Technical Report

NetApp AltaVault Cloud-Integrated Storage Appliances

Solution Deployment: AltaVault with IBM Spectrum Protect

Christopher Wong, NetApp
November 2017 | TR-4407

Abstract

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

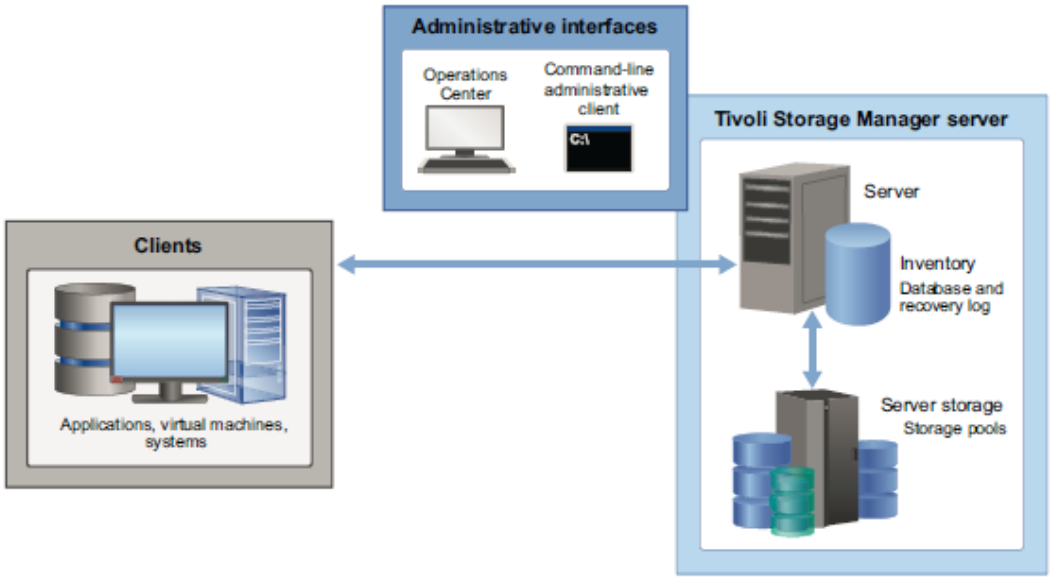
Because an AltaVault appliance is an asymmetric, stateless appliance, no hardware is needed in the cloud, and you can recover the last known good state of a broken or destroyed AltaVault appliance to a new AltaVault appliance. AltaVault appliances offer the flexibility to scale cloud storage as business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

1.1 IBM Spectrum Protect Architecture Overview

IBM Tivoli Spectrum Protect (formerly Tivoli Storage Manager, or TSM) software provides a wide range of storage management capabilities from a single point of control, helping companies address the cost, complexity, and capabilities of their backup systems. With its client/server design, Spectrum Protect helps simplify the protection and management of your data, addresses business continuity by helping to shorten backup and recovery times, and helps to maximize application availability with advanced data recovery management technologies.

In Spectrum Protect all aspects of operations from backups to server management are conducted through the Spectrum Protect Administration Console and monitored in Operations Center. Administrators can run the Administration Console from any server in the network.

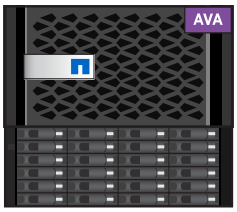
Figure 1) IBM Spectrum Protect component view.



1.2 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.

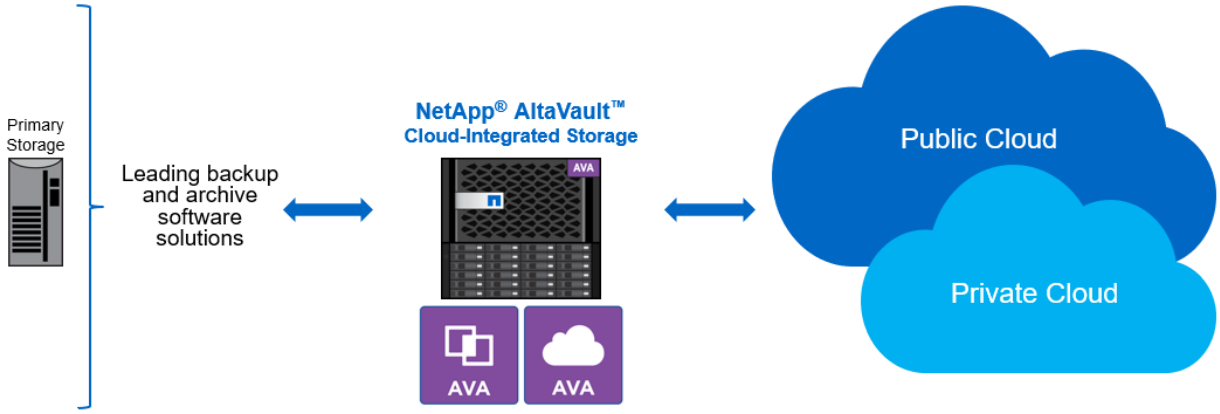
2 Deploy and Configure AltaVault with Spectrum Protect

