Technical Guide

Dell EMC PowerProtect DD Series Appliances with Commvault® Backup and Recovery : Configuration Guide

Abstract

This solution guide outlines the configuration steps for Dell EMC™ PowerProtect DD series appliance with Commvault® Complete Backup and Recovery software.

January 2021

Revisions

Date	Description
January 2021	Initial release

Acknowledgments

Author: Sonali Dwivedi

Table of contents

Executive summary

With improvements in disk technology and cost, disk-to-disk backup has become a preferred solution for protecting data, a valuable corporate asset. However, there is a world of difference between writing backups to disk and designing a disk-based data protection solution optimized for fast and reliable recoveries.

Dell Technologies is the industry's leading provider Purpose Built Backup Appliances (PBBA). PowerProtect DD series appliances are uniquely designed for cost-efficient, fast, and verifiable data protection. DD series deduplication technology provides up to 65:1 data reduction. DD series enables network-efficient WAN and FC vaulting for disaster recovery (DR), remote office data protection and tape consolidation.

In addition, DD series offers unprecedented levels of data integrity, verification and self-healing, which are unavailable in traditional file systems or conventional disk systems. DD series support a wide array of third-party backup applications, including Commvault. DD series offers remarkable improvements in performance, reliability, and TCO to any IT organization considering disk-based solutions for both onsite and offsite data protection.

This guide will go over configuring various protocols of DD series appliances with Commvault backup software.

1 Solution Components

The solution components described in this document include Commvault® Complete Backup and Recovery 11 and Dell EMC™ PowerProtect DD series appliance.

1.1 PowerProtect DD series appliances

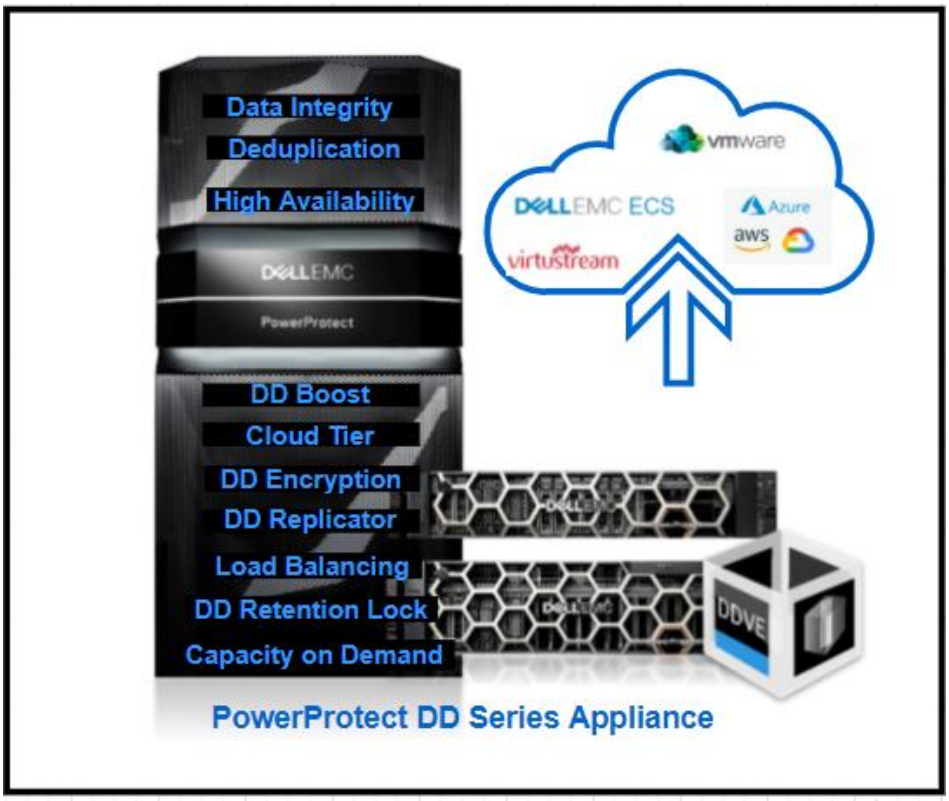
DD series appliances and older Data Domain systems are disk-based appliances that run DD OS to provide inline deduplication for data protection and disaster recovery (DR) in the enterprise environment and serves as a target appliance for backup applications.

DD series provides high-speed backup and restores with scalable deduplication. DD series incorporates a Data Invulnerability Architecture, which delivers the highest levels of data integrity and recoverability by end-to-end verification, fault tolerance and containment and continuous fault detection and healing. Its seamless integration with existing infrastructures, enabling ease-of-use with leading backup and archiving applications, and offering superior performance with Dell EMC PowerProtect Software and Dell EMC Data Protection Suite.

DD Series appliances can be deployed physically or virtually. The virtual appliance is known as PowerProtect DD Virtual Edition (DDVE) and has some different limitations from the physical appliance, such as maximum capacity. DD series supports multiple front-end protocols such as CIFS/NFS, DD VTL and its own DD Boost protocol. DD series can integrate with and supported by many popular backup software offerings. DD series uses disk storage with deduplication. Deduplication technology and, Global Compression, reduces data down to its raw essentials by pooling redundant patterns within a file, across files, and even within a block, and stores only unique data segments. This compression algorithm aggressively minimizes the capacity needed for storing backup images.

The primary storage for DD series is called the active tier. DD Series also supports a secondary tier called cloud tier. The cloud tier is a separate deduplication domain from the active tier. There is a cache disk that is set up for the cloud tier that is separate than the disk storage used for the active tier. The data is either moved

from the active tier to the cloud tier-based on age of data or by an application policy from a supported backup application.



DD OS features include:

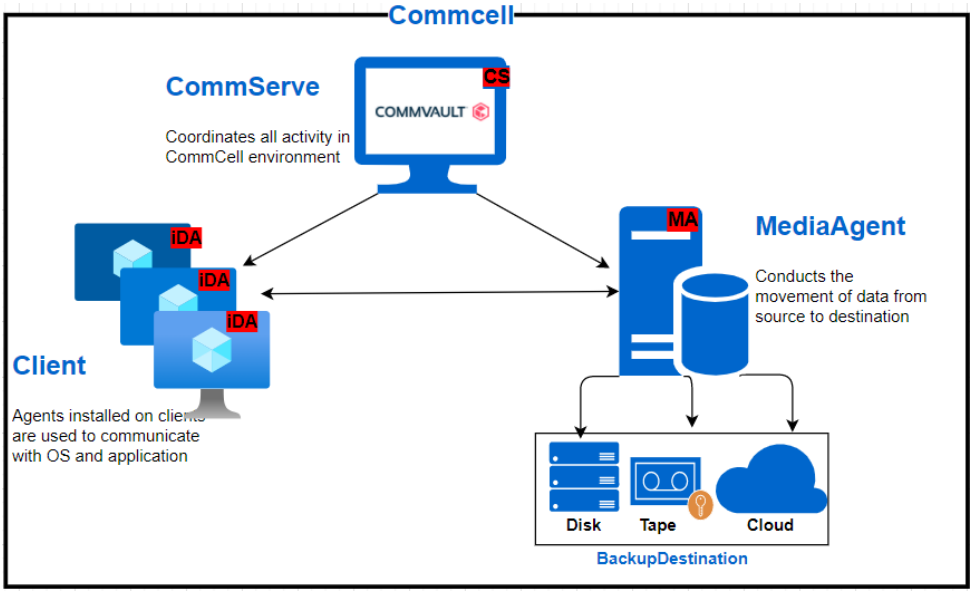
- **Data integrity**—The DD OS Data Invulnerability Architecture protects against data loss from hardware and software failures.
- **Data Deduplication**—The file system deduplicates data by identifying redundant data during each backup and storing unique data once.
- **Restore operations**—File restore operations create little or no contention with backup or other restore operations.
- **DD Replicator**—DD Replicator sets up and manages the replication of backup data between two protection systems.
- **Multipath and load balancing**—In a Fibre Channel multipath configuration, multiple paths are established between a protection system and a backup server or backup destination array. When multiple paths are present, the system automatically balances the backup load between the available paths.
- **High availability**—The High Availability (HA) feature lets you configure two protection systems as an Active-Standby pair, providing redundancy in the event of a system failure. HA keeps the active and standby systems synchronized, so that if the active node were to fail due to hardware or software issues, the standby node can take over services and continue where the failing node left off.
- **Random I/O handling**—The random I/O optimizations in DD OS provide improved performance for applications and use cases that generate larger amounts of random read and write operations than sequential read and write operations.

- **System Administrator access**—System administrators can access the system for configuration and management using a command-line interface (CLI) or a UI (user interface).
- **Licensed features**—Feature licenses allow you to purchase only those features you intend to use. Some examples of features that require licenses are DD Boost, and capacity on demand (storage capacity increases).
- **Storage environment integration**—DD OS systems integrate easily into existing data centers

1.2 Commvault Complete™ Data Protection

Commvault Complete Data Protection previously known as Simpana is an enterprise level, integrated data and information management solution, built on a single platform and unified code base. The Commvault architecture first requires discussing the various components and their functions. The iDataAgent software is deployed on all servers, workstations, and laptops where backups are needed.

The MediaAgent software is deployed on dedicated servers, maintains the deduplication databases, and manages the transfer of data between the clients and DD Series. Multiple MediaAgent are used to distribute the load. DD Series is set up as a storage target using CIFS/NFS, DD Boost, DDVTL and is a backup target. Depending on the size of the environment, or the network and physical boundaries, there can be multiple CommCell within an organization and multiple DD Series can be added as backup target.



Some of the main components of Commvault backup solution are as follows:

- **CommCell Console**
  The CommCell Console is the central management user interface for managing the CommCell group—monitoring and controlling active jobs, and viewing events related to all activities. The CommCell Console allows centralized and decentralized organizations to manage all data-movement activities through a single, common interface.

- **CommServe**
  The CommServe host is the central management component of the CommCell group. It coordinates and performs all CommCell group operations, maintaining Microsoft SQL Server databases that contain all configuration, security, and operational history for the CommCell group. There can be only one CommServe host in a CommCell group. The CommServe software can be installed in physical, virtual, and clustered

environments but only on a Microsoft Windows® host. Commvault supports high availability by replicating data to a standby CommServe host.

- **MediaAgent**
  The MediaAgent is the data-transmission manager in the CommCell group. It provides high-performance data movement and manages the storage libraries. The CommServe server coordinates MediaAgent tasks. The MediaAgent software can be installed in physical, virtual, and clustered environments. A MediaAgent can be installed on a Windows or UNIX host.

- **Client**
  A client is a logical grouping of the software agents that facilitate the protection, management, and movement of data associated with the client.

- **iDataAgent**
  An agent is a software module that is installed on a client computer to protect a specific type of data. Different agent software is available to manage different datatype on a client, such as Windows file-system data or Oracle® databases. Agent software can be installed in physical, virtual, and clustered environments, and may be installed either on the computer or on a proxy server.

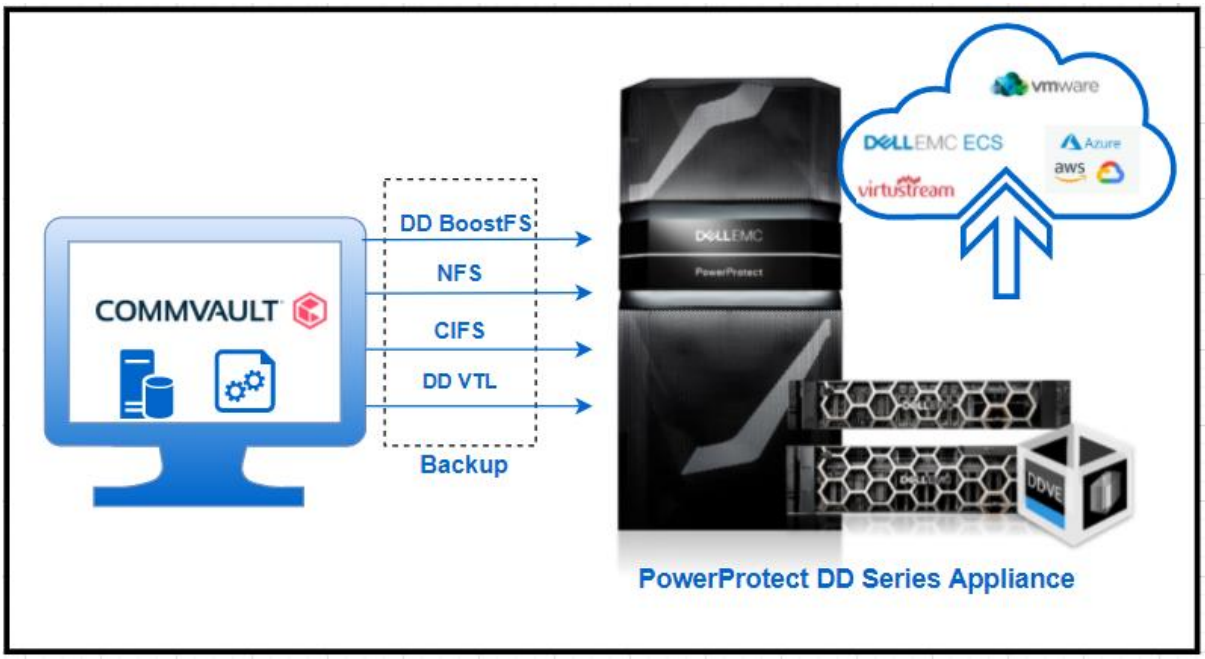
- **Storage Policy**
  Storage policies act as a channel for backup and restore operations. They map data from its original location to physical media. A policy can be used for either data protection and archiving or disaster recovery. Retention and reduplication properties can also be defined here.

- **Subclient**
  Subclients are logical containers that define the specific production data (virtual machines, drives, folders, files, databases, mailboxes) to be protected on a client.

2 Reference Architecture

DD Series is presented to the Commvault server as a CIFS/NFS/DD Boost/DD VTL storage target or depending on the media agent platform. For CIFS/NFS/DD BoostFS, the first consideration to address is what level of CIFS, NFS and DD BoostFS sharing is wanted for the DD series appliances.

Figure 3 shows the high-level architecture for a Commvault server with DD series defined as its CommCell Storage Library. With this configuration, the Storage Library settings never need to be updated as capacity is added. When capacity is added to the DD series, the CommServe and MediaAgents immediately see the additional capacity without additional configuration or manual intervention.



By default, the entire DD series directory structure `(\\datadomain\backup)` can be shared by CIFS/NFS/DD Boost to all or selected hosts. Alternatively, subfolders or an MTree can be created for explicit sharing. The choice will depend on the specific use case for the customer environment.

Note: For detailed information, please go through DD OS Administration Guide and DD BoostFS Commvault Compatibility Guide.

3 Configuration Overview

This section gives an overview of how to configure a Commvault server to work with the DD series appliances.

Prerequisites:

- System Prerequisites
  - ✓ DD series appliance running DD OS version 6.1 or later.
  - ✓ A second optional DD series appliance if replication is wanted.
  - ✓ One Commvault Complete backup and recovery server with CommCell.
  - ✓ One server with Commvault MediaAgent installed and configured MediaAgent can also be installed on the Commvault server.
  - ✓ Backup sources: Windows file servers, UNIX file servers and NDMP servers.

- Software Prerequisites:
  - ✓ Install the Commvault software, with its own prerequisites checked and configured, including SQL Server, the Windows domain controller, and other prerequisites.
  - ✓ Install the backup agent for Windows (or UNIX) on all the systems that you want to back up.
  - ✓ Install DD BoostFS plug-in for Windows server or Linux server.

- License Prerequisites:

  - ✓ DD Boost license, the online compatibility guide provides the list of qualified applications.
  - ✓ The managed file replication (MFR) feature of DD Boost also requires the DD Replicator license.
  - ✓ DD VTL licenses, if you want to back up to a VTL or an NDMP tape server.
  - ✓ Cloud Tier license, if you want to move from active tier to low-cost object store in cloud.
  - ✓ Commvault licenses, as required.

Configuration Checklist

This checklist summarizes the detailed procedures later in this document.

Procedure

1. Prepare and configure the DD series appliance backup target subdirectories and shares for CIFS access under `/backup`. Create a folder under /backup to store Commvault backup data, such as `/backup/cvbackupdata`. Alternatively, create an MTree and a share for CIFS access.
2. Create the Commvault shared magnetic libraries, which are connected by CIFS or NFS to the appropriate Commvault MediaAgent.
3. Install DD BoostFS plug-in and set the lockbox password for the storage unit for backup.
4. Create a storage policy for Client systems to use under Policies. When using the Create Storage Policy Wizard, be sure to select <proper name> as the policy type.
5. Install the Commvault Backup iDataAgent. Check the Commvault licensing requirements.
6. Add and configure the Commvault backup subclients. For most backup agents, there is default subclient.
7. Define the backup job rules.
8. Perform a test backup, verify that the job finishes successfully, and verify that data can be restored.

3.1 Configuring CIFS on DD series appliances and Commvault

3.1.1 Enabling Basic CIFS Access on DD Series

To know more options and details on PowerProtect DD Series CIFS options check DD series appliances Administration Guide.

Procedure

1. Connect to the DD series appliance as sysadmin or as a user with sysadmin privilege.
2. Determine whether CIFS is enabled:

```
sysadmin@datadomain# cifs status
CIFS is enabled.
```

3. Determine the CIFS access level defined by running the DD OS command cifs share show. The output in the example below shows the access for the DD share backup is open to all hosts.

```
sysadmin@datadomain# cifs share show
Shares information for: all shares
--------------- share cvbackupdata ---------------
path: /data/col1/cvbackup
maxconn: 0
```

```
clients: *
enabled: yes
Shares displayed: 1
sysadmin@datadomain#
```

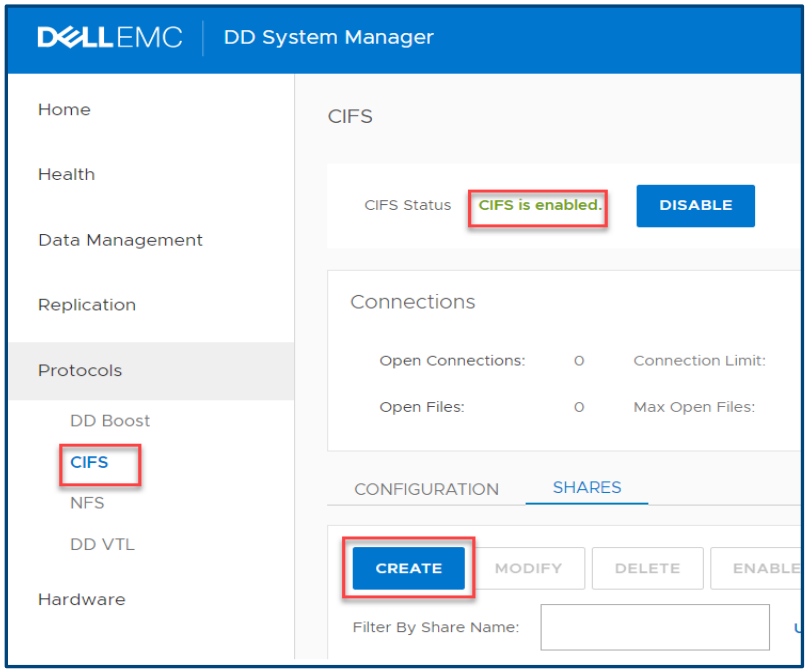
4. If the `/data/col1/cvbackup` path is not included, or the client list does not include the proper server, add the appropriate server access. Use the following DD OS command to allow access to MediaAgent host.
   In the example, access to `/data/col1/cvbackup` is open to all servers including MediaAgent host `appeng25`:

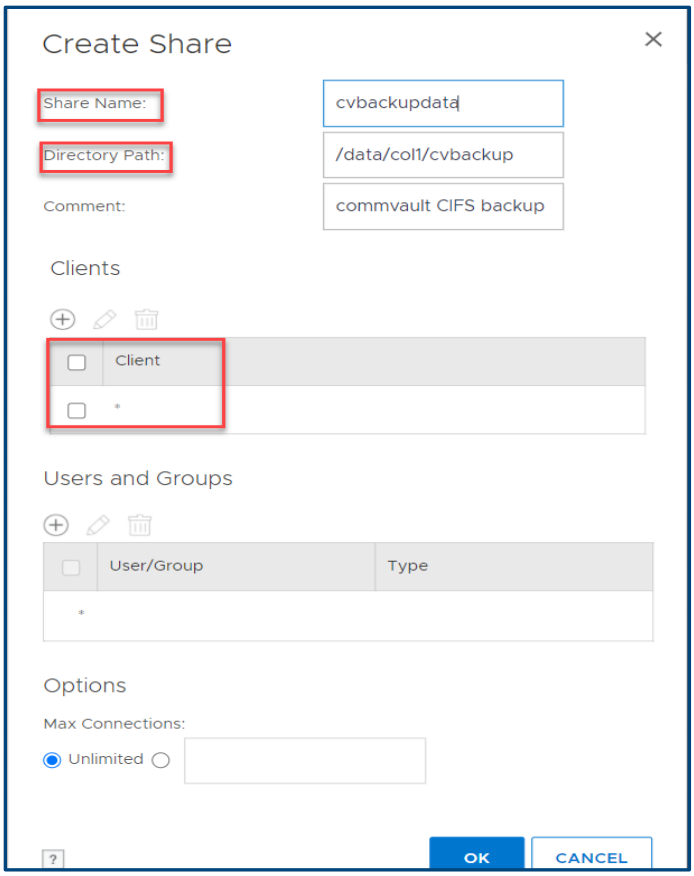
   ```
   sysadmin@datadomain# cifs share modify backup clients myclient
   Share "cvbackup" is modified for new connections.
   ```

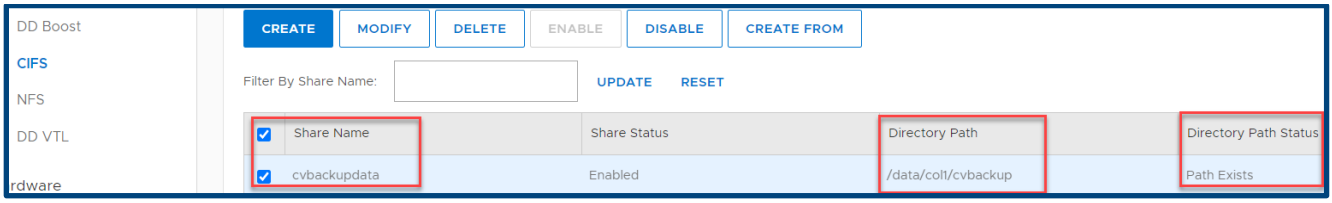
5. Verify the results:

   ```
   sysadmin@datadomain# cifs share show
   Shares information for: all shares
   --------------- share cvbackup ---------------
   path: /data/col1/backup
   maxconn: 0
   clients: myclient
   enabled: yes
   Shares displayed: 1
   sysadmin@datadomain#
   ```

6. Repeat Step 3 through 5 for all MediaAgent servers to open access to the appropriate DD share access.
7. Alternatively, you can also use 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.







