Technical Report

NetApp AltaVault Cloud-Integrated Storage Appliances

Solution Deployment: AltaVault with Veritas Backup Exec

Christopher Wong, NetApp

November 2017 | TR-4409

Abstract

This solution deployment guide outlines how easy it is to deploy and use a NetApp® AltaVault™ cloud-integrated storage appliance with Veritas™ Backup Exec™. 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.

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.

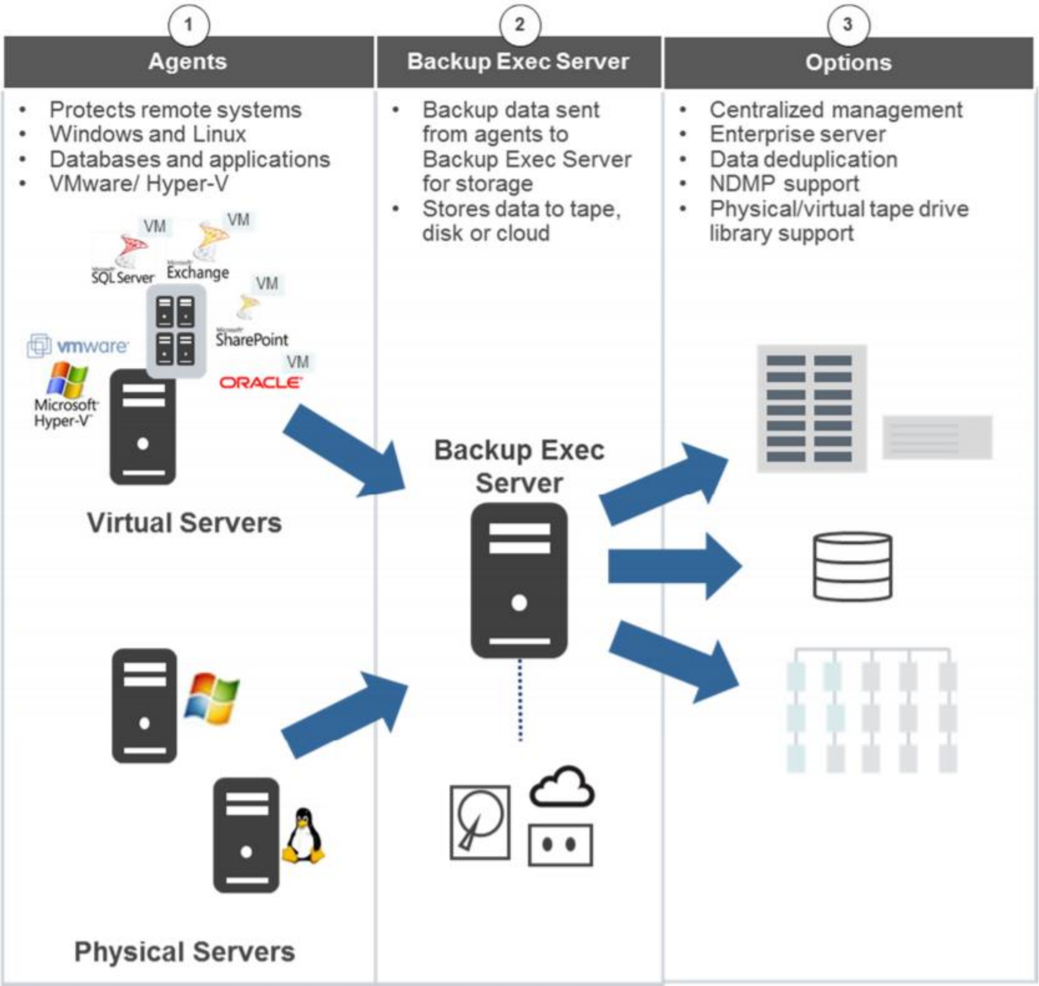
Because an AltaVault appliance is an asymmetric, stateless appliance, no hardware is needed in the cloud, and you can recover the last known good state of a broken or destroyed AltaVault appliance to a new AltaVault appliance. AltaVault appliances offer the flexibility to scale cloud storage as business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

1.2 Veritas Backup Exec Architecture Overview

Backup Exec™ is a high-performance data management solution. With its client-server design, Backup Exec provides fast, reliable backup and restore capabilities for servers and workstations across the network.

Backup Exec submits backup, restore, and utility operations using the Backup Exec Administration Console. Administrators can run the Administration Console from the server (Windows Server with storage hardware attached) or from a remote computer. After jobs are created, the Backup Exec server components on the server process the jobs. All interaction with Backup Exec, such as submitting jobs, viewing results, and performing device and media operations, is performed through the Administration Console.

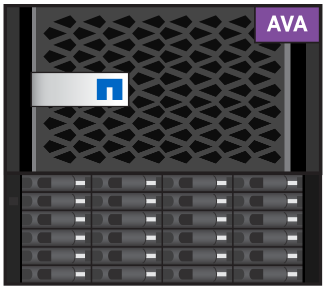
Figure 1) Backup Exec solution illustration.



1.3 AltaVault Appliance Overview

Figure 2 is an illustration of the AltaVault appliance.

Figure 2) 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.

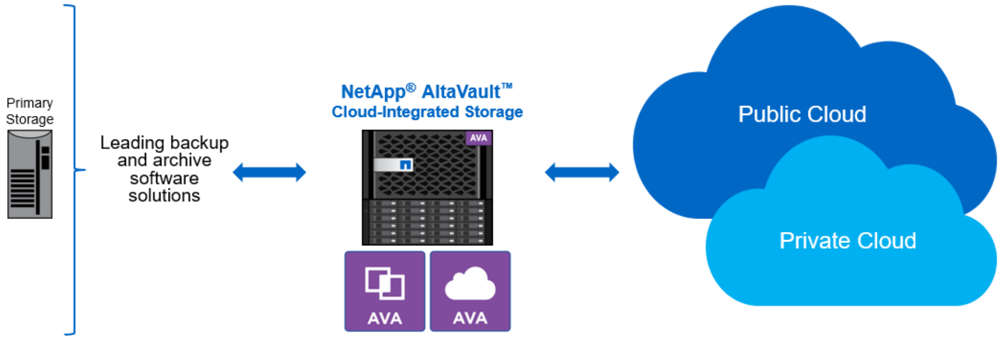
2 Deploy and Configure AltaVault with Backup Exec

Backup Exec 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 3 illustrates the AltaVault solution configuration topology. Refer to the NetApp Interoperability Matrix for current versions of the backup application supported with AltaVault.

Figure 3) 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 Backup Exec server. This server, along with clients, need minimum hardware features as identified by the backup application. Check the Veritas support site and related compatibility lists where applicable.
2. Obtain server systems and related software media supported by Backup Exec 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.

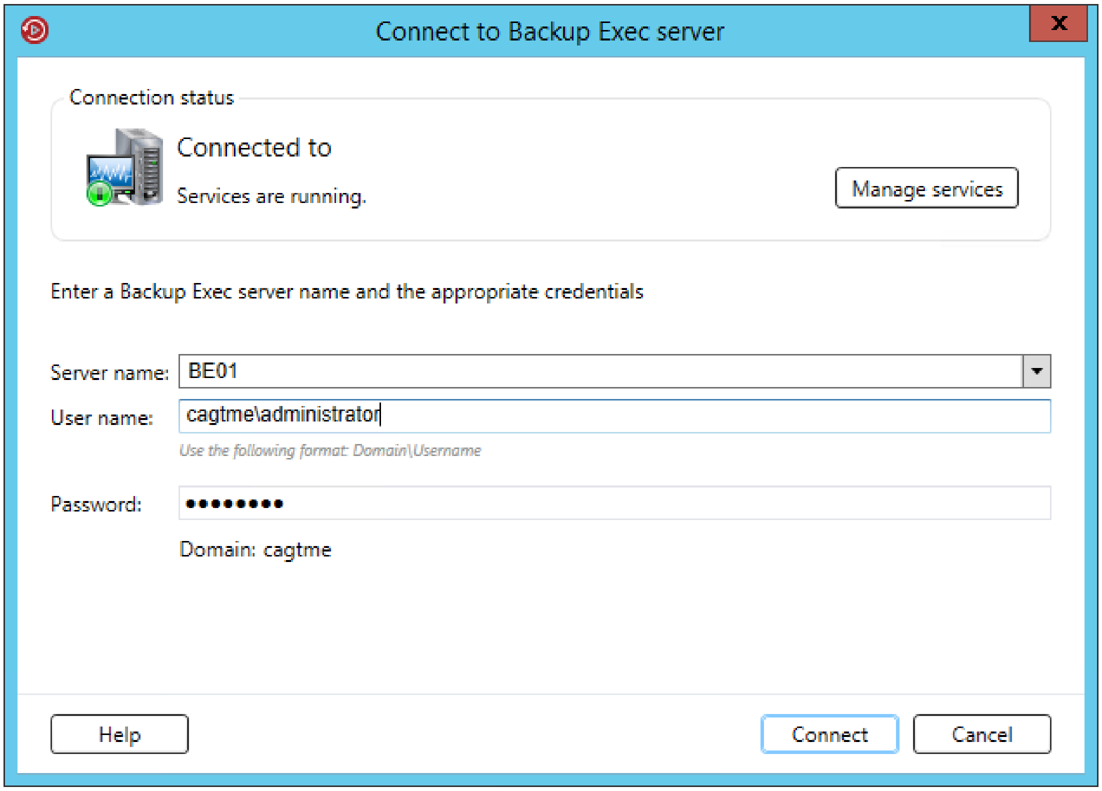
6. Verify that all LAN and WAN connections are functioning to and from your Internet and cloud storage providers.
7. If applicable, have available a Windows directory service (Active Directory) or UNIX Kerberos server.

3 Configure Backup Exec

3.1 Create a Disk Folder

A disk folder is a label that Backup Exec associates with physical storage. The following describes the steps to create a disk folder and associate it to the AltaVault appliance. These steps use the best practice configuration for the Backup Exec with the AltaVault appliance.

1. Open management console, select the Backup Exec icon from the upper left corner, and select Connect to Backup Exec Server (if not local to the management console system). Then enter the host name and Windows login credentials of the system that hosts the Backup Exec server to which you are connecting.



Connect to Backup Exec server

Connection status

Connected to

Services are running.

Manage services

Enter a Backup Exec server name and the appropriate credentials

Server name: BE01

User name: cagtme\administrator

Use the following format: Domain\Username

Password: ●●●●●●●●●

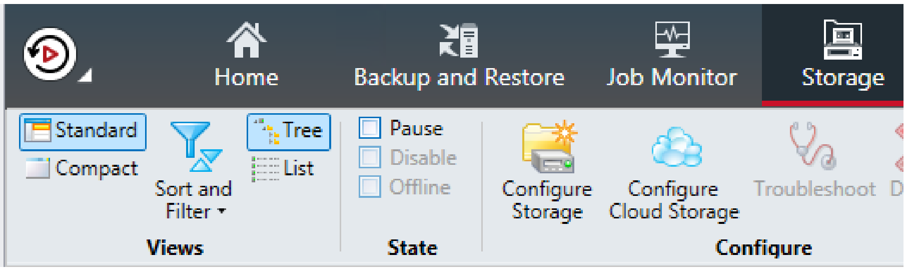
Domain: cagtme

Help

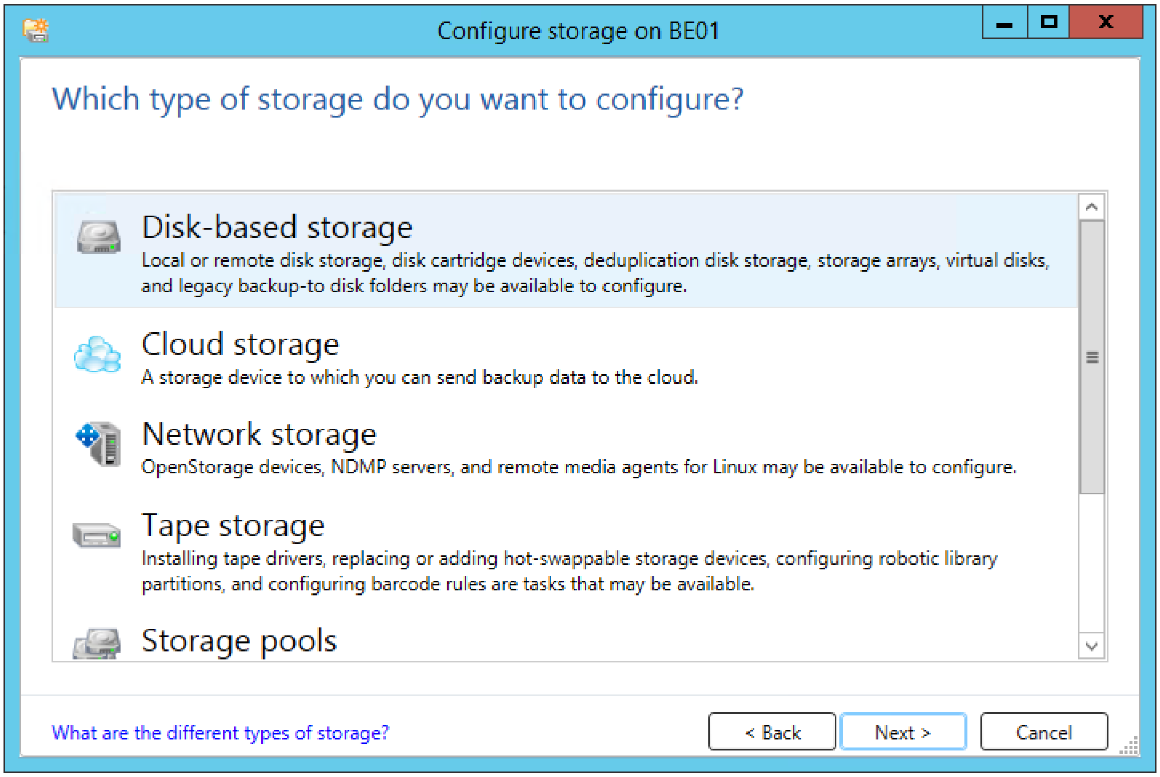
Connect

Cancel

2. Browse to the menu Storage and click the submenu Configure Storage.



3. When the wizard appears, select Disk-based storage from the storage types available and click Next.



Configure storage on BE01

Which type of storage do you want to configure?