Spectrum Protect 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 Spectrum Protect server. This server, along with clients, needs minimum hardware features as identified by the backup application. Check the IBM support site and related compatibility lists where applicable.
2. Obtain server systems and related software media supported by Spectrum Protect 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 Spectrum Protect

The Spectrum Protect Administration Console is the interface that is used to configure all settings in a Spectrum Protect server environment. In order for the Administration Console to make changes, the administration console must point to the desired Spectrum Protect server. By default, the Administration Console locates the Spectrum Protect server on the local system if present. The Administration Console can also be pointed at other Spectrum Protect servers in the environment to monitor activities and statistics for those particular Spectrum Protect servers. Alternatively, administrators can use the Spectrum Protect administrative CLI.

3.1 Create a FILE Device Class

A FILE device class is a device descriptor that specifies the device type and media management information, such as the recording format, estimated capacity, and labeling prefixes. Spectrum Protect associates device classes with physical storage such as AltaVault.

Note: AltaVault only supports the FILE device class. Do not use AltaVault as a DISK device class.

Use the DEFINE DEVCLASS command to create a FILE device class pointing to AltaVault:

```
DEFINE DEVCLASS <devclassname> DEVTYPE=FILE MOUNTLIMIT=<number> MAXCAPACITY=100G
DIRECTORY=\\<AltaVaultDataInterface>\<sharename>
```

- **<devclassname>.** Provide a new device class name. It cannot match an existing device class name.
- **DEVTYPE=FILE.** Set the device type to FILE.
- **MOUNTLIMIT=<number>.** This option controls the number of volumes that can be mounted simultaneously on a Spectrum Protect server. To tune performance, set a value higher than 1. The value will depend on your available resources and infrastructure environment. Adjust the number of mount points accordingly based on your observed performance This can be increased as needed for the given environment.
- **MAXCAPACITY=100G.** Recommend setting a value of 100GB. This option controls the maximum device file object size that can be created on AltaVault by Spectrum Protect.
- **DIRECTORY=\\<AltaVaultDataInterface>\<sharename>.** Enter a fully qualified domain name SMB share path value that corresponds to the AltaVault SMB share. The SMB share should have Everyone access, and Guest account

3.2 Create a Primary or Copy Storage Pool

A Spectrum Protect storage pool is a collection of volumes that are associated with one device class and one media type. Storage pools can have volumes that are predefined or volumes that are created from a scratch pool of volumes. Scratch volumes are created by Spectrum Protect. Backup data is written by a Spectrum Protect client to a storage pool target. You can create either a primary or a copy storage pool for use with AltaVault.

Method 1: Primary Storage Pool

Use the DEFINE STGPOOL command with POOLTYPE=PRIMARY to create a primary storage pool pointing to AltaVault.

Note: Primary sequential storage pools that point to AltaVault should not be used for direct writing of large nonsequential streams of data by backup cllients.

```
DEFINE STGPOOL <primarypoolname> <devclassname> POOLTYPE=PRIMARY
RECLAIM=90 RECLAIMPROCESS=<number> MAXSCRATCH=<number>
```

- **<primarypoolname>.** Provide a new primary storage pool name. It cannot match an existing storage pool name.
- **<devclassname>.** Identify the FILE device class name created in the previous section.
- **POOLTYPE=PRIMARY.** Identifies that the storage pool is used as a primary sequential access storage pool, which is configured later to sit behind an existing primary disk storage pool.
- **RECLAIM=90.** Set a high reclamation threshold for the new storage pool. Because Spectrum Protect operations can create partially filled volumes, this can lead to unnecessary reclamation activity of cloud-based volumes by AltaVault if the reclamation threshold is set too low. A higher value results in volumes being potentially held longer in the cloud, while lowering restore costs because fewer reclamations are performed.

- **RECLAIMPROCESS=<number>.** Specify the maximum number of reclamation processes that can be performed simultaneously. Set an initial value of 5 and modify the value according to the overall performance established by the environment.
- **MAXSCRATCH=<number>.** Specify the maximum number of scratch volumes allowed to be created on the AltaVault appliance. The overall storage pool size is calculated as the number of volumes allowed to be created, multiplied by the volume size specified in the DEFINE DEVCLASS command in the previous section.