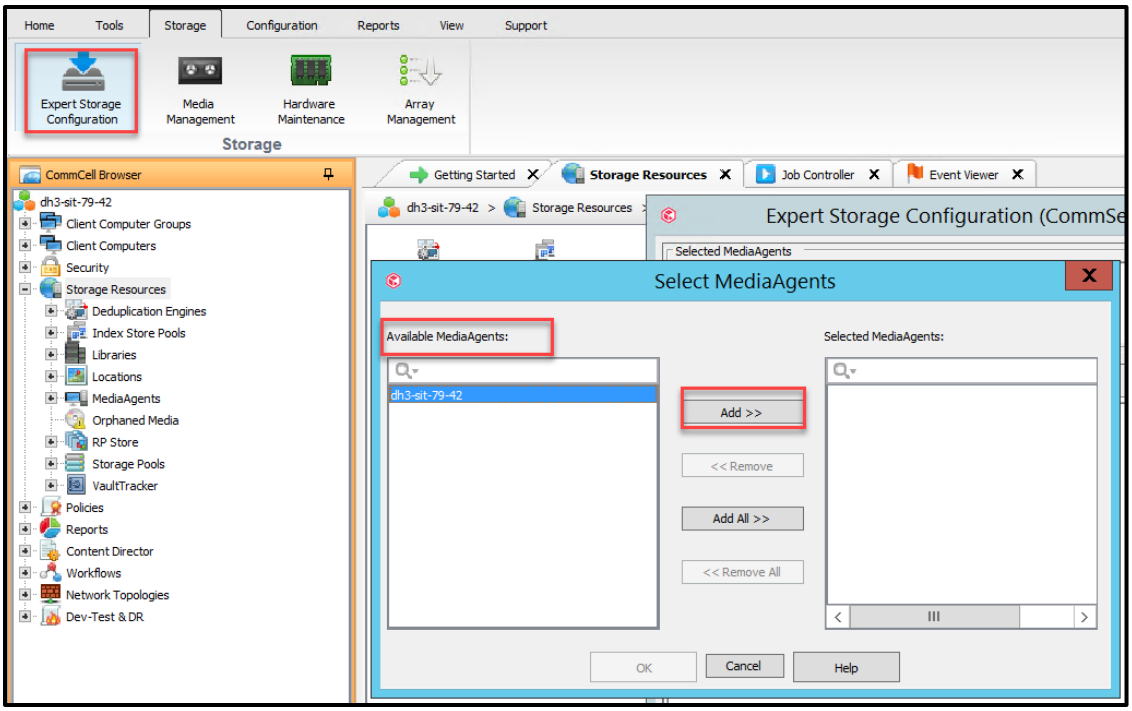
3.1.2 Creating CIFS Device in Commvault

You can use a DD series appliance as a CIFS backup target by creating a Shared Disk Device Library in with storage used from the DD series appliance over the CIFS connection.

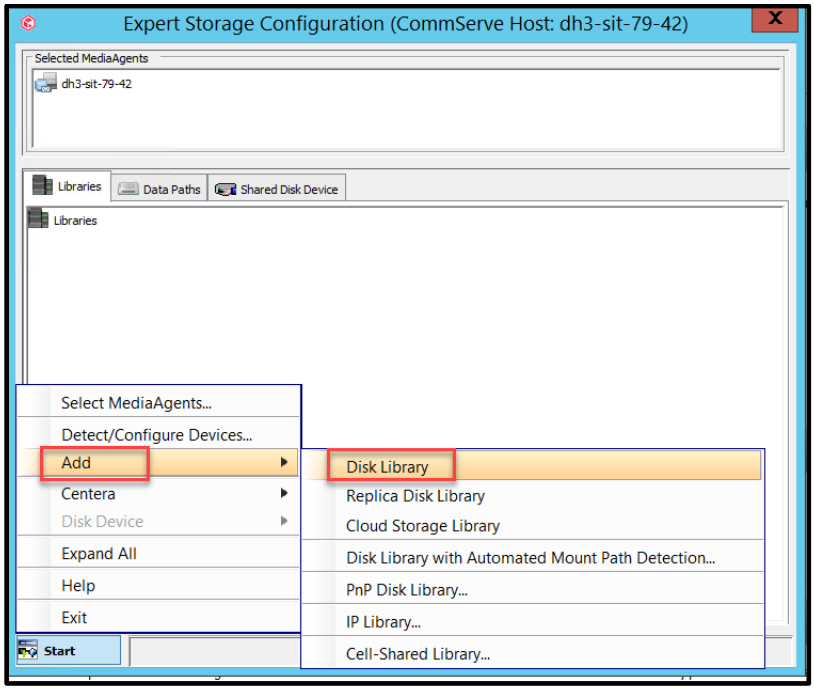
To know more options and details on Commvault CIFS, check Commvault documentation and DD series appliances Guide.

Procedure

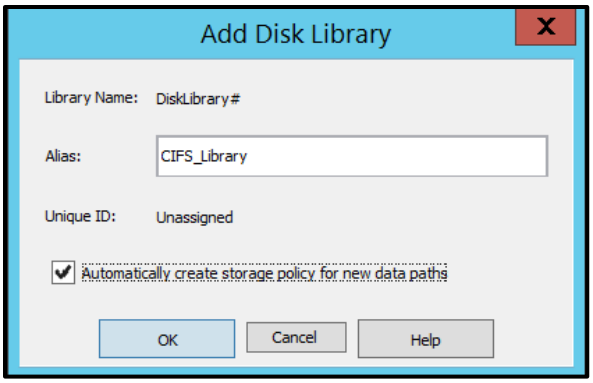
1. In the CommCell console, select **Storage** > **Expert Storage Configuration**. When prompted, add the Windows MediaAgent in the Select MediaAgents dialog box. The Expert Storage Configuration dialog box appears.



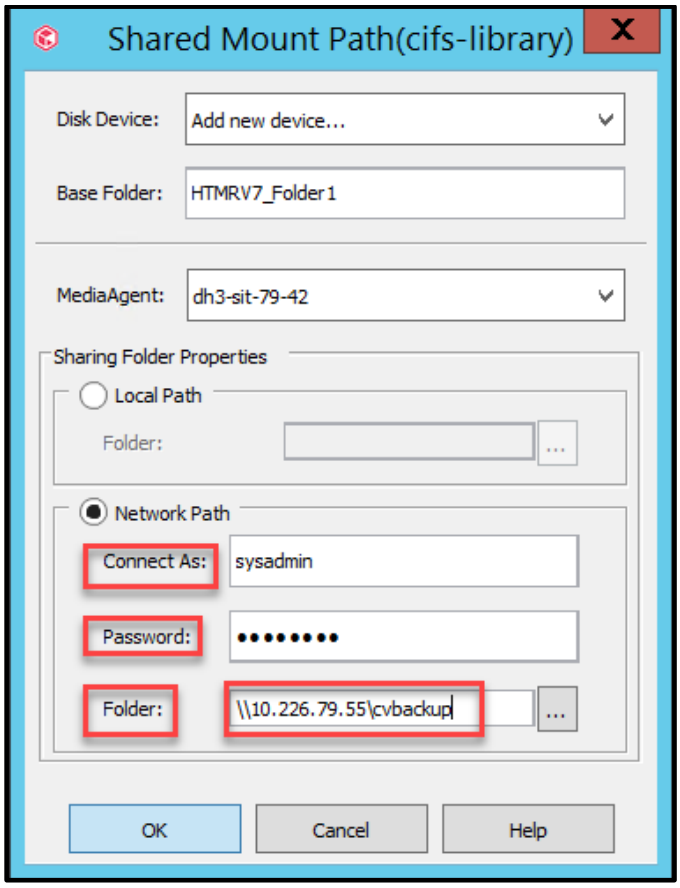
2. Right-click Libraries and select Add > Disk Library. The Add Disk Library dialog box appears.



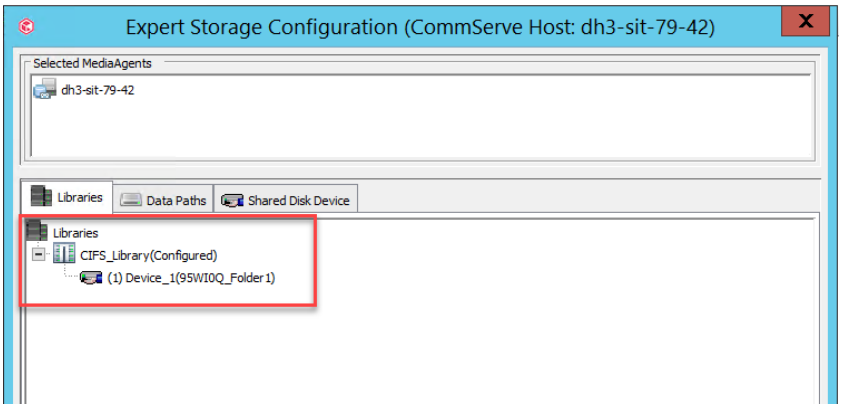
3. Type the alias for the library name, select **Automatically create storage policy for new data paths** box, and click **OK.** The Shared Mount Path (CIFS_Library) dialog box appears.



4. Type the base folder name, enter the username of the user who has access to the CIFS share on the DD series appliance in the **Connect As** box, enter the password, enter the path to the CIFS share on the DD series appliance, and click **OK.**



5. The new library is added. Close the Library and Drive Configuration window.



3.2 Configuring NFS on DD series appliances and Commvault

To know more options and details on DD series appliances NFS options, check DD series appliances Guide.

3.2.1 Enabling Basic NFS Access on DD Series Appliances

Procedure

1. Connect to the DD series appliance as sysadmin or as a user with sysadmin privilege.
2. Determine whether NFS is enabled.

```
sysadmin@datadomain# nfs status

The NFS system is currently active and running.

Total number of NFS requests handled = 112.

NFS server version(s) 3:4 enabled.

sysadmin@datadomain#
```

3. Determine the NFS access level currently defined by running the DD OS command nfs show clients.

   The output in the example below shows the access for the DD series appliance share /backup is open to all hosts as shown with '*'

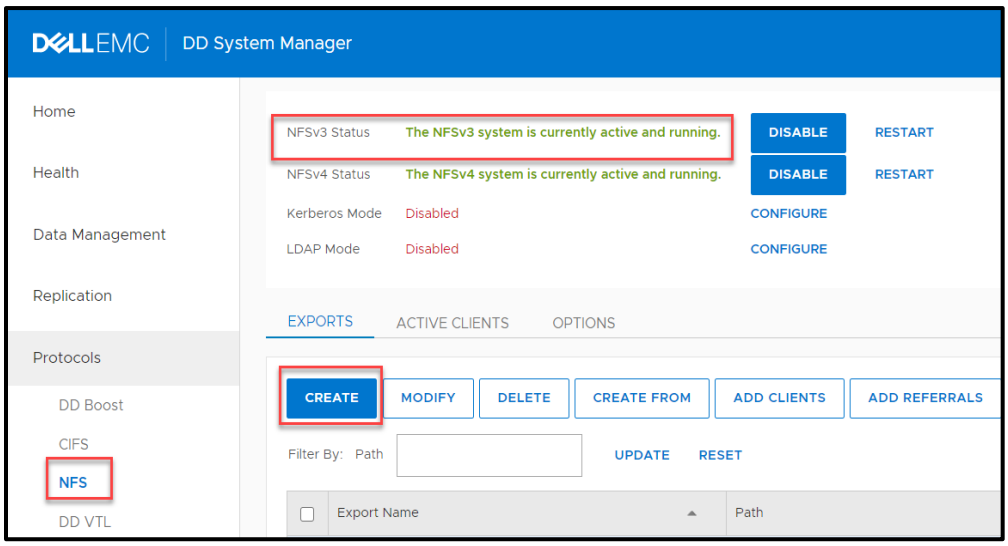
```
sysadmin@datadomain# nfs show clients
Path                Client   Options
--------------   ------   ----------------------------------------
/data/col1/backup   *       sec=sys, rw, no_root_squash, no_all_
                             squash, secure, version=3)
----------------   ------   ----------------------------------------
```

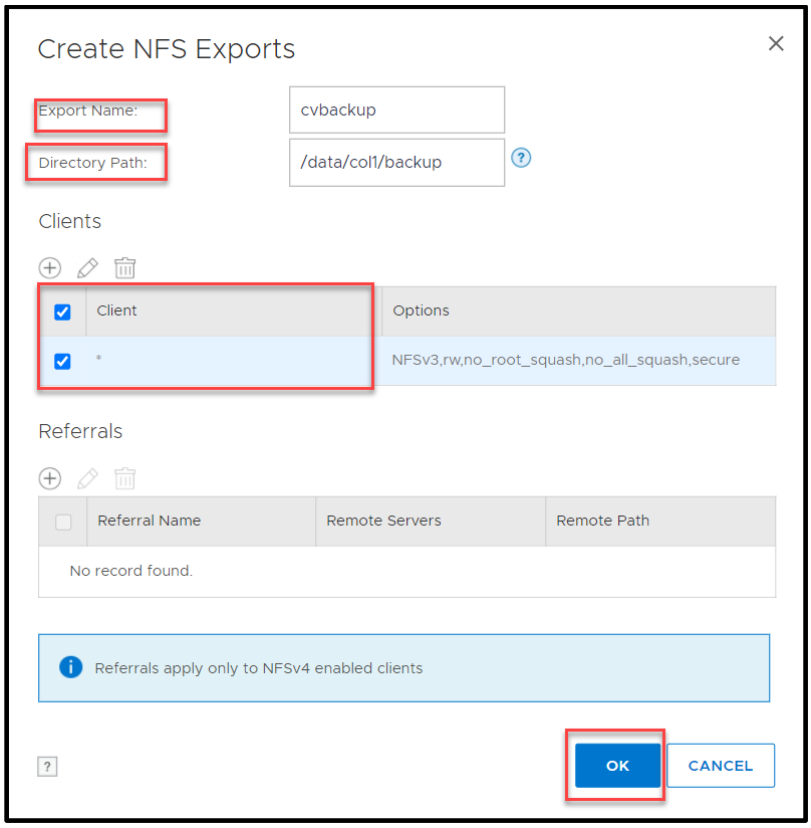
4. If the /`data/col1/backup` path is not included, or the client list does not include the proper server, add the appropriate server access. Use the following DD OS command to allow access to MediaAgent host.

```
sysadmin@datadomain# nfs add /data/col1/backup dh3-sit-79-43
NFS export for "/data/col1/backup" added.
```

Note: A * as a client name allows all servers access to the specified path on the DD series.

5. Alternatively, you can also use DD System Manager (DDSM) **Protocols** > **NFS** page allows you to perform major NFS operations such as enabling and disabling CIFS, setting authentication, managing shares, and viewing configuration and share information.





3.2.2 Creating NFS Device in Commvault

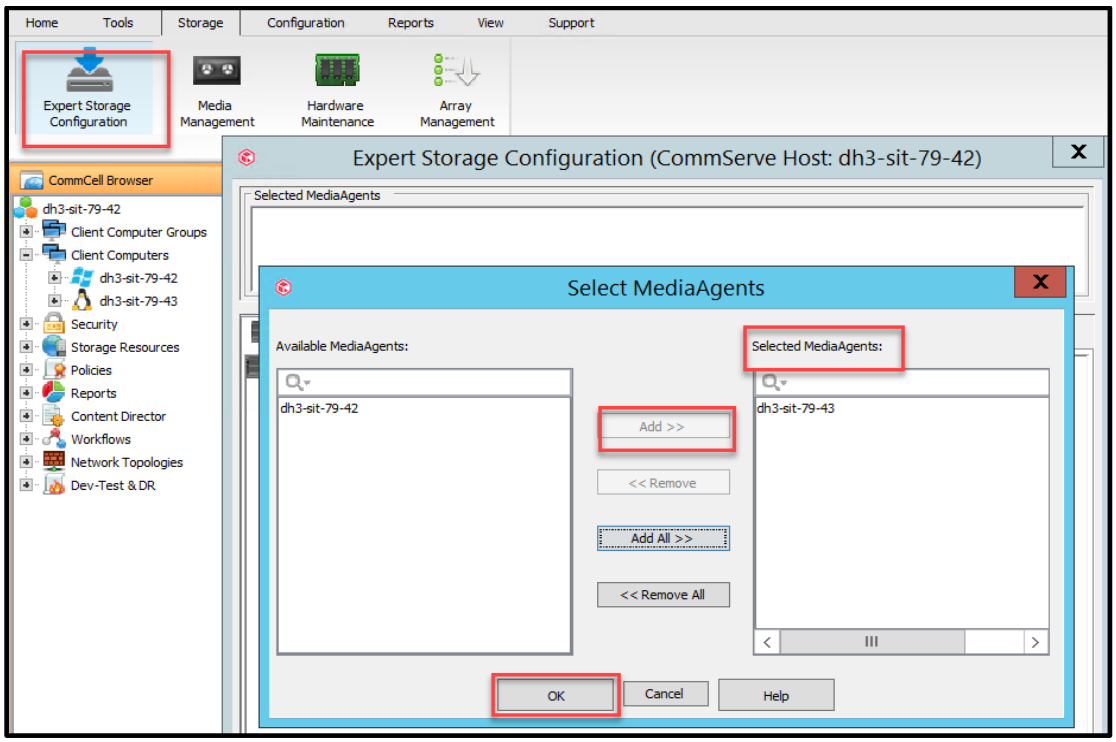
To use a DD series appliance as an NFS backup target, create a Shared Disk Device Library in with storage used from the DD series appliance over the NFS connection. This requires that a MediaAgent be running on the UNIX or Linux system. To know more options and details on Commvault NFS options, check Commvault documentation.

Procedure:

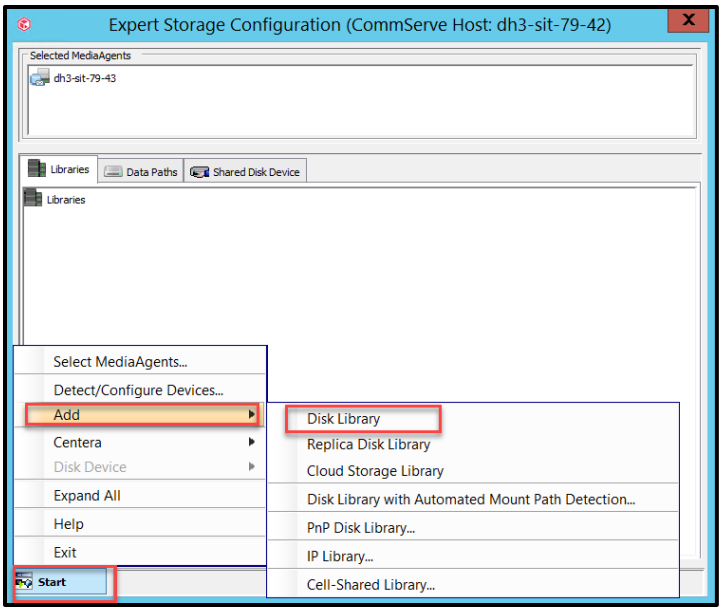
1. On the Linux MediaAgent, create a mount point and mount the /backup share from the DD series appliance

```
# mkdir /backup

# mount -t nfs -o vers=3,proto=tcp,nolock datadomain:/backup /backup

# mkdir /backup/nfs
```

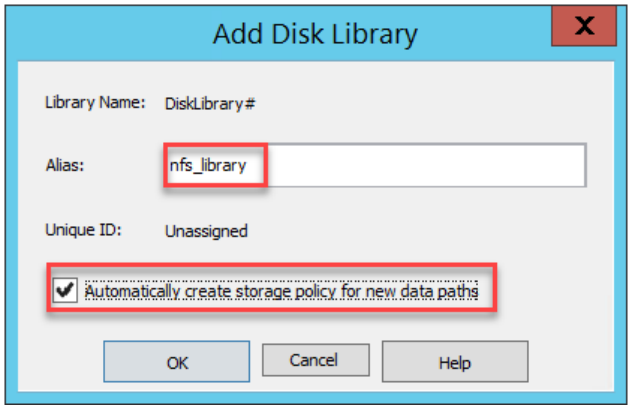
2. In the CommCell command console, select **Storage** > **Expert Storage Configuration**. When prompted, add the UNIX or Linux MediaAgent in the Select MediaAgents dialog box and click **OK**.
The Expert Storage Configuration dialog box appears.