Disk-based storage
Local or remote disk storage, disk cartridge devices, deduplication disk storage, storage arrays, virtual disks, and legacy backup-to disk folders may be available to configure.

Cloud storage
A storage device to which you can send backup data to the cloud.

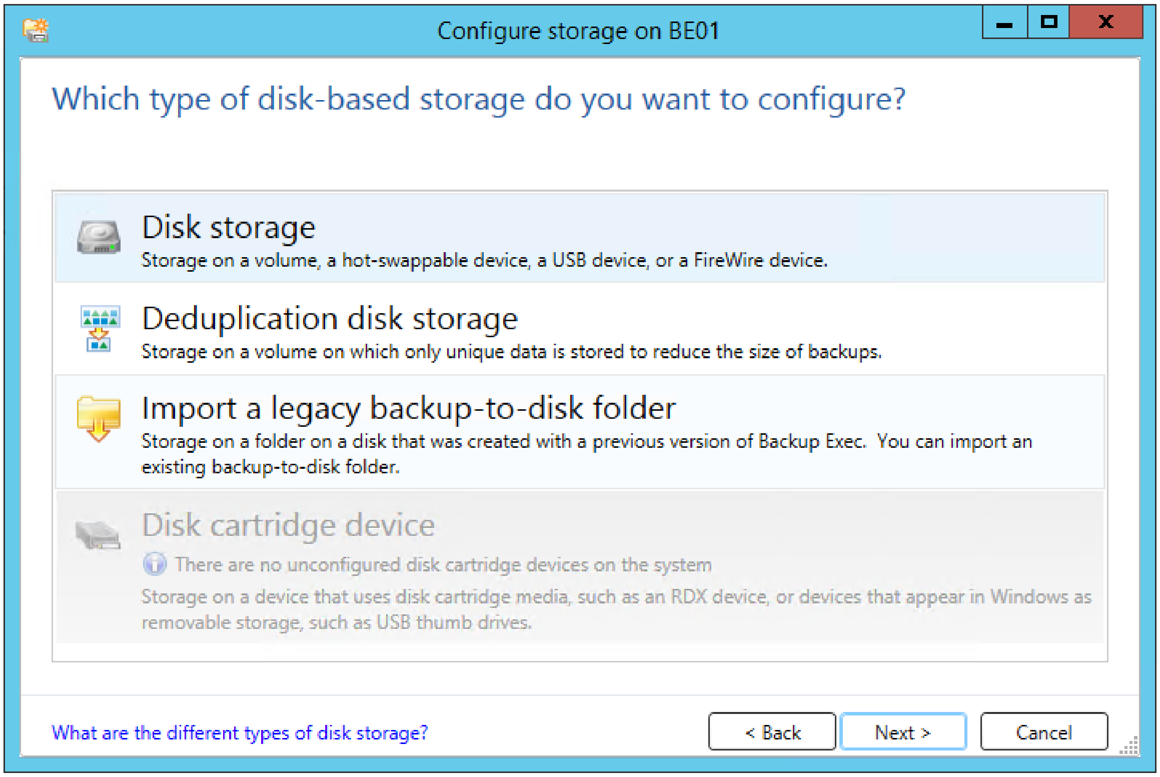
Network storage
OpenStorage devices, NDMP servers, and remote media agents for Linux may be available to configure.

Tape storage
Installing tape drivers, replacing or adding hot-swappable storage devices, configuring robotic library partitions, and configuring barcode rules are tasks that may be available.

Storage pools

What are the different types of storage?

4. In the next panel of the wizard, select Disk Storage and click Next.



Configure storage on BE01

Which type of disk-based storage do you want to configure?

Disk storage
Storage on a volume, a hot-swappable device, a USB device, or a FireWire device.

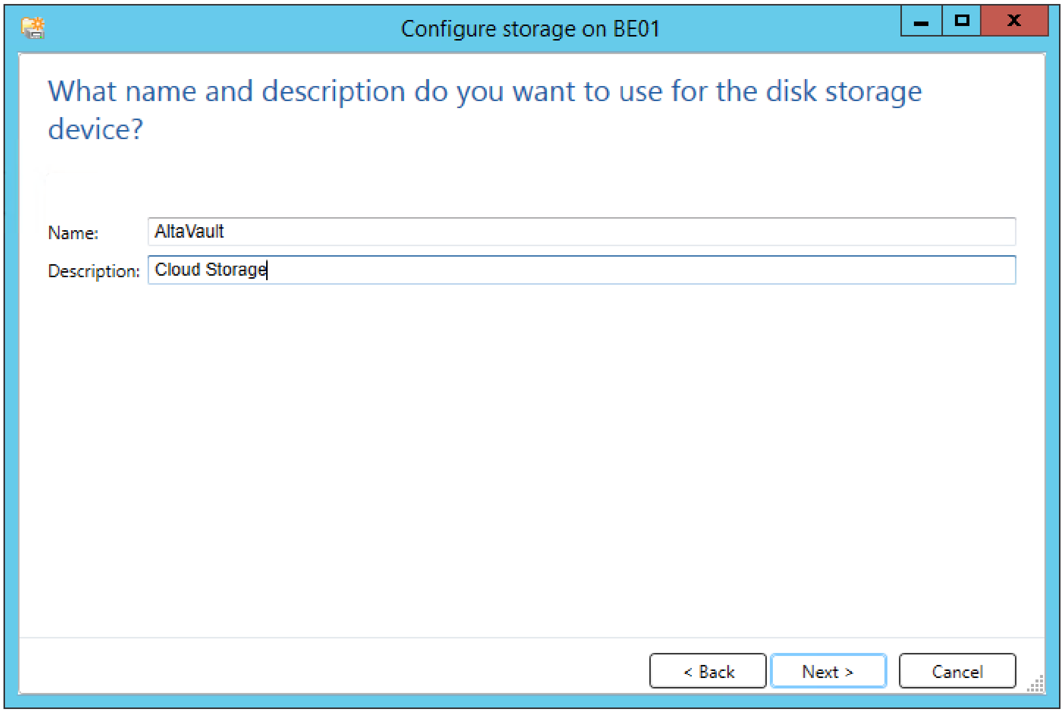
Deduplication disk storage
Storage on a volume on which only unique data is stored to reduce the size of backups.

Import a legacy backup-to-disk folder
Storage on a folder on a disk that was created with a previous version of Backup Exec. You can import an existing backup-to-disk folder.

Disk cartridge device
There are no unconfigured disk cartridge devices on the system
Storage on a device that uses disk cartridge media, such as an RDX device, or devices that appear in Windows as removable storage, such as USB thumb drives.

What are the different types of disk storage?

5. Provide a storage name and description and then click Next.



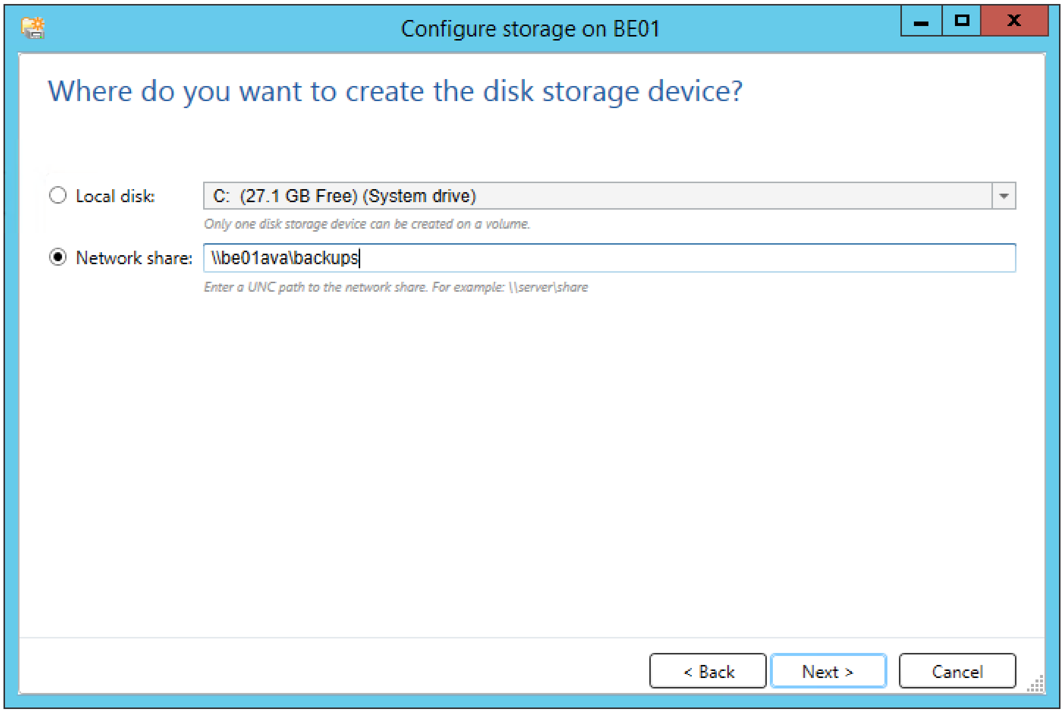
Configure storage on BE01

What name and description do you want to use for the disk storage device?

Name: AltaVault

Description: Cloud Storage

6. Select Network Share, enter in the AltaVault SMB target created previously, then click Next. Note: The share name might have to use the DNS value assigned to the data interface and not the IP address assigned to the data interface. Configure DNS or manually add entries to the Windows Hosts file as appropriate.



Configure storage on BE01

Where do you want to create the disk storage device?

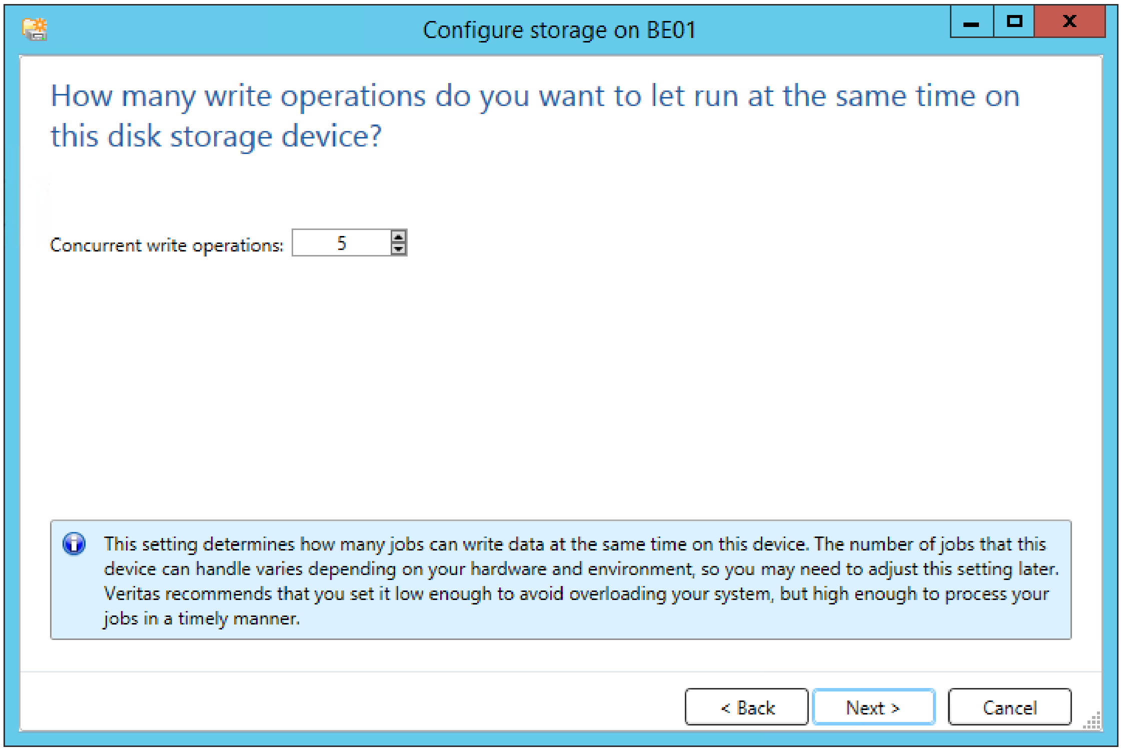
○ Local disk: C: (27.1 GB Free) (System drive)

Only one disk storage device can be created on a volume.

● Network share: \\be01ava\backups

Enter a UNC path to the network share. For example: \\server\share

7. Tune the number of concurrent write operations. To ensure concurrency, set a value higher than 1 in this field. The value will depend on your available resources and infrastructure environment. Adjust the number of streams accordingly based on your observed performance. Click Next.