Method 2: Copy Storage Pool

Use the DEFINE STGPOOL command with POOLTYPE=COPY to create a copy storage pool pointing to AltaVault. A copy storage pool receives copies of data from a primary storage pool through the BACKUP STGPOOL command.

```
DEFINE STGPOOL <copypoolname> <devclassname> POOLTYPE=COPY
RECLAIM=90 RECLAIMPROCESS=<number> MAXSCRATCH=<number>
```

- **<copypoolname>.** Provide a new primary storage pool name. It cannot match an existing storage pool name.
- **<devclassname>.** Identify the FILE device class name created in the previous section.
- **POOLTYPE=COPY.** Identifies that the storage pool is used as a copy sequential access storage pool, which is configured later as the target of a BACKUP STGPOOL operation.
- **RECLAIM=90.** Set a high reclamation threshold for the new storage pool. Because Spectrum Protect operations can create partially filled volumes, this can lead to unnecessary reclamation activity of cloud-based volumes by AltaVault if the reclamation threshold is set too low. A higher value results in volumes being potentially held longer in the cloud, while lowering restore costs because fewer reclamations are performed.
- **RECLAIMPROCESS=<number>.** Specify the maximum number of reclamation processes that can be performed simultaneously. Set an initial value of 5 and modify the value according to the overall performance established by the environment.
- **MAXSCRATCH=<number>.** Specify the maximum number of scratch volumes allowed to be created on the AltaVault appliance. The overall storage pool size is calculated as the number of volumes allowed to be created, multiplied by the volume size specified in the DEFINE DEVCLASS command in the previous section.

3.3 Associate Backups to the New Primary Storage Pool

Perform the following ONLY if you create a primary storage pool above. If you create a copy storage pool, then skip this section.

After the storage pool is created, Spectrum Protect must be configured to send data to the storage pool.

- In method 1, an existing storage pool can be associated to send data to the AltaVault storage pool as the next pool in the storage hierarchy.
- In method 2, a policy domain can be updated to send data to the new storage pool.

Note: This method is not recommended as a replacement for disk-based storage pools and is designed for use in cases where Spectrum Protect sends large sequential backups, such as with data protection for database backups. You should test AltaVault as a direct primary storage pool for client backups to ensure it meets the backup performance requirements of your environment.

Method 1: Assign the New Storage Pool as the Next Storage Pool in the Hierarchy

Storage pools can be set up in a hierarchy such that data flows from one storage pool to another at regulated schedules or in the event of data overflow. Using an AltaVault appliance in this fashion as the next storage pool behind a primary disk storage pool reduces the amount of simultaneous traffic on the

network as opposed to method 2, because data flow to the AltaVault storage pool is separate from backup data flow into the Spectrum Protect server.

Use the UPDATE STGPOOL command to associate the primary sequential storage pool based on AltaVault as the next storage pool behind a primary disk storage pool.

```
UPDATE STGPOOL <primaryDISKpoolname> NEXTSTGPOOL=<AltaVaultprimarypoolname>
```

- **< primaryDISKpoolname>.**Provide the primary DISK storage pool name from which data is migrated to the primary sequential storage pool based on AltaVault.
- **NEXTSTGPOOL=<AltaVaultprimarypoolname>.** Specify the primary sequential storage pool based on AltaVault that receives the data migrated from the primary disk storage pool identified earlier.

Method 2: Associate a Policy Domain to the New Primary Storage Pool

A policy domain describes how storage and management of backup data within a Spectrum Protect server are performed. Policies are rules that you set at the Spectrum Protect server to help you manage the client data lifecycle. Policies control how and when client data is stored and where that data resides within the Spectrum Protect storage devices.

Note: It is recommended to use the AltaVault appliance as the direct destination for sequential backup-based workloads, such as data protection for databases. Using AltaVault as the direct destination for typical client file backup workloads is not recommended. This is due to the sequential nature of AltaVault optimization and the additional network requirements to perform backups to Spectrum Protect and data movement to AltaVault simultaneously. You should test AltaVault as a direct primary storage pool for client backups to ensure it meets the backup performance requirements of your environment.

1. Use the UPDATE COPYGROUP command to associate the primary sequential storage pool based on AltaVault as the storage pool target for backups written to an existing policy domain.

```
UPDATE COPYGROUP <domain_name> <policy_set_name> <mgmt_class_name>
DESTINATION=<AltaVaultprimarypoolname>
```

- **<domain_name>.** Provide the name of the policy domain that sends data to AltaVault.
- **<policy_set_name>.** Provide the name of the policy set under the policy domain that sends data to AltaVault.
- **<mgmt_class_name>.** Provide the name of the management class under the policy set that sends data to AltaVault.
- **DESTINATION=<AltaVaultprimarypoolname>.** Specify the primary sequential storage pool based on AltaVault that receives the data from this backup policy.

2. Activate the policy to invoke the changes to the preceding policy.

```
ACTIVATE POLICYSET <domain_name> <policy_set_name>

<domain_name>
```

- **<domain_name>.** Provide the name of the policy domain that sends data to AltaVault.
- **<policy_set_name>.** Provide the name of the policy set under the policy domain that sends data to AltaVault.

3.4 Test Backup and Restore with AltaVault

There are three ways to test backup and restore, depending on which method you selected for configuring AltaVault within the Spectrum Protect storage hierarchy.

Method 1: AltaVault Appliance Used as the Next Primary Storage Pool in the Storage Pool Hierarchy

To move data to the AltaVault storage pool, update the migration thresholds for the storage pool that points to the AltaVault storage pool. This triggers a migration process that migrates data from the storage pool to the AltaVault appliance.