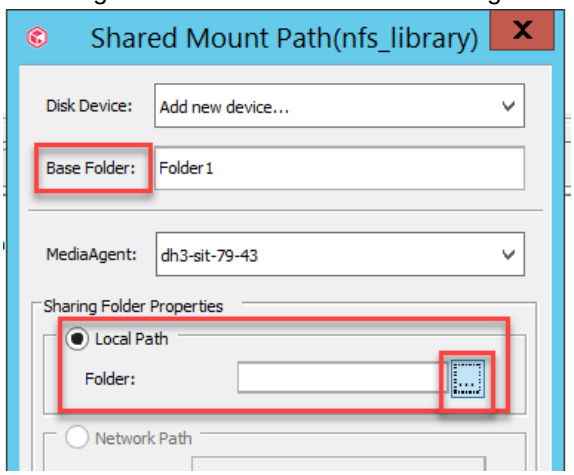
3. Click **Start** > **Add** > **Choose Disk Library.** The Add Disk Library dialog box appears. Type the alias for the library name, select **Automatically create storage policy for new data paths** box, and click **OK.** The Shared Mount Path (nfs_library) dialog box appears.



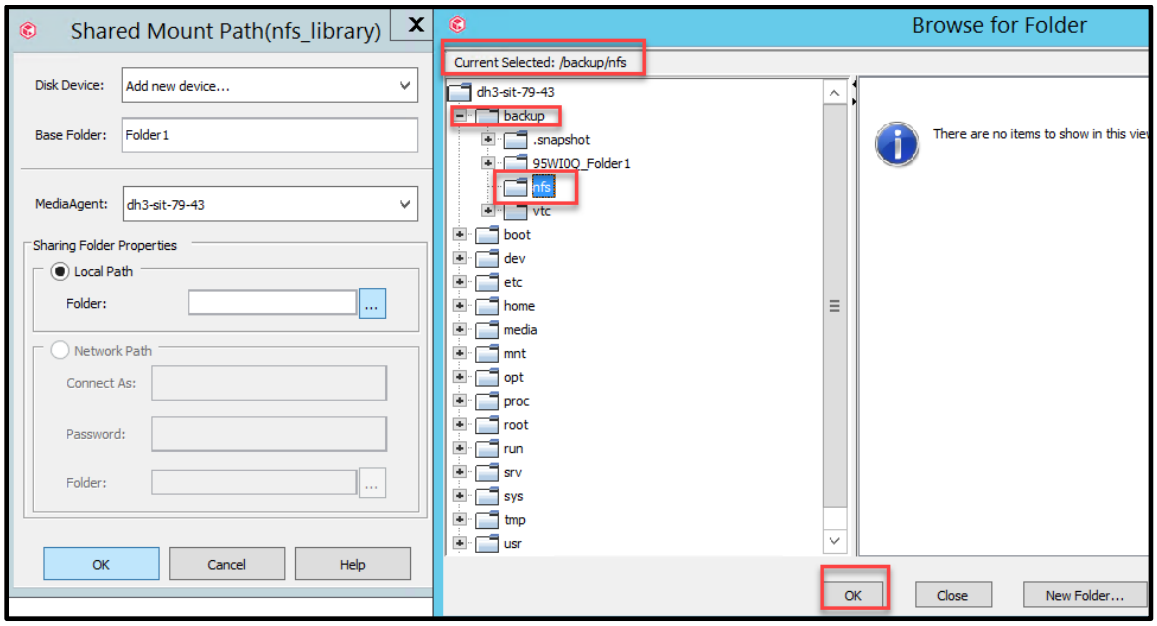
4. Type the alias for the library name, select **Automatically create storage policy for new data paths** box, and click **OK.** The Shared Mount Path (nfs_library) dialog box appears



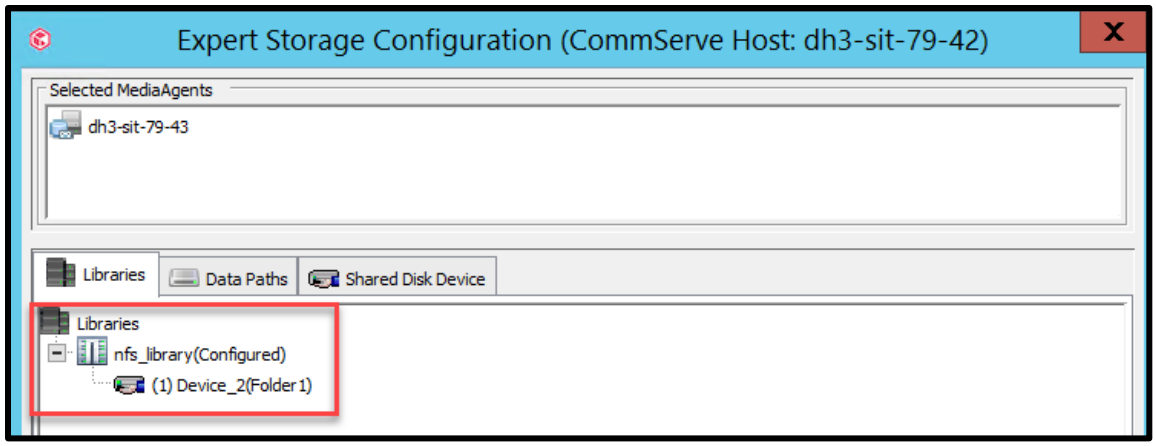
5. Type the base folder name that you want, select **Local Path**, and click… to browse for the Linux MediaAgent. The Browse for Folder dialog box appears.



6. Choose **backup** and click **OK.** The browser window closes and /backup are shown in the **Folder** box. Here we choose path /backup/nfs.



7. Click **OK**. The Expert Storage Configuration window appears, showing the new library.



Close the Library and Drive Configuration window.

3.3 Configuring DD BoostFS plug-in in Commvault

Introduced in DD OS 6.0, the DD Boost File System Plug-In (BoostFS) resides on the application system, presenting 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 qualification is needed for the application to support BoostFS, shortening the time-to-market. Also, the file system interface makes BoostFS easy to deploy, allowing it to be up and running in minutes.

By leveraging the DD Boost technology, BoostFS helps reduce bandwidth usage, can improve backup-times, offers load-balancing, in-flight encryption, and supports the DD multitenancy feature set. As a file server

system implementation, the BoostFS workflow is like NFS but also leverages the DD Boost protocol. In addition, BoostFS improves the backup times compared to NFS and various copy-based solutions. Redirecting NFS workloads to BoostFS is easy and nondisruptive to the environment in addition to being transparent to users.

BoostFS is now available for customers with active licenses for the DD Boost Software Option or DD Virtual Edition (DDVE). Check DD BoostFS for Windows and Linux to get more details.

3.3.1 Preparing DD series appliances for DD BoostFS

On the DD series appliance, log in as an administrative user.

1. Verify that the file system is enabled and running by entering:

```
$ filesys status

The file system is enabled and running.
```

2. Verify that DD Boost is already enabled:

```
$ ddboost status

DD Boost status: enabled
```

If the DD Boost status is reported as disabled, enable it by entering:

```
$ ddboost enable

DD Boost enabled
```

3. Verify that distributed segment processing is enabled:

```
ddboost option show

You should see the following output:

Option                                Value
---------------------------------- --------
Distributed-segment-processing      enabled
virtual-synthetics                  enabled
fc                                  disabled
global-authentication-mode          none
global-encryption-mode              medium
---------------------------------- ---------
```

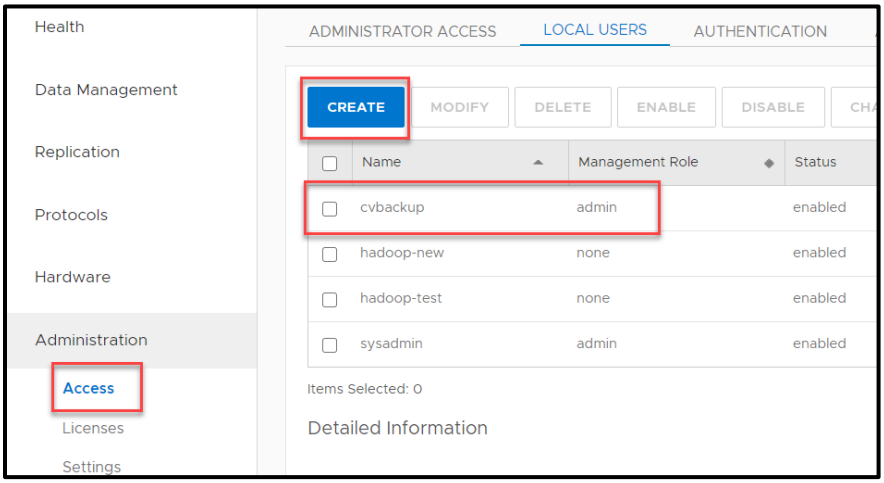
If distributed segment processing is shown as disabled, enable it by entering:

```
ddboost option set distributed-segment-processing enabled
```

4. Create a DD Boost User and set permission

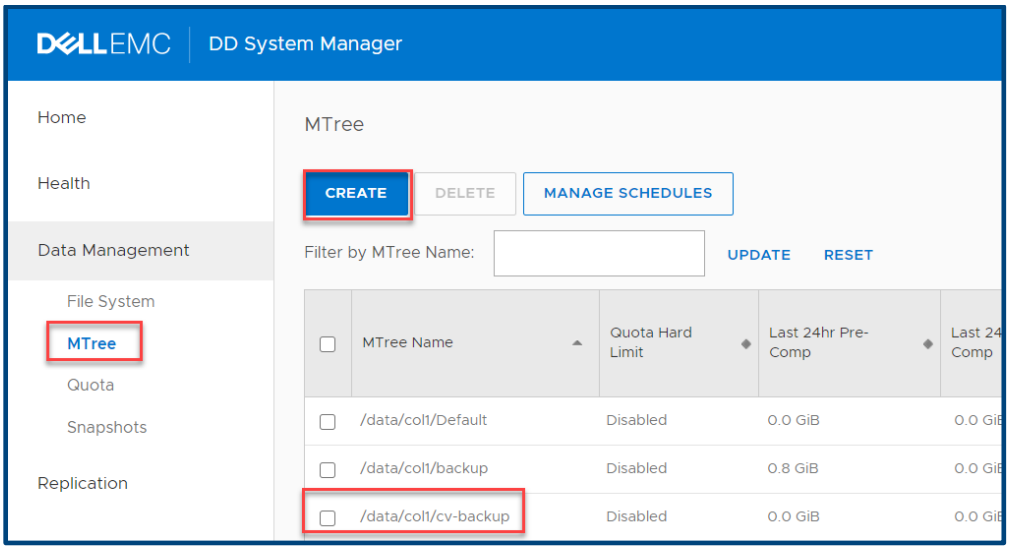
```
sysadmin@datadomain# user add cvbackup role admin
        Enter new password:
        Re-enter new password:
Passwords matched.
User "cvbackup" added.
sysadmin@datadomain# ddboost user assign cvbackup
User "cvbackup" assigned to DD Boost.
```

Alternatively, you can user the DD System Manager to create the user and assign the permissions.



5. Create a storage unit for DD BoostFS using DD Boost User

```
sysadmin@datadomain# ddboost storage-unit create cv-backup user cvbackup
Created storage-unit "cv-backup" for "cvbackup".
```



3.3.2 DD BoostFS plug-in settings for Windows Client in Commvault

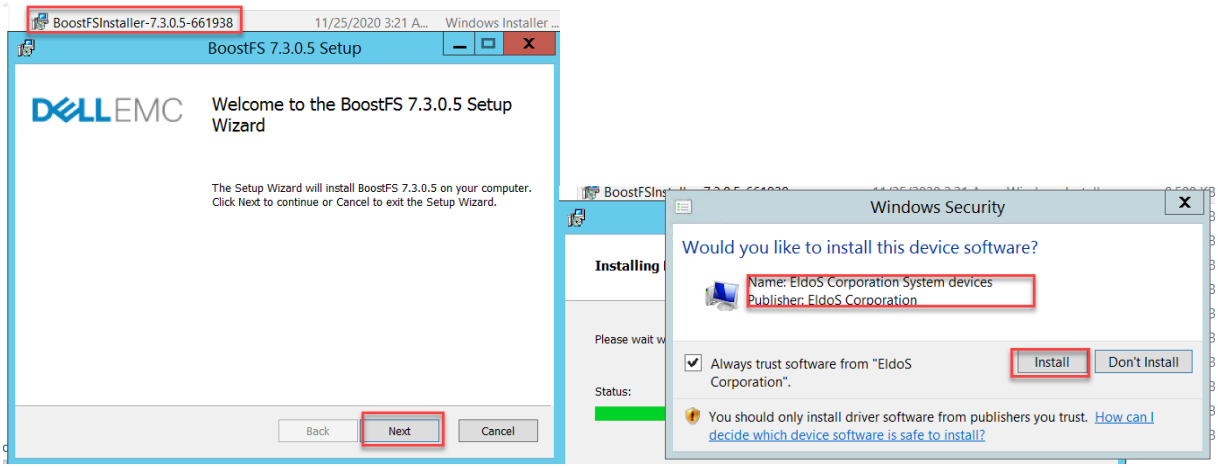
Environments that use BoostFS 7.3.0.5 must meet the following specifications. For details on another version, check DD BoostFS for Windows Guide.

BoostFS for Windows requires the following:

- DD OS version 6.1.2 or later
- Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016

Procedure:

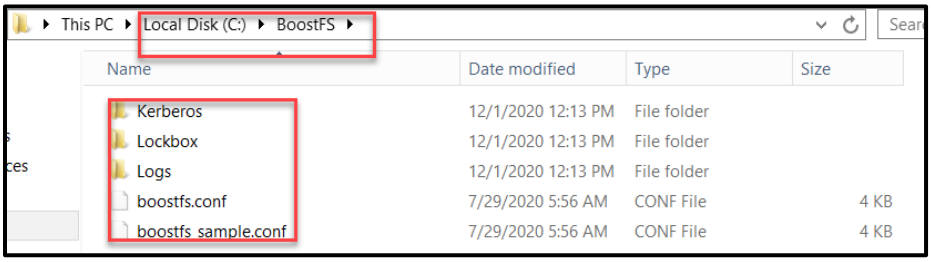
1. Install or upgrade BoostFS for Windows by using the provided MSI installer. Do not change the default settings.
2. The MSI installer includes several binary files and a device driver from EldoS Corporation.



Note: When installing or upgrading BoostFS for Windows:

- If you are prompted to restart after installing, failure to do so can cause features such as Explorer integration to not work correctly. If you are not prompted to restart, restarting is not necessary.
- 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 fail.

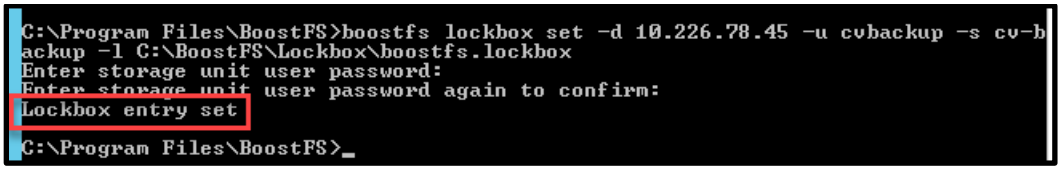
3. A directory is created at C:\BoostFS. This directory is the default location for BoostFS logs, Lockbox containers, and the sole location of the configuration file C:\BoostFS\boostfs.conf.



4. Use the Windows command prompt or PowerShell 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.

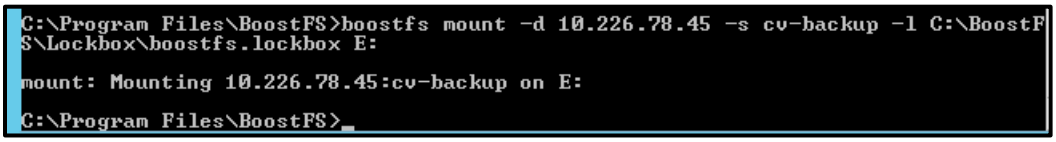
5. Run the following command to configure lockbox:

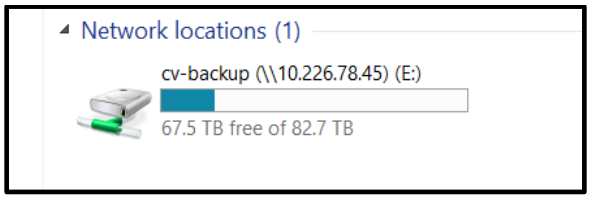
```
boostfs lockbox set -u sysadmin -d <DD Boost-IP> -s <Storage-unit> -l <lock-box-location>
```



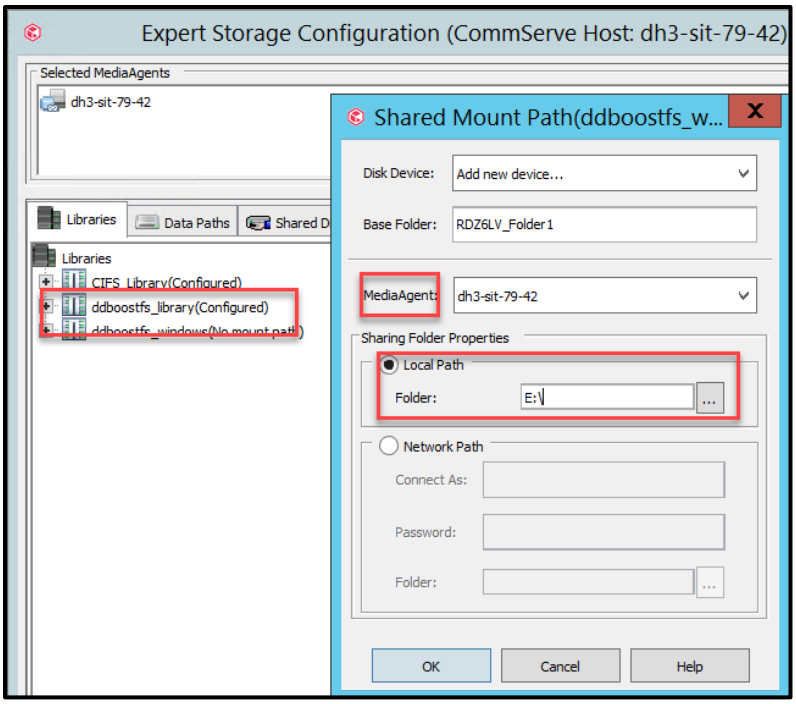
6. Run the following command to mount the DD series appliance Storage Unit.

```
boostfs mount -d <DD Boost-IP> -s <Storage-unit> -l <lock-box-location> <mapped-drive-letter>
```





7. Add the boostfs drive for backup in Commvault server. In the CommCell command console, select **Storage** > **Expert Storage Configuration**.
8. When prompted add the Windows MediaAgents. Click **Start** > **Add** > **Choose Disk Library.** The Add Disk Library dialog box appears. Type the alias for the library name, select **Automatically create storage policy for new data paths** box, and click **OK.** The Shared Mount Path (ddboostfs_library) dialog box appears.
9. Type the base folder name that you want, select **Local Path**, and enter the drive letter for dd boostfs mount and click OK. The ddboostfs_library should show configured now.



3.3.3 DD BoostFS plug-in settings for Linux Client in Commvault

Environments that use BoostFS 7.3.0.5 must meet the following specifications. For details on another version, check DD BoostFS for Linux Guide.