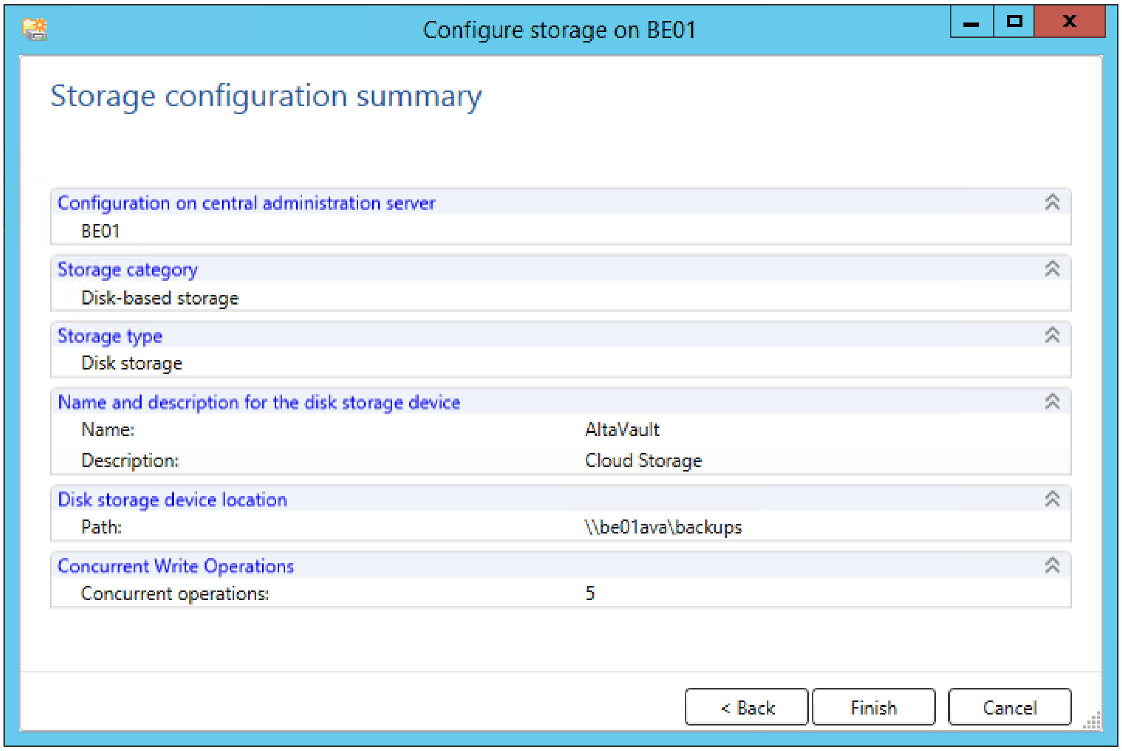


How many write operations do you want to let run at the same time on this disk storage device?

Concurrent write operations: 5

This setting determines how many jobs can write data at the same time on this device. The number of jobs that this device can handle varies depending on your hardware and environment, so you may need to adjust this setting later. Veritas recommends that you set it low enough to avoid overloading your system, but high enough to process your jobs in a timely manner.

8. Click Finish to confirm the configuration and create the AltaVault disk target storage device.



Storage configuration summary

Configuration on central administration server
BE01

Storage category
Disk-based storage

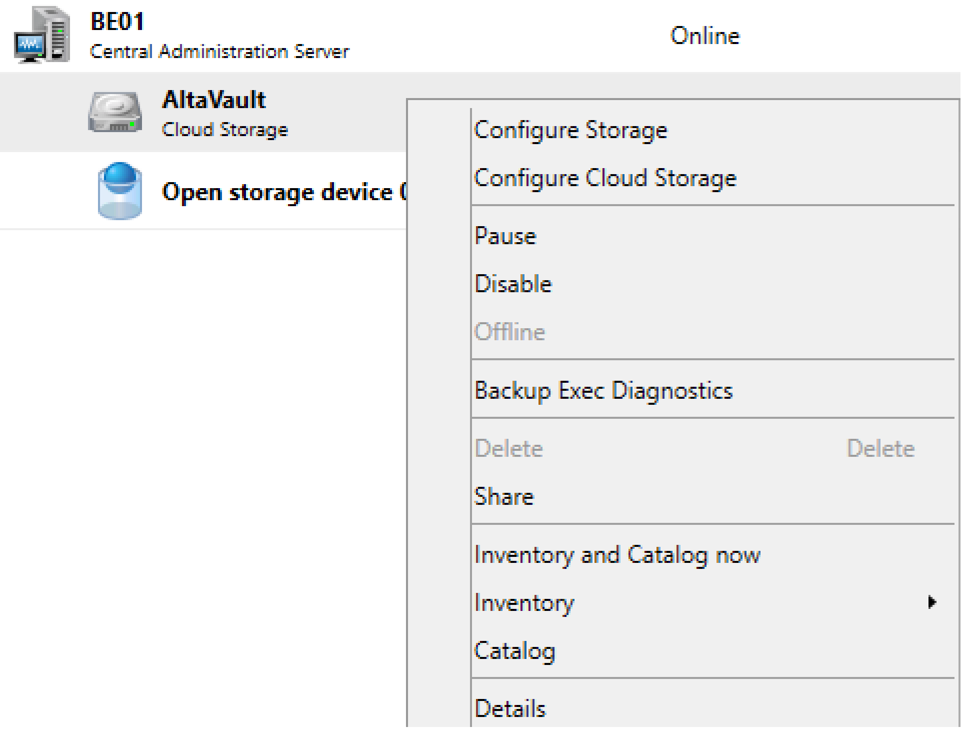
Storage type
Disk storage

Name and description for the disk storage device
Name: AltaVault
Description: Cloud Storage

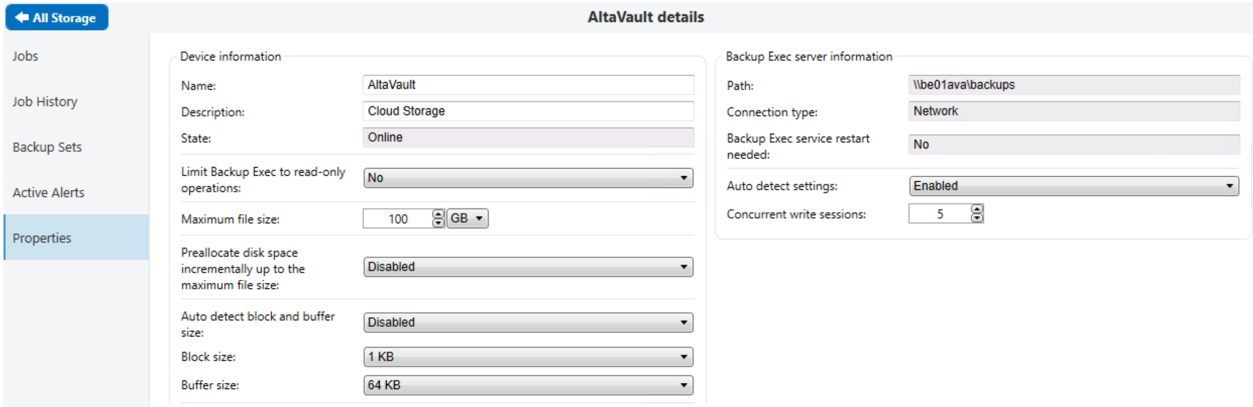
Disk storage device location
Path: \\be01ava\backups

Concurrent Write Operations
Concurrent operations: 5

9. Modify the new disk storage properties by right-clicking the storage device and selecting Details.



10. Set the following options as described next, then click Apply.



AltaVault details

Device information

Name: AltaVault
Description: Cloud Storage
State: Online
Limit Backup Exec to read-only operations: No
Maximum file size: 100 GB
Preallocate disk space incrementally up to the maximum file size: Disabled
Auto detect block and buffer size: Disabled
Block size: 1 KB
Buffer size: 64 KB

Backup Exec server information

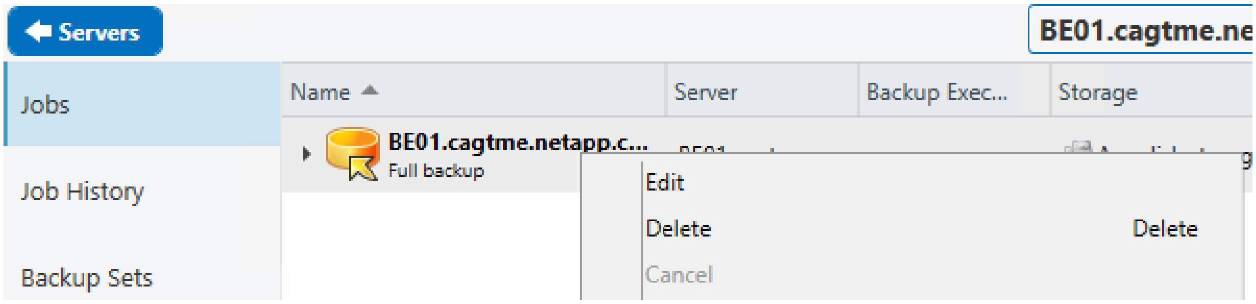
Path: \\be01ava\backups
Connection type: Network
Backup Exec service restart needed: No
Auto detect settings: Enabled
Concurrent write sessions: 5

- **Maximum File Size.** The maximum size object that Backup Exec can create to store backups. NetApp recommends using 100GB objects for the best balance of backup and restore performance.
- **Preallocate Disk Space Incrementally Up to the Maximum File Size.** Leave this selection to the default value of Disabled.
- **Block Size/Buffer Size.** Depending on your performance, you can set this value up to 1024KB (1MB).
- **Concurrent Write Sessions.** The maximum concurrent write sessions specifies the number of jobs that can be written to the storage unit at a time. To ensure concurrency set a value higher than 1 in this field. The value will depend on your available resources and infrastructure environment. Adjust the number of streams accordingly based on your observed performance. Backup Exec can split large backup jobs from a client into multiple jobs for better throughput.

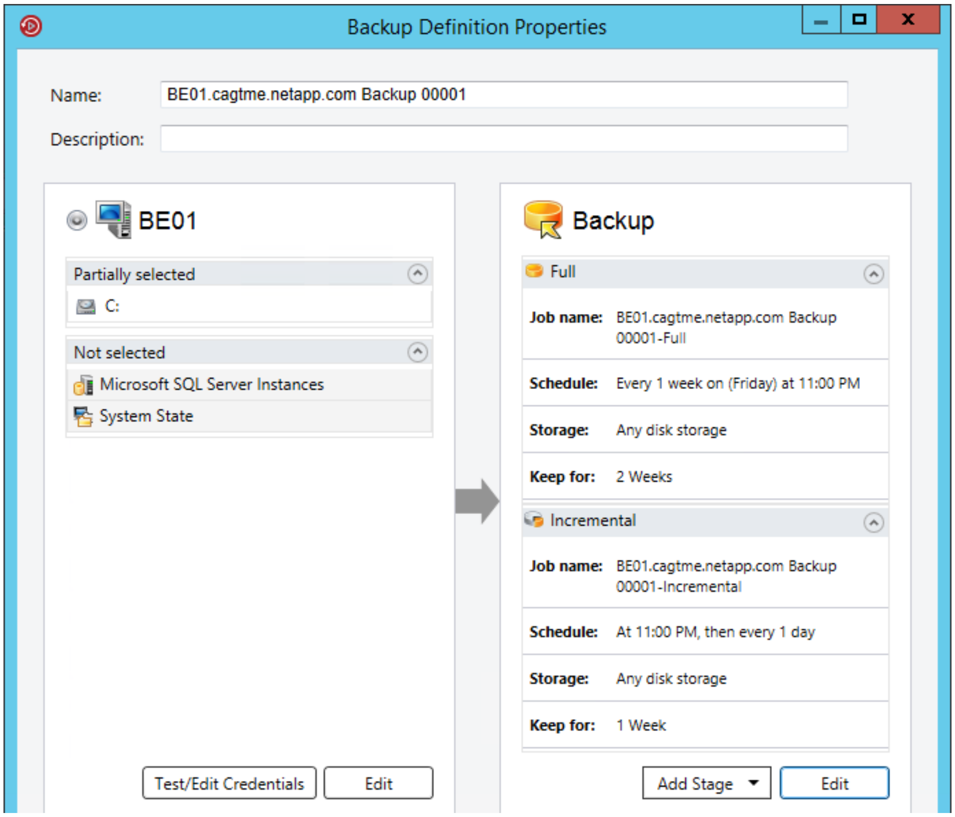
3.2 Modify a Backup Job or Policy

Backup Exec backups can be performed as independent jobs or under the control of a policy. Using policies helps align similar aspects of associated backup job properties, so that separate backup jobs do not need to be configured individually. Among the properties that can be configured for a job or a policy is the target to which the backup data is written. Use the following steps to associate a Backup Exec job or policy to a disk folder based on AltaVault.

1. Click the Backup and Restore button, select a server, right-click an existing job name, and select Edit Backups.



2. Click Edit from the Backup portion of the properties page that appears.


Backup Definition Properties

Name: BE01.cagtme.netapp.com Backup 00001

Description:

BE01

Partially selected
C:

Not selected
Microsoft SQL Server Instances
System State

Backup

Full

Job name: BE01.cagtme.netapp.com Backup 00001-Full

Schedule: Every 1 week on (Friday) at 11:00 PM

Storage: Any disk storage

Keep for: 2 Weeks

Incremental

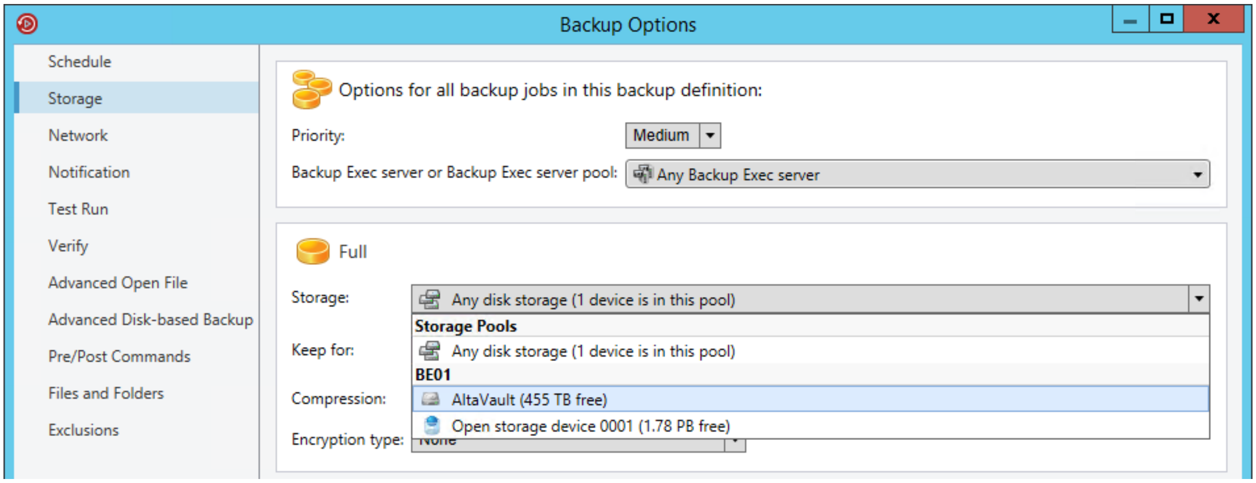
Job name: BE01.cagtme.netapp.com Backup 00001-Incremental

Schedule: At 11:00 PM, then every 1 day

Storage: Any disk storage

Keep for: 1 Week

3. Select Storage from the left tree and, in the Storage drop-down list on the right, select the AltaVault storage target from the drop-down list for both full and incremental backups.



