Technical Report

NetApp AltaVault Cloud-Integrated Storage Appliances

Solution Deployment: AltaVault with Catalogic DPX

Christopher Wong, NetApp
November 2017 | TR-4587

Abstract

This solution deployment guide outlines how easy it is to deploy and use a NetApp® AltaVault™ cloud-integrated storage appliance with Catalogic DPX. AltaVault appliances provide a simple, efficient, and secure way to offsite data to either public or private cloud storage providers. Using advanced deduplication, compression, and encryption, AltaVault enables organizations to eliminate reliance on older, less reliable data protection solutions while improving backup windows and disaster recovery capabilities.

NetApp®

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 AltaVault Overview

This chapter is an overview of the solution components.

1.1 Executive Overview

NetApp AltaVault storage enables customers to securely back up data to any cloud at up to 90% lower cost compared with on-premises solutions. AltaVault gives customers the power to tap into cloud economics while preserving investments in existing backup infrastructure and meeting backup and recovery SLAs. AltaVault appliances simply act as a network-attached storage (NAS) target within a backup infrastructure, enabling organizations to eliminate their reliance on tape infrastructure and all its associated capital and operational costs, while improving backup windows and disaster recovery capabilities.

It's easy to set up the AltaVault appliance and start moving data to the cloud in as little as 30 minutes, compared to setting up tape or other disk replication infrastructures, which can take days.

By applying industry-leading deduplication, compression, and WAN optimization technologies, AltaVault appliances shrink dataset sizes by 10x to 30x, substantially reducing cloud storage costs, accelerating data transfers, and storing more data within the local cache, which speeds recovery.

Security is provided by encrypting data on site or in flight, as well as in the cloud, using 256-bit AES encryption and TLS v1.1/1.2. AltaVault appliances provide a dual layer of encryption, which means that any data moved into the cloud is not compromised, and it creates a complete end-to-end security solution for cloud storage.

Because an AltaVault appliance is an asymmetric, stateless appliance, no hardware is needed in the cloud, and you can recover the last known good state of a broken or destroyed AltaVault appliance to a new AltaVault appliance. AltaVault appliances offer the flexibility to scale cloud storage as business requirements change. All capital expenditure planning required with tape and disk replication-based solutions is avoided, saving organizations up to 90%.

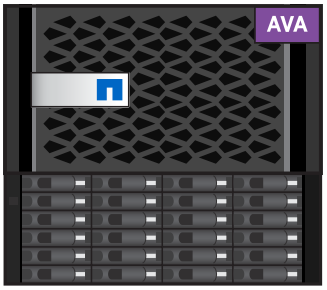
1.2 Catalogic DPX Architecture Overview

Catalogic DPX software provides a broad data protection platform, enabling businesses to secure their environments and access multiple capabilities with their backup data. Catalogic DPX stores backups as snapshots, which allows data to be accessed for recovery, reporting, dev-test, analytics, and additional use cases. Detailed reporting, powered through the DPX Reporter tool, can further expand understanding of backup data through reports on nodes, storage, job details, and growth.

1.3 AltaVault Appliance Overview

Figure 1 is an illustration of the AltaVault appliance.

Figure 1) AltaVault appliance.



AltaVault appliances are optimized and purpose built for data protection. They easily integrate into your existing backup infrastructure and favorite cloud storage provider. Setup and installation are easy because backup applications allow you to add an AltaVault appliance as a common target within its existing infrastructure. The backup server connects to the AltaVault appliance using standard SMB or NFS protocol.

When you back up to an AltaVault device, it performs inline, variable-segment-length deduplication, compression, and encryption of the backup data to minimize storage consumption and transmission times. AltaVault appliances also use their local disk cache for fast recovery of recent backups, providing LAN performance for the most likely restores. The AltaVault appliance then securely writes the deduplicated backup data to cloud storage and accelerates restores from the cloud by moving only needed segments of deduplicated data over the WAN. An easy-to-use graphical management console enables you to manage one or more AltaVault appliances through a web browser interface.

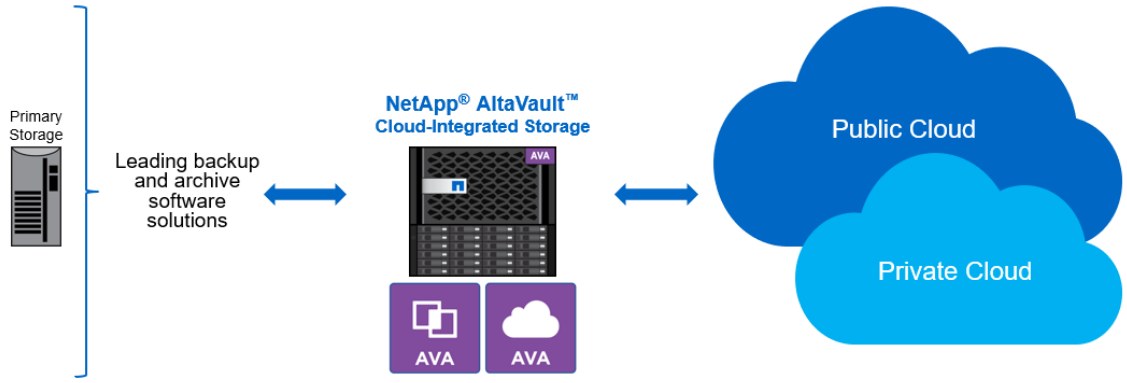
2 Deploy and Configure AltaVault with Catalogic DPX

Catalogic DPX with AltaVault appliances is a flexible, easy to configure and use solution that can be deployed with major cloud storage providers. See the AltaVault Deployment Guide for the detailed steps to deploy an AltaVault appliance.