BoostFS for Linux requires the following:

- DD OS version 6.0 or later
- FUSE 2.8 or later

The following Linux distributions are supported:

- Red Hat Enterprise Linux versions 6 and 7
- CentOS 7
- SUSE Linux Enterprise Server versions 11 and 12
- Ubuntu 14.04 and 15
- Oracle Linux version 7

Procedure:

1. Install the FUSE File system and its dependencies on the MediaAgent.
2. Install or upgrade BoostFS for Linux using RPM Installation package. It is available in both RPM and .deb formats. The RPM package includes the boostfs executable.

```
[root@dh3-sit-79-43 opt]# rpm -Uvh DDBoostFS-7.3.0.5-661938.rhel.x86_64.rpm
Preparing...                          ################################# [100%]
Updating / installing...
   1:ddboostfs-7.3.0.5-661938         ################################# [100%]
[root@dh3-sit-79-43 opt]# cd /opt/emc/boostfs
[root@dh3-sit-79-43 boostfs]# ls
bin  etc  lib  license.txt  lockbox  log  man
[root@dh3-sit-79-43 boostfs]#
```

3. You can verify the installation from the following location:
   `#/opt/emc/boostfs`
4. Set the lock box between the DD series appliance and MediaAgent using the following command:
   `# cd /opt/emc/boostfs/bin`
   `#./boostfs lockbox set -s <Storage-unit> -d <data-domain-system> -u <storage-unit-username>`

```
[root@dh3-sit-79-43 bin]# ./boostfs lockbox set -s cv-backup -d 10.226.78.45 -u
cvbackup
Enter storage unit user password:
Enter storage unit user password again to confirm:
Lockbox entry set
[root@dh3-sit-79-43 bin]#
```

5. Mount this storage unit on the MediaAgent using the following command:
   `# mkdir <mount-point>`
   `#./boostfs mount -d <data-domain-system> -s <Storage-unit> -l <location of the lockbox> <mount-point>`

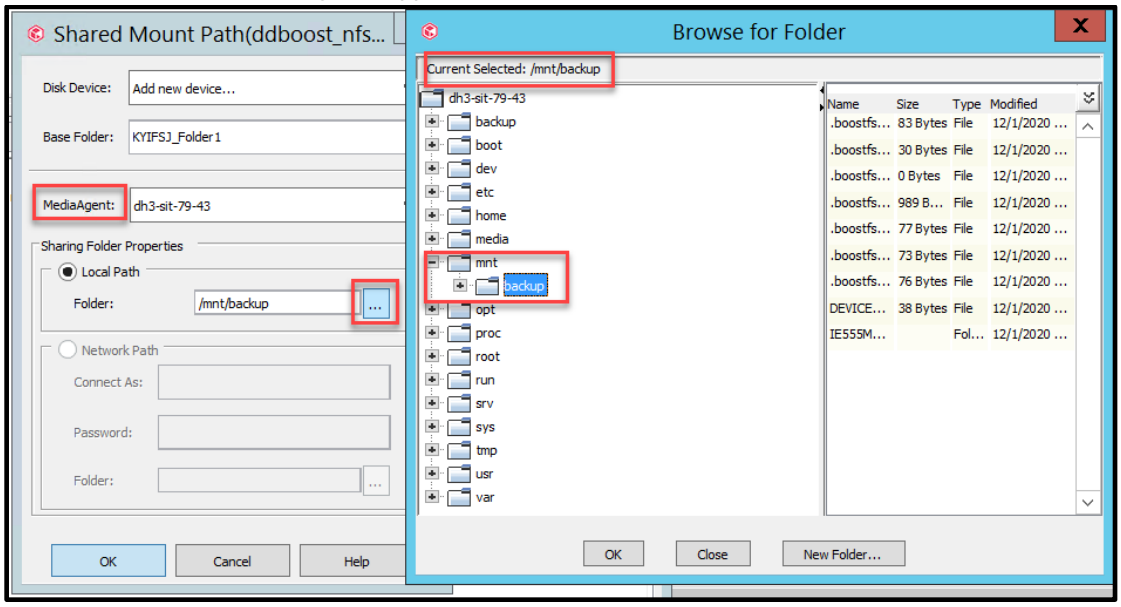
```
[root@dh3-sit-79-43 bin]# ./boostfs mount -s cv-backup -d 10.226.78.45 -l /opt/e
mc/boostfs/lockbox/boostfs.lockbox /mnt/backup

mount: Mounting 10.226.78.45:cv-backup on /mnt/backup
[root@dh3-sit-79-43 bin]#
```

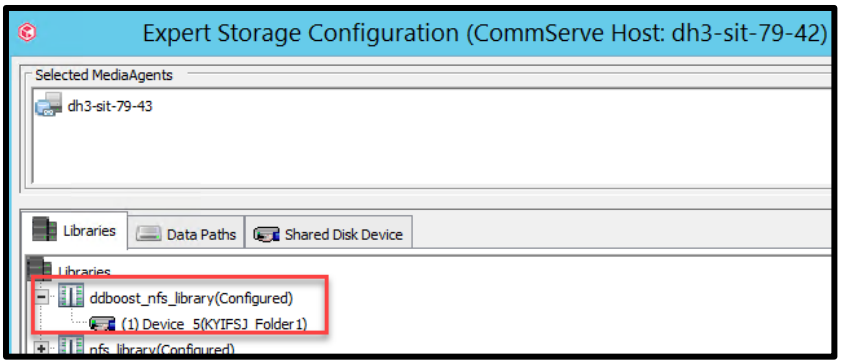
6. Add the boostfs drive for backup in Commvault server. In the CommCell command console, select **Storage** > **Expert Storage Configuration**.

7. When prompted add the Windows MediaAgents. Click **Start** > **Add** > **Choose Disk Library.**

8. The Add Disk Library dialog box appears. Type the alias for the library name, select **Automatically create storage policy for new data paths** box, and click **OK.** The Shared Mount Path (ddboostfs_library) dialog box appears.

9. Type the base folder name that you want, select **Local Path**, and click… to browse for the Linux MediaAgent. The Browse for Folder dialog box appears.

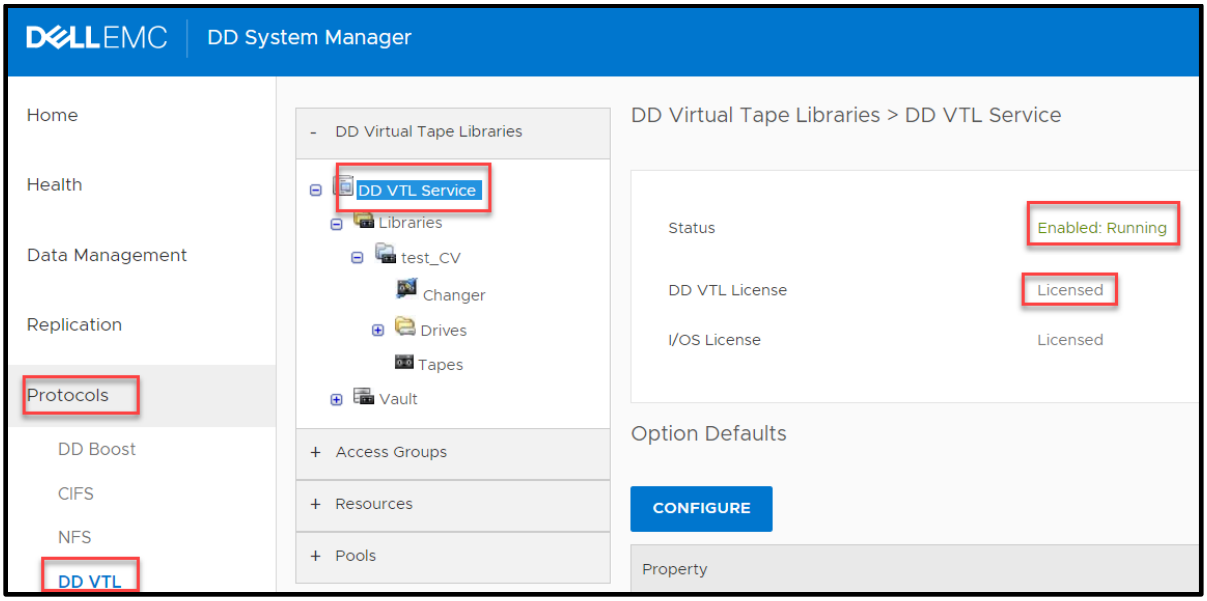




3.4 Configuring DD VTL and adding it to Commvault

DD Virtual Tape Library (VTL) is a licensed feature that must have licenses registered on both the DD series appliances and for one or more defined MediaAgent servers on the CommServe. Valid MediaAgent servers appear under **Storage Resources > MediaAgents** on the CommCell Console.

To configure a DD series appliance as a VTL target device for data protection operations, perform the procedures listed below. Check the following sections for details.



3.4.1 Configure and setup DD series appliances as VTL target

1. Establish the FC connection, install drivers, and verify the connection on the Commvault MediaAgent server.

Procedure

a) Physically connect and configure a Fibre Channel (FC) connection between the DD series appliance and the Commvault MediaAgent server.

b) Check that the correct changer driver and tape device driver are installed and loaded on the Commvault MediaAgent server.

Note: For the required changer and tape device drivers, check the DD series appliances Compatibility Guide. Also check the Commvault compatibility documentation for information about supported driver versions.

c) Log in to the command-line interface (CLI) on the DD series appliance as sysadmin and run following command:

```
# scsitarget initiator show detailed
```

d) If the Storage Area Network (SAN) connection is configured correctly, the initiator on the Commvault MediaAgent server appears with the status of Online.

```
# scsitarget initiator show detailed
```

2. Create a VTL group on the DD series appliances

You can create a VTL group at the DD OS command line or with the web interface. Check the "DD Virtual Tape Library" chapter of the *DD Series Appliance OS Administration Guide* for more information about the VTL feature, including the creation of virtual tape drives, virtual tape media, and virtual changers.

Procedure

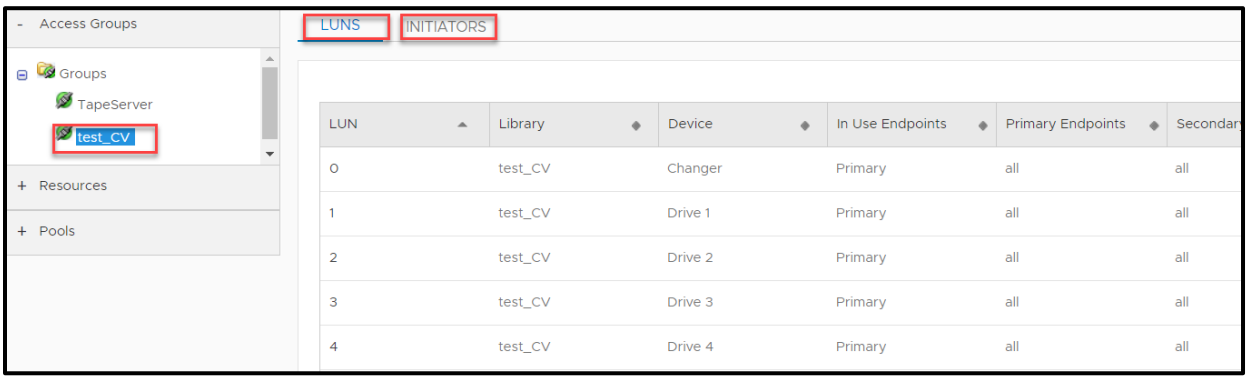
a) On the DD series appliance, create an access group.

b) Add the VTL and the initiator to the access group.

c) Confirm the VTL configuration with the command:

```
#vtl group show groupname
sysadmin@datadomain# vtl group show test_CV

Group: test_CV

Initiators:
Initiator Alias Initiator WWPN
--------------- -----------------------
initiator-1     26:00:00:22:ff:33:05:10
--------------- -----------------------

Devices:
Device Name       LUN   Primary Ports   Secondary Ports   In-use Ports
---------------   ---   -------------   ---------------   ------------
test_CV changer     0             all               all            all
test_CV drive 1     1             all               all            all
test_CV drive 2     2             all               all            all
test_CV drive 3     3             all               all            all
```

```
test_CV drive 4     4             all                all             all
---------------   ---   -------------   ---------------   ------------
```



d) Check that the marker type is set to auto:

```
sysadmin@datadomain# filesys option show
Option                              Value
------------------------------   --------
Local compression type              lz
Marker-type                         auto
app-optimized-compression           none
randomio                            enabled
anchoring-algorithm                 variable
Report-replica-as-writable          disabled
warning-space-usage                 80
critical-space-usage                90
Current global compression type     9
Staging reserve                     disabled
------------------------------   --------
sysadmin@datadomain#
```

3. Verify the Fibre Channel configuration for the VTL.

Before discovering the new VTL device within the Commvault MediaAgent server, follow the steps below to ensure that the operating system and HBA driver discover the VTL devices.

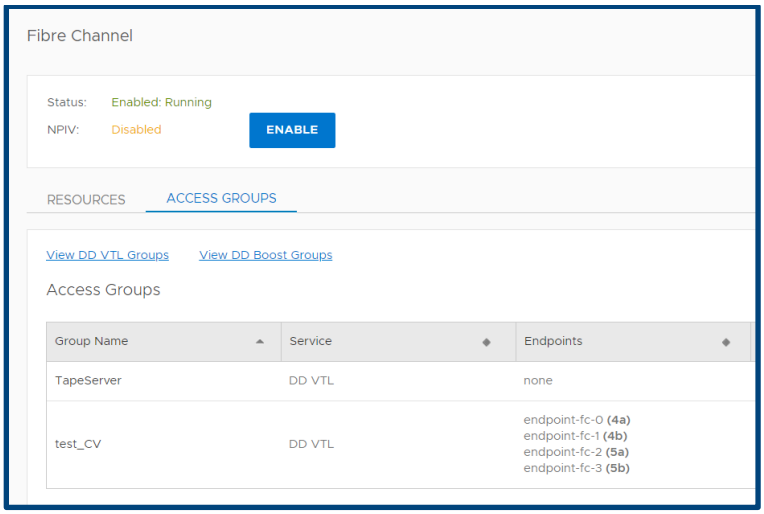
Procedure

a) On the Fibre Channel switch, check that the target DD series appliance Fibre Channel port and the initiator (Commvault MediaAgent server Fibre Channel HBA port) are both zoned properly.

b) If the zoning is correct but you still cannot see the VTL target devices, ensure that both the DD VTL HBA and the Commvault MediaAgent HBA are online in the switch name server.

c) Use the FC HBA management tool to ensure that the LUNs for both the changer and the tape drives are discovered and mapped properly.
DD series appliance recommends that you configure the HBA driver for target persistent binding.

d) At the operating system level, check that the changer and tape drives are discovered properly. For example, use Device Manager on a Windows system.

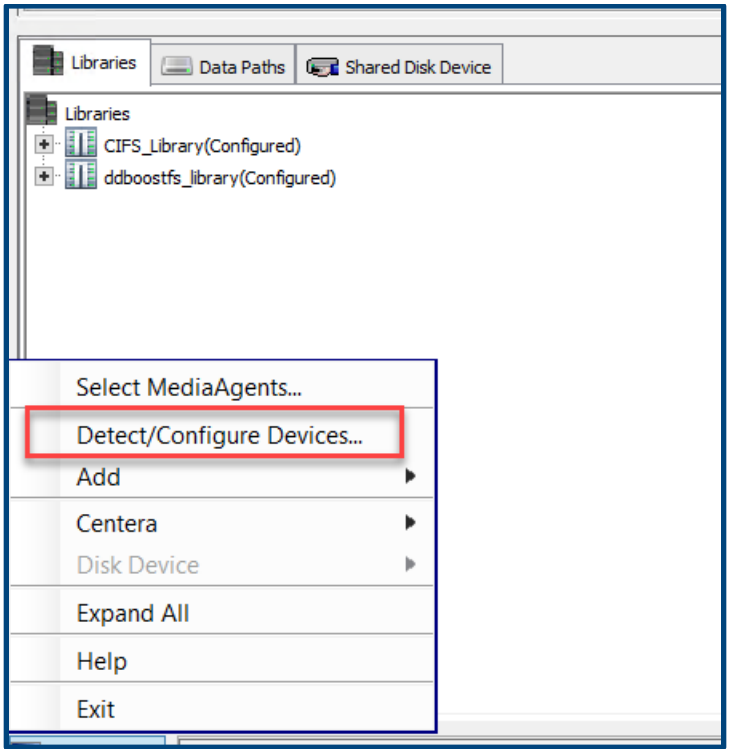


3.4.2 Configure the new VTL on the Commvault MediaAgent server.

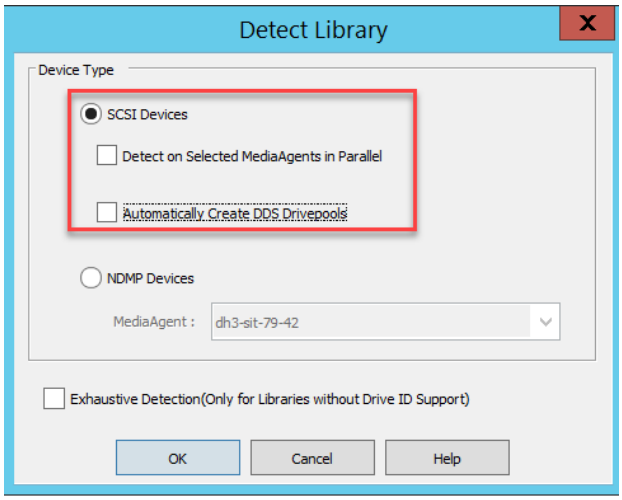
This section describes the steps to configure a new DD series appliance VTL within a Commvault MediaAgent. If you need more details, please go to Commvault Documentation.

Procedure

a) On MediaAgents, install the tape device drivers that the Commvault compatibility documentation recommends.
b) In the Commvault console, select **Storage** > **Library and Drive Configuration**.
c) From the Select MediaAgents window, select the MediaAgent that connects to the DD VTL library and click **OK**.
d) Right-click **Libraries** and select **Detect/Config Devices**. The Detect Library dialog box appears.



e) Clear **Automatically Create DDS Drive pools** and click **OK**. Auto detection should now start. All the drives that the Commvault software recognizes appear in the Log window.



f) Right-click the device and select **Configure**.
g) Select **Library and all drives** and click **OK.**
h) After you create the library, right-click the newly added library and choose **Properties.** The Library Properties dialog box appears.
Note: If you close the Library and Drive Configuration window without configuring a library, the unconfigured library disappears from the Libraries tab list. Configure all the libraries before closing the window.
i) Close the Library and Drive Configuration window. In the CommCell console browser, the new library appears under MediaAgent and Libraries. Also, a storage policy for this library appears under Storage Policies.

4 Backups

Before performing a backup, check the following items:

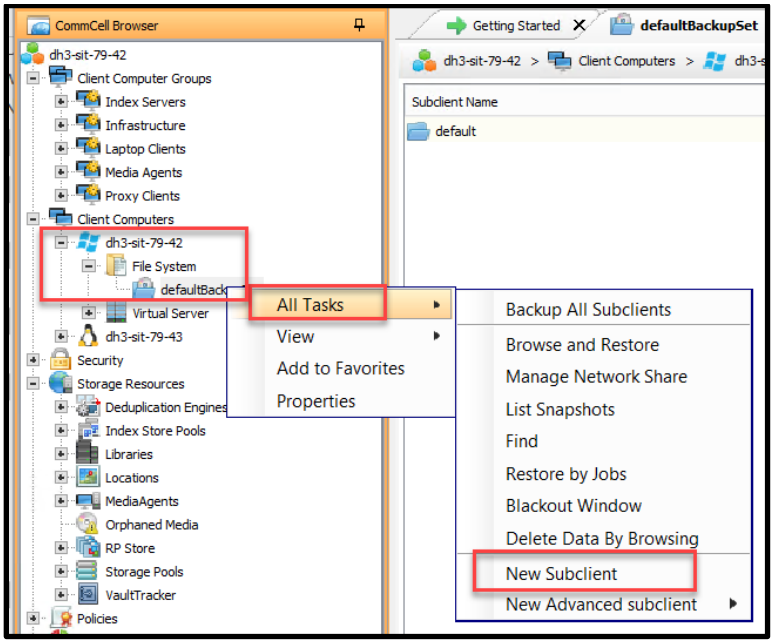
- Check that the backup source and destination are correctly defined in the subclient. The backup source is defined as content in subclient property and backup destination is defined as storage policy in the Subclient Properties dialog box.
- Enough media are available in the scratch group under the target tape library, or enough free space is available under the target disk library.
- The library and drive are in the Ready state.

4.1 Performing a Windows or Linux Server Backup

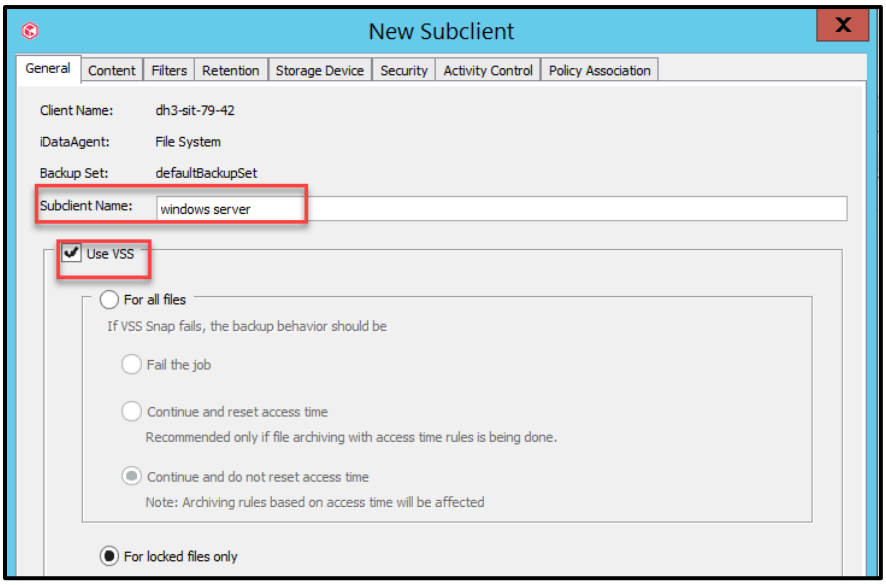
The procedures for performing backups in Windows and Linux/UNIX are similar. This example uses Windows.

