Technical Report

NetApp AltaVault Cloud-Integrated Storage Appliance

Solution Deployment: AltaVault with Commvault IntelliSnap for NetApp

Mike Braden, NetApp
July 2017 | TR-4457

Abstract

This solution deployment guide outlines how easy it is to deploy and use a NetApp® AltaVault® cloud-integrated storage appliance with Commvault IntelliSnap for NetApp software. The AltaVault appliance provides a simple, efficient, and secure way to move data off site 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

1.1 Executive Overview

NetApp AltaVault storage enables customers to securely back up data to any cloud at up to 90% less cost compared to that of 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 act as a NAS target within a backup infrastructure. Having this capability enables organizations to eliminate their reliance on tape infrastructure and all of its associated capital and operational costs while improving backup windows and disaster recovery capabilities.

It is simple to set up the AltaVault appliance. You can start moving data to the cloud in as little as 30 minutes; setting up tape or other disk replication infrastructures can take days. By leveraging industry-leading deduplication, compression, and WAN optimization technologies, AltaVault appliances shrink dataset sizes by 10 to 30 times. They also substantially reduce cloud storage costs, accelerate data transfers, and store more data within the local cache, speeding recovery.

Security is provided by encrypting data on site, in flight, as well as in the cloud using 256-bit AES encryption and SSL v3/TLS v1. AltaVault appliances provide a dual layer of encryption that prevents any data moved into the cloud from being 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. You can also recover the last known good state of a broken or destroyed AltaVault appliance to a new AltaVault appliance. AltaVault appliances provide flexibility to scale cloud object storage as business requirements change. Organizations avoid all of the capital expenditure planning required with tape and disk replication–based solutions, saving up to 90%.

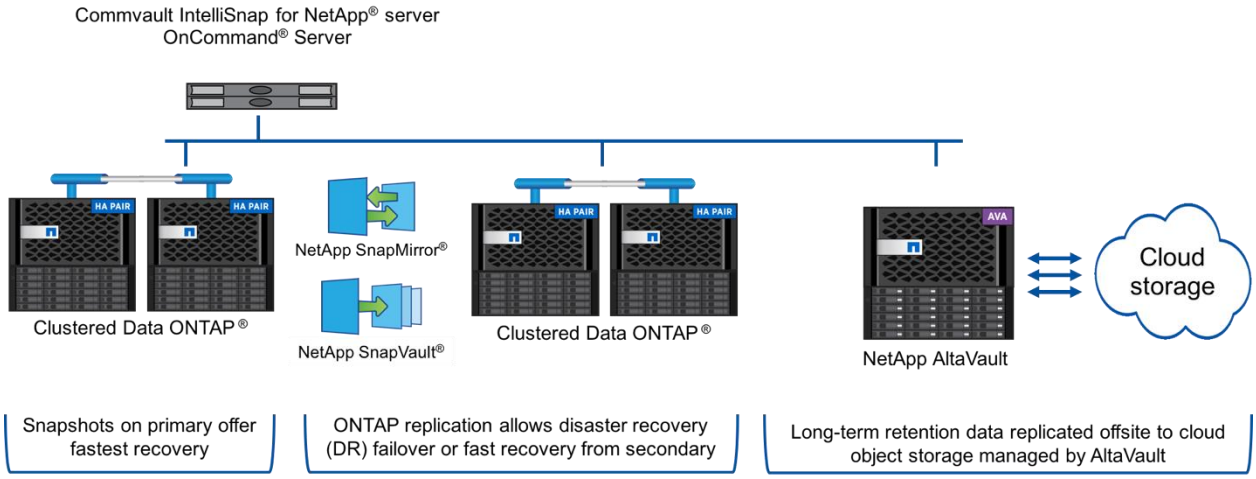
1.2 Commvault IntelliSnap for NetApp Architecture Overview

Commvault IntelliSnap for NetApp, with its revolutionary single-platform architecture, liberates companies from the expense and chaos of legacy data protection software not designed to handle today's IT realities. Modern data management is a tightly integrated blend of snapshot, replication, and persistent copies that are securely managed and accessible through a single, unified platform.

Commvault IntelliSnap for NetApp is application, operating system, and disk aware. The software quickly creates consistent copies by integrating and leveraging NetApp Snapshot® copies in the NetApp Data ONTAP® operating system. After a consistent Snapshot copy is created, data is efficiently moved to a secondary storage controller using the market-leading replication technologies of NetApp SnapMirror® and NetApp SnapVault® software.

Commvault IntelliSnap for NetApp utilizes software modules called iData Agents that share a common set of back-end services to talk through the common platform. Backups always start with a Data ONTAP Snapshot copy. Then they can be directed to alternate storage locations such as a replication target storage appliance or disk-based libraries where the destination is a cloud object storage service leveraging AltaVault. The following figure provides an overview of a typical Commvault IntelliSnap for NetApp deployment.

Figure 1) Typical Commvault IntelliSnap for NetApp network view.

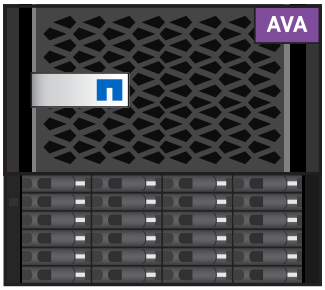


With Commvault IntelliSnap for NetApp, all backup operations start with a Snapshot copy. When using AltaVault to move data to the cloud, Commvault IntelliSnap for NetApp uses a MediaAgent to access the Snapshot copy and stream the data to a disk library on an AltaVault share. The Snapshot copy can be on the primary storage controller or it can be on a secondary storage controller. This flexibility enables backing up from either a second data center or nonprimary storage so that there is no impact on applications using primary storage during the backup operation.

Commvault IntelliSnap for NetApp uses storage policies to determine the operations to perform for a backup. The initial Snapshot copy operation is followed by one or more copy operations. Transferring the data to AltaVault happens in a copy operation and can use a different type of retention than that of the Snapshot copy. The retention can be either a basic retention or extended retention rules that can assign a different retention period to some backup copies, such as weekly or quarterly backups.

1.3 AltaVault Appliance Overview

Figure 2) AltaVault appliance.



AltaVault appliances are optimized and purpose built for data protection. AltaVault appliances 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 CIFS or NFS protocols.

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

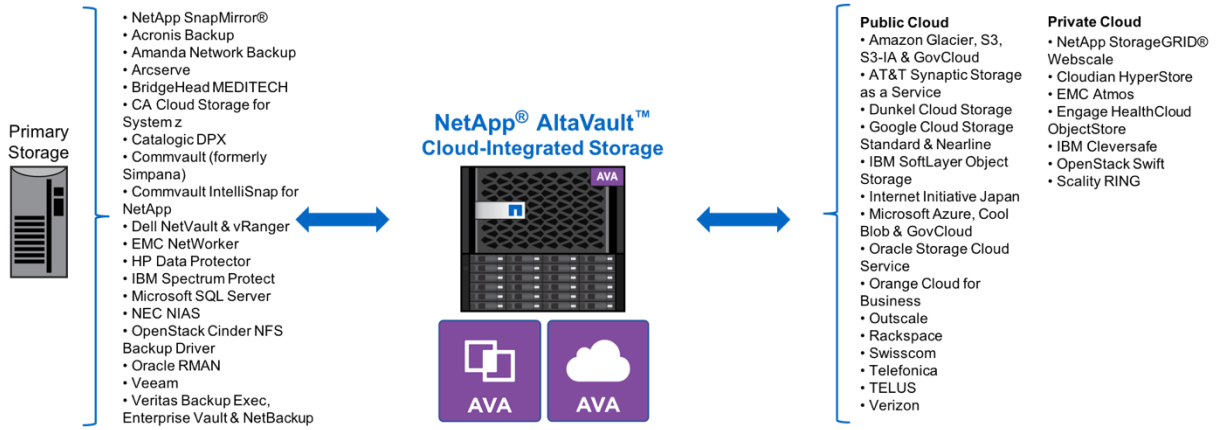
deduplicated backup data to cloud storage and accelerates restores from the cloud by moving only needed segments of deduplicated data over the WAN. An easy-to-use graphical management console enables you to manage one or more AltaVault appliances through a web browser interface.

2 Deploy and Configure AltaVault with Commvault IntelliSnap for NetApp

Commvault IntelliSnap for NetApp with AltaVault appliances provides you with 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 required to deploy an AltaVault appliance.

2.1 AltaVault Solution Configuration Topography

Figure 3) AltaVault ecosystem.



2.2 Hardware and Software Prerequisites

To properly deploy AltaVault into a backup environment, be sure that the following prerequisite requirements have been met before installing and deploying AltaVault.

1. You need at least one server that acts as the CommServe and MediaAgent server. Check the NetApp Support site and related compatibility lists where applicable.
2. The Commvault IntelliSnap for NetApp solution requires NetApp OnCommand® Unified Manager as well as a data source on a Data ONTAP storage system, such as a NetApp FAS array.
3. You must have server systems and related software media supported by Commvault IntelliSnap for NetApp and the AltaVault appliance.
4. A physical AltaVault appliance or a virtual AltaVault appliance needs to be online and connected to the physical network infrastructure. A minimum of two IP addresses must be available for AltaVault.
5. You must procure and set up all necessary software licenses from each vendor using vendor-specific guidelines. This includes obtaining cloud storage credentials from your designated cloud storage provider.
6. Perform physical stacking and racking of equipment at each site. All cabling and power must be operational.
7. Verify that all LAN and WAN connections are functioning to and from Internet and cloud storage providers.
8. If applicable, have available a Windows Active Directory Domain Services.

3 Configuring Commvault IntelliSnap for NetApp

When adding an AltaVault appliance to a Commvault IntelliSnap for NetApp environment, two primary tasks are required. The first is to add a disk library to the MediaAgent that points to AltaVault. The second is to modify the storage policy so that client backups are directed to use the new disk library target.

In these examples a single disk library is created. It is also possible to have additional disk libraries, each on separate shares on the AltaVault appliance. Additionally, it is possible to have more MediaAgents, each with disk libraries writing to the same AltaVault appliance. In such a case NetApp recommends using a share for each MediaAgent and disk library combination.