2.1 AltaVault Solution Configuration Topography

Figure 2 shows the AltaVault solution configuration topology. Refer to the NetApp Interoperability Matrix for current versions of the backup application supported with AltaVault.

Figure 2) AltaVault ecosystem.



2.2 Hardware and Software Prerequisites

To install and deploy AltaVault in a backup environment, you must first complete the following prerequisites:

1. Have at least one server that acts as the Catalogic DPX server. Check the Catalogic DPX Support site and related compatibility lists where applicable.
2. Obtain server systems and related software media supported by Catalogic DPX and the AltaVault appliance.
3. A physical AltaVault appliance or virtual AltaVault appliance must be online and connected to the physical network infrastructure. A minimum of two IP addresses must be available for AltaVault.
4. Procure and set up all necessary software licenses from each vendor, using vendor-specific guidelines, including cloud storage credentials from your designated cloud storage provider.

5. Provide physical stacking and racking of equipment at each site. All cabling and power must be operational.
6. Verify that all LAN and WAN connections are functioning to and from your Internet and cloud storage providers.
7. If applicable, have available a Windows directory service (Active Directory) or UNIX Kerberos server.

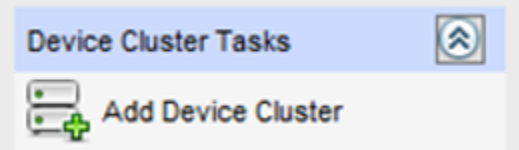
3 Configuring Catalogic DPX

When adding an AltaVault appliance to a Catalogic DPX environment, two primary tasks are required. The first is to add a device cluster that points to AltaVault. The second is to configure the media pool to point backups to a device within a device cluster.

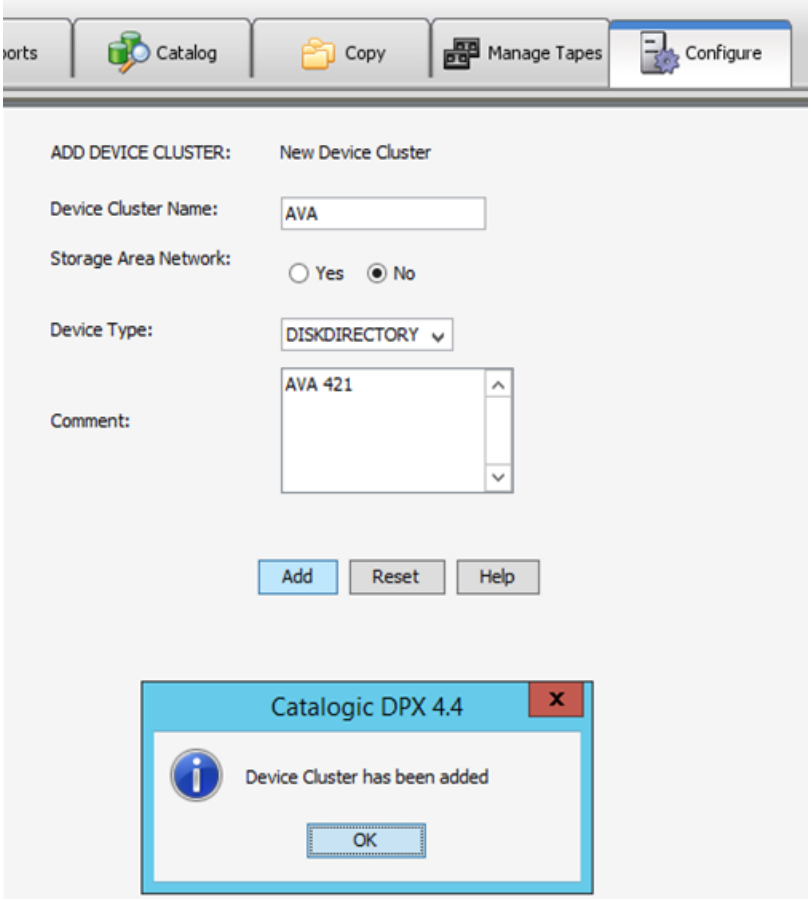
3.1 Add a Device Cluster and Device

Set up a device cluster and one or more devices, which will direct backups to an AltaVault SMB share.