Procedure

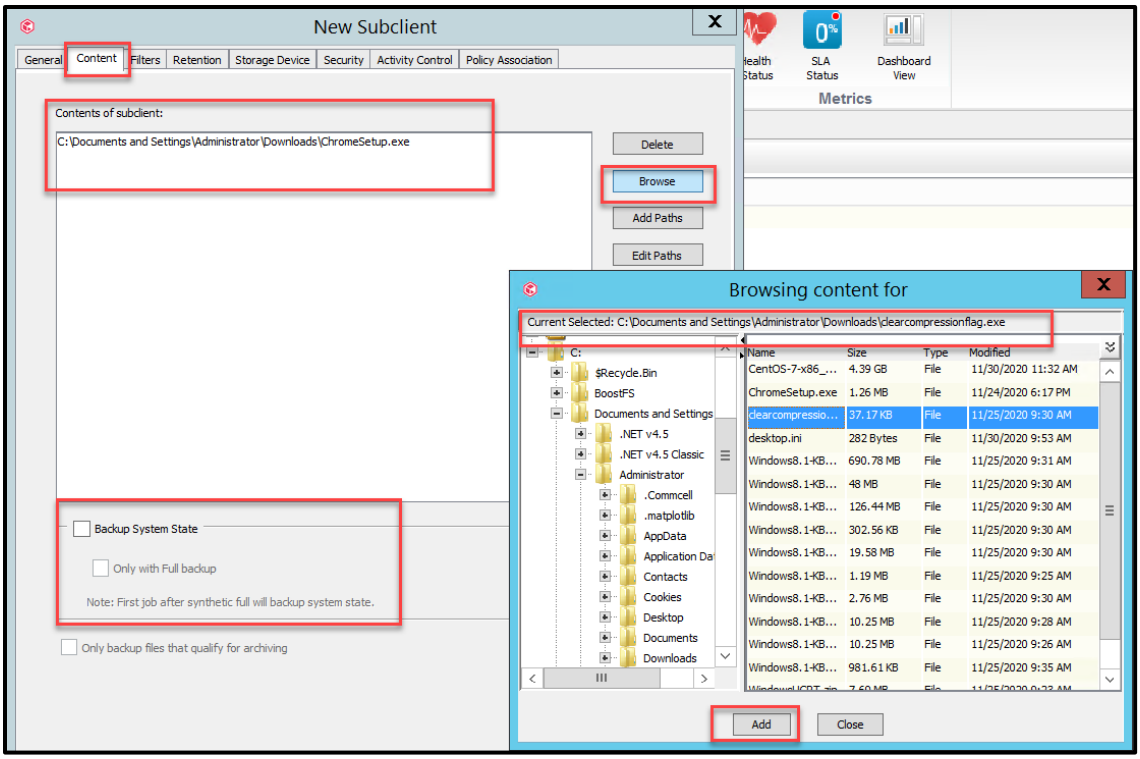
1. In the CommCell Console, expand the Windows client in the CommCell Browser, right-click **defaultBackupSet** and choose **All Tasks** > **New Subclient** to create a subclient.



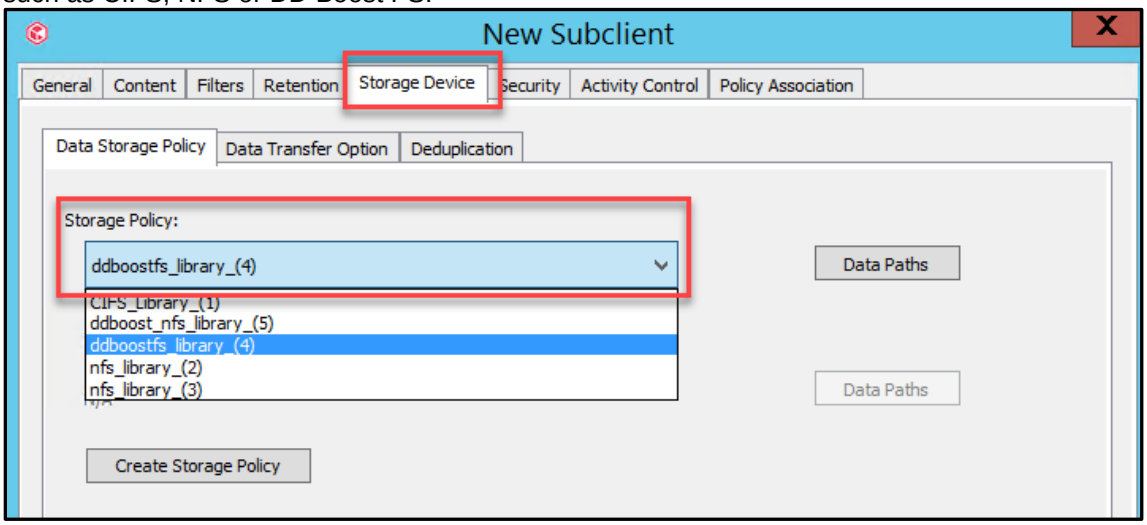
2. In the Subclient Properties dialog box General tab, enter as the **Subclient name**.



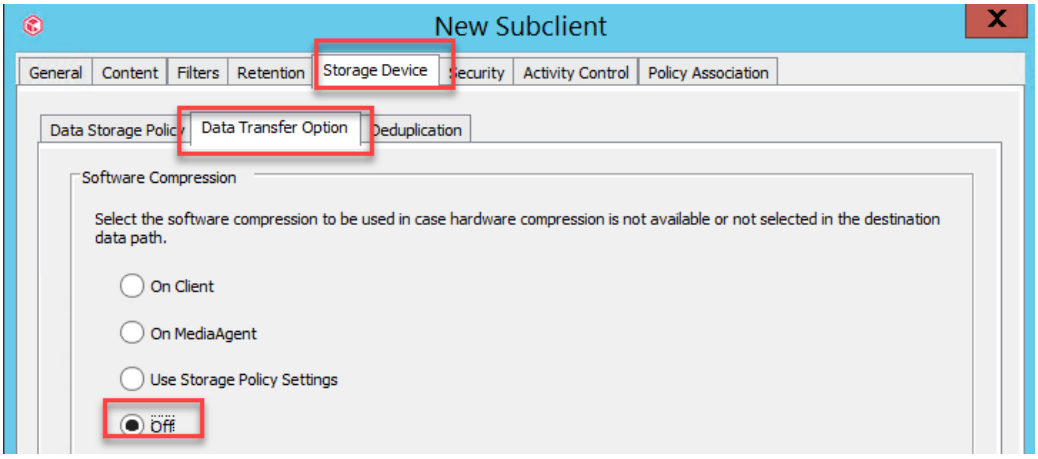
3. In the Content tab, click **Browse**, select the folders to be backed up (for example, C:\can_data\blah), and click **Add**. Repeat this step for each folder and then click **Close**



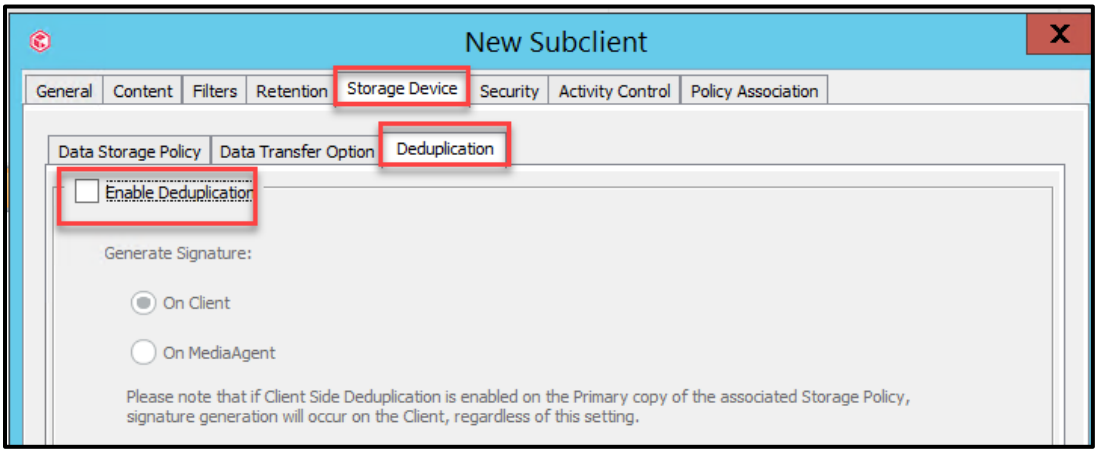
4. In the Storage Device tab, Data Storage Policy tab, choose the policy where backup data is to be written, such as CIFS, NFS or DD Boost FS.



5. In the Storage Device tab, Data Transfer Option tab, set **Software Compression** to **Off.**

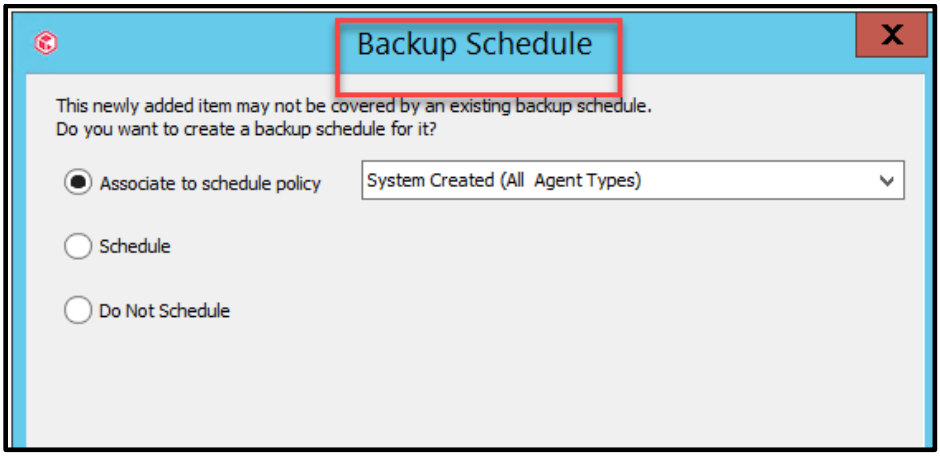


6. In the Storage Device tab, Deduplication tab, clear Enable Deduplication**.**

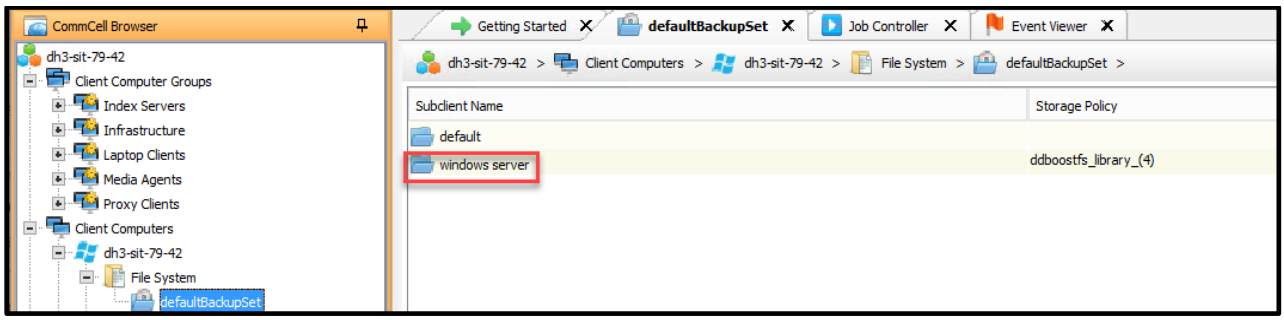


7. Click **OK** to close the Subclient Properties window. The Backup Schedule dialog box opens.

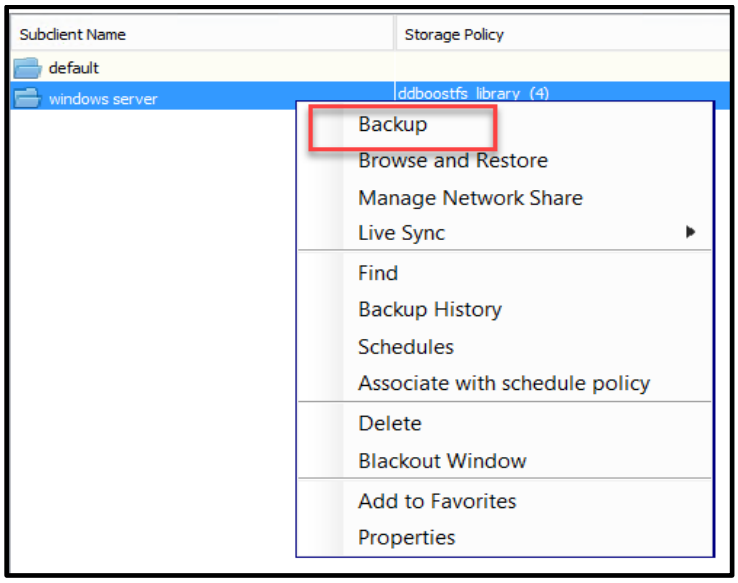
8. Choose a schedule option and click **OK**.
   - To use an existing backup schedule for this subclient, select **Associate to schedule policy** and choose a policy from the list.
   - To create a schedule, select **Schedule.**
   - If you do not want to schedule this backup, select **Do Not Schedule**.



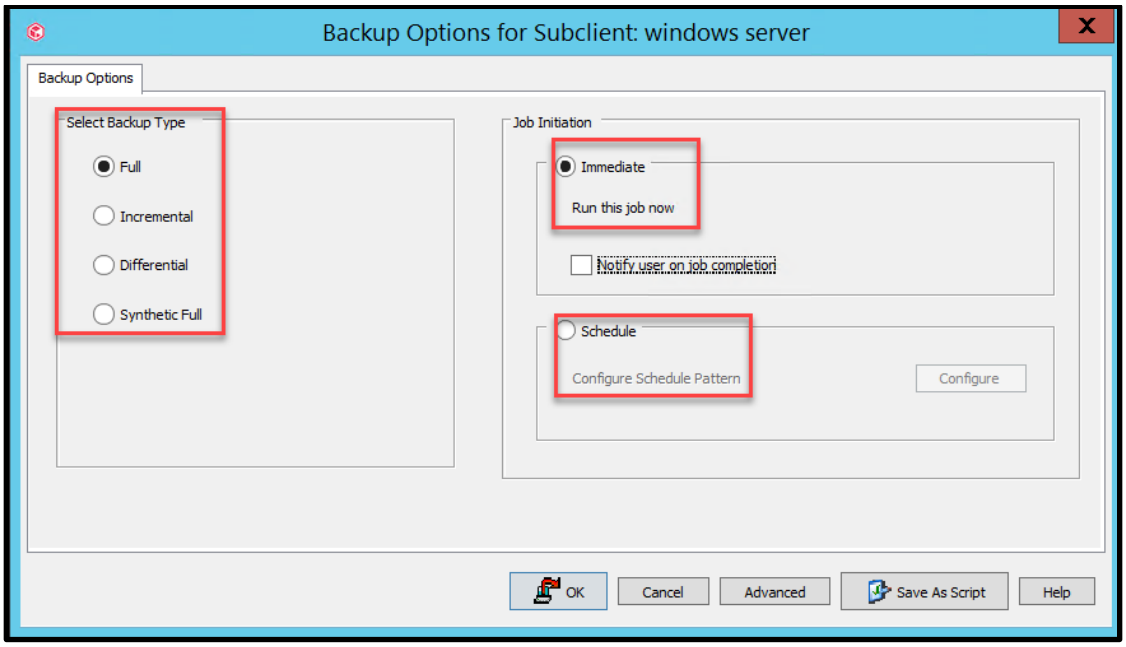
9. The windows subclient appears in the defaultBackupSet tab of the CommCell Browser.



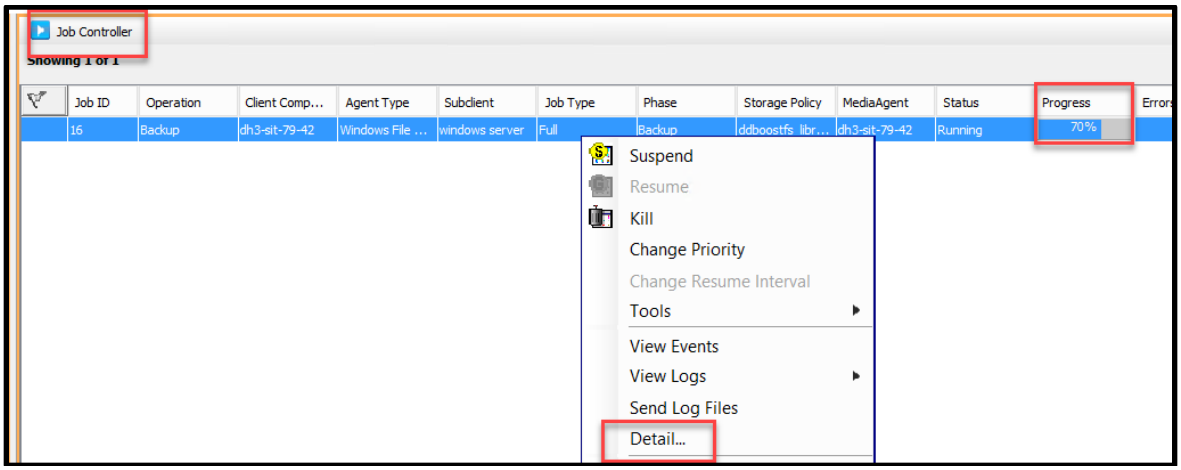
10. To run a backup, right-click a subclient name and choose **Backup.**



11. The Backup Options for Subclient window appears. Choose options under Select Backup Type and Job Initiation and click **OK.**



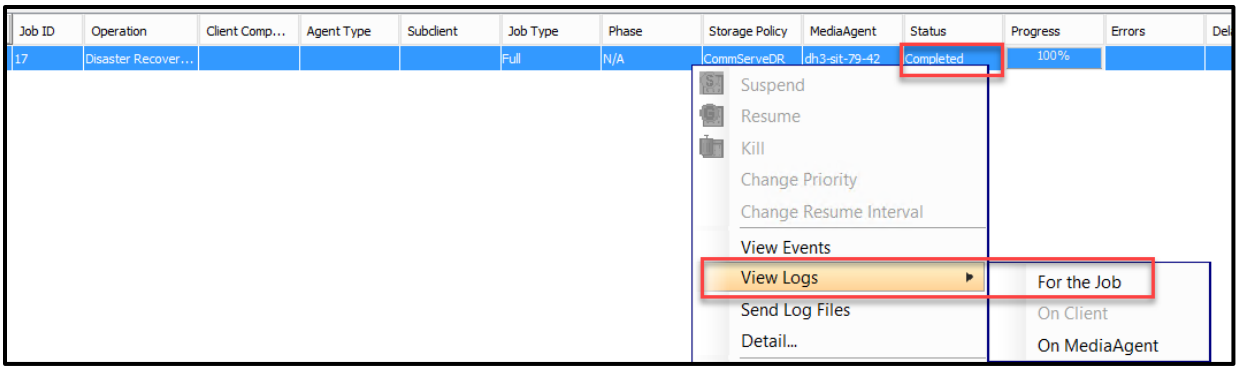
12. The backup job starts as seen in the Job Controller. Job progress can be seen in the Job Controller window and job events can be monitored in the Event Viewer window. To see detailed job status, right-click the job entry and choose **Detail.**



Results

If the job finishes successfully, the status will change to Completed. For other status results, look at the Errors field and logs in the Event Viewer window. To view the detailed job log, right-click the job entry and choose **View Logs**.

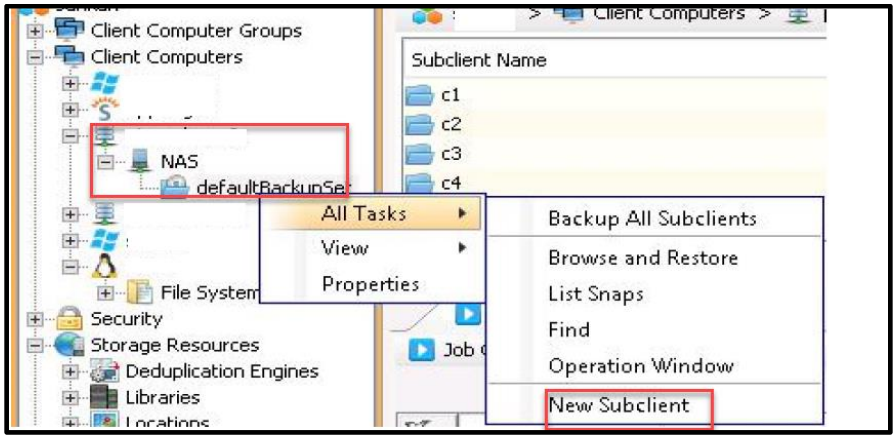
To know more details about each option for backup Check Commvault documentations.