It is possible to tune AltaVault's cache on a per-share basis. Depending on the source data type it might be beneficial to have a disk library and share for each source data type. For example, when backing up VMs they could be sent to one disk library and share. The catalogs could be backed up to a different disk library and share on the same AltaVault appliance.

It is also possible to write the Commvault IntelliSnap for NetApp DR backups to AltaVault. When you do so, NetApp recommends creating a separate AltaVault share and disk library that is dedicated to DR backups so that they are separate from other backup data.

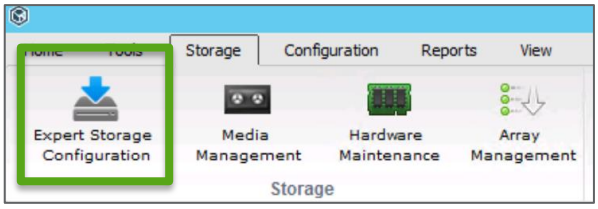
Schedule policies are not described in this guide. These policies are described in the Commvault IntelliSnap for NetApp documentation and apply to the Snapshot backup job as well as the backup copy job. See the Commvault IntelliSnap for NetApp online documentation for information about creating schedules.

3.1 Add a Disk Library to the MediaAgent

A library is used by a MediaAgent to communicate and store backup data on a specific device. For the purposes of this configuration, the library created will be configured to point to an AltaVault CIFS share, rather than to a local disk volume.

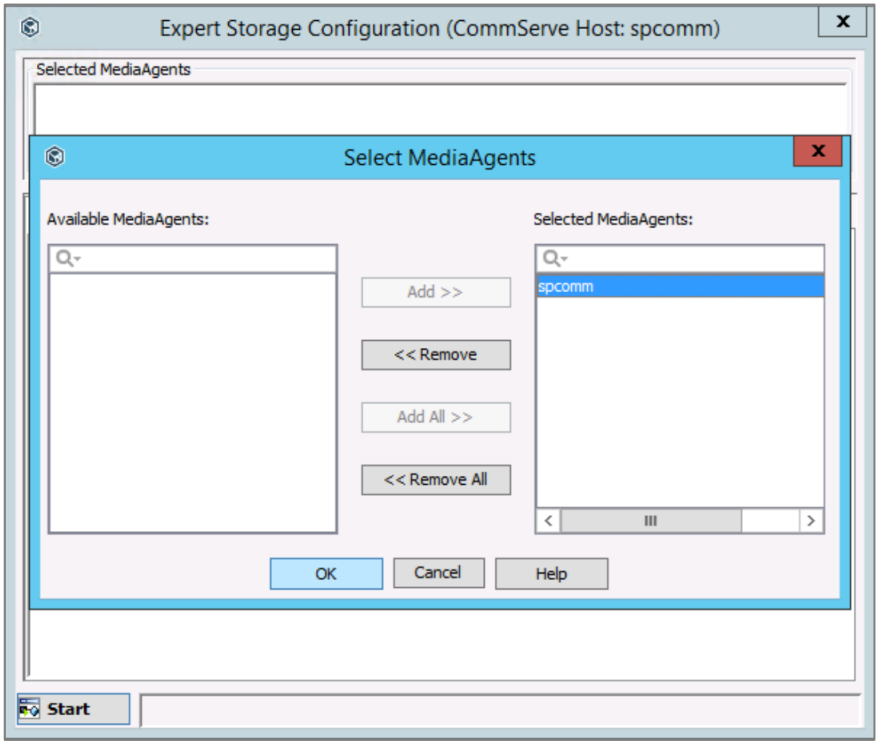
1. Select the Storage tab from the top menu, and then click Expert Storage Configuration.

Figure 4) Library and drive configuration.



2. Identify the MediaAgent to use and click the Add button to select it. Click OK to continue.

Figure 5) Select MediaAgent.



3. When the Library and Drive Configuration panel appears, select the Libraries icon, right-click it, and select Add > Disk Library.
4. Click OK at the Information dialog

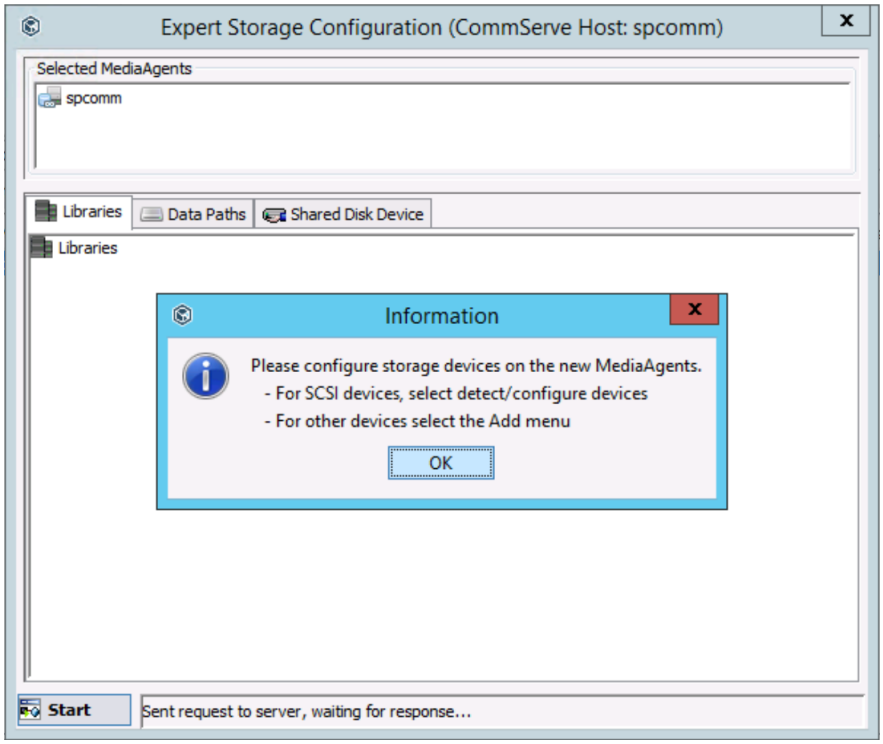
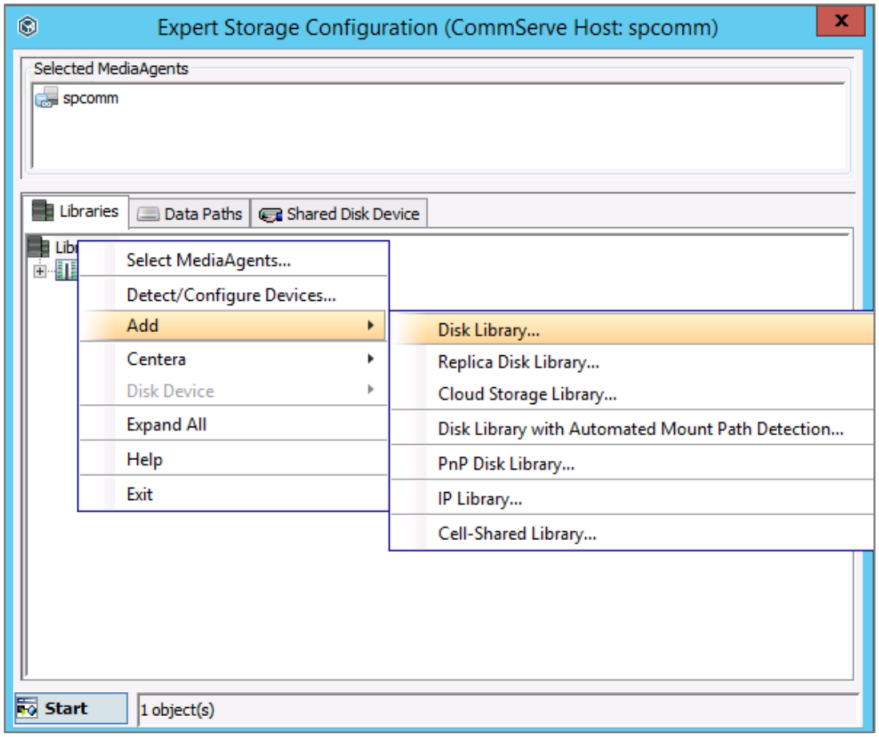
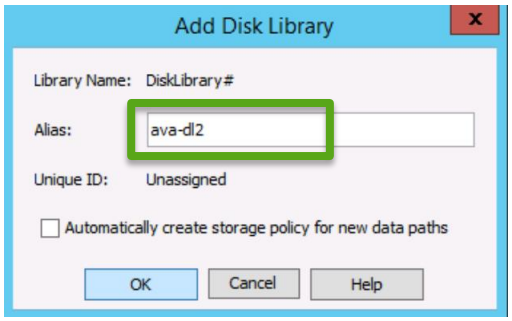


Figure 6) Add a disk library.



5. Identify the library name you want to use, then click OK.

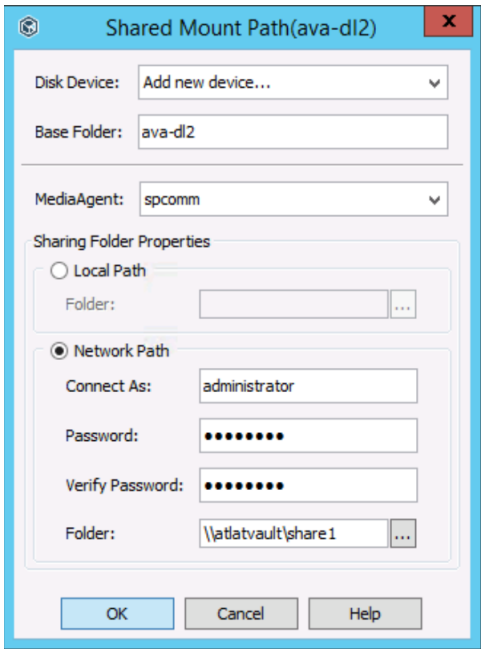
Figure 7) Library name selection.



6. Provide a base folder name in which to store the data. In the Sharing Folder Properties section:
   — If the AltaVault appliance is configured with local permissions, provide the fully qualified CIFS share name to the AltaVault target in the Local Path section.