Note: This applies only if you configured the AltaVault appliance as the next primary storage pool in a storage pool hierarchy. If you configured the AltaVault appliance as a copy storage pool, go to method 2. If you configured the AltaVault appliance as the primary storage pool for backups, go to method 3.

Use the UPDATE STGPOOL command to force the migration of the data from the current primary disk storage pool to the AltaVault primary storage pool.

```
UPDATE STGPOOL <primaryDISKpoolname> HIGHMIG=10 LOWMIG=0
```

- **< primaryDISKpoolname>.** Provide the primary DISK storage pool name from which data is migrated to the primary sequential storage pool based on AltaVault.
- **HIGHMIG=10.** HIGHMIG forces migration to start if the storage pool is higher than 10% utilized. This assumes that data already exists in the storage pool and that utilization is greater than 10%. If this is not the case, adjust the HIGHMIG value accordingly.
- **LOWMIG=0.** LOWMIG sets the migration to stop if the storage pool is empty (0% utilized).

Method 2: AltaVault Appliance Used as a Copy Storage Pool

In this method AltaVault is used as an off-site copy storage pool by Spectrum Protect. A copy of the data from the primary storage pool is made to the copy storage pool using AltaVault.

Note: This applies only if you configured the AltaVault appliance as a copy storage pool. If you configured the AltaVault appliance as the next primary storage pool in a hierarchy, go to method 1. If you configured the AltaVault appliance as the primary storage pool for backups, go to method 3.

Use the BACKUP STGPOOL command to force a copy of the data from the current primary disk storage pool to be created on the AltaVault copy storage pool.

```
BACKUP STGPOOL <primarypoolname> <AltaVaultcopypoolname> MAXPROCESS=5
```

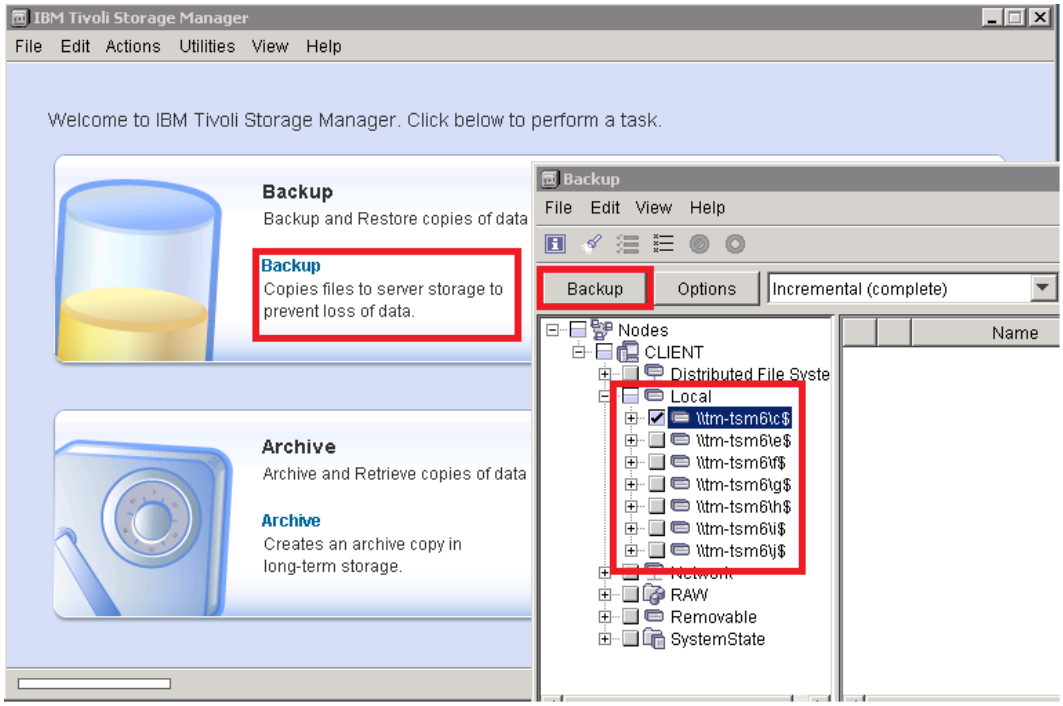
- **<primarypoolname>.** Provide the primary storage pool name from which data is copied to the copy sequential storage pool based on AltaVault.
- **<AltaVaultcopypoolname>.** Specify the copy storage pool name that represents the AltaVault appliance target.
- **MAXPROCESS=5.** Specify the maximum number of processes that can be performed simultaneously. Set an initial value of 5 and modify the value according to the overall performance established by the environment.

