capacidade.
- Mantém registros do histórico de uso de capacidade em um buffer circular.
- Por padrão, ele mantém 756 registros (um mês de uso de capacidade por hora).
- O Mecanismo de previsão usa um modelo de regressão linear

$$\text{Capacidade futura} = \text{Capacidade atual} + (\text{Taxa de ingestão} * \text{Tempo})$$

#### Quais são os diferentes tipos de limpeza automática?

- Scheduled Automatic Cleaning or Skip Schedule
- Fully Automatic Cleaning or Auto Schedule

**Nota:** Apenas um tipo de limpeza automática pode ser definido por vez, seja Skip Schedule ou Auto Schedule.

#### Quais são as diferenças entre os dois tipos de limpeza automática?

##### Scheduled Automatic Cleaning or Skip Schedule

Compatível com sistemas com Cloud Tier

O agendamento de limpeza regular ou tradicional deve estar presente.

A limpeza regular agendada será ignorada se for previsto um aumento da capacidade utilizada do sistema além da porcentagem configurada dentro dos dias definidos.

Se Skip Schedule estiver desativado ou redefinido, o agendamento normal de limpeza permanecerá como está.

##### Fully Automatic Cleaning or Auto Schedule

Não compatível com sistemas com Cloud Tier

O agendamento de limpeza regular é desativado automaticamente depois que o agendamento automático é definido.

A limpeza só será executada se for previsto que a capacidade utilizada agendada exceda o limite percentual configurado nos dias definidos.

Se Auto Schedule estiver desativado ou redefinido, o agendamento normal de limpeza deverá ser definido manualmente.

Assista no [YouTube](#)

#### Quais são os comandos usados para configurar a limpeza automática?

- Scheduled Automatic Cleaning or Skip Schedule

##### Configuração

##### Sintaxe:

```
filesys clean skip schedule { [days <day(s)> estimate-percent-used <percent>] | show | reset }
```

##### Exemplo:

No momento do agendamento de limpeza regular, se a previsão indicar que a capacidade utilizada do sistema não crescerá além de 90% nos próximos 10 dias, a limpeza será ignorada. O seguinte deve ser feito para configurar isso:

1. Verifique se o agendamento de limpeza regular existe e certifique-se de que ele não esteja definido como "never".

```
# fileys clean show schedule
```

Se o agendamento de limpeza regular não existir ou for definido como never, use a sintaxe abaixo para defini-lo ou usar o caminho da IU do DD conforme abaixo:

#### Sintaxe da CLI:

```
fileys clean set schedule { daily <time> | <day(s)> <time> | biweekly <day> <time> |
monthly <day(s)> <time> }
```

Ou

Paça login na GUI do DD > Data Management > Filesystem > Clique no ícone de engrenagem à direita para "Settings" > Vá para a guia "Cleaning" > Selecione Frequency, Time e day.

2. Em seguida, defina a configuração de skip schedule conforme abaixo:

```
# fileys clean skip schedule days 10 estimate-percent-used 90
```

**Para exibir** a configuração atual de skip schedule

```
# fileys clean skip schedule show
```

**Para desativar** o skip schedule

```
# fileys clean skip schedule reset
```

#### • Fully Automatic Cleaning or Auto Schedule

##### Configuração

##### Sintaxe:

```
fileys clean auto schedule {[days <day(s)> estimate-percent-used <percent>]|[interval-days
<days>]|show | reset }
```

##### Exemplo:

Se o requisito for executar a limpeza quando espera-se que a capacidade utilizada do sistema cresça além de 85% nos próximos 10 dias, veja abaixo como ela é definida:

```
# fileys clean auto schedule days 10 estimate-percent-used 85
```

O/p: As limpezas agendadas automaticamente serão executadas se o espaço usado pelo sistema crescer além de 85% nos próximos 10 dias.

A quantidade mínima de dias entre a limpeza agendada automaticamente é definida como sete dias.

**NOTA:** Por padrão, a quantidade mínima de dias entre dois dias consecutivos de limpeza automática é definida como sete dias.

Isso também pode ser alterado e definido usando a opção "**interval-days**", conforme abaixo:

```
# fileys clean auto schedule days 10 estimate-percent-used 85 interval-days 5
```

O/p: As limpezas agendadas automaticamente serão executadas se o espaço usado pelo sistema crescer além de 85% nos próximos 10 dias.

A quantidade mínima de dias entre a limpeza agendada automaticamente é definida como cinco dias.

**NOTA:** Depois que o agendamento automático é definido, o agendamento de limpeza regular é desativado automaticamente, conforme abaixo:

```
# fileys clean show schedule
```

A limpeza do file system está agendada para "nunca" ser executada.



– Para exibir a configuração da limpeza com Auto Schedule:

```
# fileSYS clean auto schedule show
```

– Para desativar o Auto Schedule

```
# fileSYS clean auto schedule reset
```

**NOTA:** Após desativar a limpeza com Auto Schedule, o ciclo de limpeza regular deve ser manualmente definido como abaixo:

**Sintaxe da CLI:**

```
fileSYS clean set schedule { daily <time> | <day(s)> <time> | biweekly <day> <time> |  
monthly <day(s)> <time> }
```

Ou

**UI:** Faça login na GUI do DD > Data Management > Filesystem > Clique no ícone de engrenagem à direita para "Settings" > vá para a guia "Cleaning" > Selecione Frequency, Time & day.

Para obter mais detalhes, consulte o Guia de Administração do DD OS do respectivo sistema operacional no [Solve Desktop](#).

## Propriedades do artigo

### Produto afetado

Data Domain, Integrated Data Protection Appliance Family

### Produto

PowerProtect Data Protection Appliance

### Data da última publicação

21 jun. 2023

### Versão

8

### Tipo de artigo

How To





# Replication

(/dell/dell-  
emc-  
powerprotect  
dd-dd-  
series-  
appliance  
hardware-  
assisted-  
compression-  
1/dd/dell-  
emc-  
17/cloud-  
tier-  
3/)

- Replication between previous generation Data Domain appliances and DD series appliances continues to be supported.
- There is no performance impact due to the different compression algorithms used on Data Domain appliances without hardware assisted compression when replicating to or from a DD series appliance with hardware assisted compression.

## Replication

- Replication between previous generation Data Domain appliances and DD series appliances continues to be supported.
- There is no performance impact due to the different compression algorithms used on Data Domain appliances without hardware assisted compression when replicating to or from a DD series appliance with hardware assisted compression.

(//dell/dell-  
emc-  
powerprotect-  
dd-dd-  
series-  
appliances  
without-hardware-  
assisted-  
compression-  
1/dd/dell-  
boost-  
17/)cloud-  
tier-  
3/)