Options for all backup jobs in this backup definition:

Priority: Medium

Backup Exec server or Backup Exec server pool: Any Backup Exec server

Full

Storage: Any disk storage (1 device is in this pool)

Storage Pools

Any disk storage (1 device is in this pool)

BE01

AltaVault (455 TB free)

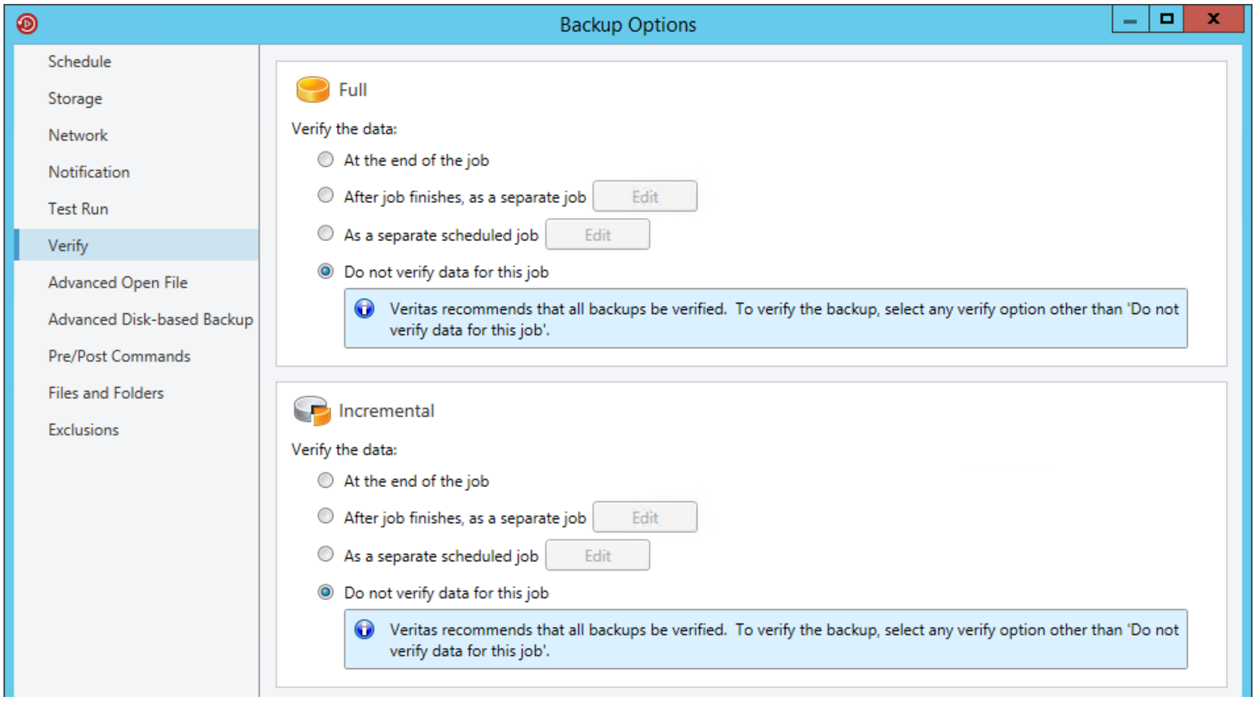
Open storage device 0001 (1.78 PB free)

Keep for:

Compression:

Encryption type: None

4. Select Verify from the left tree and on the right panel make sure that Do not verify data for this job is selected. Click OK to close the properties page.



Full

Verify the data:

○ At the end of the job

○ After job finishes, as a separate job

○ As a separate scheduled job

● Do not verify data for this job

Veritas recommends that all backups be verified. To verify the backup, select any verify option other than 'Do not verify data for this job'.

Incremental

Verify the data:

○ At the end of the job

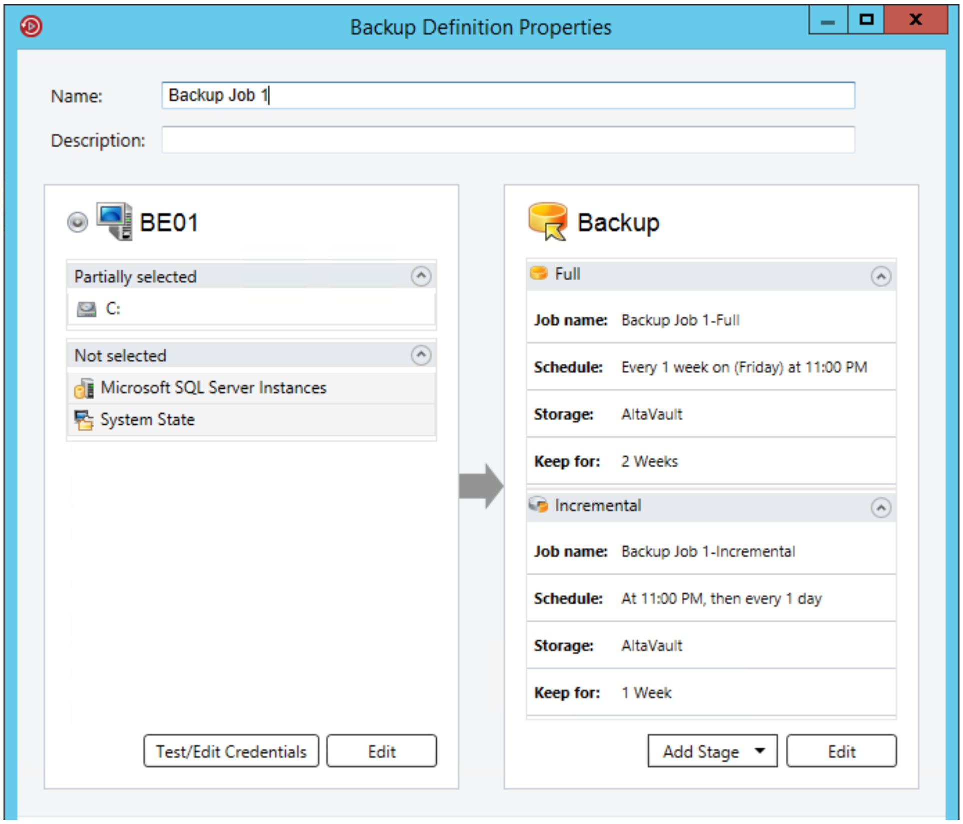
○ After job finishes, as a separate job

○ As a separate scheduled job

● Do not verify data for this job

Veritas recommends that all backups be verified. To verify the backup, select any verify option other than 'Do not verify data for this job'.

5. Confirm the storage configuration change in the properties window and then click the OK button to close the window.



Name: Backup Job 1

Description:

BE01

Partially selected
C:

Not selected
Microsoft SQL Server Instances
System State

Backup

Full

Job name: Backup Job 1-Full

Schedule: Every 1 week on (Friday) at 11:00 PM

Storage: AltaVault

Keep for: 2 Weeks

Incremental

Job name: Backup Job 1-Incremental

Schedule: At 11:00 PM, then every 1 day

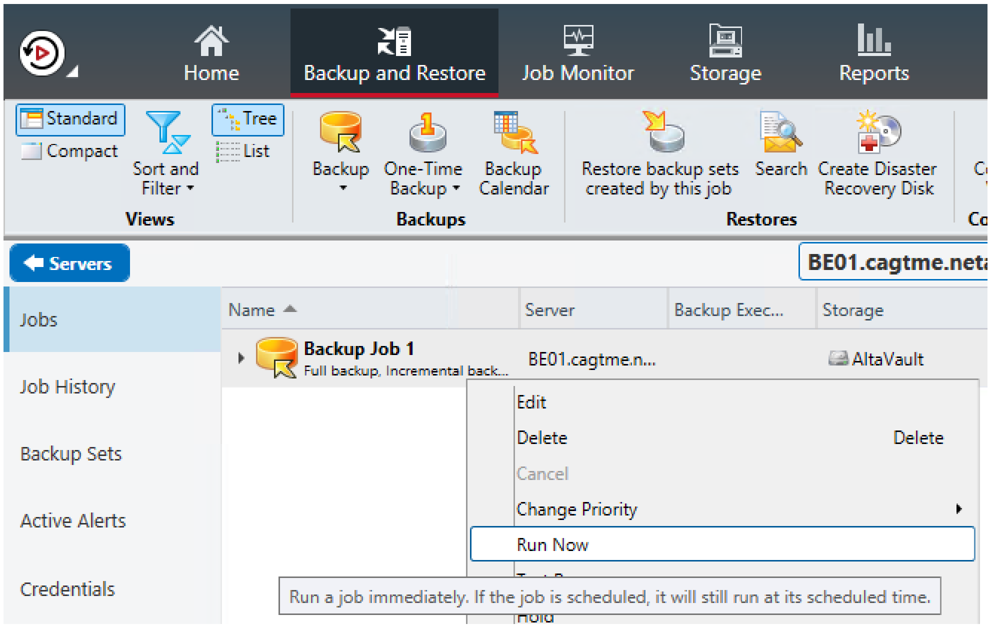
Storage: AltaVault

Keep for: 1 Week

3.3 Perform a Test Backup

To test Backup Exec with the AltaVault appliance, you can run a manual backup of a job modified in the previous step.

1. To run a manual backup, right-click the backup name and select Run Now.

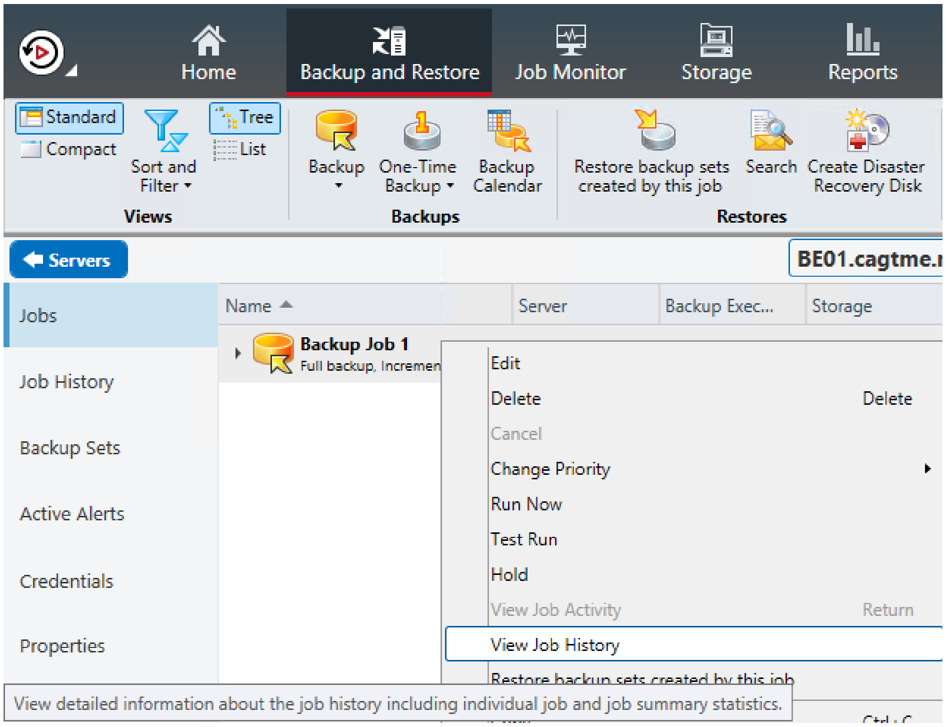


Name	Server	Backup Exec...	Storage
Backup Job 1 Full backup, Incremental back...	BE01.cagtme.n...		AltaVault

Run a job immediately. If the job is scheduled, it will still run at its scheduled time.

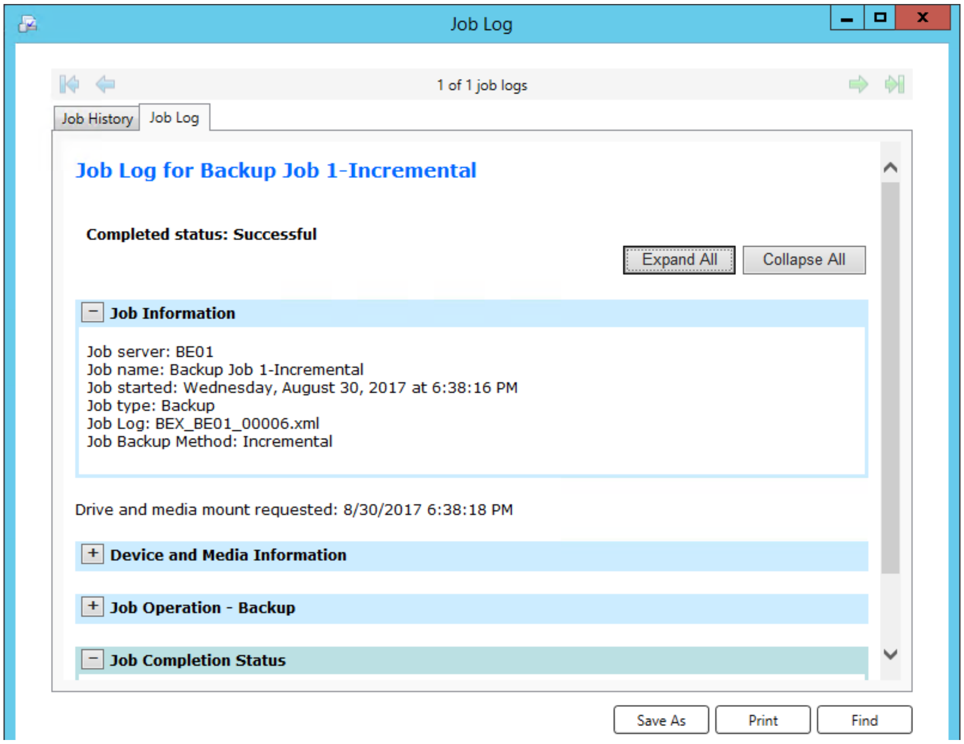
3.4 Monitor the Backup

1. Use the Job or Job History selections from the Backup and Restore tab to monitor and control Backup Exec jobs, services, processes, and drive. Alternatively, right-click the backup job that is running and select View Job Activity.