   — If the AltaVault appliance is configured with Active Directory, select the Network Path section instead. Provide Windows login credentials and the fully qualified SMB share name to the AltaVault target.

Figure 8) Shared Mount Path identification.



7. Click OK to complete library creation.

3.2 Tuning the Disk Library Settings

It Is recommended to do some performance tuning for most environments. There are several ways that tuning can be performed with the goal of optimizing data transfer for backup jobs as well as completing backups within allocated windows.

From the AltaVault aspect, it is possible to set the number of writers allowed for each disk library and each media agent. The goal should be to start with a low number of simultaneous writers to spread the backups throughout the backup window. Increasing the number of writers as needed up to the maximum number of concurrent streams the AltaVault supports. Going beyond the supported concurrent stream limit will result in write failures with jobs failing.

For the most current recommendations on the number of concurrent streams and recommendations for the number of media agents refer to TR-4414_AltaVault Best Practices Guide for Backup Applications.

1. From the main console view, expand Storage Resources > Libraries. Right-click the library just created. Select Properties. When the Properties window appears, select the Mount Paths tab and set the Allocate Number of Writers value.

Figure 9) Library properties.

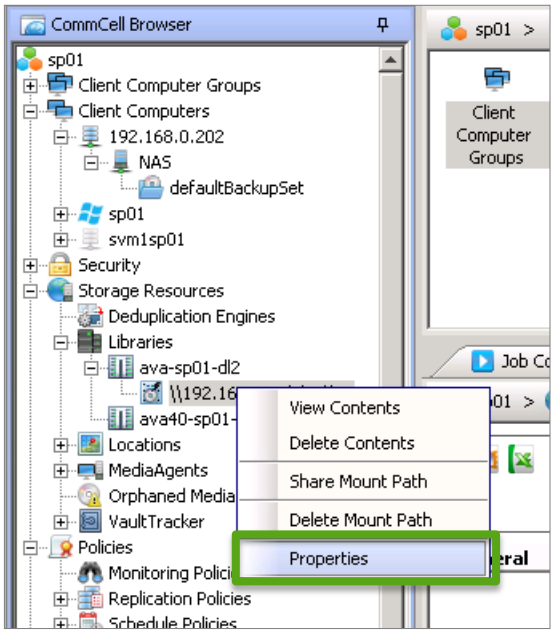
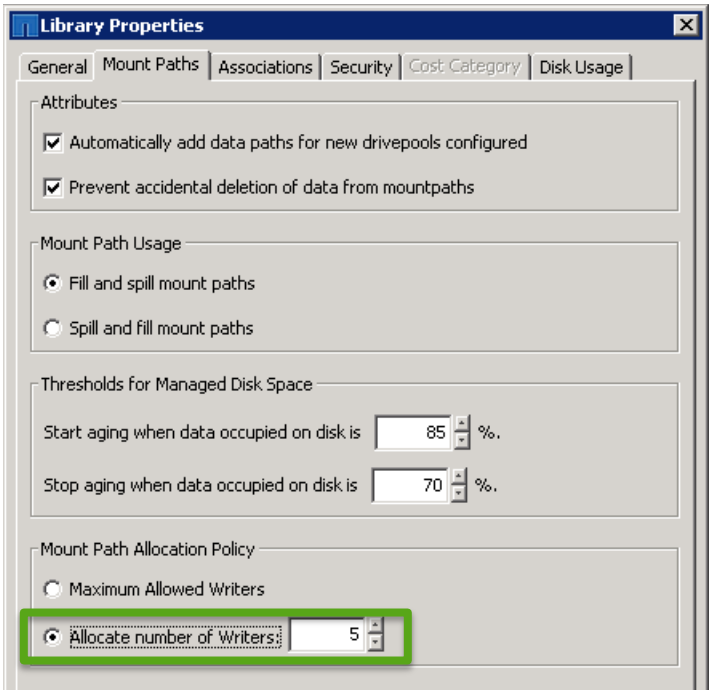


Figure 10) Mount Paths Allocate Number of Writers.

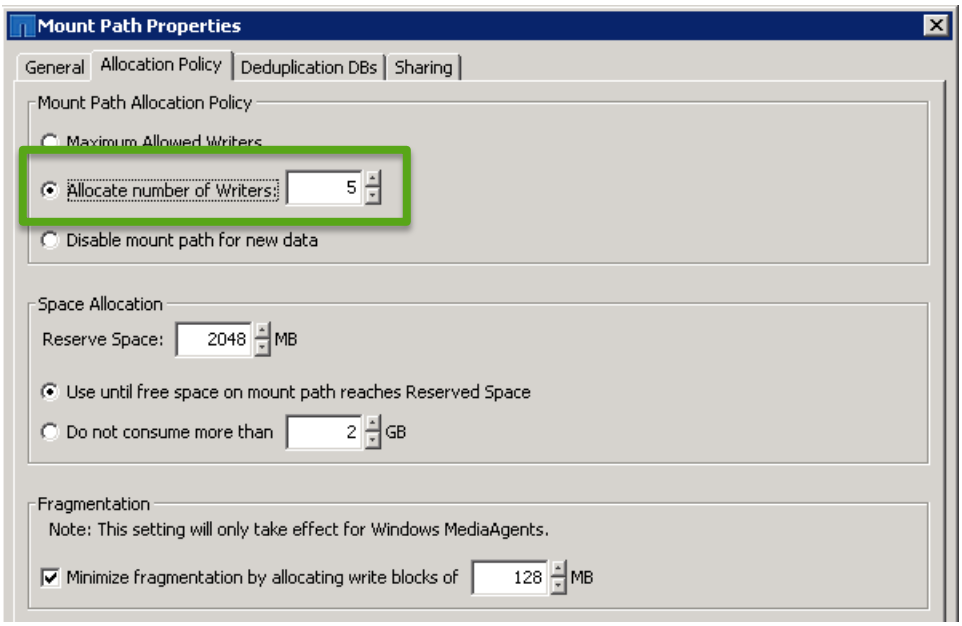


Allocate Number of Writers

- This value establishes how many writes are allowed by data protection clients. NetApp recommends setting an initial value of 5 and increasing this value based on network and resource availability.

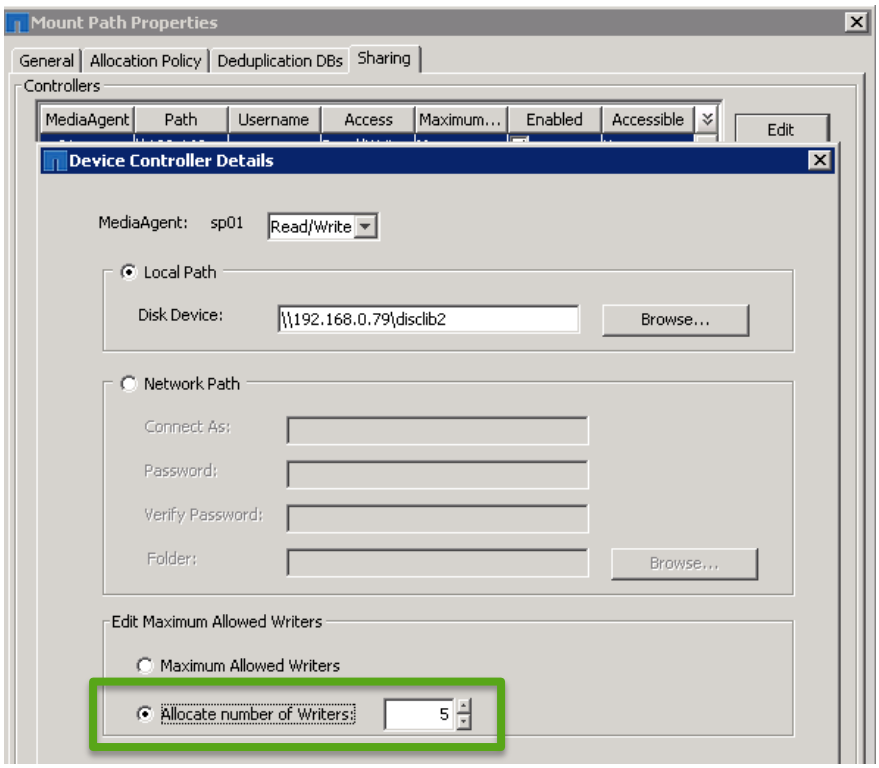
2. Now expand the selected library and select the mount path for the library. Right-click it and select Properties. In the Allocation Policy tab, set the Allocate Number of Writers value to 5.

Figure 11) Device Paths Allocate Number of Writers.



3. Select the Sharing tab, then select the mount path created and click Edit. In the Device Controller Details window, edit the Allocate Number of Writers value to 5.

Figure 12) Device Controller Details.

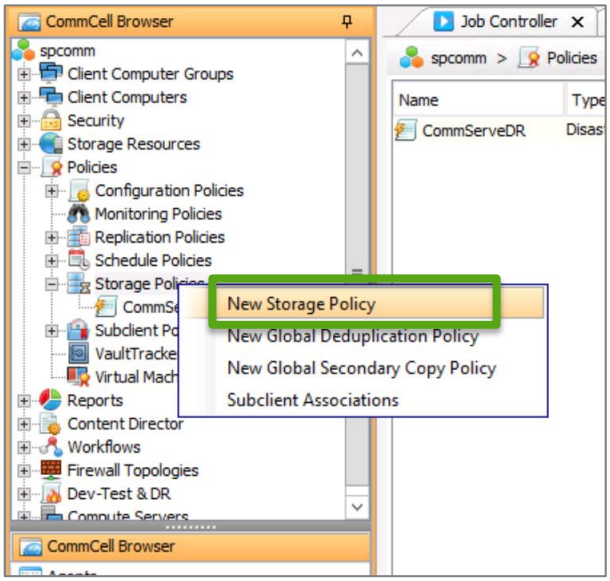


3.3 Create a Storage Policy

Storage policies act as the primary channels through which data is included in data protection and data recovery operations. A storage policy forms the primary logical entity through which a subclient or instance is backed up. The policy's chief function is to map data from its original location to a physical media. For Commvault IntelliSnap for NetApp servers with existing storage policies to which you would like to add AltaVault, you can modify the existing policy and create a copy that uses the previously created disk library that is located on AltaVault. In this example, we create a new storage policy.