1. In the management console, click the Configure tab. Click Devices in the left pane and then click Add Device Cluster.

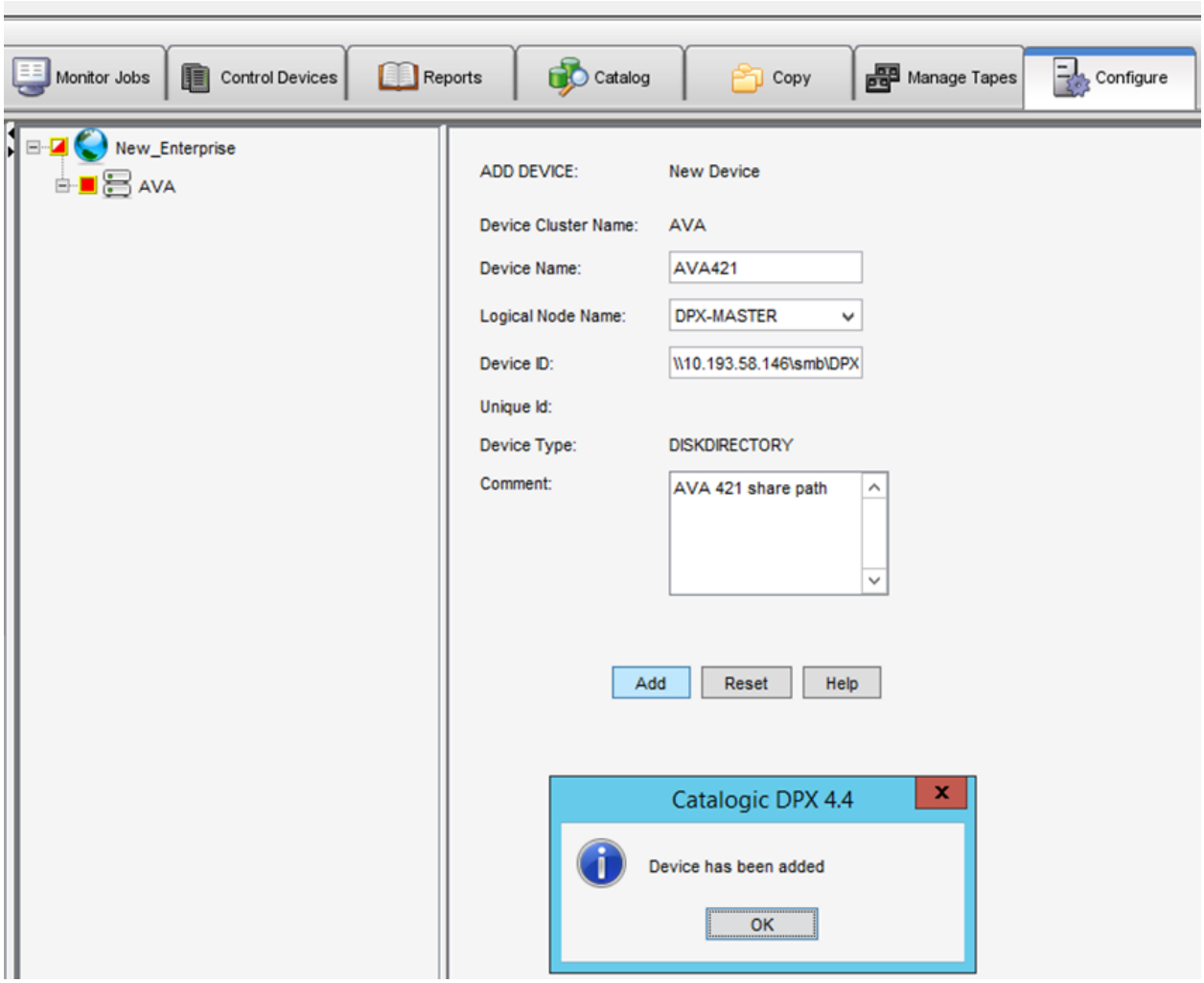


2. Fill in the fields as follows and click Add to add the device cluster.



- **Device Cluster Name**. Give this device cluster a meaningful name to address it by.
- **Storage Area Network**. Select No.
- **Device Type**. Select DISKDIRECTORY.
- **Comment**. Add a field as needed to help distinguish this disk cluster.

3. After the device cluster is added, right-click it and click Add Device. In the add device page that opens, fill in the fields as follows and then click Add. Repeat this step as needed to add more drives to the configuration. Each device should point to a unique AltaVault share path.

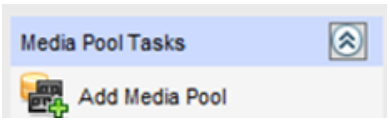


- **Device Name**. Give this device a meaningful name to address it by.
- **Device ID**. Provide the shared folder path to the AltaVault SMB share. Each device should point to a unique AltaVault share path.
- **Comment**. Add a field as needed to help distinguish this disk.