View detailed information about the job history including individual job and job summary statistics.

2. The Job Activity details dialog box that appears contains detailed job information. Information about the elapsed time, transfer rate (in KBps), and current object processed is provided.



Job Log for Backup Job 1-Incremental

Completed status: Successful

Job Information

Job server: BE01
Job name: Backup Job 1-Incremental
Job started: Wednesday, August 30, 2017 at 6:38:16 PM
Job type: Backup
Job Log: BEX_BE01_00006.xml
Job Backup Method: Incremental

Drive and media mount requested: 8/30/2017 6:38:18 PM

Device and Media Information

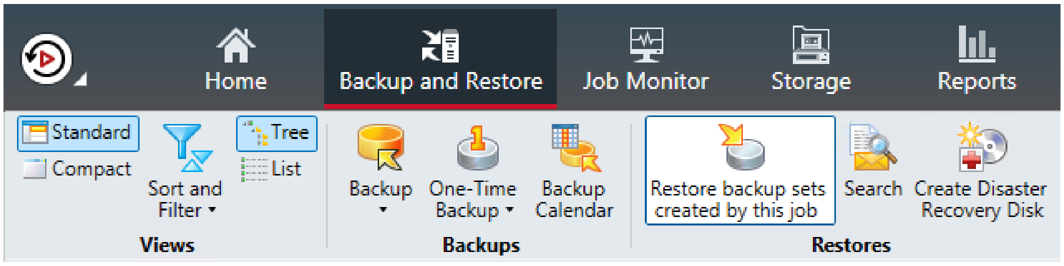
Job Operation - Backup

Job Completion Status

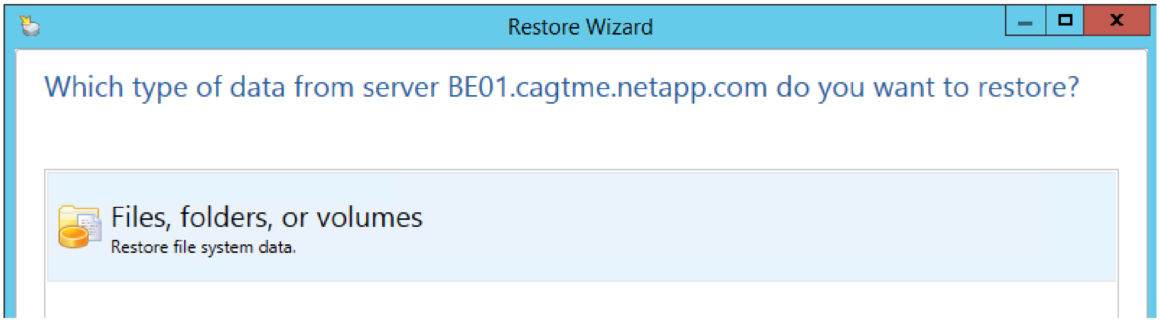
3.5 Restore a Backup

When the backup is complete, perform a restore to validate that the AltaVault appliance can restore the backed-up data.

1. From the Backup Exec management console, select the Backup and Restore tab and select Restore backup sets created by this job.



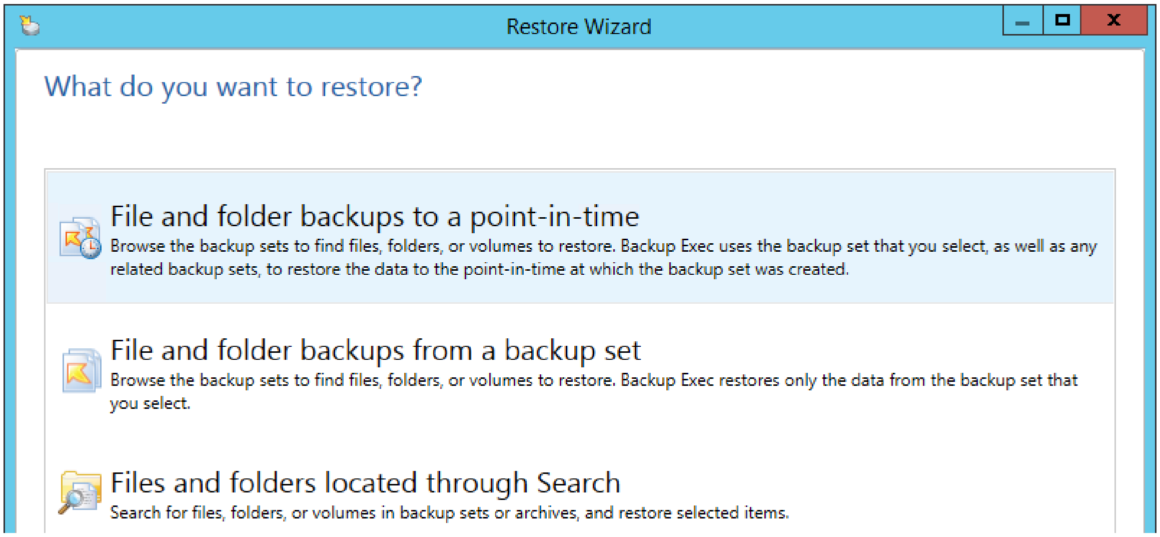
2. Select Files, folders, or volumes from the selection list and click Next.


Restore Wizard

Which type of data from server BE01.cagtme.netapp.com do you want to restore?

Files, folders, or volumes
Restore file system data.

3. In the next panel, select the restore method you want. Click Next.


Restore Wizard

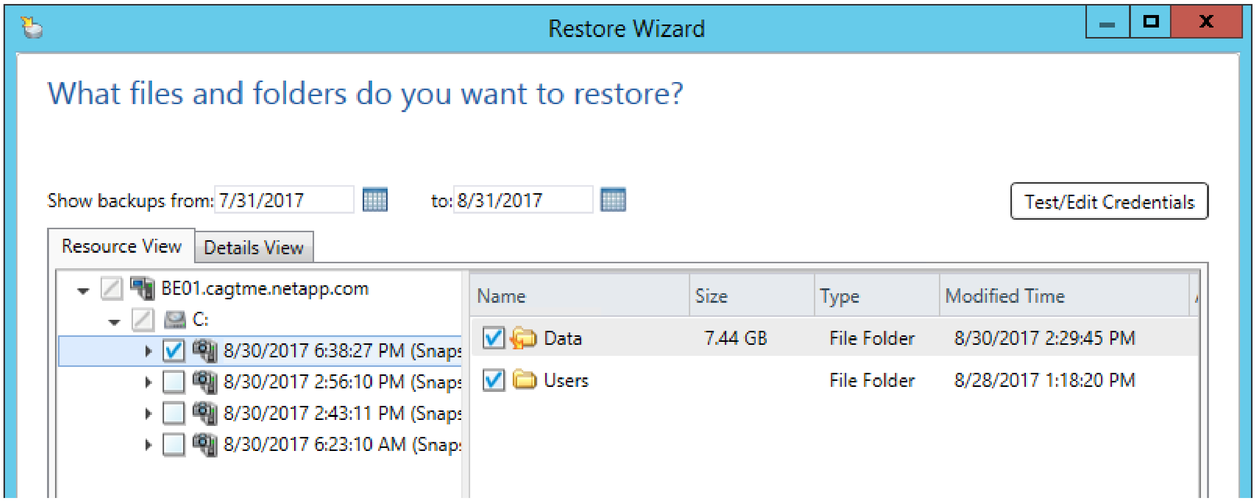
What do you want to restore?

File and folder backups to a point-in-time
Browse the backup sets to find files, folders, or volumes to restore. Backup Exec uses the backup set that you select, as well as any related backup sets, to restore the data to the point-in-time at which the backup set was created.

File and folder backups from a backup set
Browse the backup sets to find files, folders, or volumes to restore. Backup Exec restores only the data from the backup set that you select.

Files and folders located through Search
Search for files, folders, or volumes in backup sets or archives, and restore selected items.

4. Find the specific backup job to restore, select the contents to restore, and then click Next.



Restore Wizard

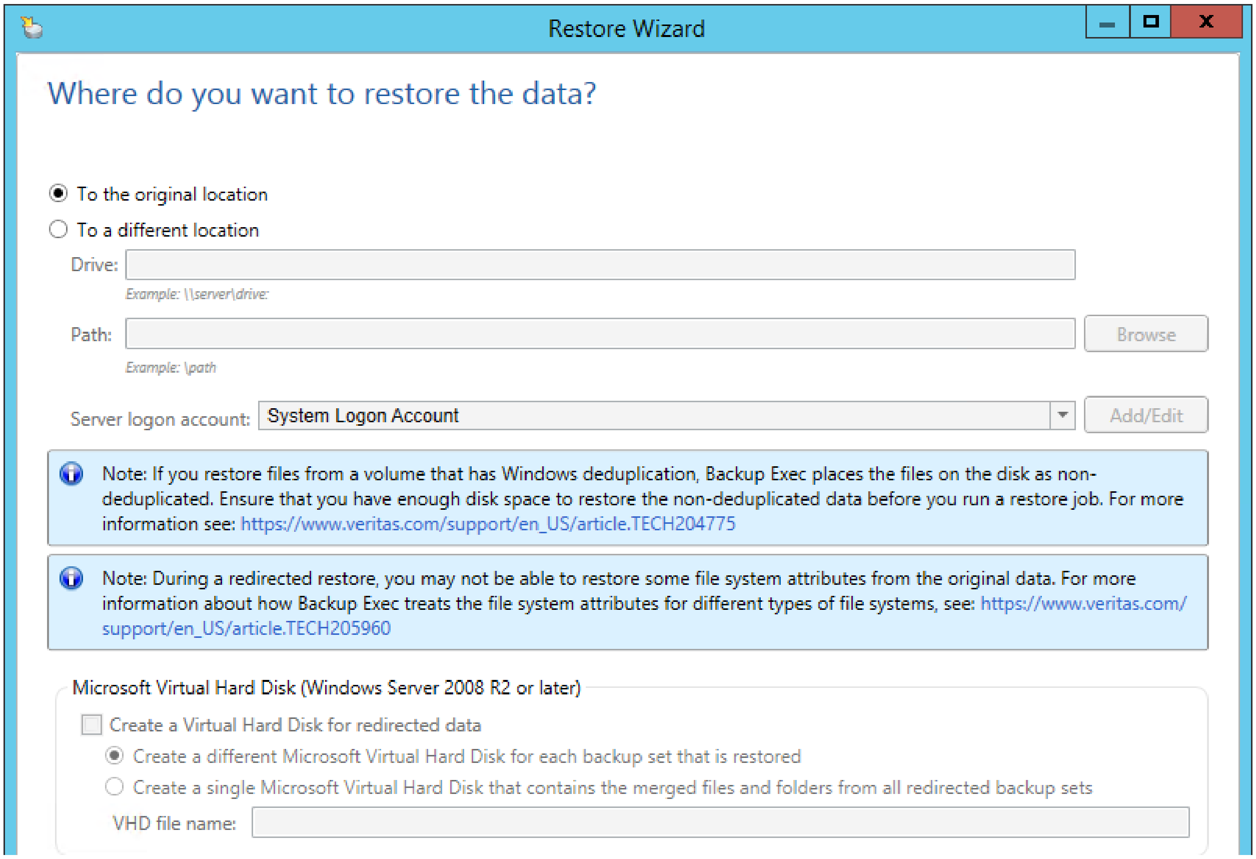
What files and folders do you want to restore?

Show backups from: 7/31/2017 to: 8/31/2017

- BE01.cagtme.netapp.com
  - C:
    - ☑ 8/30/2017 6:38:27 PM (Snaps
    - □ 8/30/2017 2:56:10 PM (Snaps
    - □ 8/30/2017 2:43:11 PM (Snaps
    - □ 8/30/2017 6:23:10 AM (Snaps

Name	Size	Type	Modified Time
☑ Data	7.44 GB	File Folder	8/30/2017 2:29:45 PM
☑ Users		File Folder	8/28/2017 1:18:20 PM

5. Select the restore location and then click Next.



Restore Wizard

Where do you want to restore the data?