Method 3: AltaVault Used as a Primary Storage Pool

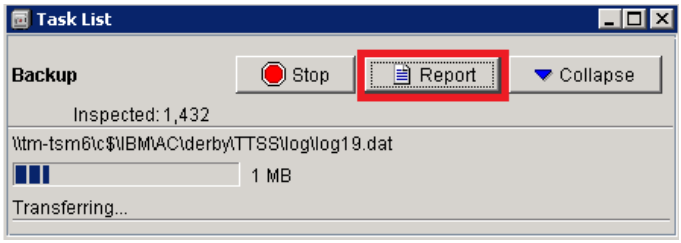
This applies only if you configured the AltaVault appliance as a primary storage pool for backups from a policy domain. If you configured the AltaVault appliance as the next primary storage pool in a storage pool hierarchy, go to method 1. If you configured the AltaVault appliance as a copy storage pool, go to method 2.

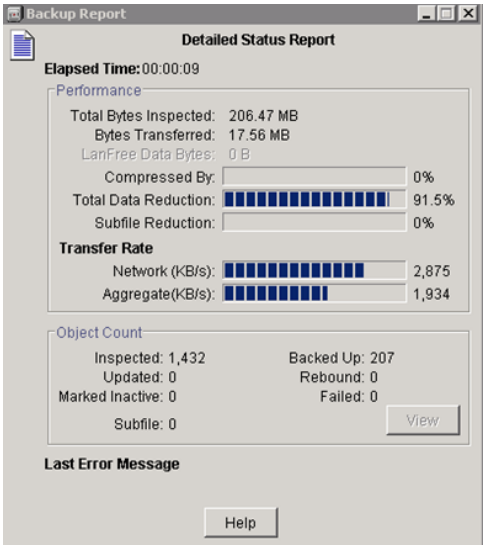
Note: It is recommended to use the AltaVault appliance as the direct destination for sequential backup-based workloads, such as data protection for databases. Using AltaVault as the direct destination for typical client file backup workloads is not recommended. This is due to the sequential nature of AltaVault optimization and the additional network requirements to perform backups to Spectrum Protect and data movement to AltaVault simultaneously. You should test AltaVault as a direct primary storage pool for client backups to ensure it meets the backup performance requirements of your environment.

1. To use Spectrum Protect with the AltaVault appliance, you can run a manual backup. Start the Spectrum Protect Backup-Archive GUI, and when the window appears, click Backup. In the Backup window that appears, select the local drives or files to back up and click Backup to begin the operation.

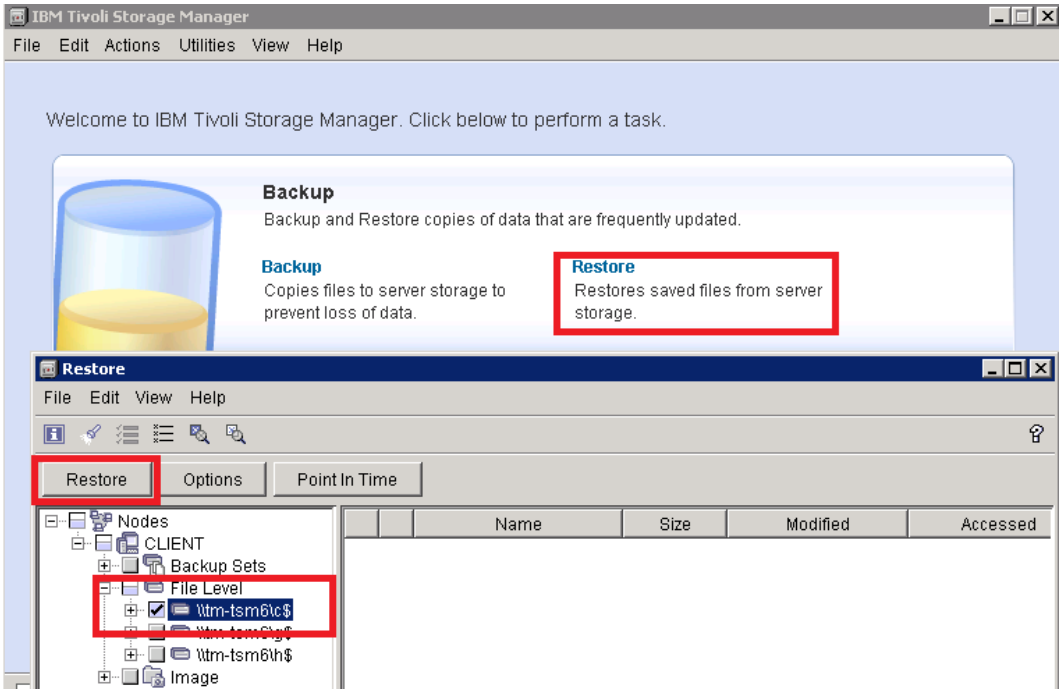


2. Backup activity is provided in the Task List window. By clicking the Report button, you can view detailed status of the operation, including throughput metrics and object counts.