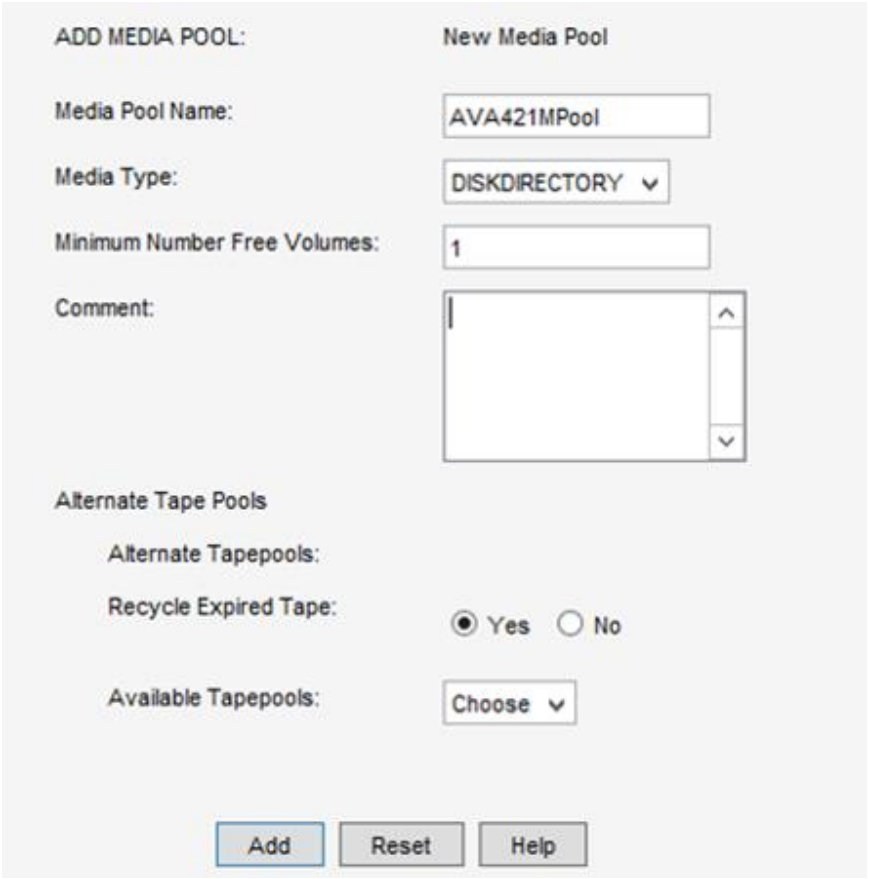
3.2 Add a Media Pool

After the device cluster and device are created, create a media pool and media to use with backups.

1. In the management console, click the Configure tab. Select Media from the left pane and then select Add Media Pool from the Media Pool Tasks list.

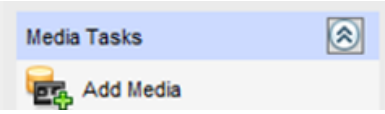


2. Fill in the fields as follows and then click Add.

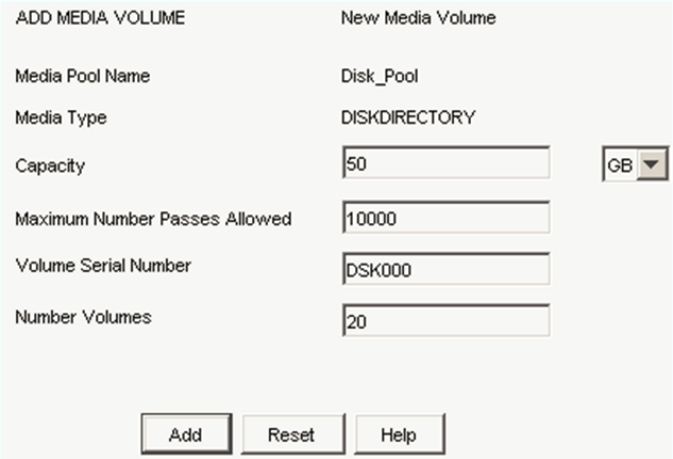


- **Media Pool Name**. Give this media pool a meaningful name to address it by.
- **Media Type**. Select DISKDIRECTORY.
- **Minimum Number Free Volumes**. Enter the minimum number of free media volumes to allow in the pool. When the number of free volumes falls below this number, DPX displays a warning message. A practical threshold value is 2 times the number of drives. This quantity ensures that you receive warnings early enough to acquire new media volumes.
- **Comment**. Add a field as needed to help distinguish this media pool.
- **Recycle Expired Tape**. When DPX uses a media volume from an alternate pool, it becomes part of the primary pool. DPX allows you to recycle those volumes back to the alternate pools upon expiration. Click Yes to allow Catalogic DPX to clean up the expired volumes back to the alternate pool.
- **Available Tapepools**. Select an alternate pool from the drop-down menu of previously defined media pools in your enterprise. The menu contains only alternate pools of the same media type as your primary pool. Your selection appears in the Alternate Pools list above this field. DPX uses alternate pools in the order in which they are listed. To clear the Alternate Pools List, select Select This to Remove All from the drop-down menu. Select Add from the task menu at the top right of the destination pane. If you don't see the task menu, resize the destination pane.