● To the original location

○ To a different location

Drive:

Example: \\server\drive:

Path:

Example: \path

Server logon account: System Logon Account

Note: If you restore files from a volume that has Windows deduplication, Backup Exec places the files on the disk as non-deduplicated. Ensure that you have enough disk space to restore the non-deduplicated data before you run a restore job. For more information see: https://www.veritas.com/support/en_US/article.TECH204775

Note: During a redirected restore, you may not be able to restore some file system attributes from the original data. For more information about how Backup Exec treats the file system attributes for different types of file systems, see: https://www.veritas.com/support/en_US/article.TECH205960

Microsoft Virtual Hard Disk (Windows Server 2008 R2 or later)

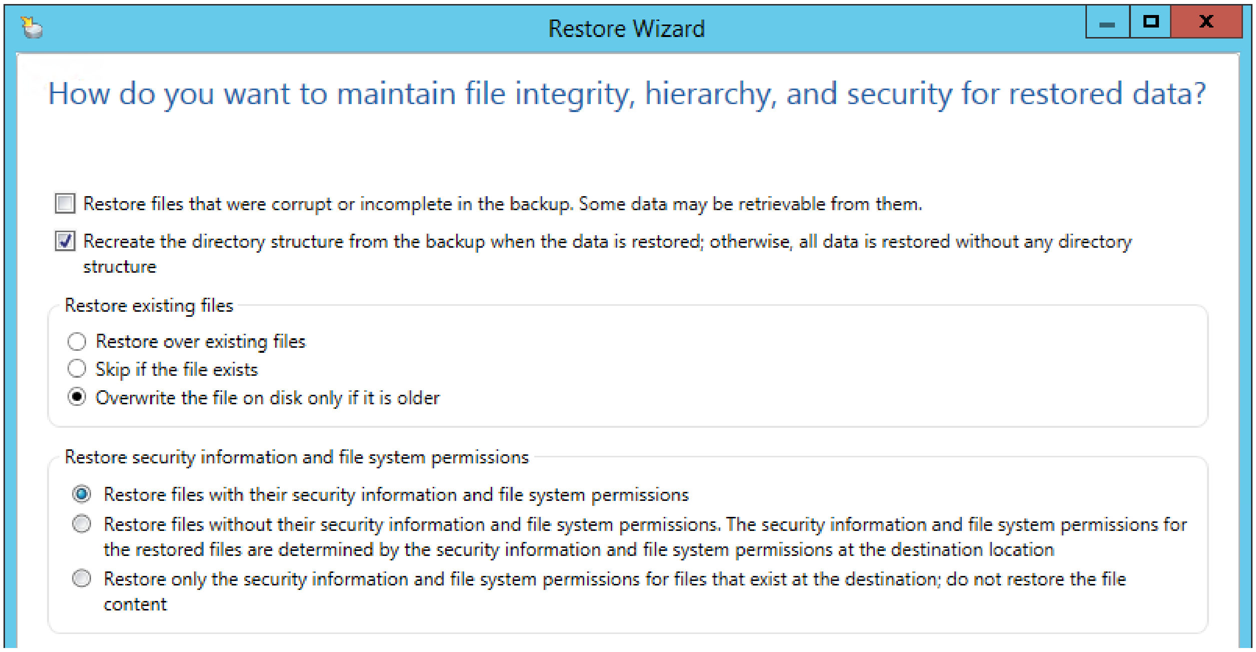
□ Create a Virtual Hard Disk for redirected data

● Create a different Microsoft Virtual Hard Disk for each backup set that is restored

○ Create a single Microsoft Virtual Hard Disk that contains the merged files and folders from all redirected backup sets

VHD file name:

6. Select the options for restore and then click Next.



How do you want to maintain file integrity, hierarchy, and security for restored data?

□ Restore files that were corrupt or incomplete in the backup. Some data may be retrievable from them.

☑ Recreate the directory structure from the backup when the data is restored; otherwise, all data is restored without any directory structure

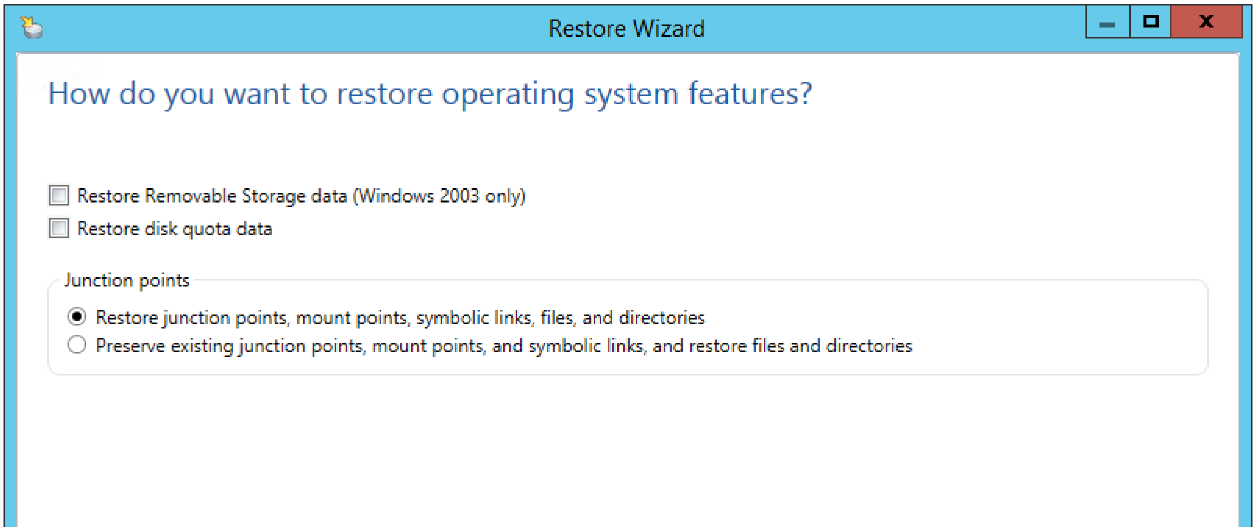
Restore existing files

○ Restore over existing files
○ Skip if the file exists
● Overwrite the file on disk only if it is older

Restore security information and file system permissions

● Restore files with their security information and file system permissions
○ Restore files without their security information and file system permissions. The security information and file system permissions for the restored files are determined by the security information and file system permissions at the destination location
○ Restore only the security information and file system permissions for files that exist at the destination; do not restore the file content

7. Select additional restore options in the next two panels, clicking Next to advance through each page.

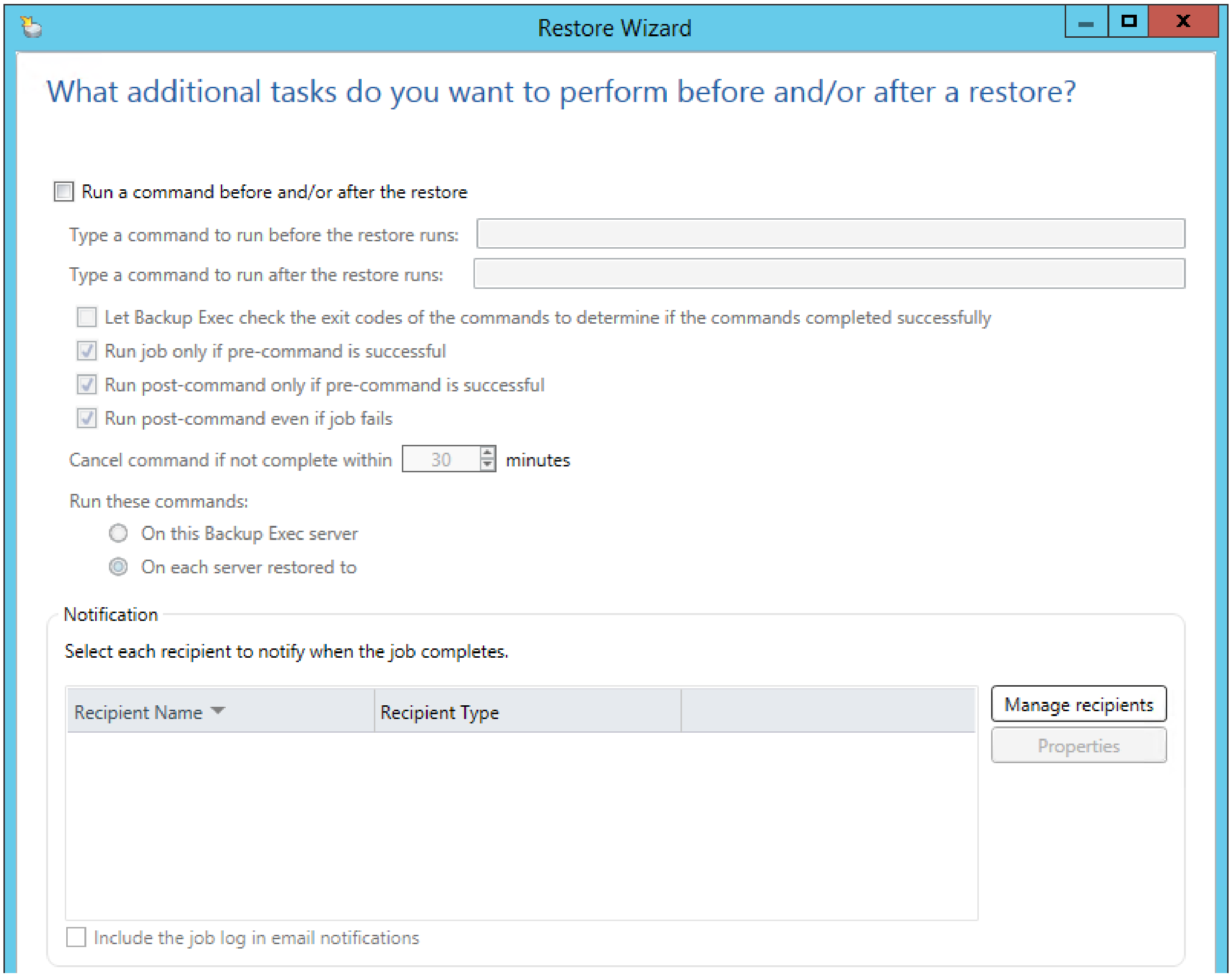


How do you want to restore operating system features?

□ Restore Removable Storage data (Windows 2003 only)
□ Restore disk quota data

Junction points

● Restore junction points, mount points, symbolic links, files, and directories
○ Preserve existing junction points, mount points, and symbolic links, and restore files and directories



What additional tasks do you want to perform before and/or after a restore?

□ Run a command before and/or after the restore

Type a command to run before the restore runs:

Type a command to run after the restore runs:

□ Let Backup Exec check the exit codes of the commands to determine if the commands completed successfully

☑ Run job only if pre-command is successful

☑ Run post-command only if pre-command is successful

☑ Run post-command even if job fails

Cancel command if not complete within 30 minutes

Run these commands:

○ On this Backup Exec server

● On each server restored to

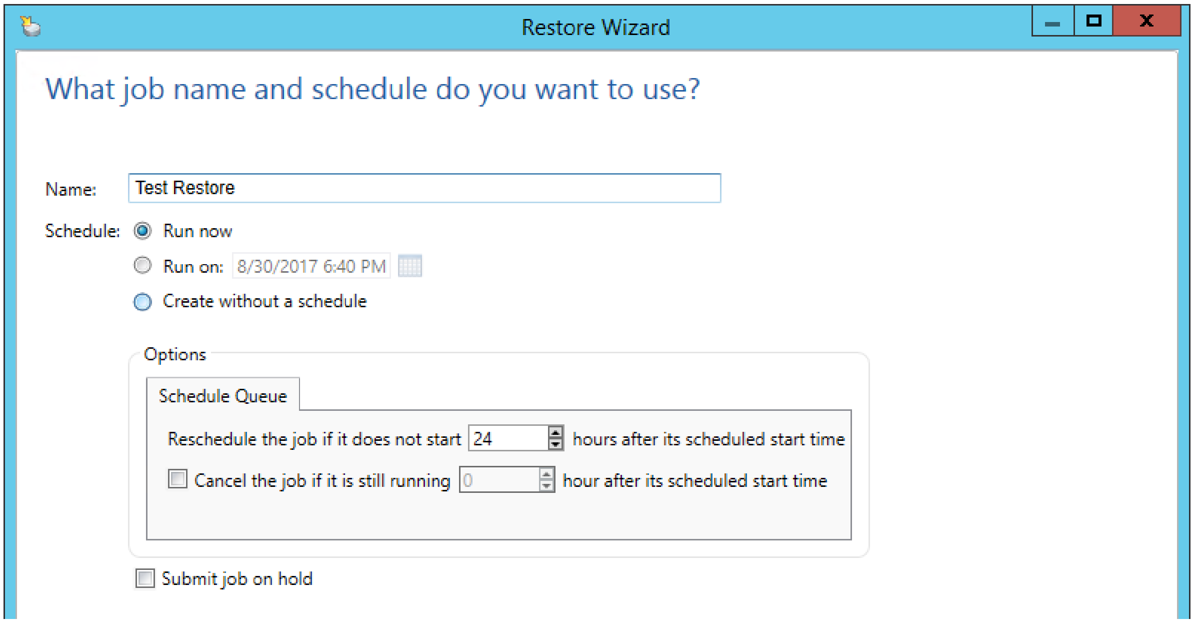
Notification

Select each recipient to notify when the job completes.

Recipient Name	Recipient Type

□ Include the job log in email notifications

8. Provide a name for the restore job, select when to run it, and then click Next.



What job name and schedule do you want to use?