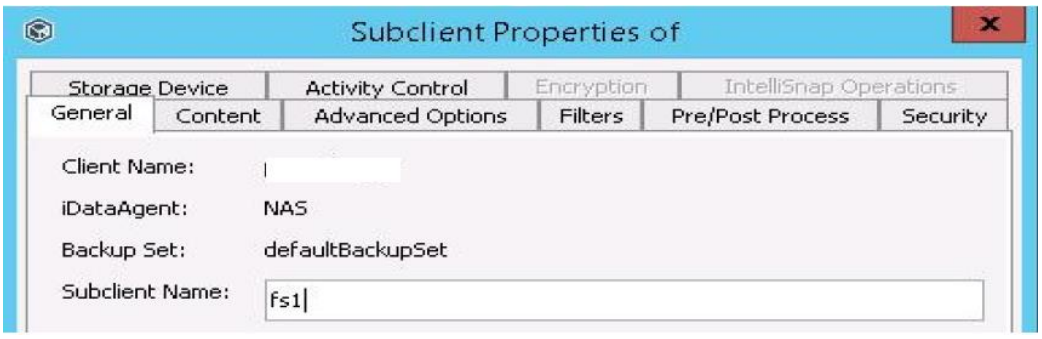
4.2 Performing NAS Client Backup

Procedure

1. In the CommCell Console, expand the NAS client in CommCell Browser, right-click **defaultBackupSet**, and choose **All Tasks > New Subclient** to create a subclient.



2. In the General tab of the Subclient Properties window, enter **`name`** as the **Subclient name**.



3. In the Content tab, under Backup Content Path, select the file system, enter the path of the folder to be backed up in that file system (/fs1/dir in the example), and click **Add**. Repeat this step for each folder.

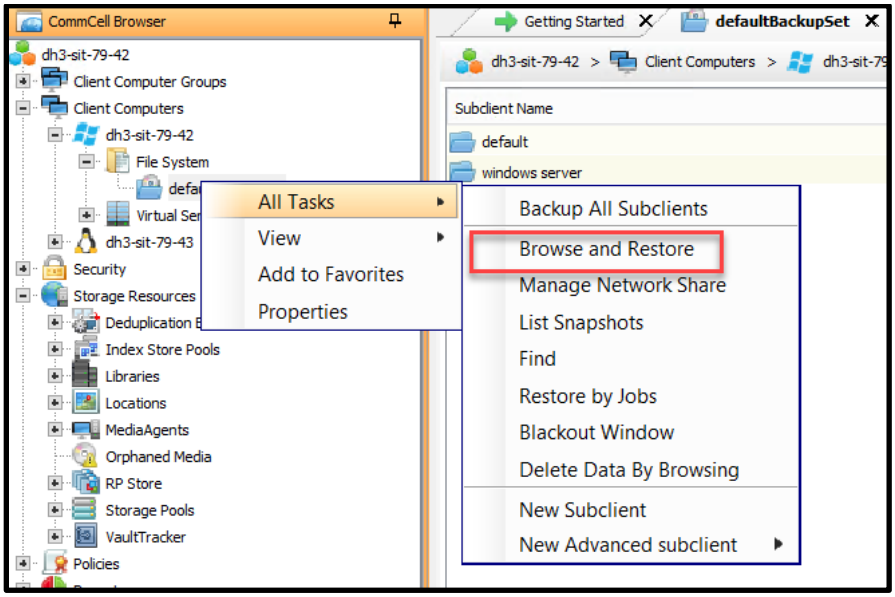
4. Check Performing a Windows or Linux Backup and continue from step 4.To know more options with NAS backup check Commvault documentation on NAS client.

5 Restores

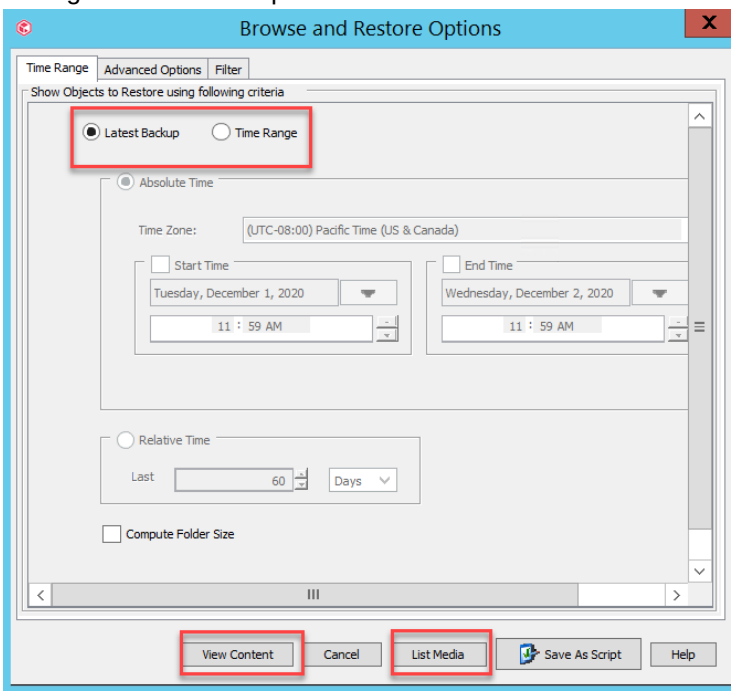
The procedures for performing restores with Windows, Linux/UNIX, and NAS clients are similar. This example uses Windows.

Procedure

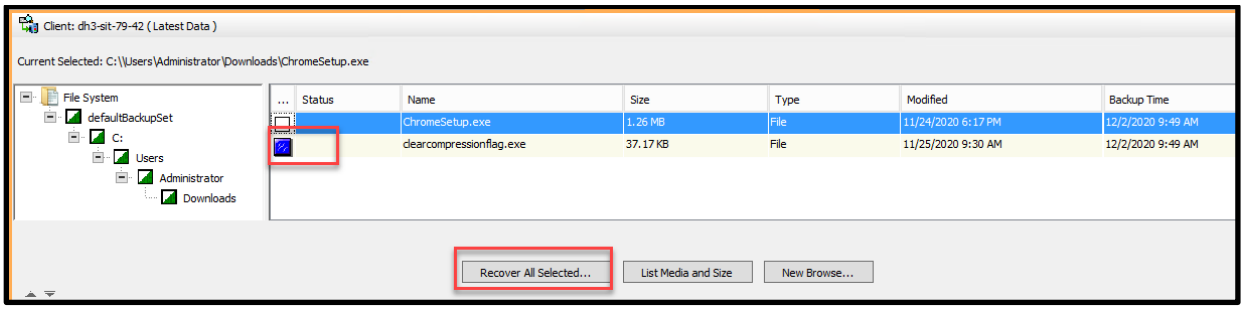
1. In the CommCell Console, expand the Windows client in the CommCell Browser, right-click **defaultBackupSet** and choose **All Tasks** > **Browse and Restore**.



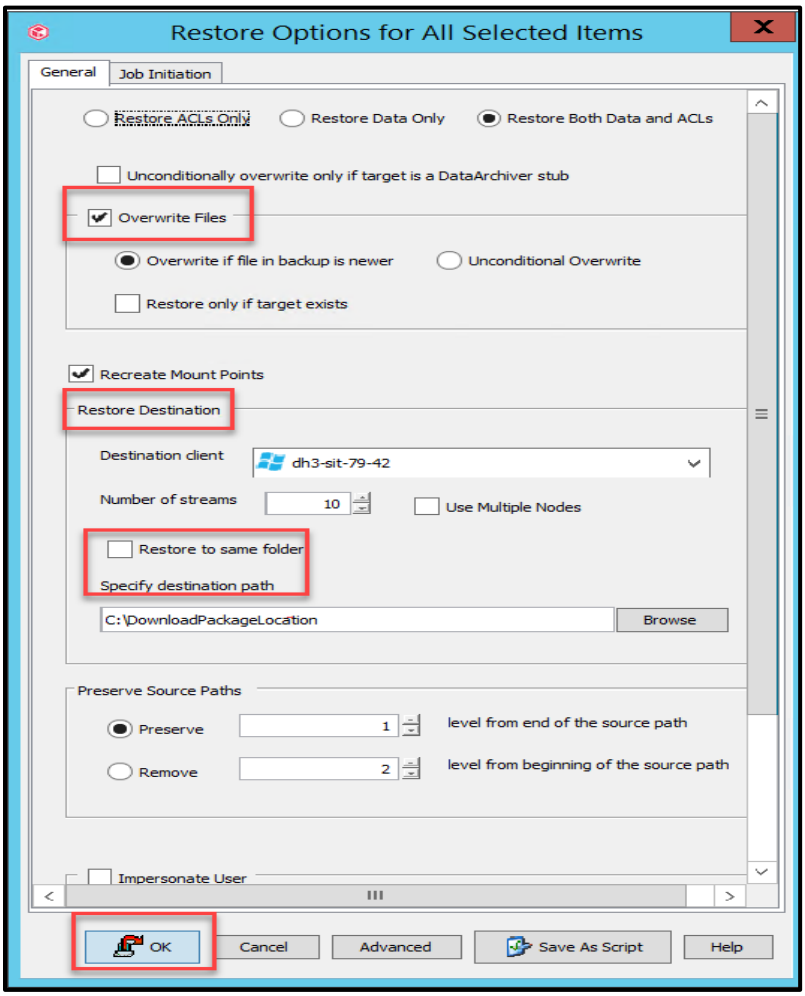
2. The Browse Options dialog box appears. You can view the latest data (consolidation of all backups) by choosing **Browse the Latest Data**, or you can browse backup data up to a time by choosing **Specify Browse Time**. You can also exclude backup data from before a specified time by clicking **Advanced** and setting the advanced options.



3. Click **View Content**.
   The backup data browser window opens for this client. This example shows the latest backup data for this client.



4. Explore the data, choose folders and files to be restored, and click **Recover All Selected**. The Restore Options for All Selected Items dialog box appears.
   Choose the required options. You can restore data to a different client by choosing a **Destination client**. You can restore data to a new location by clearing **Restore to same folder** and specifying a destination path. Click **OK** when you finish choosing restore options.



5. The restore job starts. Monitor the job in the Job Controller and Event Viewer windows. When the restore job finishes, the restored data will become available in the destination folder.

6 PowerProtect DD Replication and Restore from Replication

DD Replicator provides automated, policy-based, network-efficient, and encrypted replication for DR (disaster recovery) and multisite 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.

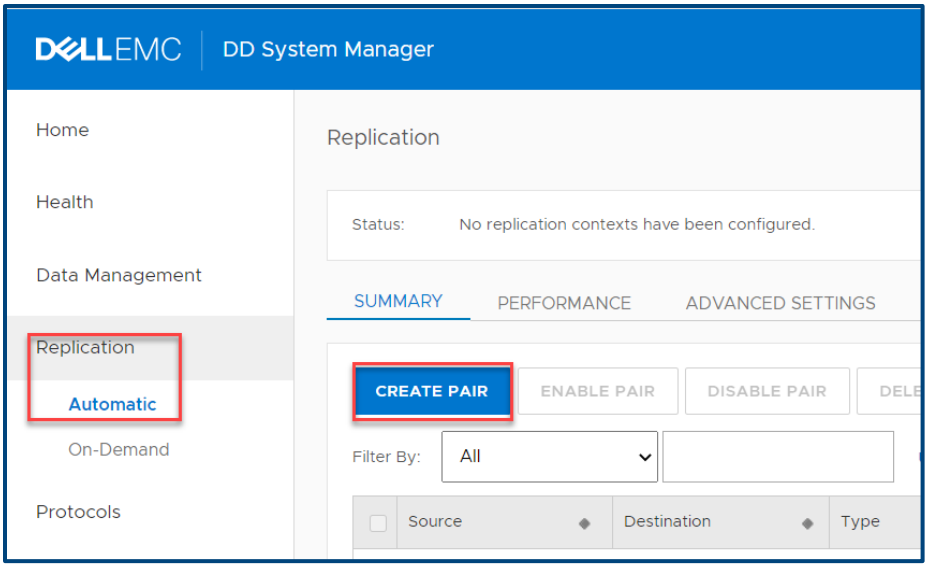
With cross-site deduplication, any redundant segment previously transferred by any other site, or as a result of a local backup or archive, will not be replicated again. This improves network efficiency across all sites and reduces daily network bandwidth requirements, making network-based replication 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.

Before getting started with DD Replicator, note the following general requirements:

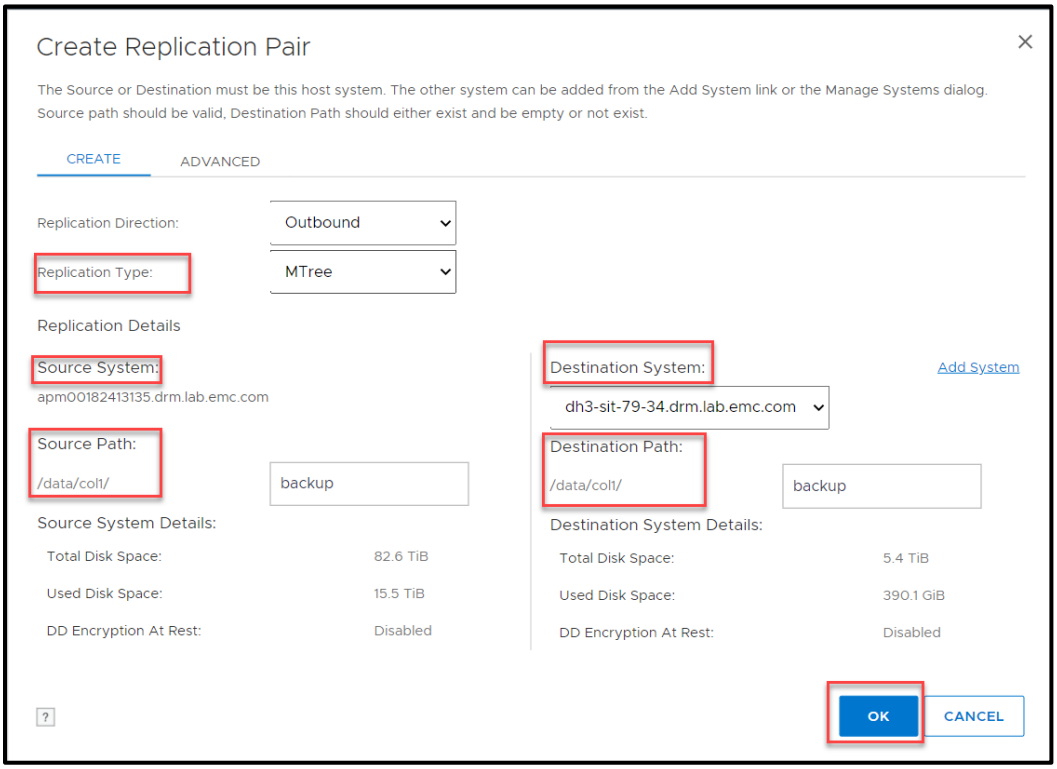
- DD Replicator is a licensed product. Check with your Dell EMC sales representative to purchase licenses.
- You can usually replicate between machines that are within five releases of each other, for example, from 6.0 to 7.2. However, there may be exceptions to this, so review the tables in the *Replication 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*.

Procedure:

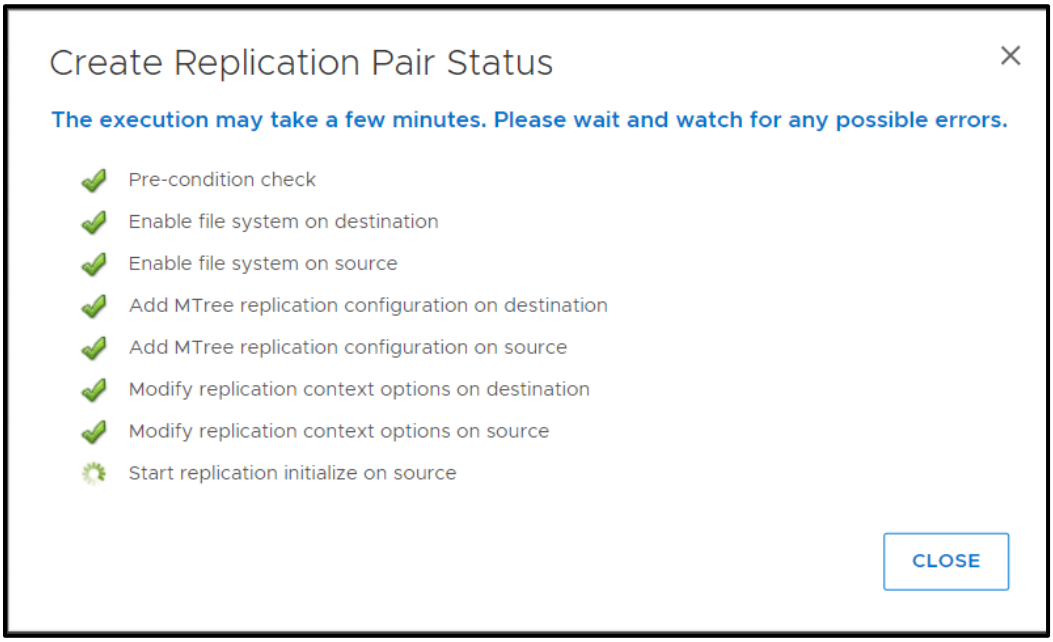
1. Log in to DD System Manager as sysadmin or any administrator user.
2. Go to **Replication →Automatic → Select Create Pair.**



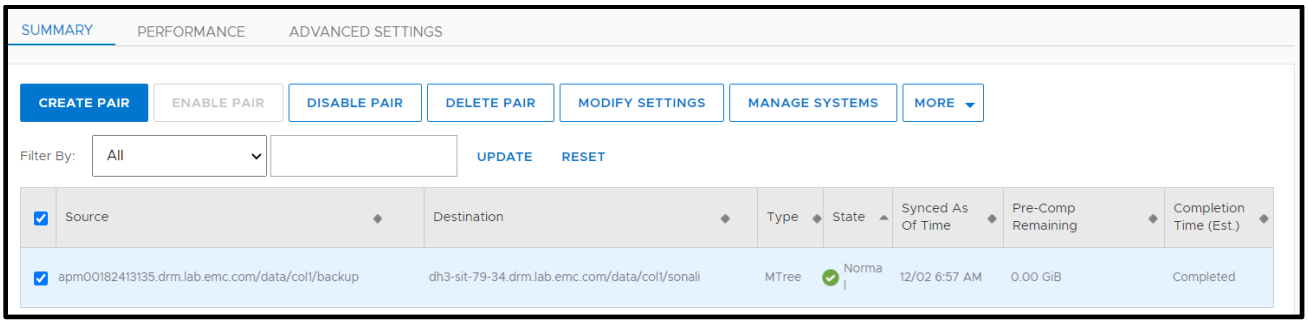
3. The Create Replication Pair window will open. Enter the Replication Direction, Replication Type, Enter Replication Source Path -> Enter the CIFS, NFS, DD Boost storage unit and set the Destination PowerProtect DD details along with path then do OK.



4. When you complete the destination information, it will be saved and click OK and validation/pre-checks will run.



5. You can now see the replication pair in Summary Tab.



Note: To know more about compatibility, options, limitations, and method of replication please check PowerProtect DD OS Administration guide

If there are issues with source backup copy, restore from replication copy of backup can be done using following process. Before use of following process ensure that replication is fully synchronized.

6.1 CIFS restore

- In server go to Expert Storage configuration wizard.

- Choose media agent, under 'Shared Disk Device' tab right click path, choose 'Properties', and replace source DD Series appliance share path with destination DD series appliance share path. Also check 'Read only'.

-Now any restore will restore data from replication copy.

6.2 NFS restore

- On Unix/Linux media agent, unmount source DD series appliance MTree and mount replication DD series appliance MTree as read-only at same mount point.

-Now any restore will restore data from replication copy.

6.3 DD BoostFS restore

-In server go to Expert Storage configuration wizard.

- Choose media agent, under 'Shared Disk Device' tab right click path, choose 'Properties', and replace source DD series appliance share path with destination DD series appliance share path. Also check 'Read only'.

-Now any restore will restore data from replication copy.