3. After the media pool is created, select Add Media from the Media Tasks list.

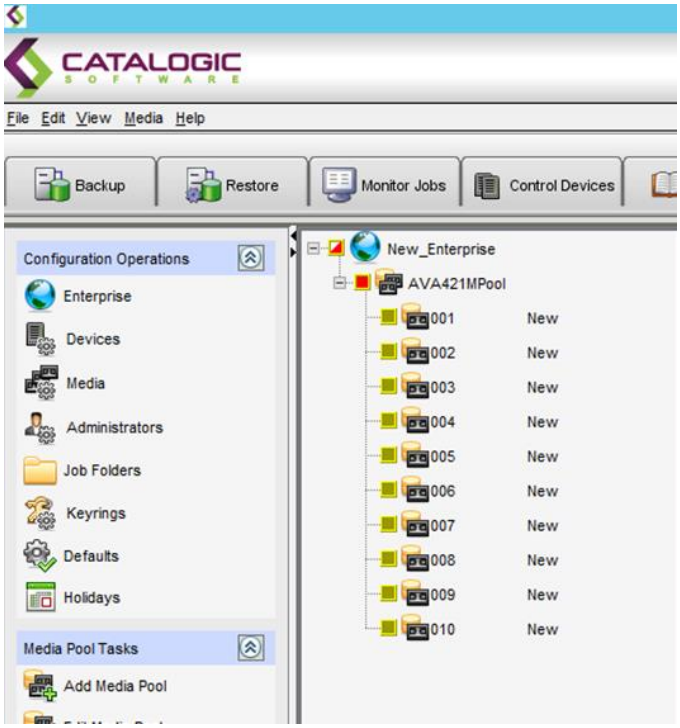


4. Fill in the fields as follows and then click Add.



- **Capacity**. Assigns the native storage capacity of the media volumes. Enter a number, then select a unit of measure from the drop-down menu, megabytes (MB) or gigabytes (GB). DPX uses this field to estimate free space on a media volume, but this field does not affect the amount of data that DPX can store on the media volume. For example, you can set the value to 20480MB (20GB) or larger. NetApp recommends a value of 100GB.
- **Maximum Number Passes Allowed**. (Optional) Assign the number of times a media volume can be written to, including second passes. After the specified number of passes, DPX no longer requests the media volume for backups and will not accept it if it is mounted for backup. It is still available for restores.
- **Volume Serial Number**. Enter a volume name with a maximum of 6 alphanumeric characters without spaces. The name cannot be the same as that of an existing media volume. If you are defining a set of consecutively named volumes, this must be the name of the first volume in the set. To define a set, the value you enter in this field must end with a number; for example, ENG001. BEX automatically creates consecutively named volumes; for example, ENG002, ENG003, etc., depending on the number you enter in the Number Volumes field (described next). If you enter 1 in the Number Volumes field, the Volume Serial Number is simply the name of the one volume you are adding.
- **Number Volumes**. Define a set of consecutively numbered media volumes. DPX automatically names and incrementally numbers the volumes, beginning with the volume entered in the Volume Serial Number field. For example, if the entry in the Volume Serial Number field is ENG001 and you specify 3 for Number Volumes, DPX accepts ENG001 and automatically creates volumes ENG002 and ENG003. To define only one media volume, enter 1 in this field.

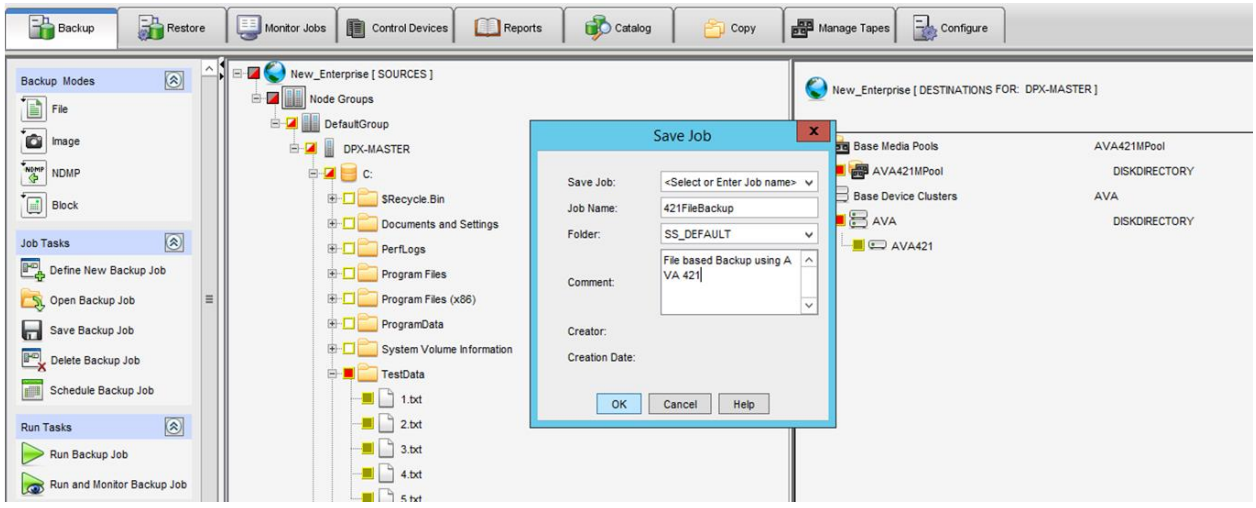
5. The media pool and media are now ready to be used for operations.



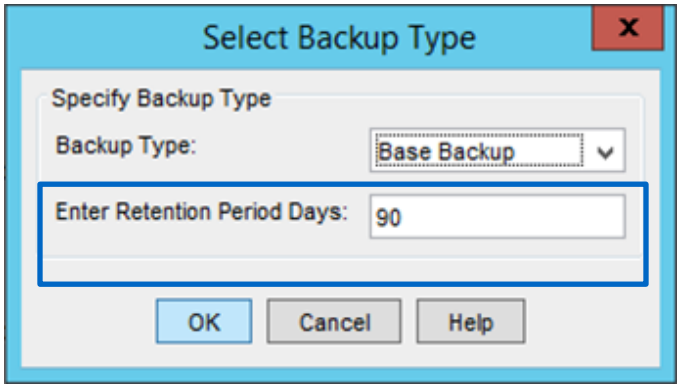
3.3 Perform a Test Backup

Backup jobs direct the client backups to flow to an AltaVault share. To create a backup job, follow these steps.