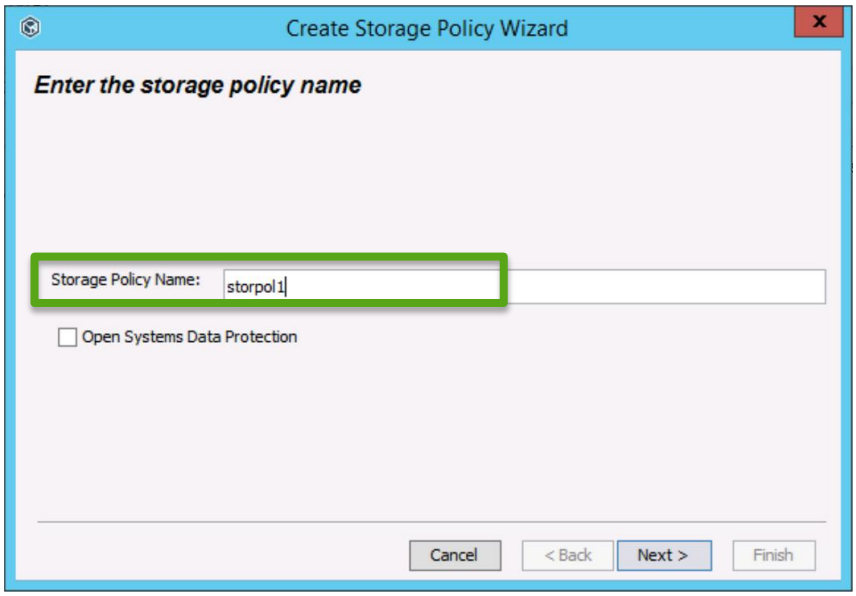
1. Use the Policies section of the CommCell console and select Storage Policies. Right-click and select New Storage Policy.

Figure 13) Create New Storage Policy.



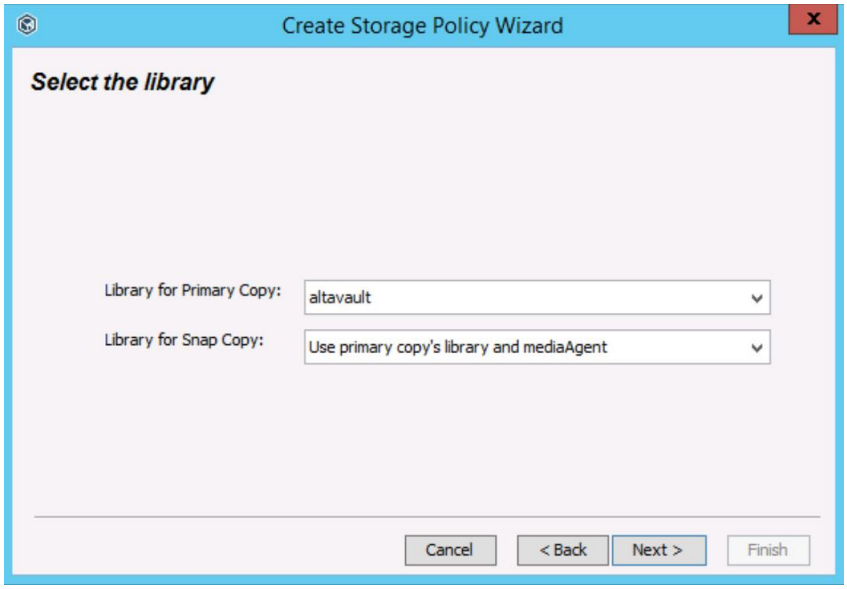
2. Provide a unique storage policy name and click Next.

Figure 14) Storage Policy Name entry.



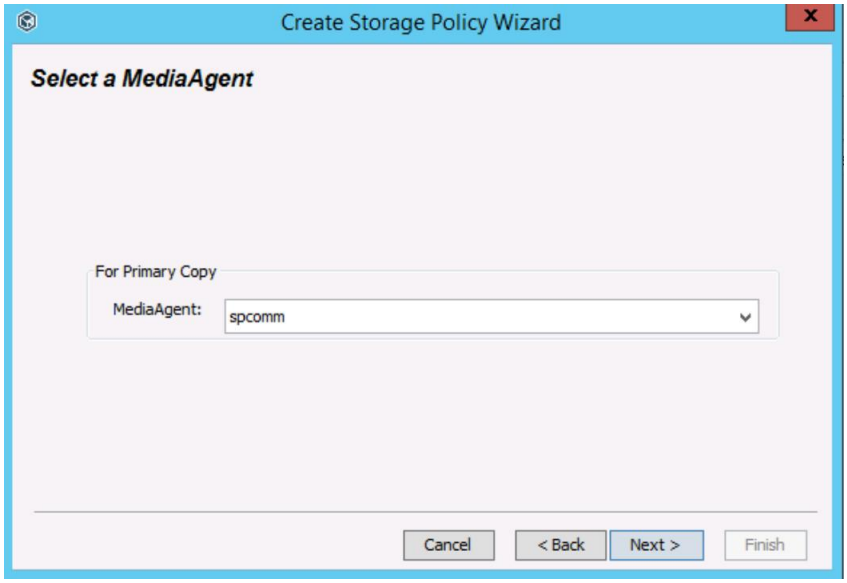
3. Select the previously created library to use for this storage policy and click Next.

Figure 15) Library selection.



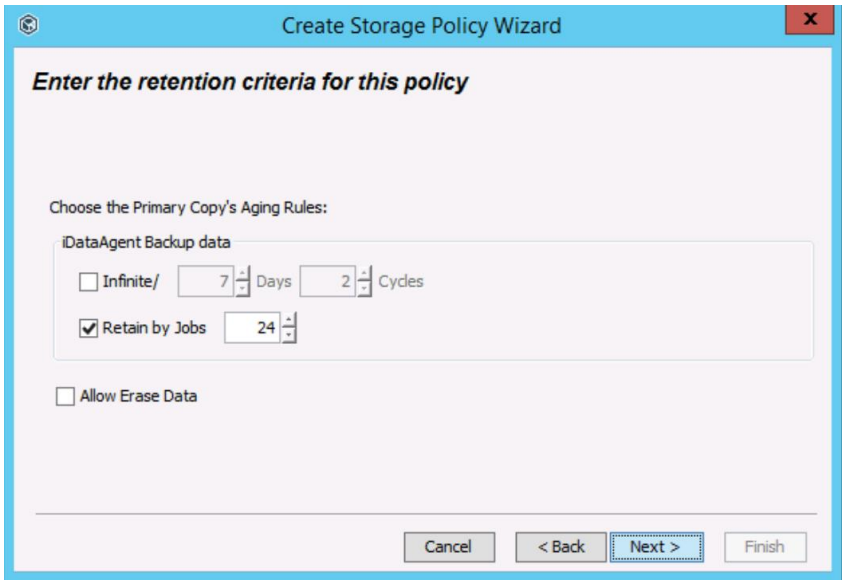
4. Select the MediaAgent from the drop-down list and click Next.

Figure 16) MediaAgent selection.



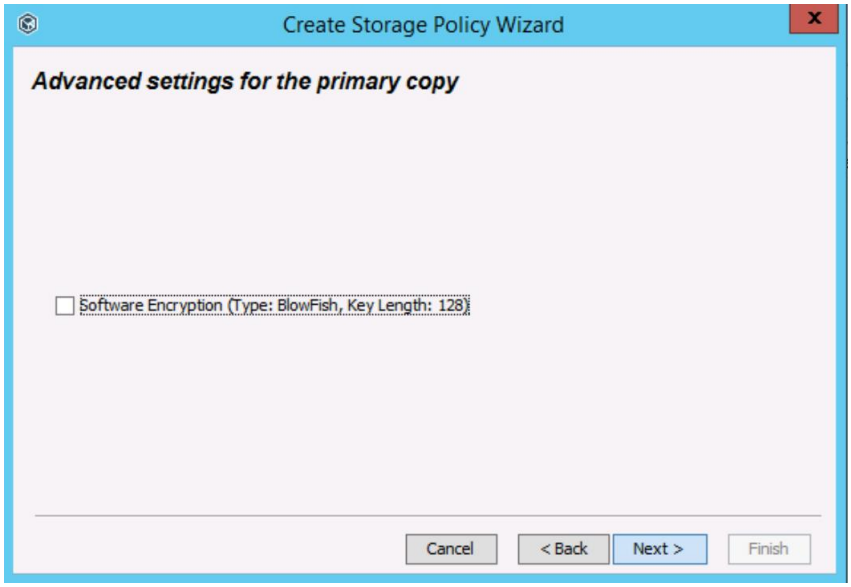
5. Choose the appropriate retention type and period. For Retain by Jobs, this setting will retain that number of Snapshot copies on the volume.

Figure 17) Retention selection.



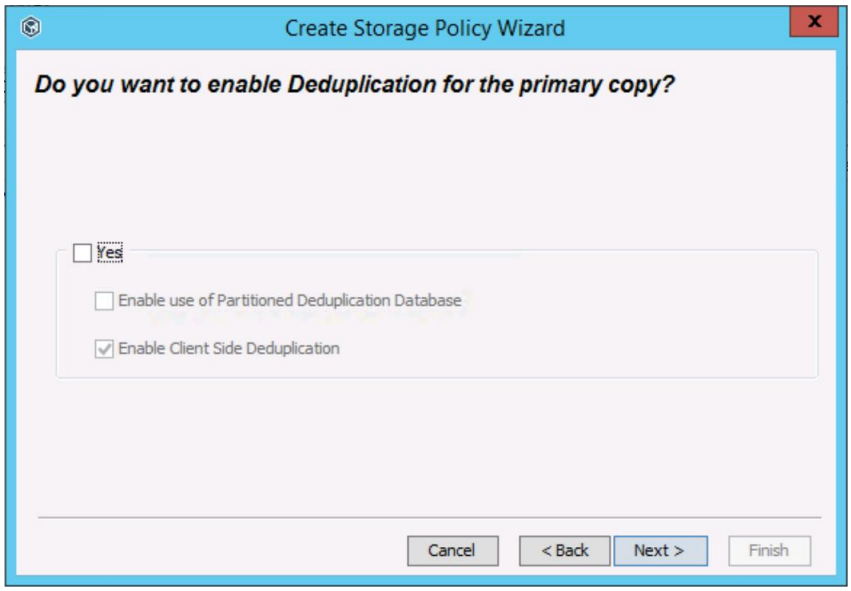
6. Make sure Software Encryption is not checked and click next.