Name: Test Restore

Schedule: ● Run now

○ Run on: 8/30/2017 6:40 PM

○ Create without a schedule

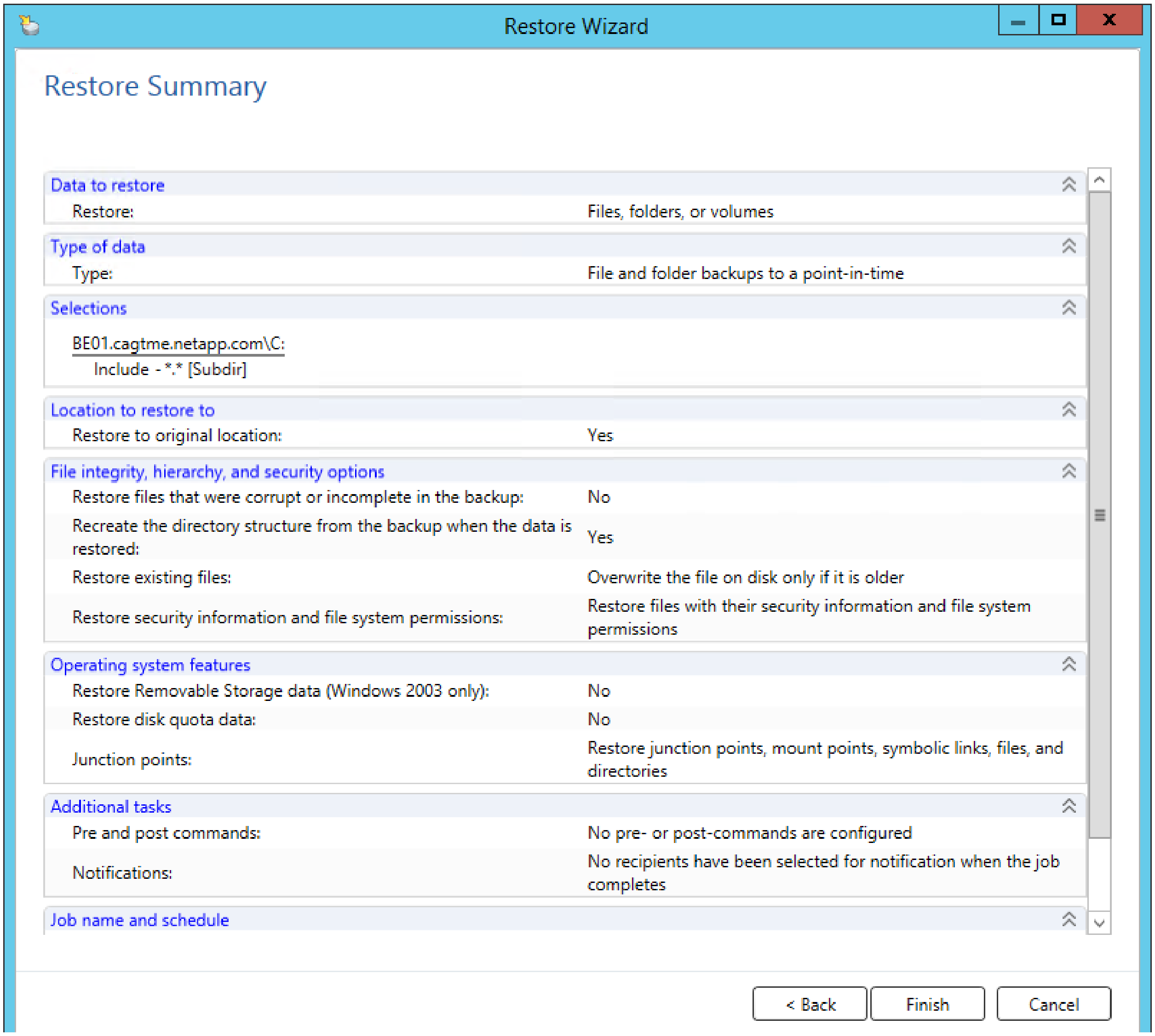
Options

Reschedule the job if it does not start 24 hours after its scheduled start time

□ Cancel the job if it is still running 0 hour after its scheduled start time

□ Submit job on hold

9. Finally, review the restore summary and click Finish to begin the restore job.



Restore Wizard

Restore Summary

Data to restore

Restore: Files, folders, or volumes

Type of data

Type: File and folder backups to a point-in-time

Selections

BE01.cagtme.netapp.com\C:
Include - *.* [Subdir]

Location to restore to

Restore to original location: Yes

File integrity, hierarchy, and security options

Restore files that were corrupt or incomplete in the backup: No

Recreate the directory structure from the backup when the data is restored: Yes

Restore existing files: Overwrite the file on disk only if it is older

Restore security information and file system permissions: Restore files with their security information and file system permissions

Operating system features

Restore Removable Storage data (Windows 2003 only): No

Restore disk quota data: No

Junction points: Restore junction points, mount points, symbolic links, files, and directories

Additional tasks

Pre and post commands: No pre- or post-commands are configured

Notifications: No recipients have been selected for notification when the job completes

Job name and schedule

4 Solution Recommendations and Best Practices

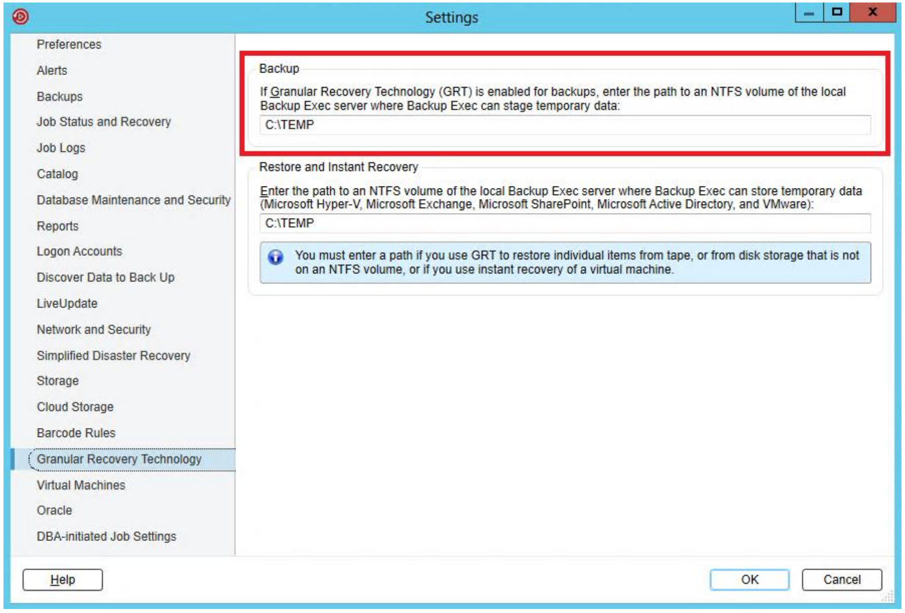
This chapter lists recommendations and best practices for deploying AltaVault in Backup Exec environments. The best practices are not requirements, but NetApp recommends that you follow these suggestions for the best solution experience.

4.1 Backup Exec Best Practices

Table 1 describes the recommended best practices for using Backup Exec with AltaVault.

Table 1) Backup Exec best practices.

Item	Description
Use disk folders	AltaVault has been tested with storage disk folders.

Item	Description
Use 100GB (102400MB) storage unit fragment size	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.
Disable the preallocate disk space incrementally up to the maximum file size option	Improves backup performance by allocating space in advance and not during operations.
Disable verify and encryption for backup jobs	Improves deduplication and throughput to AltaVault, while reducing the amount of time taken to commit backups.
Set concurrent write sessions	Sets a value to allow multiple sessions to write data to AltaVault, improving overall performance. To ensure concurrency set 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.
Configure GRT to a local folder if backing up Exchange data	Backup Exec GRT for Exchange uses multiple technologies to back up Exchange data, such as mailboxes, databases, transaction logs, and so on. These types of backups might not succeed if written directly to an AltaVault share. The process of backing up Exchange transaction logs uses multiple open file handles, which the AltaVault appliance was not designed to manage. To perform backups of Exchange, set up your Exchange backup job to first back up to a local staging area. Then duplicate the data in the local staging area to the AltaVault share. This approach leads to increased network throughput and potentially increased deduplication factors.  Settings Preferences Alerts Backups Job Status and Recovery Job Logs Catalog Database Maintenance and Security Reports Logon Accounts Discover Data to Back Up LiveUpdate Network and Security Simplified Disaster Recovery Storage Cloud Storage Barcode Rules Granular Recovery Technology Virtual Machines Oracle DBA-initiated Job Settings Help OK Cancel Backup If Granular Recovery Technology (GRT) is enabled for backups, enter the path to an NTFS volume of the local Backup Exec server where Backup Exec can stage temporary data: C:\TEMP Restore and Instant Recovery Enter the path to an NTFS volume of the local Backup Exec server where Backup Exec can store temporary data (Microsoft Hyper-V, Microsoft Exchange, Microsoft SharePoint, Microsoft Active Directory, and VMware): C:\TEMP You must enter a path if you use GRT to restore individual items from tape, or from disk storage that is not on an NTFS volume, or if you use instant recovery of a virtual machine.

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
```

4.3 Solaris Best Practices

NFS networking parameters on Solaris operating systems should be configured to optimally send data to AltaVault through configured NFS mounts. In addition to tuning the rsize and wsize mount options appropriately, nfs3_max_transfer_size and nfs3_bsize should also be tuned. nfs3_max_transfer_size and nfs3_bsize should be greater than or equal to the minimum of rsize and wsize. To set the values, edit the /etc/system file and change/add the following lines to the file:

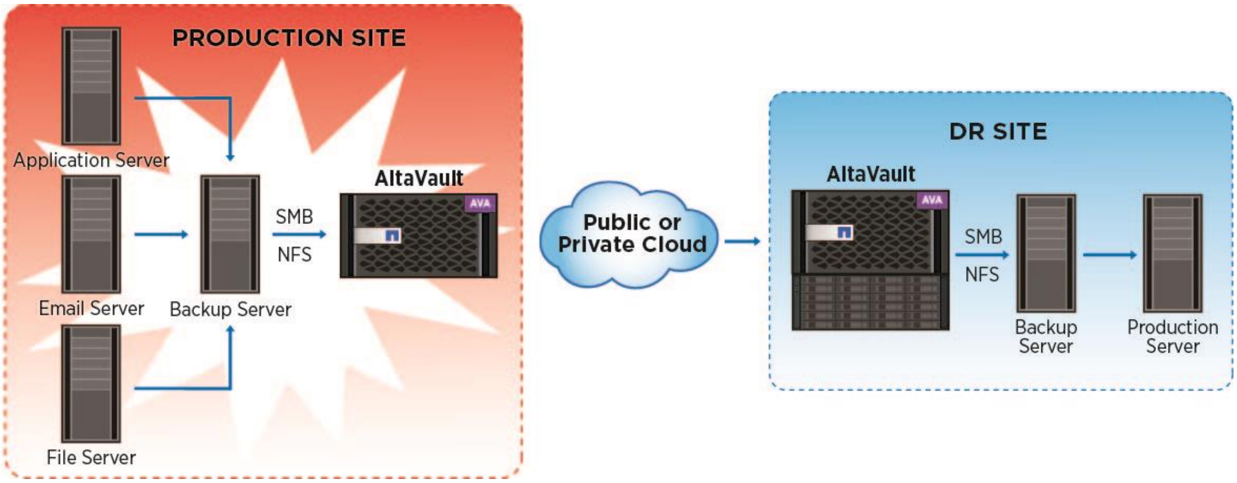
```
nfs:nfs3_max_transfer_size=<value>
nfs:nfs3_bsize=<value>
```

A reboot of the system is required in order for the configuration changes to take effect.

5 Disaster Recovery Process

Disaster recovery (DR) is the process of recovering the technology infrastructure after a natural or human-made disaster.

Figure 4) Disaster recovery overview.

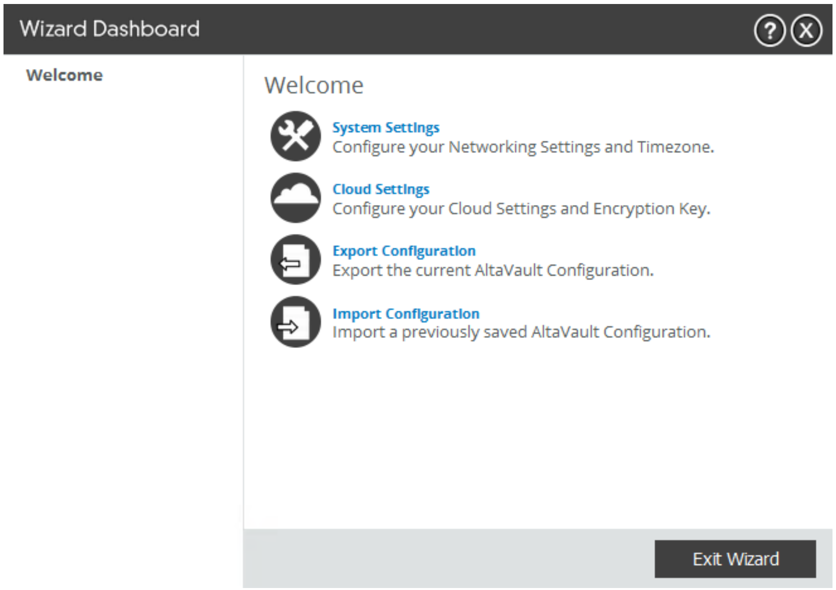


For example, consider a Backup Exec DR scenario with an AltaVault appliance where the entire production site, including the AltaVault appliance and the Backup Exec master server, are lost. However, at least one or more backups of that production environment exist in the cloud storage. To rec over the data at the DR site, you need a new Backup Exec server and a new physical AltaVault appliance or virtual AltaVault appliance.

Note: You do not need an AltaVault license to restore the data. The virtual AltaVault appliance can be downloaded from the Support site at http://support.netapp.com.

5.1 Predisaster Recovery Checklist

1. Export the current AltaVault configuration and encryption key. Browse to the menu Configure → Setup Wizard and select Export Configuration to export the configuration file. By default, the naming of the file is altavault_config_(HOSTNAME)_(DATETIME).tgz.



Welcome

System Settings
Configure your Networking Settings and Timezone.

Cloud Settings
Configure your Cloud Settings and Encryption Key.

Export Configuration
Export the current AltaVault Configuration.

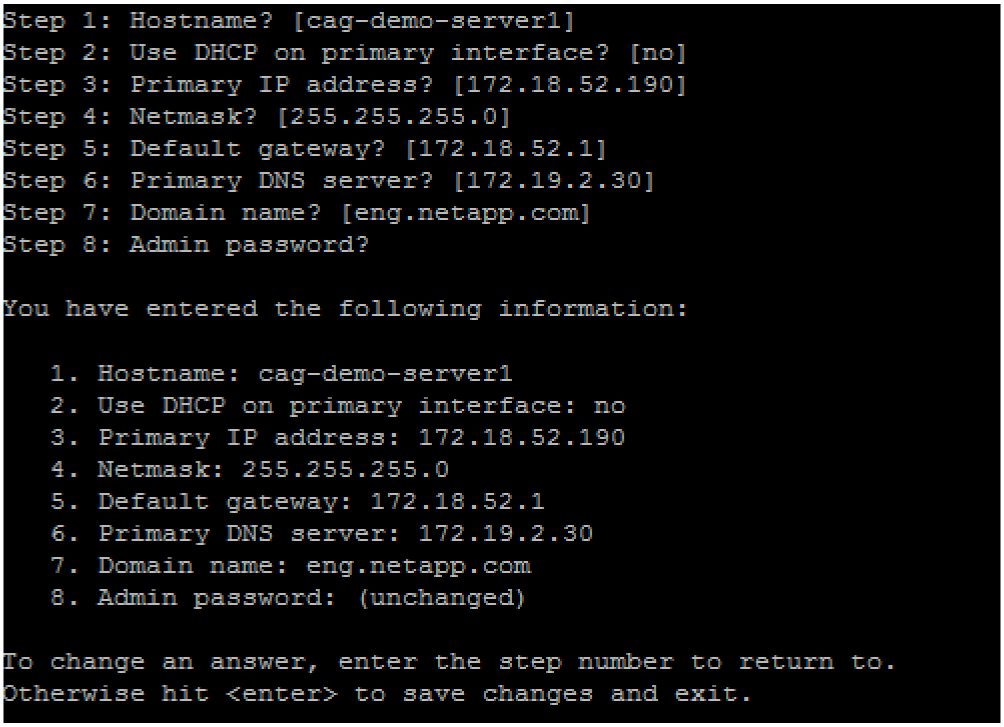
Import Configuration
Import a previously saved AltaVault Configuration.

Note: NetApp recommends that you store the exported configuration file in different physical locations. You should also keep the configuration file within the DR site. The file contains information about the configuration, including the encryption key.

5.2 AltaVault Appliance Recovery

The first step to recover from a catastrophic failure of a production site is to install and configure for disaster recovery a new physical AltaVault appliance or virtual AltaVault appliance. Using a virtual AltaVault appliance, which can be downloaded from the Support site and quickly deployed within a VMware, Hyper-V, or KVM environment at the DR site, is recommended for the initial recovery. It is suggested but not required that the AltaVault appliance at the DR site have the same or greater local storage capacity as the original AltaVault appliance at the lost production site. This configuration is helpful if you decide to make these resources at the DR site your production resources after the DR is complete. The following describes the steps to fully recover and restore the backup data from the cloud to the new AltaVault appliance.

1. Configure the AltaVault appliance to the new network environment at the DR site:
   a. Plug a serial cable into the console port and a terminal or, in the case of the virtual AltaVault appliance, use the virtual VMware console.
   b. Log in to the AltaVault CLI using the default login admin and default password.
   c. Configure the AltaVault network information. For details, see the AltaVault Cloud Integrated Storage Administration Guide.



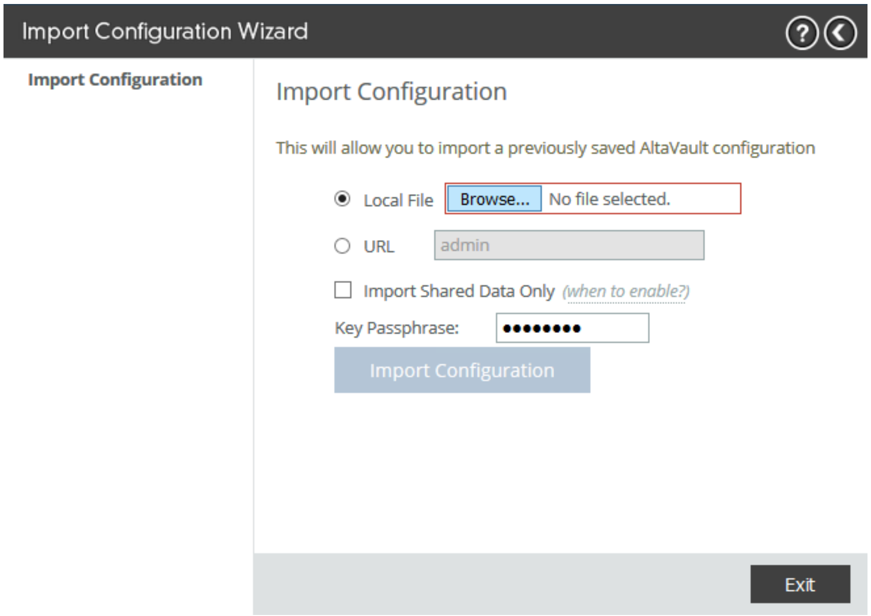
```
Step 1: Hostname? [cag-demo-server1]
Step 2: Use DHCP on primary interface? [no]
Step 3: Primary IP address? [172.18.52.190]
Step 4: Netmask? [255.255.255.0]
Step 5: Default gateway? [172.18.52.1]
Step 6: Primary DNS server? [172.19.2.30]
Step 7: Domain name? [eng.netapp.com]
Step 8: Admin password?