1. Click the Backup tab. In the Backup Modes pane, select File. In the middle pane, browse and select the file/folder objects to back up from systems that are available for backup. In the right pane, specify the backup media pool and base device cluster that you created for AltaVault. Click Save Backup Job to save the backup job configuration.



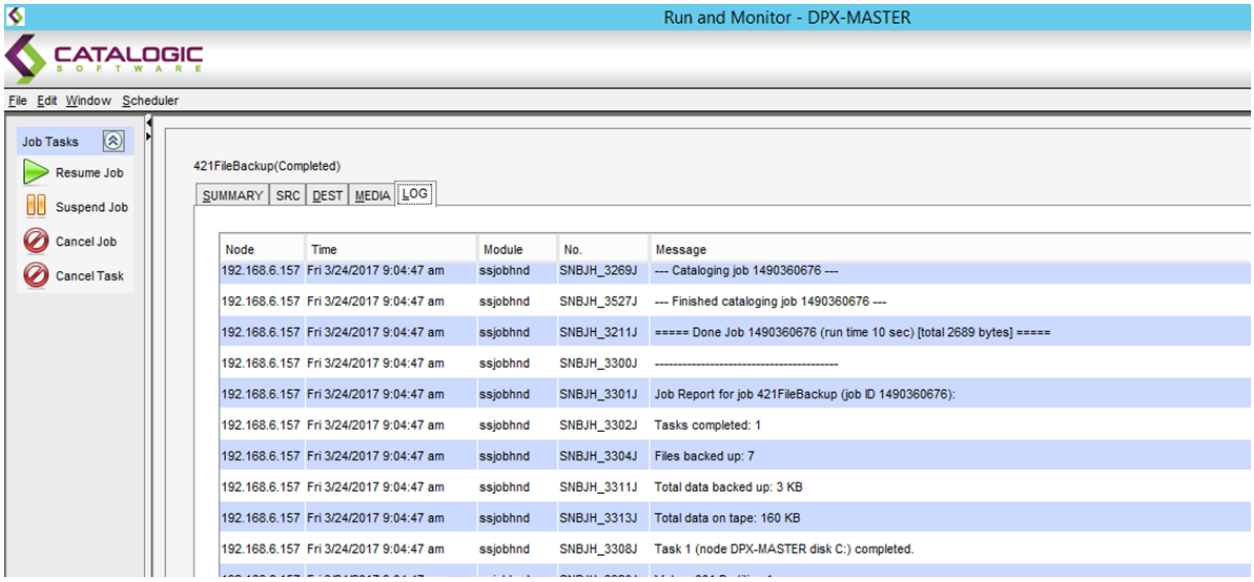
2. Select Run and Monitor Backup Job from the left pane to execute the backup job that you created. In the Select Backup Type window that opens, fill in the fields as follows and then click OK.



- **Backup Type**. Select the backup type operation to perform. By default, select Base Backup if this is a first-time backup operation.
- **Enter Retention Period Days**. Specify how long the backup should exist before expiring.

3.4 Monitor the Backup

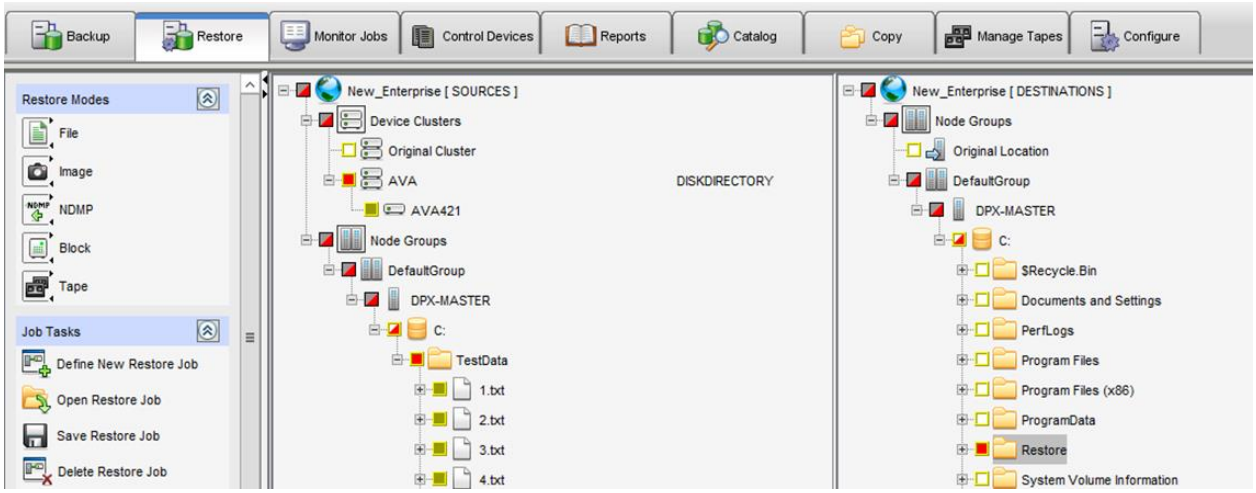
Click the Monitor Jobs tab to view operations related to the backup job.