Figure 18) Retention selection.



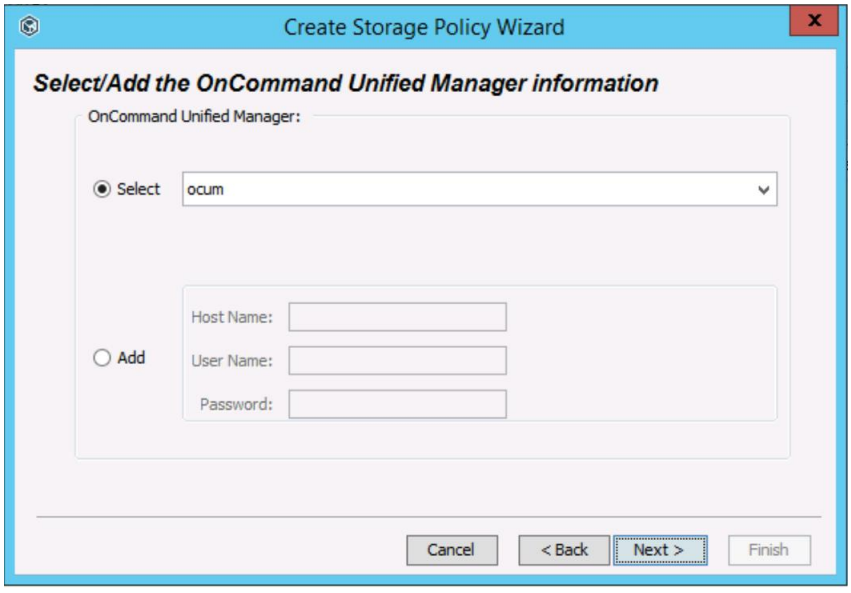
7. When prompted regarding deduplication, clear the Yes checkbox to disable deduplication.

Figure 19) Deduplication selection.



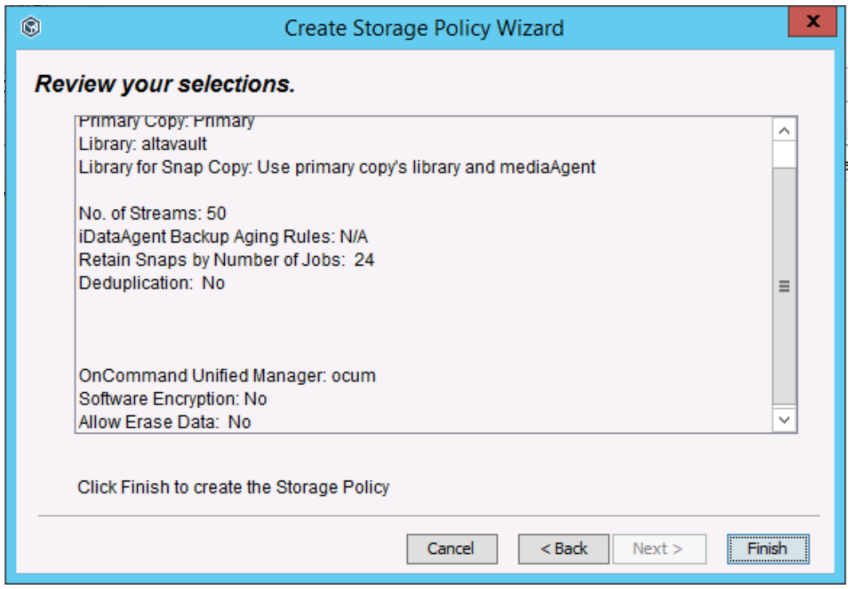
8. Select the OnCommand Unified Manager system for this policy.

Figure 20) OnCommand setting.



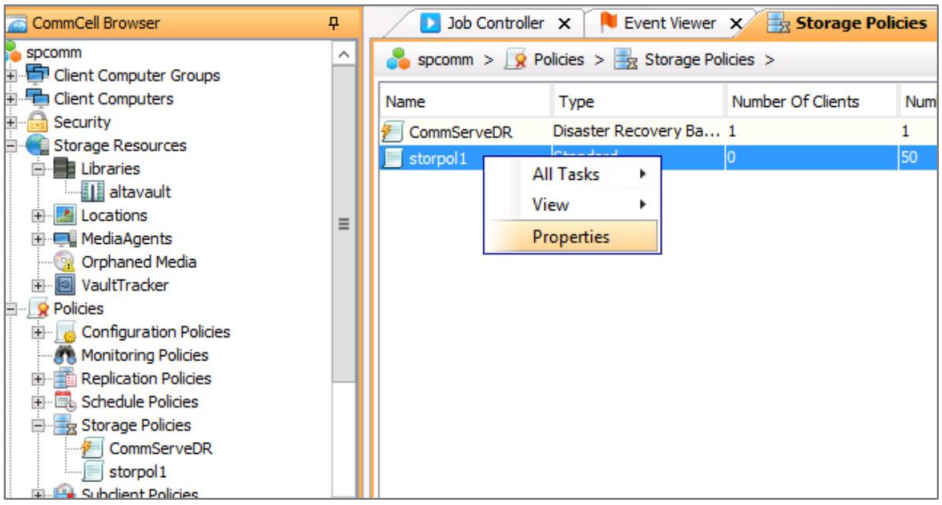
9. Review the summary and click Finish to complete the storage policy creation.

Figure 21) Review selections.



10. Right-click the storage policy created in the previous step and choose Properties.

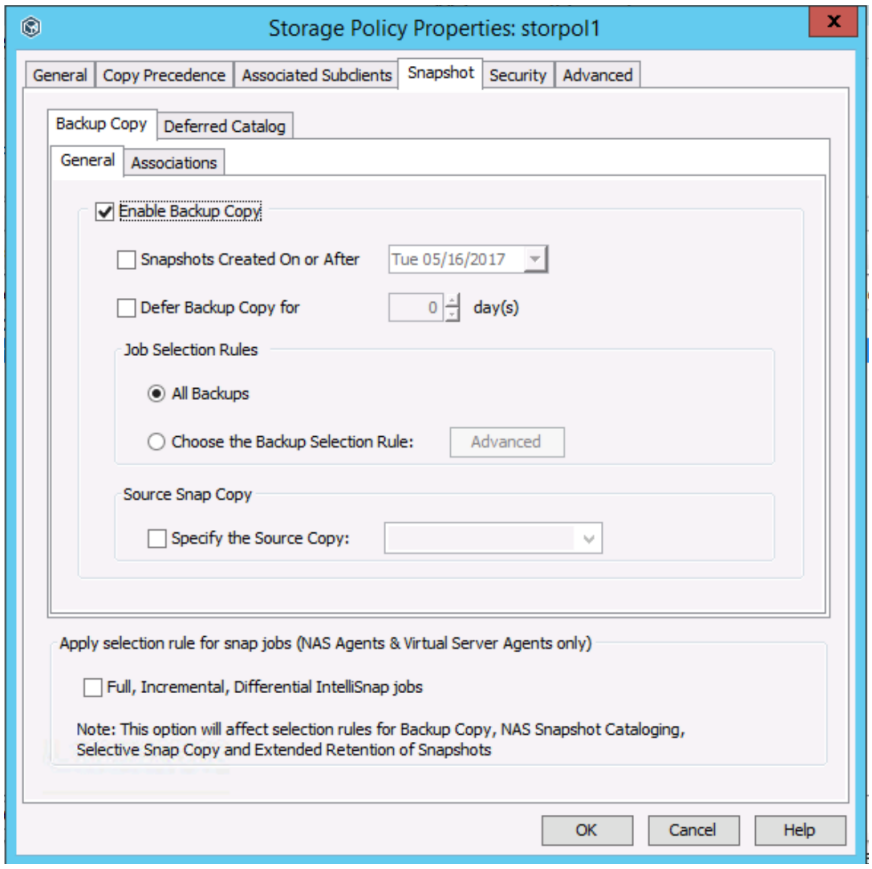
Figure 22) Policy properties.



11. Click the Snapshot tab.

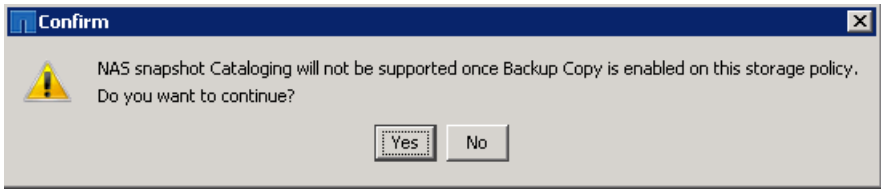
12. Click Enable Backup Copy to allow streaming of the Snapshot copies.

Figure 23) Enable backup copy.