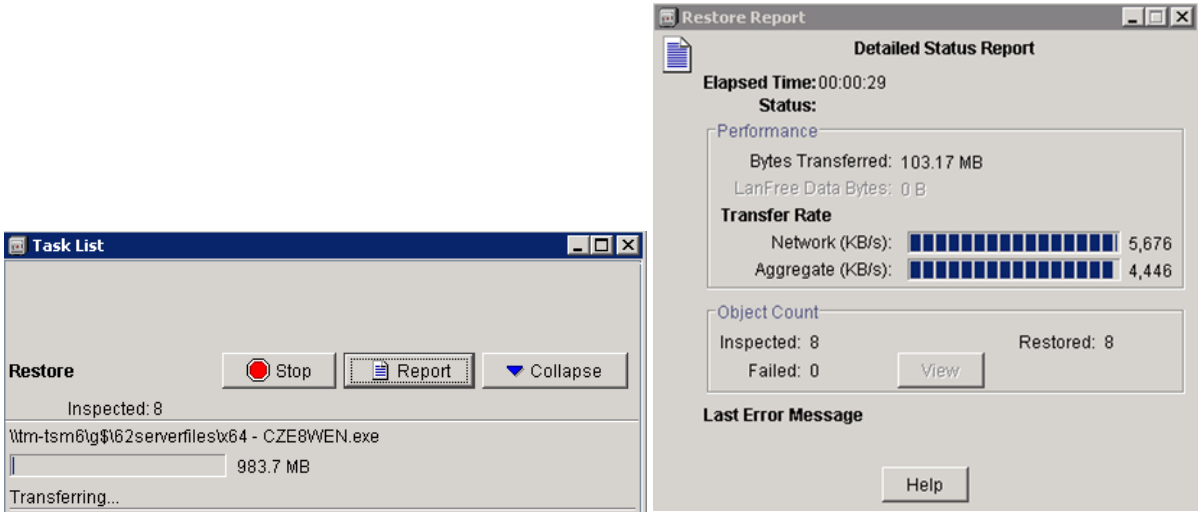




3. When the backup is complete, perform a restore to validate that the AltaVault appliance can restore the backed-up data. From the Spectrum Protect Backup-Archive GUI, click Restore. In the Restore window that appears, select the local drives or files to restore and click Restore to begin the operation.



4. Restore activity is provided in the Task List window. By clicking the Report button, you can view detailed status of the operation, including throughput metrics and object counts.



4 Solution Recommendations and Best Practices

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

4.1 Spectrum Protect Best Practices

Table 1 table describes the recommended best practices for using Spectrum Protect with AltaVault.

Table 1) Spectrum Protect best practices.

Item	Description
Configure AltaVault in a Windows AD and use the same AD account with AltaVault and Spectrum Protect	Spectrum Protect FILE device class configuration requires that you have Spectrum Protect services running with the same Windows domain account as configured for the SMB share provided by AltaVault. These services include the TSM server instance, as well as the DB2 instance configured for the TSM server instance.
Use AltaVault as a Spectrum Protect FILE device class and Spectrum Protect sequential storage pool.	AltaVault has been tested with the Spectrum Protect FILE device class. Do not use AltaVault as a DISK device class. When configuring a Spectrum Protect storage pool, use AltaVault as a sequential storage pool target. It is recommended to use AltaVault as a primary sequential storage pool that is second in a hierarchy behind a primary DISK storage pool or as a copy sequential storage pool. Only use AltaVault as a direct primary storage pool target for sequential backups such as data protection for database workloads.
Use 100GB (102400MB) storage unit fragment size and allow multiple mount points.	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 of the maximum volume 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. Allowing a high mount limit improves overall throughput to AltaVault. The value will depend on your available resources and infrastructure environment. Adjust the number of mount points accordingly based on your observed performance.
Disable Spectrum Protect compression, encryption, and deduplication in storage pools.	This frees resources and allows AltaVault to optimize data.
Increase storage pool reclamation thresholds for storage pools based on AltaVault.	Spectrum Protect reclamation of partially filled volumes can cause increased cloud restore activity with AltaVault. To reduce the occurrences of this behavior, increase the reclamation threshold to 90% or higher. AltaVault optimizes data written to the cloud and performs garbage collection appropriately to minimize cloud storage costs.
Use Spectrum Protect active storage pools to a pinned AltaVault share if you want to guarantee a current backup version resides on the AltaVault appliance cache.	AltaVault uses a least recently used algorithm to determine which data is evicted from cache when space is needed for new data. This approach can affect recovery of Spectrum Protect data if the data is spread over many incremental backups. Using an active storage pool to direct backups to a pinned share on AltaVault guarantees that a full set of the most recent backup data is always available. Make sure to determine that the amount of data that is pinned does not exceed the 80% maximum capacity of the AltaVault appliance cache.
Use Spectrum Protect 7.1.5 or higher when using AltaVault in Windows environments	IBM has released a fix to a high impact defect reported in APAR IT13542 regarding writes to case sensitive file systems that can result in data loss. Ensure you are at 7.1.5 or higher to protect against this defect when using AltaVault.