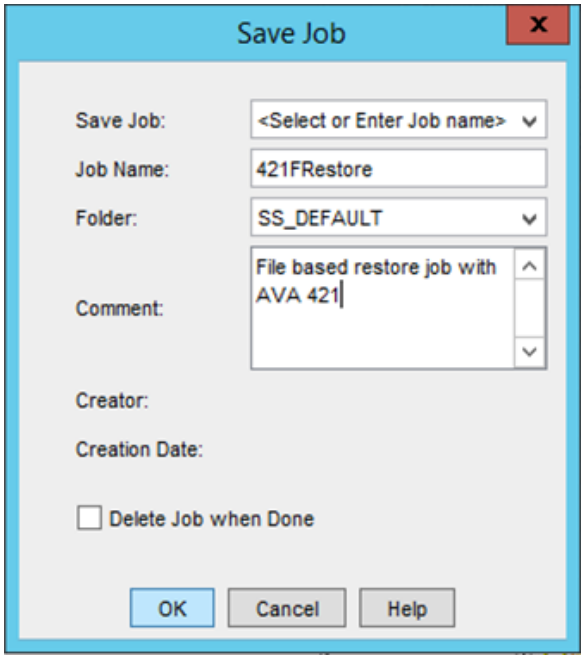
3.5 Restore a Backup

To restore a file from a backup job, follow these steps.

1. In the management console, click the Restore tab. In the left pane of the window that opens, select the type of Restore Mode to use, such as File. In the middle pane, select the Device Cluster that contains the backups on AltaVault, and in the right pane select the target location to restore the objects to.