13. A warning message is shown to confirm the action. Click the Yes button to accept.

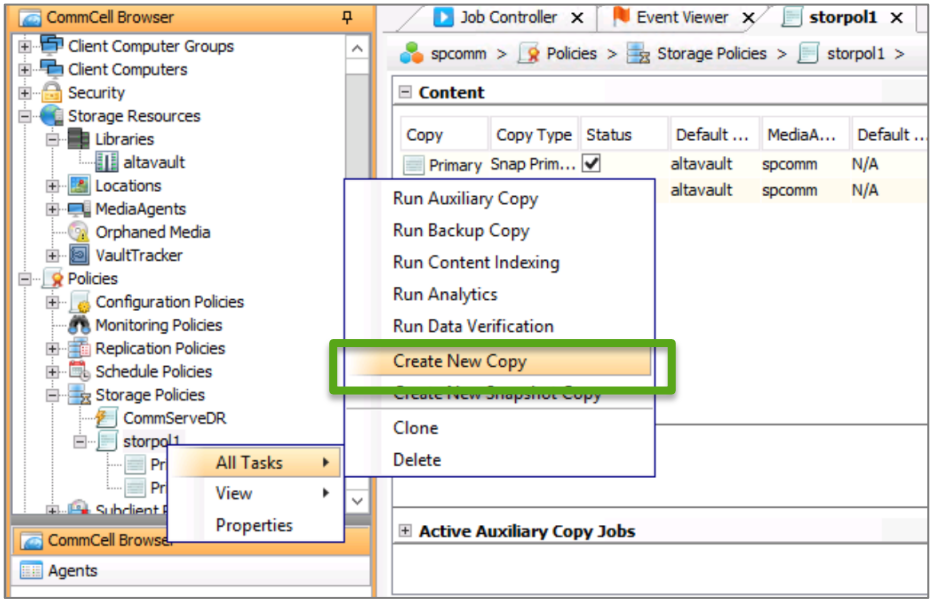
Figure 24) Snapshot catalog warning.



Next, create a storage policy operation to copy the Snapshot copy data to the disk library created for the AltaVault appliance.

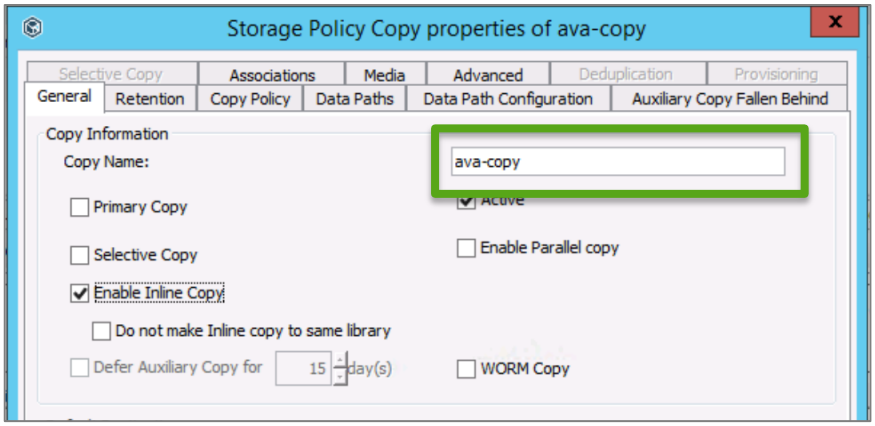
14. Click the storage policy created previously, select All Tasks, then select Create New Copy.

Figure 25) Create new copy.



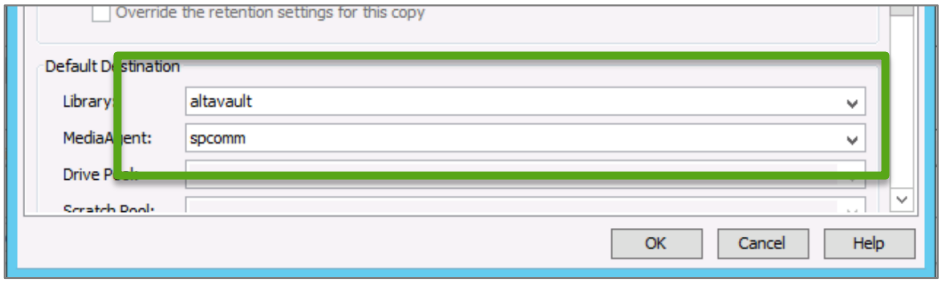
15. Enter a name for the copy.
16. Check the box next to Enable Inline Copy

Figure 26) Copy properties.



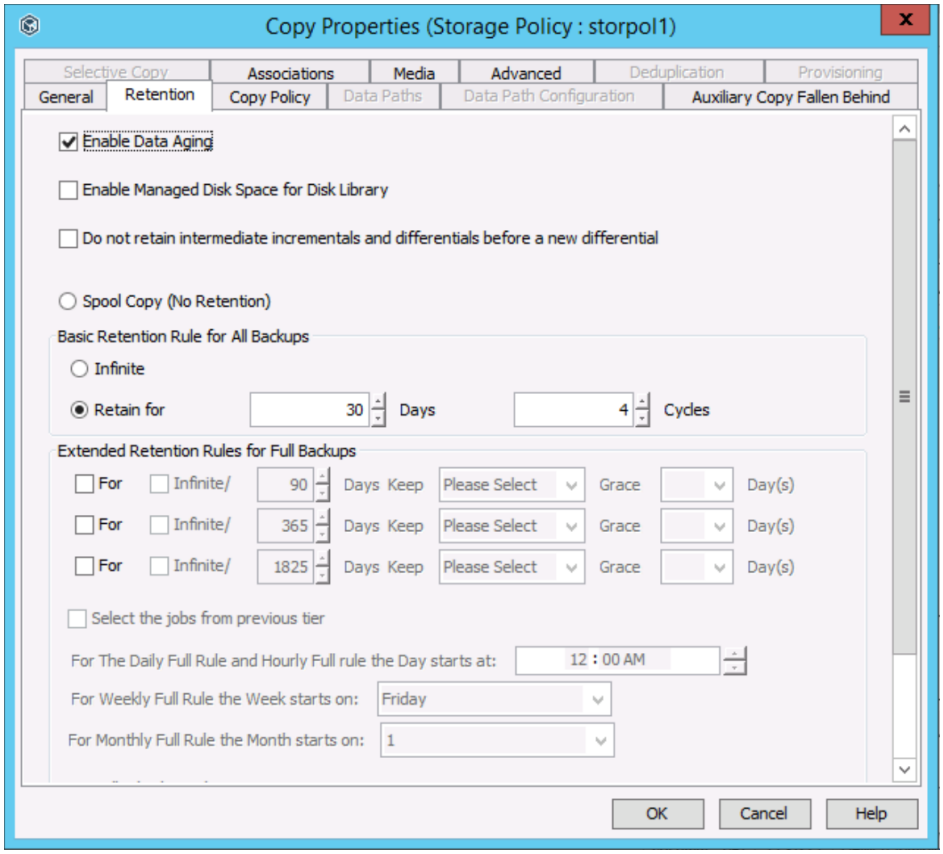
17. From the drop-down menus choose the MediaAgent that will perform the copy.

Figure 27) Copy properties media agent selection.



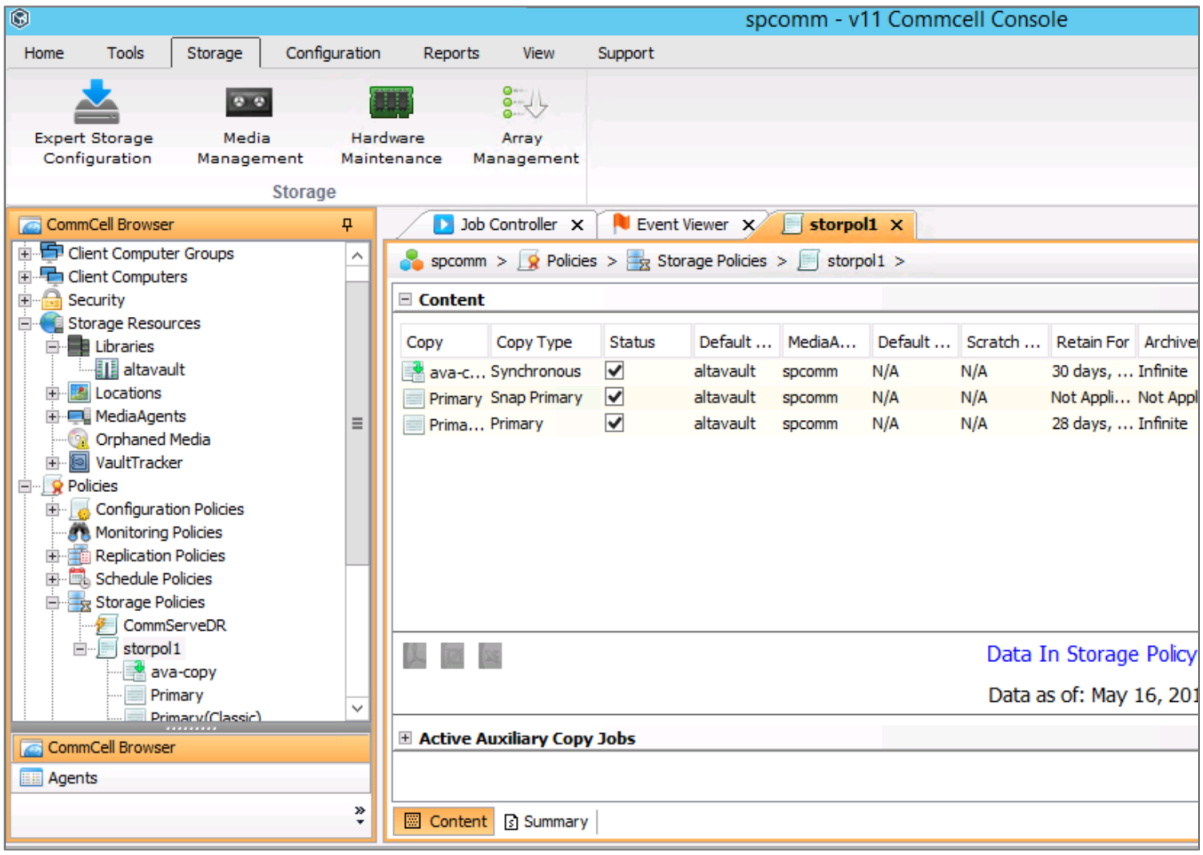
Optionally set the retention specifics for the copy stored on the AltaVault appliance (in the cloud). You can also set extended retention specifics for certain copies such as Monthly Full. For more information see the Commvault IntelliSnap for NetApp documentation.

Figure 28) Copy retention properties.



The following screenshot shows the completed storage policy with the primary Snapshot copy and the AltaVault (cloud) copy.

Figure 29) Storage policy.