Note:

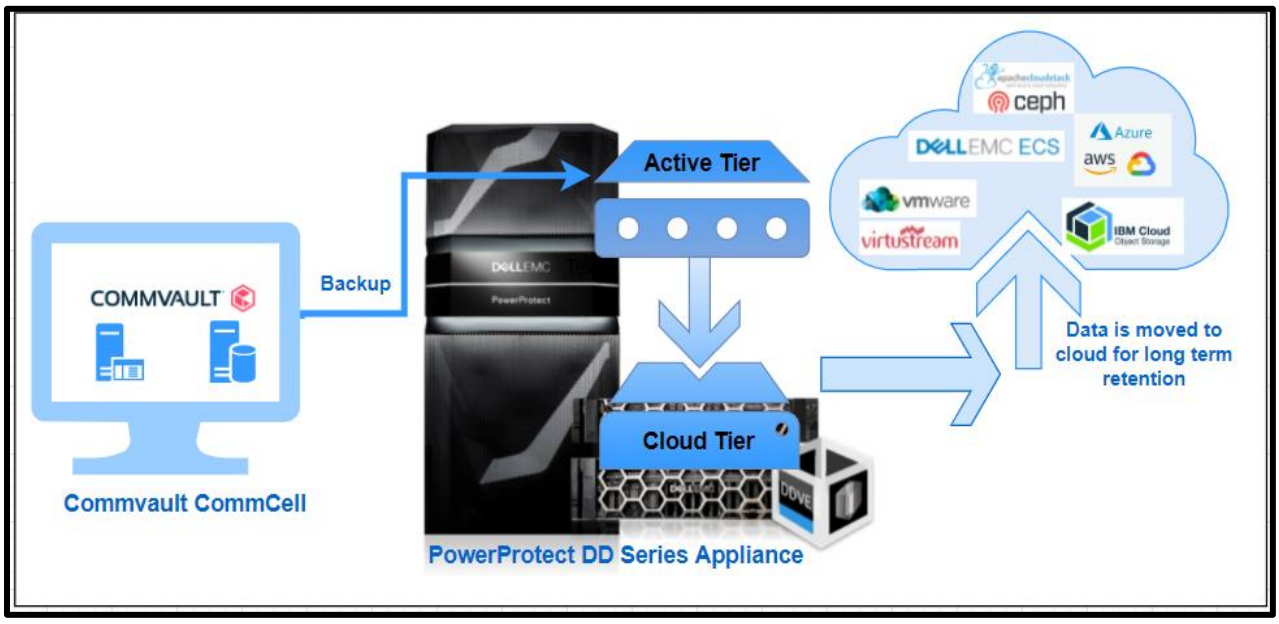
- There is no need to break replication pair and make target MTree read/write. Read only is fine for restore.
- At this instance backup cannot be run as device is read-only.
- Replicating DD VTL tape cartridges (or pools) means replicating MTrees or directories that contain DD VTL tape cartridges. Media pools are replicated by MTree replication, as a default.

- DD Boost users should have the same user ID (UID) and primary group ID (GID) on both the source and destination systems

7 Dell EMC Cloud Tier

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 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.



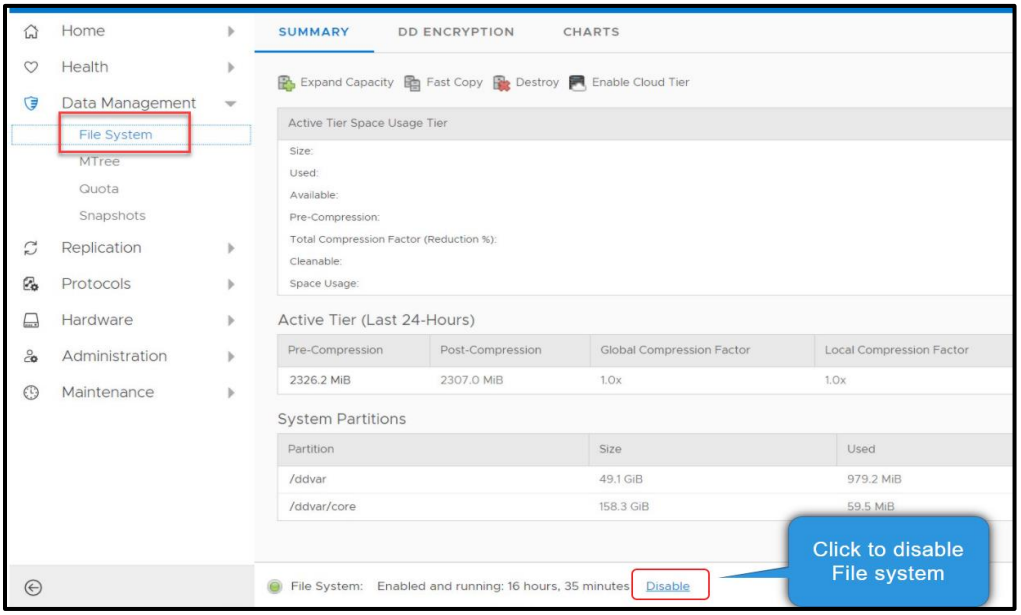
Note:

- 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, check the applicable DD OS Release Notes for the most up-to-date information about product features, software updates, software compatibility guides, and information about protection products, licensing, and service.
- To know about Cloud Tier Requirements, check DD OS Administration Guide.

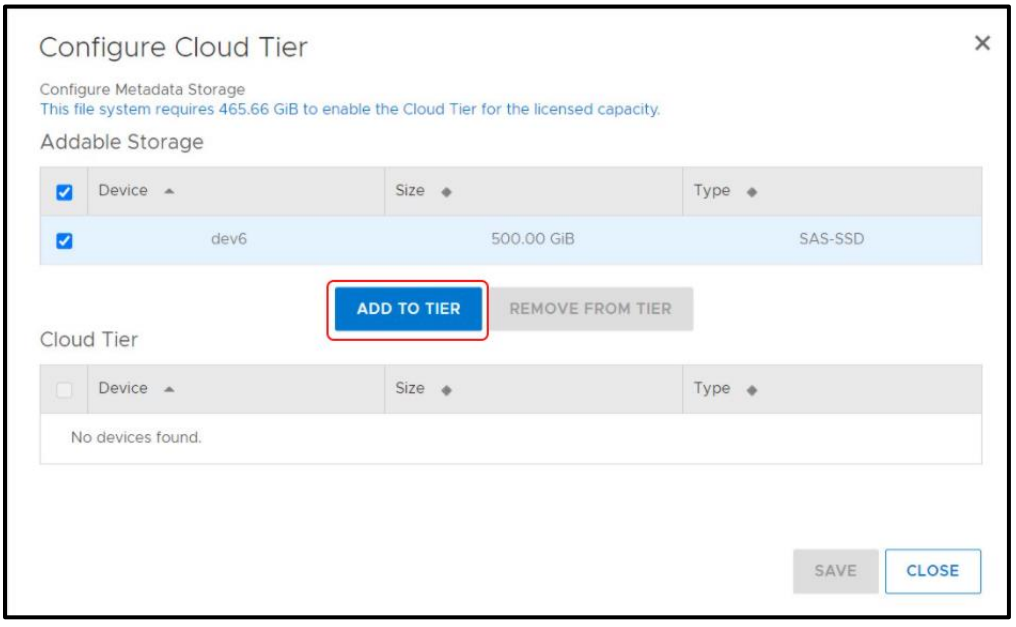
7.1 Enable Cloud Tier on DD series appliances

Procedure:

1. Select **Data Management** > **File System** and click **Disable** (at the bottom of the screen) to disable the file system.

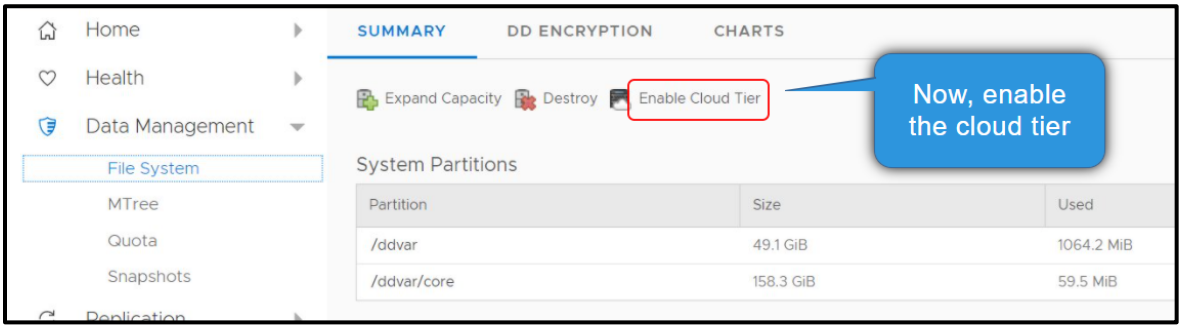


2. Select **Hardware** > **Storage**. In the Overview tab, expand **Cloud Tier**. Click **Configure**.
The Configure Cloud Tier dialog box is displayed. Select the checkbox for the shelf to be added from the Addable Storage section.

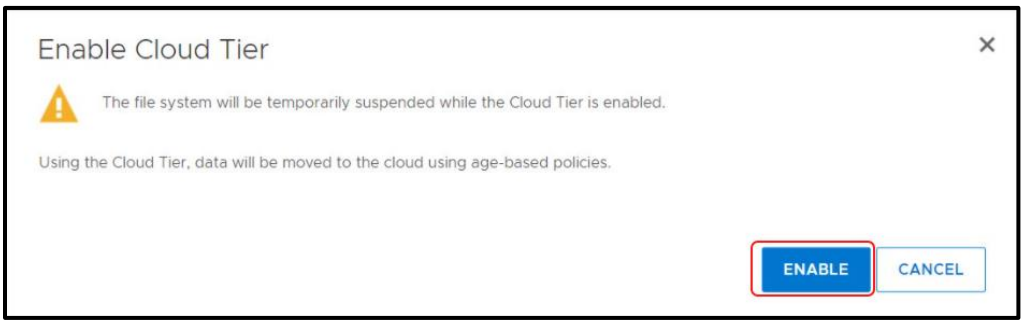


3. Click the **Add to Tier** button. Click **Save** to add the storage.
4. Select **Data Management > File System** and click **Enable Cloud Tier**.
To enable the cloud tier, you must meet the storage requirement for the licensed capacity. Configure the cloud tier of the file system. Click **Next**.

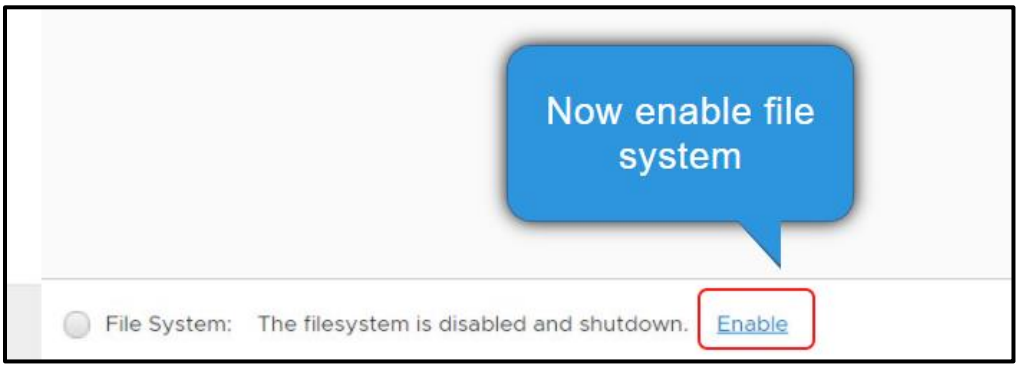
A cloud file system requires a local store for a local copy of the cloud metadata.



5. Click **Enable**.
   The cloud tier is enabled with the designated storage.



6. Select **Enable file system**.



7. Check Cloud Units Tab is available under File System.

8. Configuring the network, including firewall and proxy settings.

- 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.
- 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.

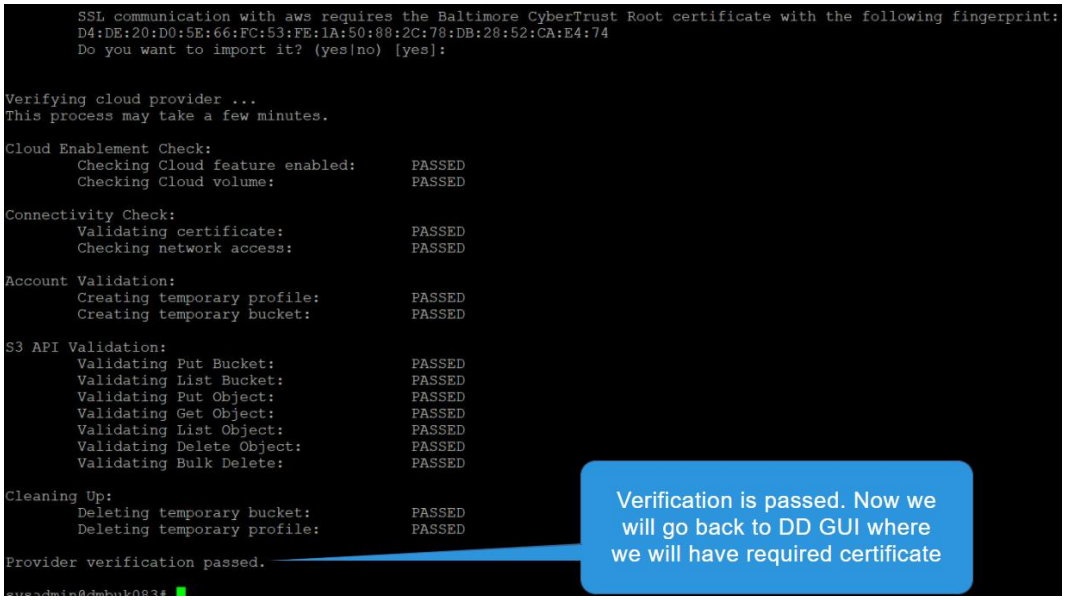
9. Import CA certificates:
   Before you can add cloud units for Alibaba, Amazon Web Services S3 (AWS), Azure, Elastic Cloud Storage (ECS), and Google Cloud Provider (GCP), you must import CA certificates.

   Steps

   i. Select **Data Management** > **File System** > **Cloud Units**.
   ii. In the tool bar, click **Manage Certificates**.
   iii. The Manage Certificates for Cloud dialog is displayed.
   iv. Click **Add**.
   v. Select one of these options:
   I want to upload the certificate as a .pem file.
   vi. Browse to and select the certificate file.
   I want to copy and paste the certificate text.
   vii. Copy the contents of the .pem file to your copy buffer. Paste the buffer into the dialog.
   viii. Click **Add**.

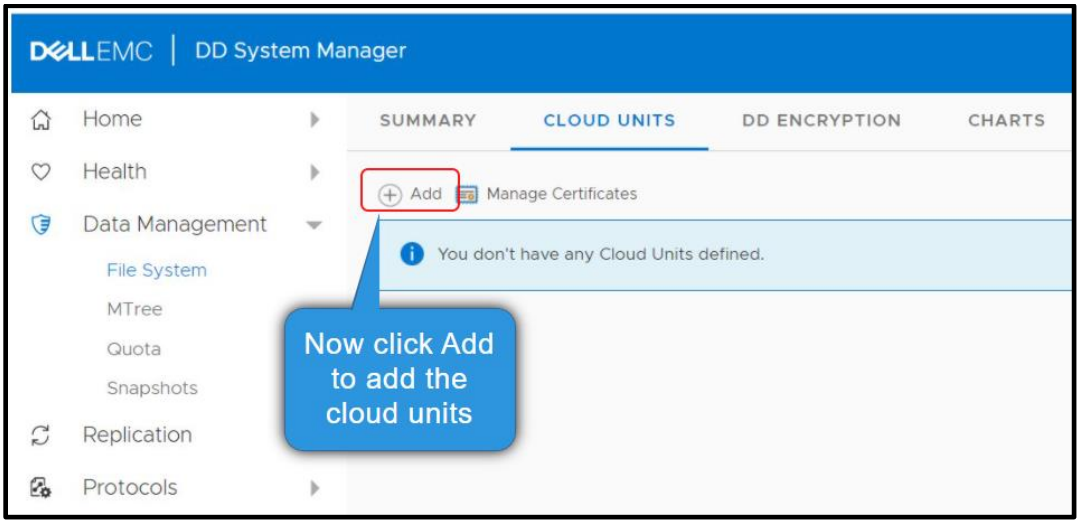
Using CLI run command `cloud provider verify`, enter the provider name and enter the secret key. Enter the region and yes to continue. Ensure to get a verified message.

```
sysadmin@dmbuk083# sysadmin@dmbuk083#
sysadmin@dmbuk083# 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]: yes

        Enter provider name (alibabacloud|aws|azure|ecs|google|s3_flexible): aws
        Enter the access key:
        Enter the secret key:
        Enter the storage class (STANDARD|STANDARD_IA|ONEZONE_IA) [STANDARD]: STANDARD
        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|eu-west-2|us-gov-east-1|
                        us-gov-west-1): ap-southeast-2
        Do you want to enter proxy details? (yes|no) [no]:

        SSL communication with aws requires the Baltimore CyberTrust Root certificate with the following fingerprint:
        D4:DE:20:D0:5E:66:FC:53:FE:1A:50:88:2C:78:DB:28:52:CA:E4:74
        Do you want to import it? (yes|no) [yes]:
```



10. Add a Cloud Unit for any storage provider.

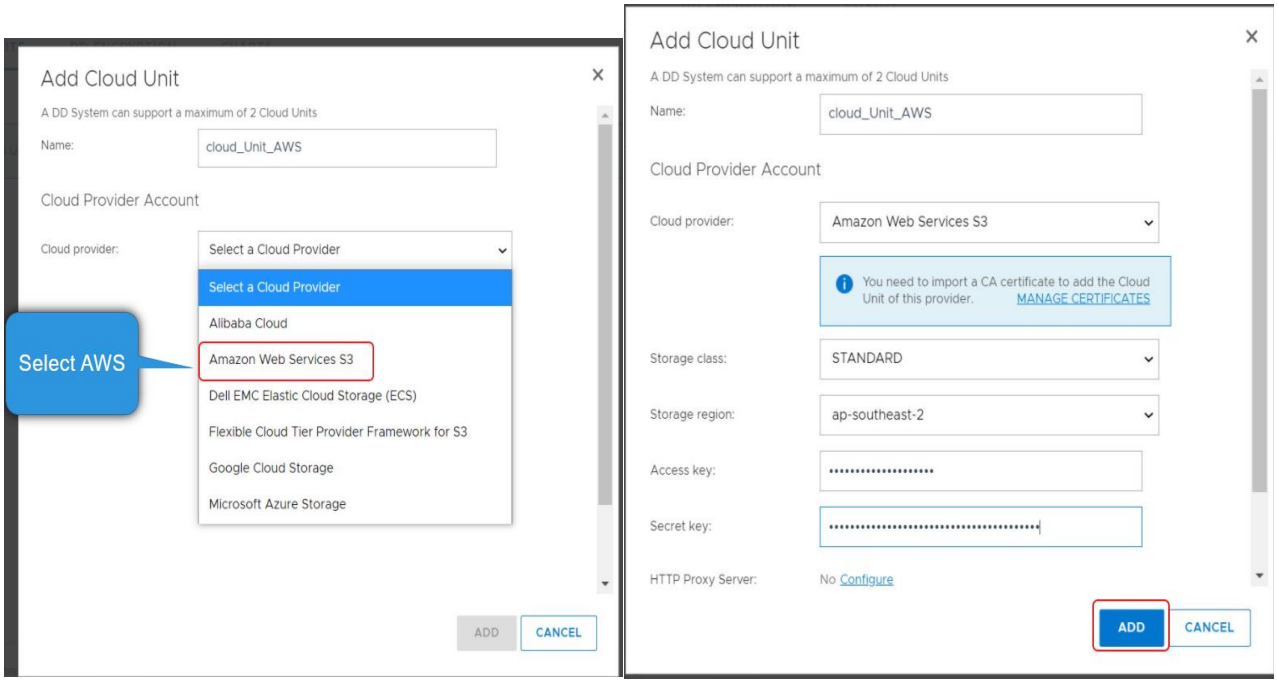
Select **Data Management > File System > Cloud Units**



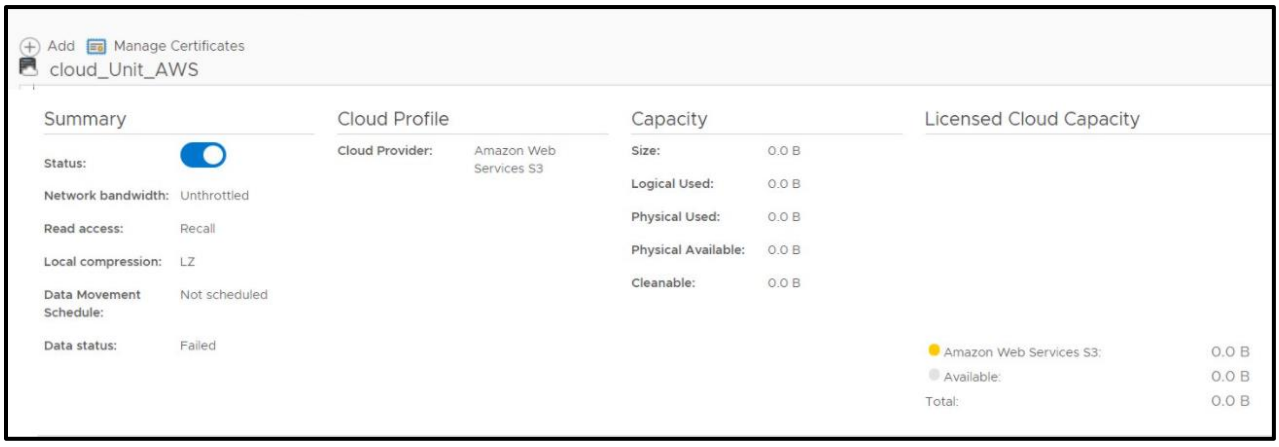
Click **Add**.