You have entered the following information:

   1. Hostname: cag-demo-server1
   2. Use DHCP on primary interface: no
   3. Primary IP address: 172.18.52.190
   4. Netmask: 255.255.255.0
   5. Default gateway: 172.18.52.1
   6. Primary DNS server: 172.19.2.30
   7. Domain name: eng.netapp.com
   8. Admin password: (unchanged)

To change an answer, enter the step number to return to.
Otherwise hit <enter> to save changes and exit.
```

2. Recover the original configuration of the AltaVault appliance to the new AltaVault appliance at the DR site. Go to Configure → Setup Wizard and import the previously saved AltaVault_config_(HOSTNAME)_(DATETIME).tgz configuration file. Make sure that you leave the default “Import Shared Data Only” checkbox selected.



Import Configuration Wizard

Import Configuration

Import Configuration

This will allow you to import a previously saved AltaVault configuration

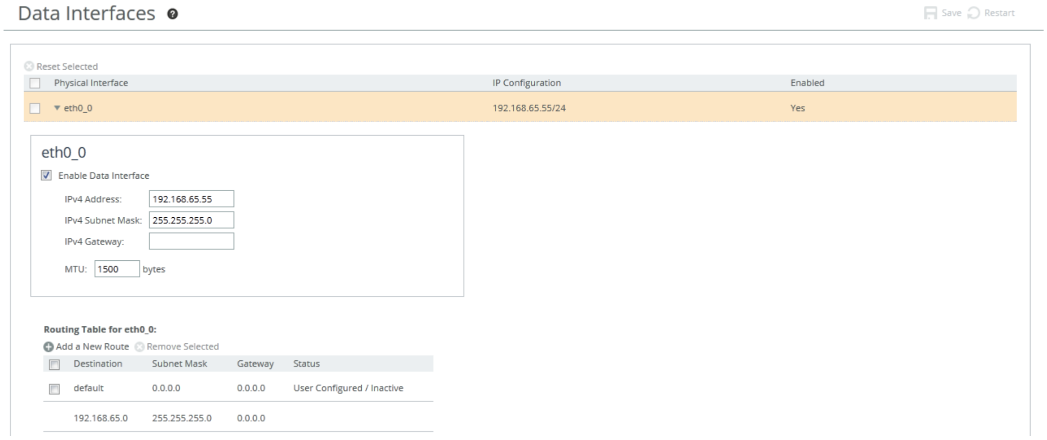
● Local File Browse... No file selected.

○ URL admin

□ Import Shared Data Only *(when to enable?)*

Key Passphrase: ●●●●●●●●

3. Configure AltaVault data interfaces to the new network environment at the DR site. Browse to the menu Configure > Data Interfaces and configure data interfaces network information.



Data Interfaces

□	Physical Interface	IP Configuration	Enabled
□	▾ eth0_0	192.168.65.55/24	Yes

eth0_0

☑ Enable Data Interface

IPv4 Address: 192.168.65.55

IPv4 Subnet Mask: 255.255.255.0

IPv4 Gateway:

MTU: 1500 bytes

Routing Table for eth0_0:

□	Destination	Subnet Mask	Gateway	Status
□	default	0.0.0.0	0.0.0.0	User Configured / Inactive
	192.168.65.0	255.255.255.0	0.0.0.0	

4. After the configuration is complete, connect to the AltaVault CLI using SSH and initiate the replication recovery procedure. For details, see the AltaVault Command-Line Interface Reference Guide. Issue the following commands:

```
AltaVault > enable
AltaVault # configure terminal
AltaVault (config) # no service enable
AltaVault (config) # replication recovery enable
AltaVault (config) # service restart
```

Note: The replication recovery enable command fails to execute if the optimization service is enabled or if the AltaVault appliance detects existing data in the new AltaVault cache. Assuming this is a new, empty AltaVault appliance, you do not receive any failures, and the commands are all executed without error. This process can take a few seconds to several hours, depending on the backups being restored. During the recovery process, the system communicates with the cloud provider and recovers all the namespace files that existed before the failure.

5. (Optional) Because the recovery process downloads only the namespace and metadata, initial file access might be slow, because the AltaVault appliance downloads all of the data from the cloud. Therefore, it is recommended that you also prepopulate the actual data from the cloud back onto the new AltaVault appliance to accelerate the recovery of your production systems. To do so, enter the following:

```
AltaVault (config) # datastore prepop {[num-days <number of days>] | [pattern <pattern>] |
[recursive]} dryrun
```

Where the parameters are provided as shown in the following table.

Table 2) Datastore prepopulation command parameters.

Parameter	Description
Num-days <number of days>	Filters the data retrieved by number of last-modified days.
Pattern <pattern>	Filters the data retrieved by the pattern you specify.
Recursive	Enables the data to be prepopulated in subdirectories under a given directory.
dryrun	AltaVault calculates the estimated amount of cloud data to be recovered by the operation, and the amount of actual data to be recovered by the operation. No data is restored in this case.

Note: Backup Exec requires that certain parts of a backup be recovered first, because it contains metadata specific to the backup contents. For example, if Backup Exec is writing data through AltaVault to Amazon Glacier, you can use the following prepop commands to retrieve the metadata information:

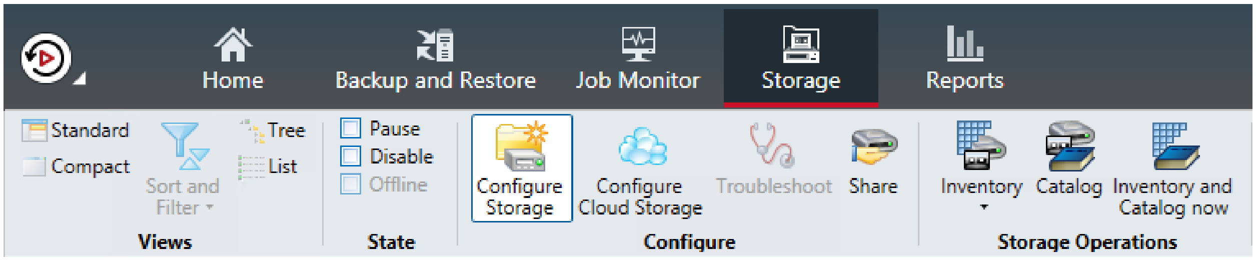
```
AltaVault (config) # datastore prepop pattern *.bkf bue-footer retrieval-type
[standard|expdited|bulk]
AltaVault (config) # datastore prepop pattern *.bkf bue-header retrieval-type
[standard|expdited|bulk]
```

Note: If the AltaVault appliance storage capacity is less than the space used in the cloud, you can still initiate the recovery process. However, in this case the AltaVault appliance only recovers as much actual data as the size of its storage. If the recovery process attempts to bring back more data than the disaster recovery AltaVault appliance can manage, then the recovery process might fail. A virtual AltaVault appliance, for example, can store up to 8TB of cloud data. For more details on AltaVault appliance sizes, see the AltaVault Cloud Integrated Storage Installation and Service Guide for Virtual Appliance. At this point the AltaVault recovery procedure is complete. Now you need to recover the Backup Exec server.

5.3 Backup Exec Recovery

After the AltaVault appliance has been recovered, you need to install and configure the Backup Exec server. See Backup Exec documentation and technotes for detailed information about how to perform the following operations.

1. Install Backup Exec server to a new host system at the DR site.
2. Run the Inventory & Catalog Now task to introduce the media stored on AltaVault to Backup Exec and to catalog the file content found on the media. If this is the first time that Backup Exec has encountered this server, the media label is also added to the Media view.



3. After the media is inventoried and cataloged, use the Restore over existing files option within Backup Exec to restore the Backup Exec server's hard drives and shadow copy components. Reboot the system as necessary through this process.
4. (Optional) With the Backup Exec server now recovered, you might optionally need to recatalog the media again to reflect the most current catalog state of the media to this restored Backup Exec server.

5.4 Production Systems Recovery

From this point forward, the AltaVault appliance and Backup Exec are configured as they were before the disaster, and you can begin system restores of any production systems that need to be recovered at the DR site using normal Backup Exec recovery strategies such as intelligent disaster recovery. See Backup Exec documentation for recovering additional systems.

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	May 2015	Initial version
Version 1.1	November 2015	Updated for 4.1 release
Version 1.2	April 2016	Updated for 4.2 release
Version 1.3	August 2016	Updated for 4.2.1 release
Version 1.4	January 2017	Updated for 4.3 release
Version 1.5	April 2017	Updated for 4.3.1 release
Version 1.6	September 2017	Updated for 4.3.2 release, Backup Exec 16
Version 1.7	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.

Copyright Information

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

TR-4409-1117