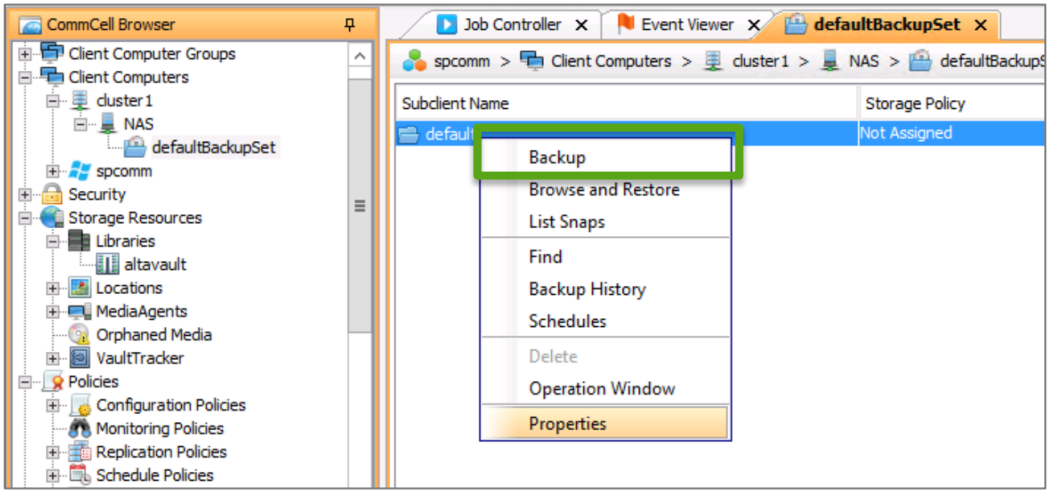


3.4 Perform a Test Backup

To test Commvault IntelliSnap for NetApp with the AltaVault appliance, run a manual backup of a client that uses a storage policy configured in the previous step.

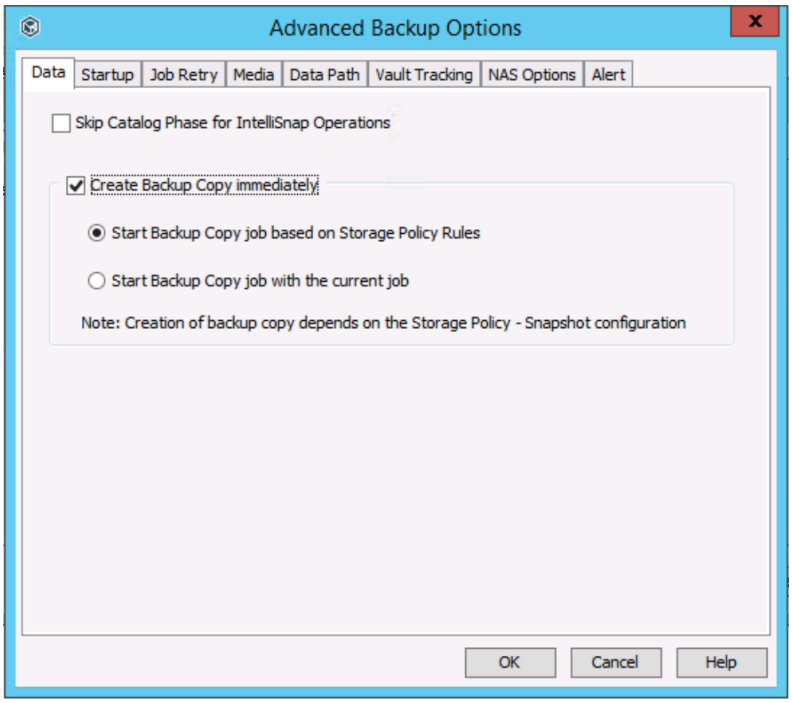
1. Expand the client to back up. In this case, the appliance contains the NAS volume to back up. Open the defaultBackupSet to show the subclients.
2. Right-click the file subclient to back up and select Backup. Use the defaults of Full Backup and Immediate job initiation.

Figure 30) Backup action.



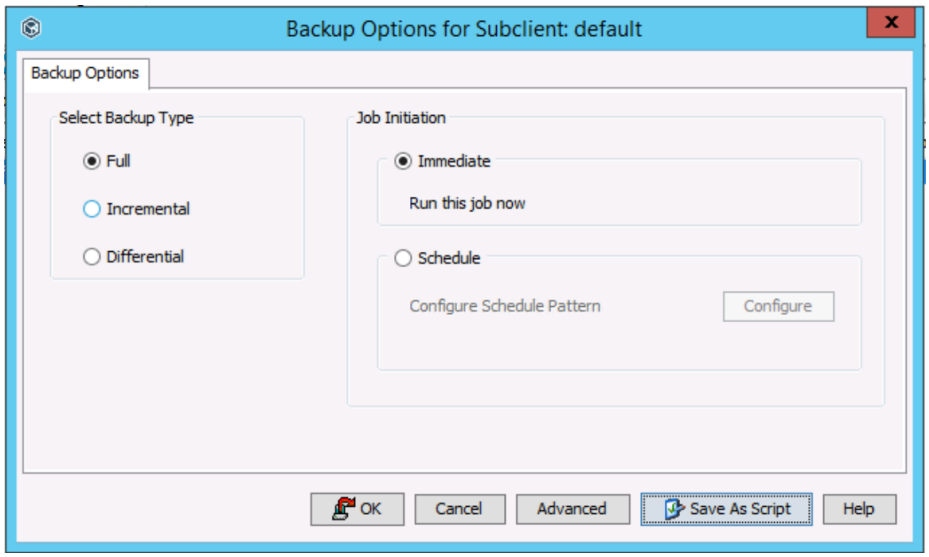
3. Click the Advanced button
4. Uncheck Skip Catalog Phase
5. Check Create Backup Copy Immediately, leave Start Backup Copy job based on Storage Policy Rules selected

Figure 31) Advanced options



6. Click OK to close the Advanced Backup Options dialog.
7. Click OK to initiate the backup.

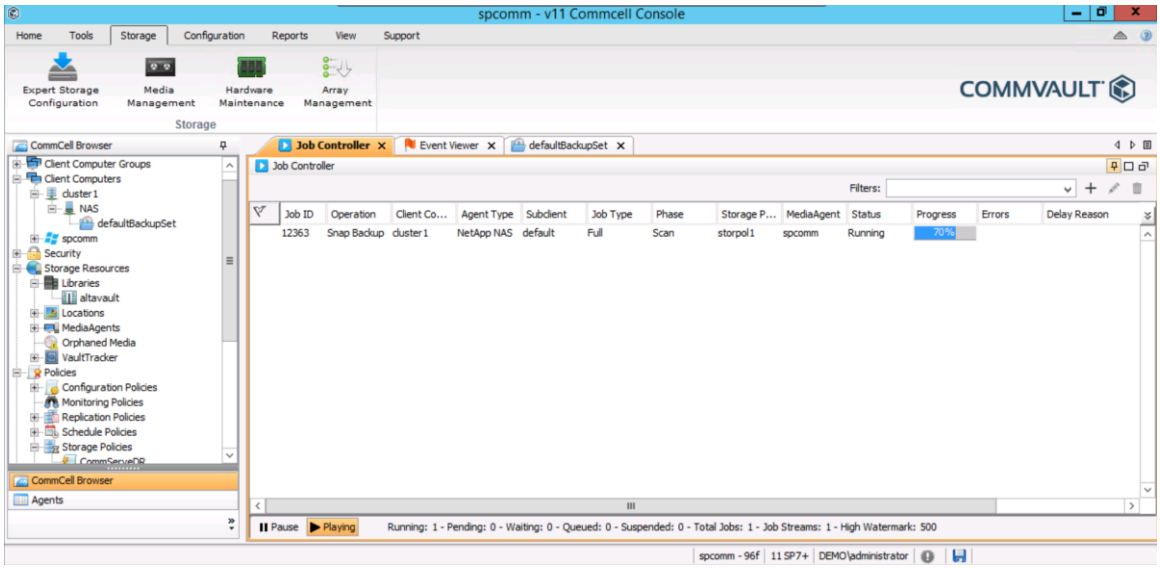
Figure 32) Backup options.



3.5 Monitor the Backup

Use the Job Controller view within the left tree of the CommCell console to monitor and control backup jobs. The current running backup jobs are reported under the right panel of the window and you can access a detailed view by right-clicking on the job name and selecting Details.

Figure 33) Job controller

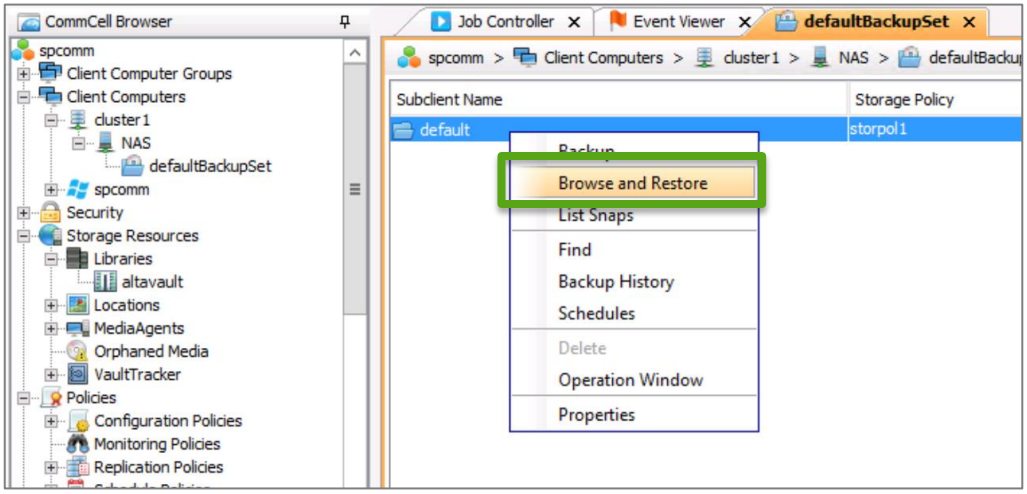


3.6 Restore a Backup

You can use the CommCell console to perform restores of backup data for clients. In this example, we set the copy precedence to 3, which is the copy job to AltaVault as specified in the Storage Policy we created earlier.