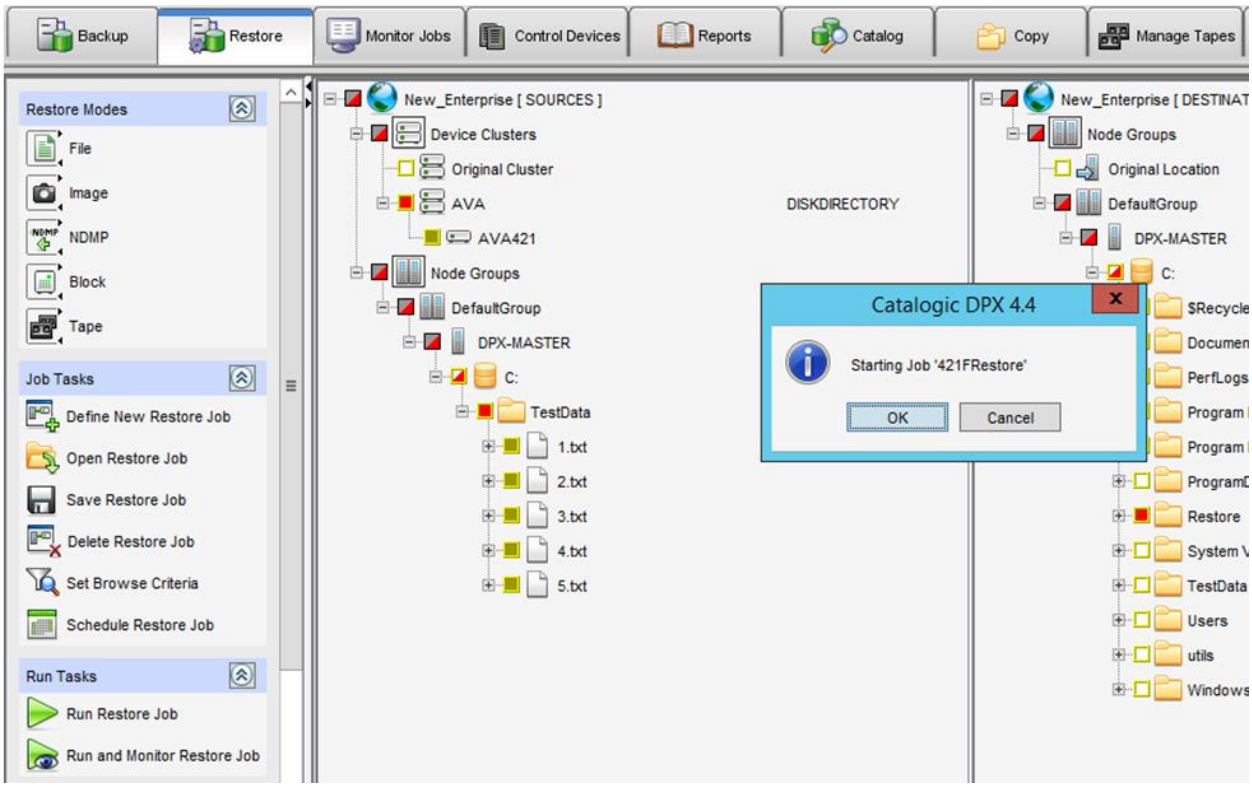


2. Optionally, click Save Restore Job to save the restore job. Fill in the fields as follows and then click OK.

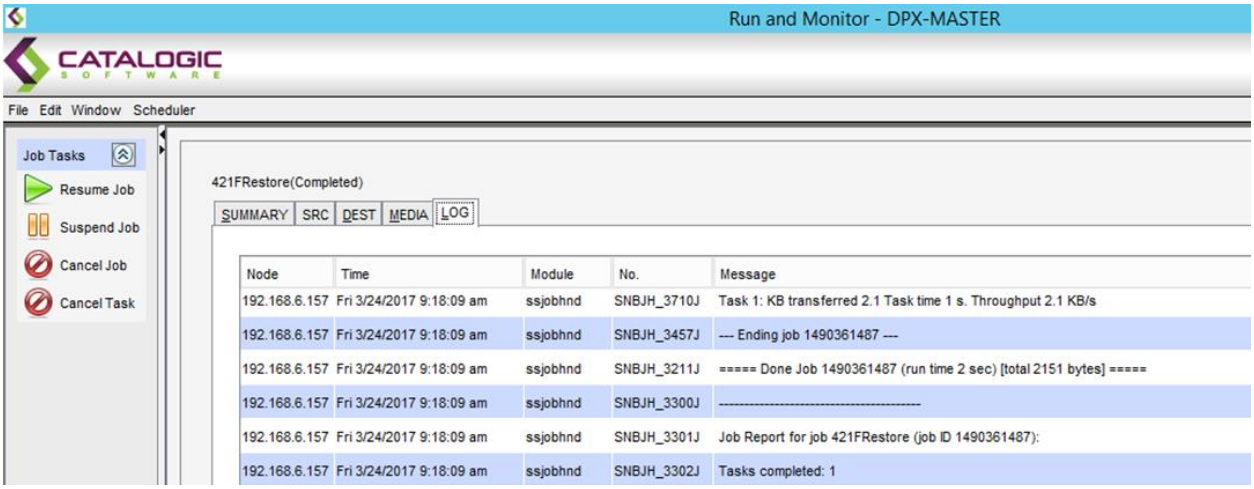


- **Save Job**. If you want to overwrite an existing restore job name, select it from this drop-down list. Otherwise, specify the job name in the next field.
- **Job Name**. If this is a new restore job, enter a name for the job.
- **Folder**. Specify the folder for the saved job.
- **Comment**. Add a field as needed to help distinguish this restore job.

3. In the left pane, select Run and Monitor Restore Job. The restore operation begins.



4. The restore operation is monitored in the monitor tab.



4 Solution Recommendations and Best Practices

This chapter lists recommendations and best practices for deploying AltaVault in Catalogic DPX environments. The best practices are not requirements, but NetApp recommends that you follow these suggestions for the best solution experience.

4.1 Catalogic DPX Best Practices

Table 1 describes the recommended best practices for using Catalogic DPX with AltaVault.

Table 1) Catalogic DPX best practices.

Item	Description
Use device clusters for AltaVault	AltaVault has been tested with Catalogic DPX device clusters.
Mount path permissions	Make sure that the mount path is using an account that matches the configuration of the SMB share permissions from AltaVault. In a Windows Active Directory domain, use a domain user account that is configured on the AltaVault SMB share. If not in a Windows AD domain, use a local account that matches the configured local account you specify for the AltaVault SMB share.
Disable compression, encryption, and deduplication in Catalogic DPX backup policies	NetApp highly recommends disabling the backup application data optimization techniques listed at left. This frees resources for the backup application server, and it also allows AltaVault to optimize data most efficiently, resulting in lower transmission and cloud provider storage costs. If deduplication is required when using Catalogic DPX, this leads to lower deduplication on AltaVault, as well as a significant performance impact.
Capacity	Specifies the media size of volumes written to AltaVault. AltaVault performs optimally when receiving large sequential streams of data from the backup application. NetApp recommends using 100GB objects for the best balance of backup and restore performance. If necessary, adjust the size based on your requirements. Note that although very large values can improve throughput and decrease volume counts created by the backup application, they can result in more data being downloaded from the cloud and increased costs if these larger volumes need to be prepopulated from the cloud for recovery operations.

4.2 Windows Best Practices

You can modify Windows networking parameters for SMB to improve overall backup application performance. To make these changes, go to the Start menu and enter regedit to start the Windows registry editor. Enter administrative permissions if prompted. Changes made in the Windows registry editor are permanent upon entry, so use extreme caution when making the changes or additions. A reboot is required.

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanworkstation\parameters]
"SESSTIMEOUT"=DWORD:00000e10

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters]
"DefaultSendWindow"=DWORD:00040000
"DefaultReceiveWindow"=dword:00040000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]
"GlobalMaxTcpWindowSize"=dword:00040000
"TcpWindowSize"=dword:00040000
"Tcp1323Opts"=dword:00000003
```

If Windows 2012 or Windows 8 or later is used with AltaVault versions earlier than 4.2, the Secure Negotiate feature in those products requires SMB signing negotiation messages to be signed themselves; otherwise, the connection fails. AltaVault versions earlier than 4.2 do not sign negotiation messages, and this can cause the SMB connections to AltaVault to fail repeatedly. To work around this limitation, if you cannot upgrade AltaVault to version 4.2 or later, disable the Secure Negotiate feature on the Windows server by using the following command from Windows PowerShell. Refer to Microsoft Knowledge Base article 2686098 for details.

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters"
RequireSecureNegotiate -Value 0 -Force
```

Where to Find Additional Information

To learn more about the information described in this document, refer to the following documents and/or websites:

- AltaVault Cloud-Integrated Storage product page
  http://www.netapp.com/us/products/cloud-storage/altavault-cloud-backup.aspx
- AltaVault Resources page
  http://mysupport.netapp.com/altavault/resources

Version History

Version	Date	Document Version History
Version 1.0	April 2017	Initial version
Version 1.1	November 2017	Updated for 4.4 release

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

TR-4587-1117