The Add Cloud Unit dialog is displayed.

Enter a name for this cloud unit. Only alphanumeric characters are allowed. For **Cloud provider**, select provider from the drop-down list. Enter all details and add the provider.



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.



The Commvault integration with the Cloud Tier provides a Data Protection Administrator with the ability to perform the following functions:

- Ability to move data from the Active Tier device to the Cloud Tier device.
- Recover data to a client from the cloud, including FLR/GLR recoveries.

Commvault supports multiple cloud services. Check Cloud Tier with Commvault compatibility guide for the same.

Configuring Commvault for Cloud Tier devices

Commvault allows users to move their backup datasets to the active tier location (that is MTree) and from there, files are moved to cloud using DD series “data-movement” commands.

7.2 Cloud Configuration on DD series appliances

Note: Commvault is supported with multiple cloud vendors, and the example below is for ECS using DD command line.

a. Create an ECS Cloud Profile. Here “Cloud_ECS” is the profile name.

```
sysadmin@datadomain# cloud profile add Cloud_ECS.

Enter provider name (aws|azure|virtustream|ecs|s3_flexible): ecs

Enter the access key:

Enter the secret key:

Enter the endpoint: http://new-test_VM.emc.local:9020

Do you want to enter proxy details? (yes |no) [no]: no

Cloud profile 'Cloud_ECS' added successfully

sysadmin@datadomain#
```

b. Create a Cloud Unit. Here “`test-ECS`” is the cloud unit name.

```
sysadmin@ datadomain # cloud unit list

Name      Profile   Status

---------  -------  ------

test_ECS   ECS      Active

---------  -------   ------

sysadmin@ datadomain #
```

c. Once the backup is done on DD series appliance, run file report.

```
# filesys report generate file-location path <MTree path>.
```

Ensure that backup dataset is moved to DD series appliance Active tier.

7.3 Moving files from Active Tier to Cloud Tier

Procedure:

a. To check any data-movement policy is set on DD series appliance by running below command.

```
# data-movement policy show
```

b. Set data-movement policy age-threshold to number of days as per requirement to specific MTree we are setting 14 days.

```
sysadmin@datadomain# data-movement policy set age-threshold 14 to-tier cloud
cloud-unit Cloud_ECS mtrees /data/col1/backup

The data-movement age-threshold policy is set to "14" days for the following
MTree(s):

/data/col1/backup
sysadmin@datadomain#
```

c. Verify age-threshold is set successfully.

```
sysadmin@datadomain# data-movement policy show

 MTree          Target (Tier/Unit Name) Policy        Value

--------------- ---------------------- ------------- ------

/data/col1/backup   Cloud/test_ECS      age-threshold 14 days

--------------- ----------------------  ------------  ------

sysadmin@datadomain#
```

d. Run data movement command in order to move from Active Tier to cloud Tier.

```
# data-movement start mtrees <mtree path>

sysadmin@ datadomain # data-movement start mtrees /data/col1/backup
Data-movement started.
Run "data-movement watch" to monitor progress.
sysadmin@datadomain #
```

e. Run “data-movement watch” command to watch the status of data-movement.

```
sysadmin@datadomain# data-movement watch
Data-movement:
98% complete; time: 0:03:03
Moved (post-comp): 300.50 MB, (pre-comp): 2.00 GB,
Files inspected: 10, Files eligible: 10, Files moved: 10, Files failed: 0
Data-movement was started on Dec 12 2020 06:02 and completed on Dec 12 2020
06:05
Moved (post-comp): 300.50 MB, (pre-comp): 2.00 GB,
Files inspected: 10, Files eligible: 10, Files moved: 10, Files failed: 0
sysadmin@datadomain#
```

f. Now, again run file report and ensure file is now available on cloud. The location of file is now “ecs-unit1” instead of “active”

```
# filesys report generate file-location path <mtree path>
```

g. Now, to restore back files from cloud (ECS) to active tier (DD series appliances), file should be recalled and run file report to ensure location is set to “active”

```
# data-movement recall path <file location>

sysadmin@ datadomain # data-movement recall path
/data/col1/backup/Folder3/comV_MAGNETIC/V_42/CHUNK_200
```

```
Recall initiated for
"/data/col1/backup/Folder3/comV_MAGNETIC/V_42/CHUNK_200". Run the status
command to monitor its progress.
sysadmin@ datadomain #
```

h. Check “data-movement” status.

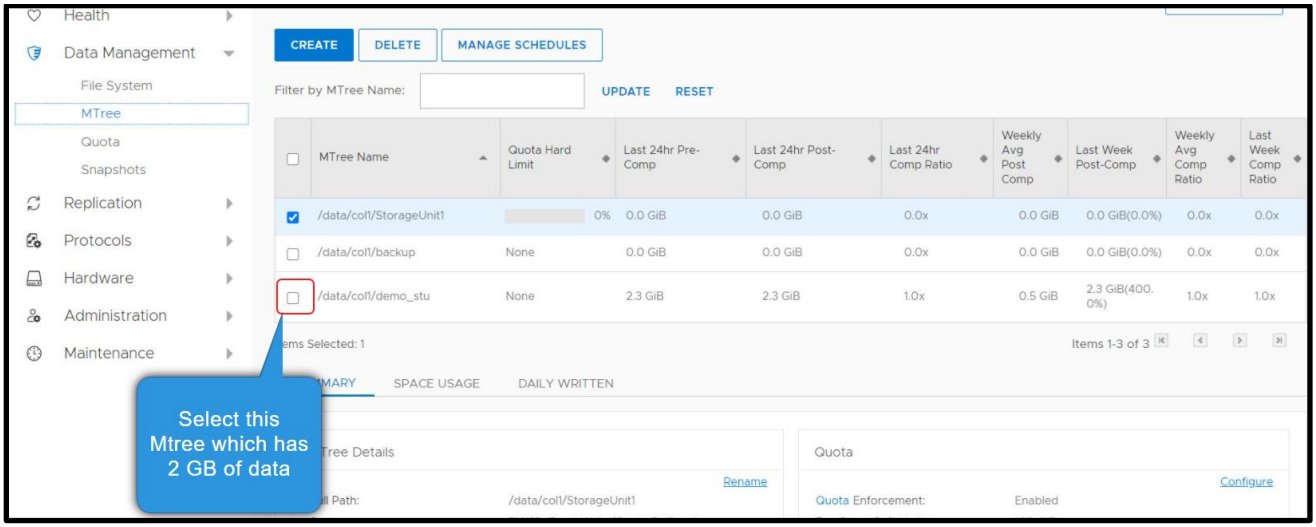
```
# data-movement status

sysadmin@dd7200-26# data-movement status
Data-movement to cloud tier:
----------------------------
Data-movement was started on Dec 12 2020 06:02 and completed on Dec 12 2020
06:05
Moved (post-comp): 300.50 MB, (pre-comp): 2.00 GB,
Files inspected: 10, Files eligible: 10, Files moved: 10, Files failed: 0
Data-movement recall:
---------------------
No recall operations found.
sysadmin@datadomain#
```

i. Generate report for file location and verify that all movements are completed.

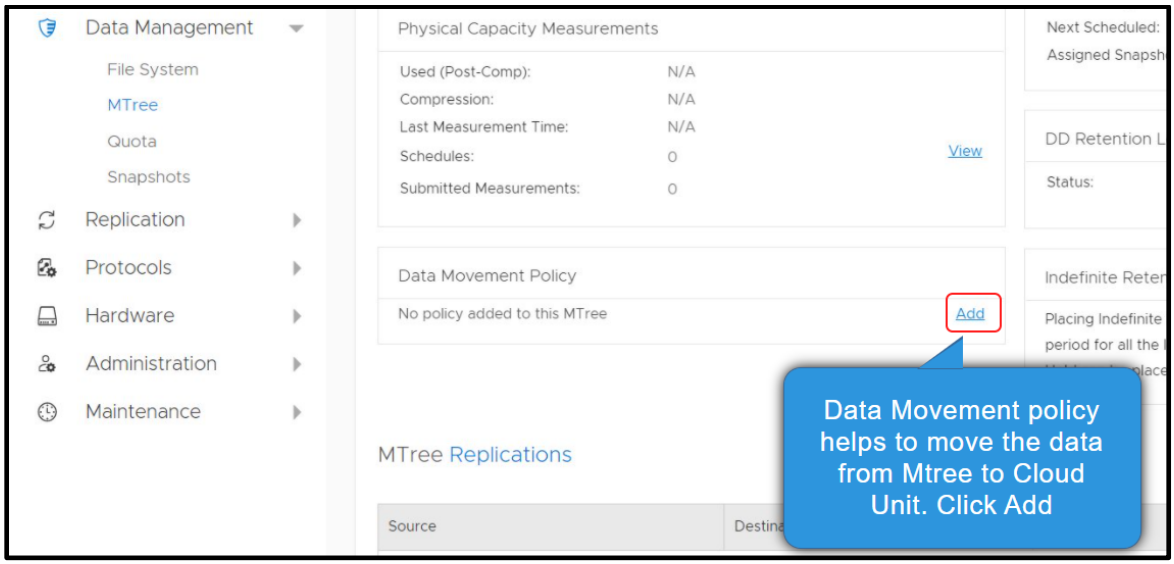
```
# filesys report generate file-location path <mtree path>.
```

Alternatively, you can also use DD System Manager (DDSM) to create a profile and move the data to cloud. The example below is AWS.

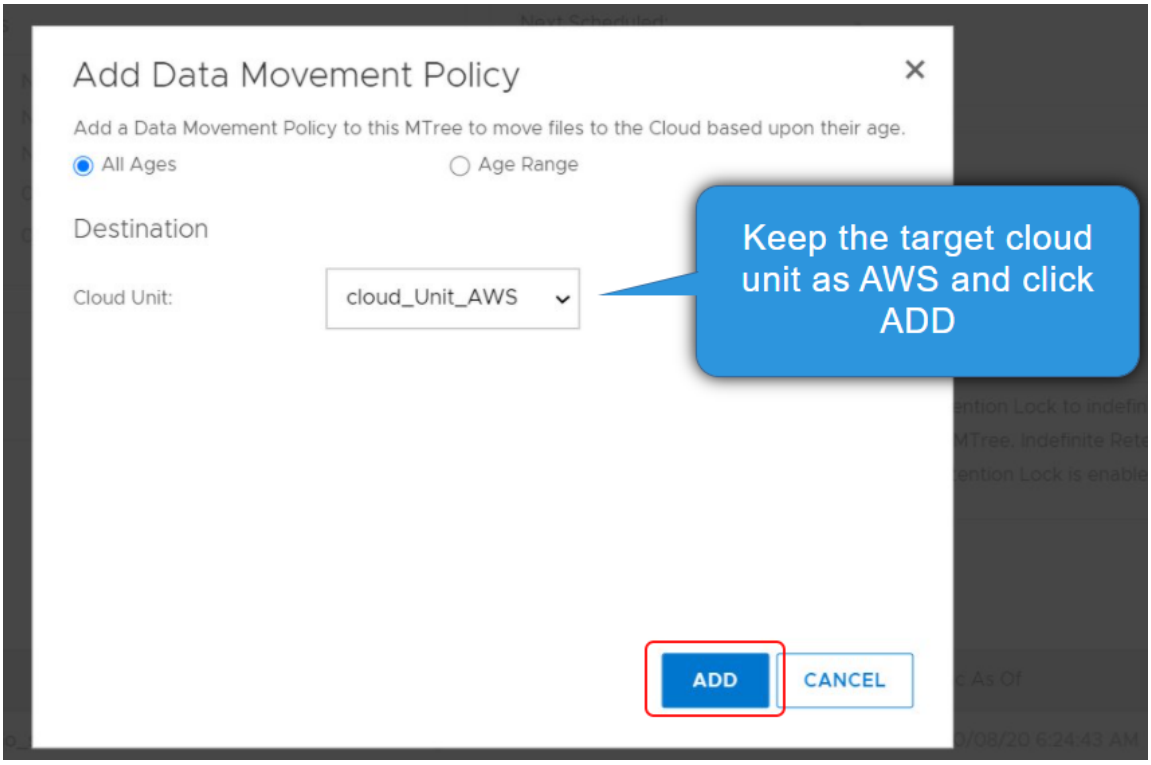
a) Select **Data Management** > **Mtree.** In the top panel, select the MTree to which you want to add a data movement policy.



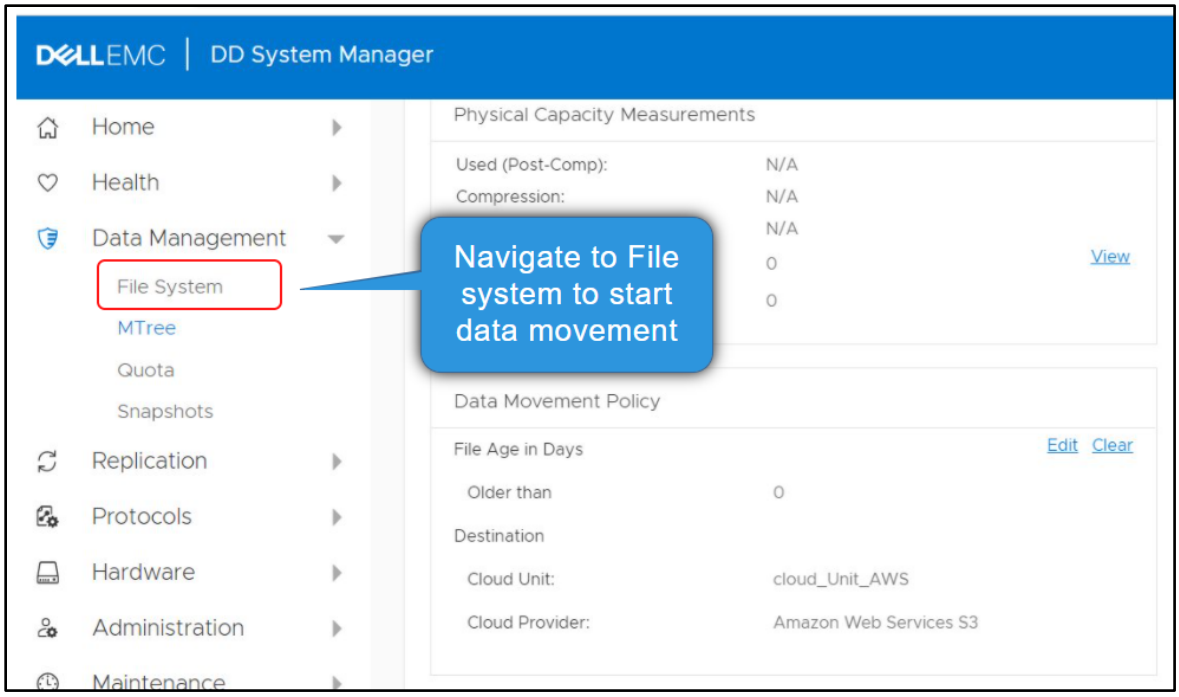
b) Click the **Summary** tab. Under **Data Movement Policy** click **Add**.



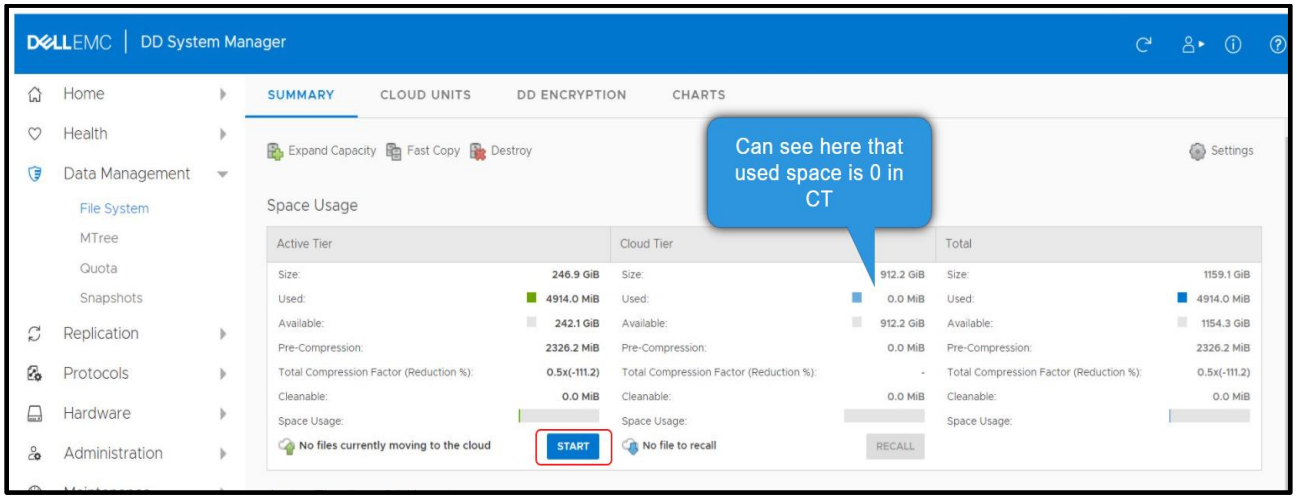
c) For **Destination**, specify the destination cloud unit. Click **Add**.



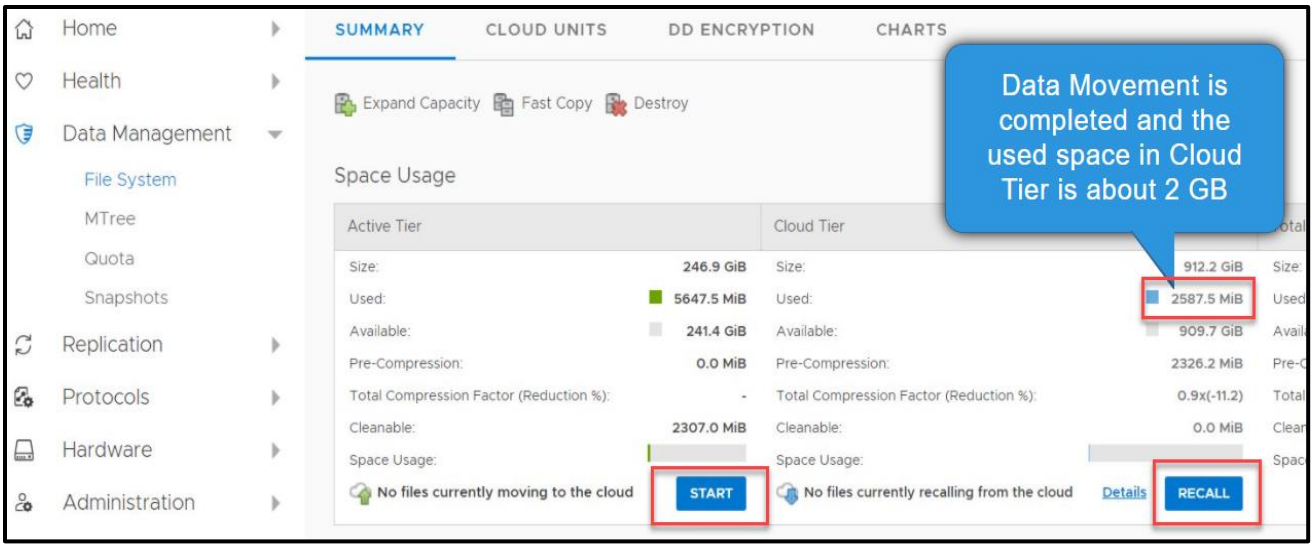
d) Select **Data Management** > **File System**.



e) For **Data Movement**, click **Start**.



f) After data movement is complete , you can see the used **capacity increased** and **Recall** option becomes available.



You can move data automatically, using a schedule and a throttle. Schedules can be daily, weekly, or monthly.

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

2. Click the **Data Movement** tab.

3. Set the throttle and schedule.

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.

If a file resides only in a snapshot, it cannot be recalled directly. To recall a file in a snapshot, use fast copy 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.

A Technical support and resources

Dell.com/support is focused on meeting customer needs with proven services and support.

Storage technical documents and videos provide expertise that helps to ensure customer success on Dell Technologies storage platforms.

A.1 Related resources

Additional resources that may be helpful when configuring Commvault with DD series appliances.

Description	Detail/Link
Commvault V11 Documentation	Commvault version 11 documentation
Commvault Backup Agents Overview	All Backup Agents architecture and information
Commvault Tape Library	Complete Information on Physical and Virtual Tape Libraries
Commvault Cloud Connection Performance Tuning	Commvault recommendations to get the maximum performance for cloud-based backup and restore for high-speed networks
Commvault Best Practice	Commvault recommendation and best practices
Commvault NAS Client Backup	Commvault NDMP and NAS client settings for backup
DD OS Administration Guide	Version 7.2, Version 7.3 ,Version 7.4
DD Command-Line Reference Guide	Version 7.2, Version 7.3 ,Version 7.4
DD BoostFS Linux Guide	Version 1.3, Version 7.2, Version 7.3 ,Version 7.4
DD BoostFS Windows Guide	Version 1.3, Version 7.2, Version 7.3 ,Version 7.4
Compatibility Guide	Commvault and Cloud Tier Commvault and DD BoostFS Compatibility Guide
DD Boost Partner Integration Guide	DD Boost Partner Integration Administration Guide