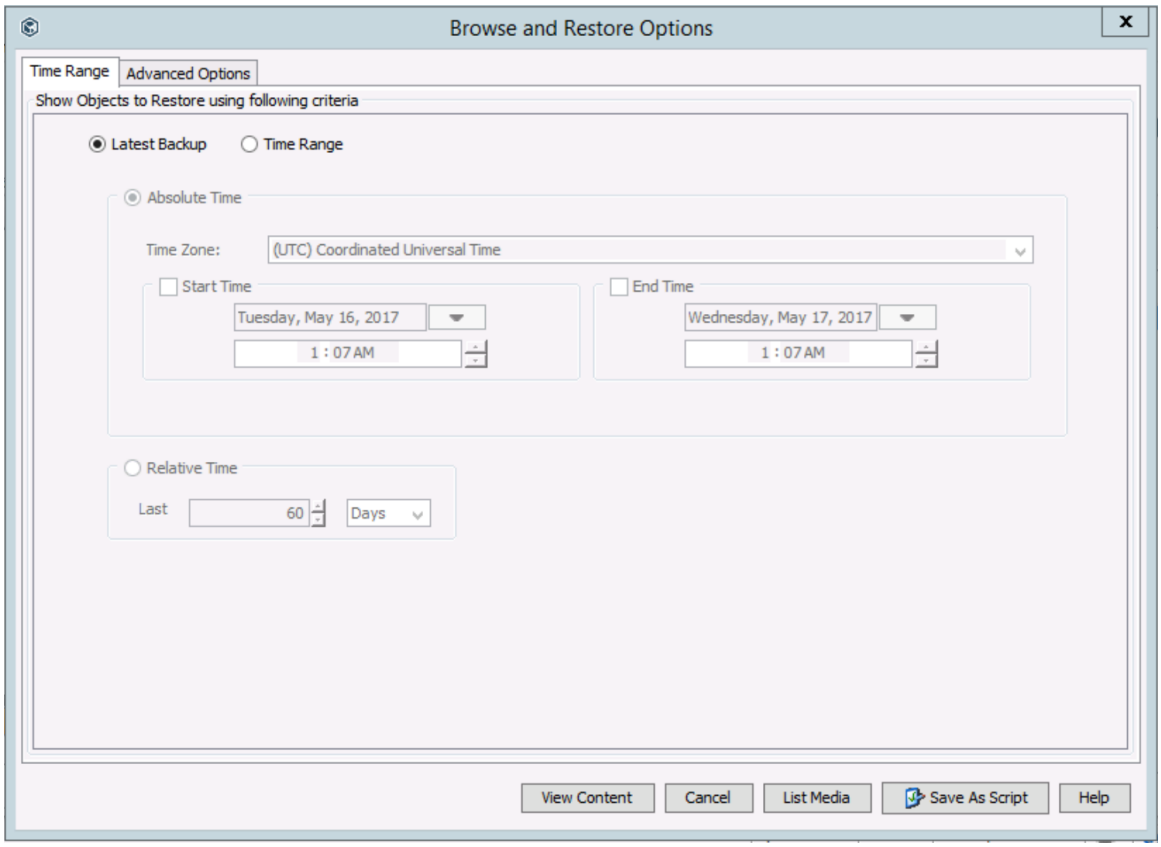
1. Click on the Browse and Restore button from the CommCell console menu to launch the recovery tool.

Figure 34) Recovery initialization.



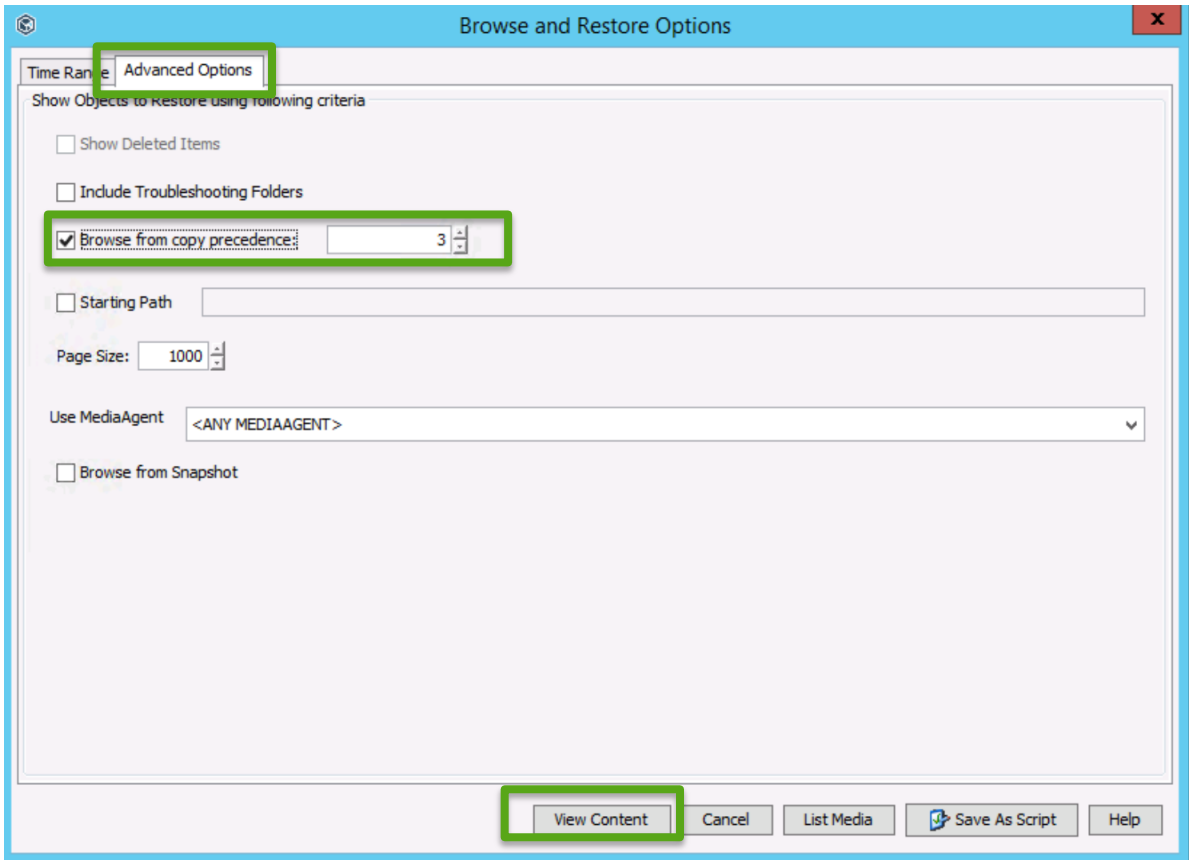
2. Provide the options you want to use when selecting what to recover.

Figure 35) Client and MediaAgent selection.



3. Click the Advanced Options tab. Select Browse from copy precedence and enter 3 for the AltaVault copy as specified in the Storage Policy. Then click View Content.

Figure 36) Browse and restore options.



4. Expand the tree and select the objects to recover. Click the Recover All Selected button to initiate the restore.
5. Monitor the progress using the Job Controller.

4 Solution Recommendations and Best Practices

This chapter lists recommendations and best practices for deploying AltaVault within Commvault IntelliSnap for NetApp environments. The best practices are not requirements, but NetApp recommends that you follow them to achieve an ideal solution experience.

4.1 Commvault IntelliSnap for NetApp Best Practices

The following table displays the recommended best practices for using Commvault IntelliSnap for NetApp with AltaVault.

Table 1) Commvault IntelliSnap for NetApp best practices.

Item	Description
Use disk libraries for AltaVault	AltaVault has been tested with Commvault IntelliSnap for NetApp disk libraries.
Use separate disk libraries for each MediaAgent	Commvault IntelliSnap for NetApp supports many MediaAgents. NetApp recommends creating a disk library and AltaVault share combination for each MediaAgent.
Use an AltaVault share and a disk library to separate datasets	AltaVault offers tuning on a per-share basis for compression, deduplication, and cache lifecycle. Configure a share and a disk library for each type of data that requires tuning settings differently than for the default. An AltaVault share for SMB or NFS allows a maximum of 500TB raw data written (before calculating deduplication and compression). Use SMB shares for Windows MediaAgents. Use NFS share for Linux/UNIX MediaAgents.
Mount path permissions - SMB	Ensure that the mount path is using an account that matches the configuration of the SMB share permissions from AltaVault. In a Windows AD 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 which matches the configured local account you specify for the AltaVault SMB share.
Allocate number of writers	This establishes how many writers are allowed by data protection clients. Tune performance by setting a value higher than 1. The value will depend on your available resources and infrastructure environment. Adjust the number of streams accordingly based on your observed performance.
Commvault IntelliSnap for NetApp backup encryption and deduplication	Commvault IntelliSnap for NetApp does not offer backup-level deduplication or client-side deduplication.
Disable compression in backup policies	NetApp highly recommends disabling backup application data optimization techniques listed at left. This not only frees resources for the backup application server, but it also allows AltaVault to optimize data most efficiently, leading to lower transmission and cloud provider storage costs.
Data ONTAP deduplication and compression	Any compression or deduplication settings in Data ONTAP should not change. Data will be returned to the original state when it is streamed to AltaVault. When a restore of streamed data occurs, the files written back to the volume will be optimized using the storage efficiency settings of the volume in which they are restored.
Chunk size	A chunk is the unit of data that the MediaAgent software uses to store data on media. AltaVault performs optimally 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 needed, adjust the size based on your requirements. Note that while very large values can improve throughput and decrease volume counts created by the backup application, it 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.
Block Size	MediaAgents can write to media using different block sizes if the operating system that is associated with the MediaAgent on which the library is configured supports a higher block size. NetApp recommends setting a value of 1MB (1024K) for Windows environments.

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 Start Menu and enter regedit to start the Windows registry editor. Provide administrative permissions if prompted. Changes and additions made within the Windows registry editor are permanent upon entry so use extreme caution when making them. 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
```

Version History

Version	Date	Document Version History
Version 1.0	September 2015	Initial version
Version 2.0	July 2017	Updated to CI4N and AVA 4.3.1

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.

Copyright Information