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:

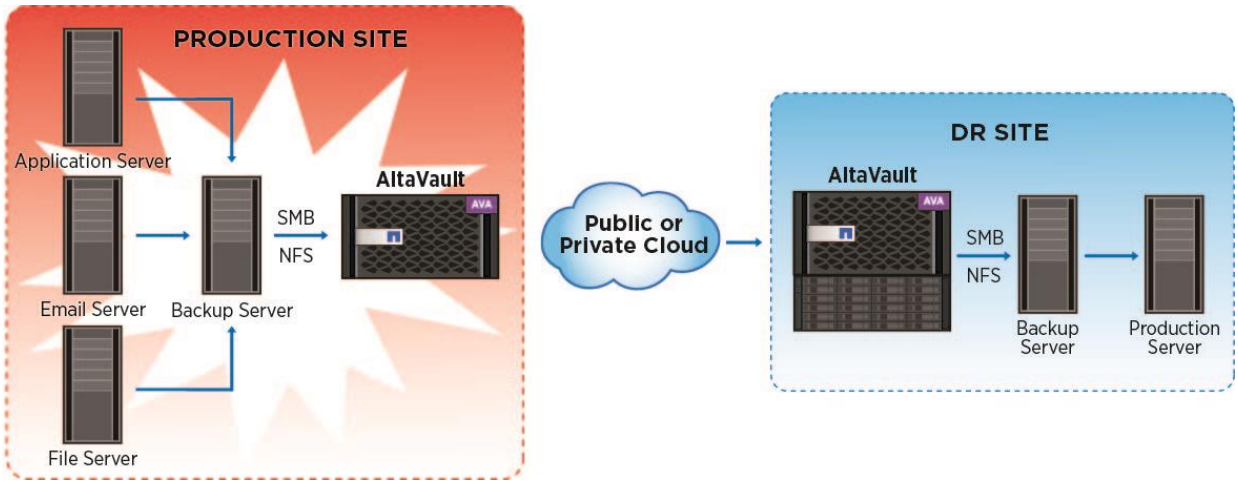
```
nfs:nfs3_max_transfer_size=<value>
nfs:nfs3_bsize=<value>
```

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-caused disaster.

Figure 4) Disaster recovery overview.

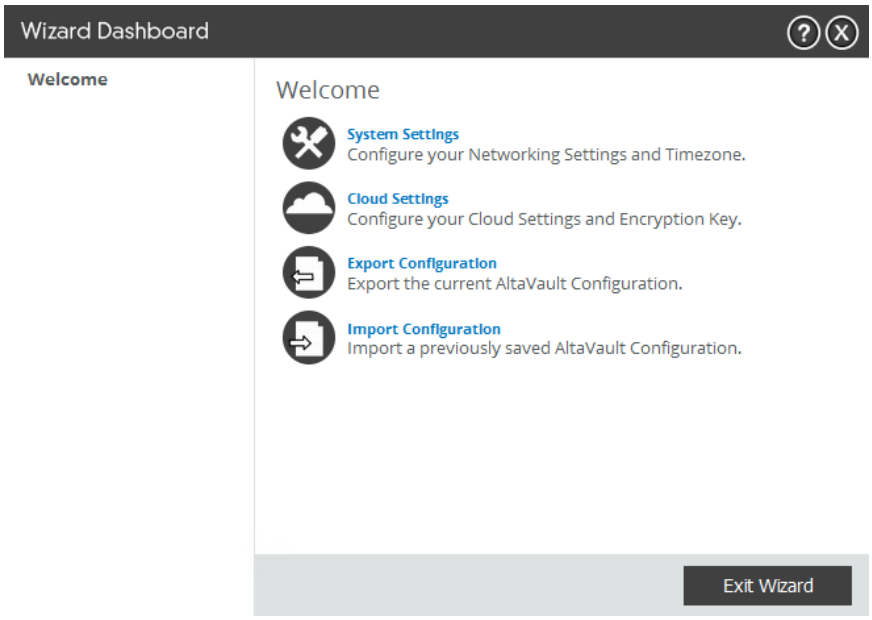


For example, consider a Spectrum Protect DR scenario with an AltaVault appliance where the entire production site, including the AltaVault appliance and the Spectrum Protect master server, are lost. However, at least one or more backups of that production environment exist in the cloud storage. To recover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

Note: You do not need an AltaVault license to restore the data. Moreover, 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.



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.

2. If using the AltaVault appliance as a copy storage pool target, prepare the Spectrum Protect server environment with Spectrum Protect Disaster Recovery Manager (DRM). Issue the following Spectrum Protect server commands to set up DRM to manage AltaVault copy storage pool volumes:
   - SET DRMCOPYSTGPOOL <AltaVault-copy-storagepool-name>
   - SET DRMFILEPROCESS YES
   - QUERY DRMEDIA COPYSTGPOOL=<AltaVault-copy-storagepool-name>
3. Manage the DRM volumes and set their status as off site as you would any typical DRM volumes using the MOVE DRMEDIA command.

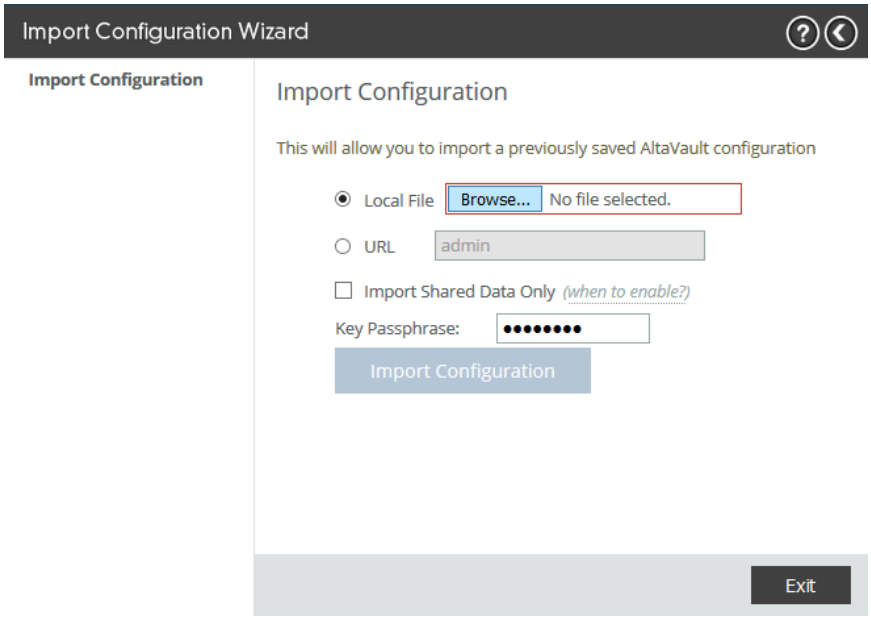
5.2 AltaVault Appliance Recovery

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. Although not required, the AltaVault appliance at the DR site is suggested to have the same or greater local storage capacity as the original AltaVault appliance at the lost production site should you decide to make these resources at the DR site your production resources after the DR is complete. The following steps describe how to fully recover and restore the backup data from the cloud to the new AltaVault appliance.

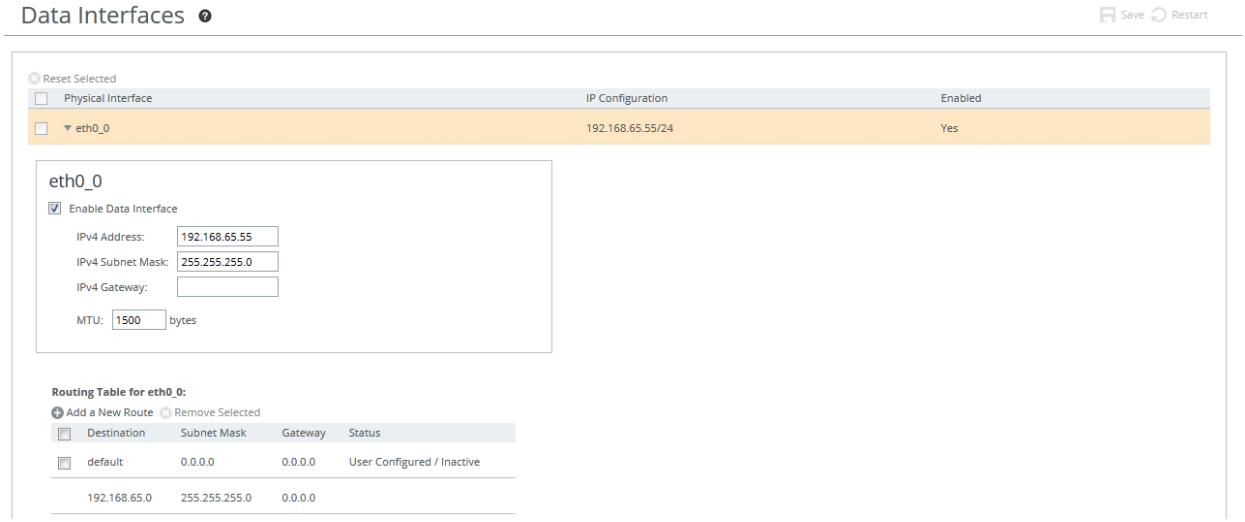
1. Configure the AltaVault appliance to the new network environment at the DR site.
   a. Plug a serial cable into the console port and a terminal, or, in the case of the virtual AltaVault appliance, use the virtual VMware console.
   b. Log in to the AltaVault CLI using the default login admin and default 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 you leave the default “Import Shared Data Only” checkbox selected.



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.



4. After the configuration is complete, connect to the AltaVault CLI using SSH and initiate the replication recovery procedure. For details, see the AltaVault Cloud Integrated Storage Administration 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 in order 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 prepop command parameters.

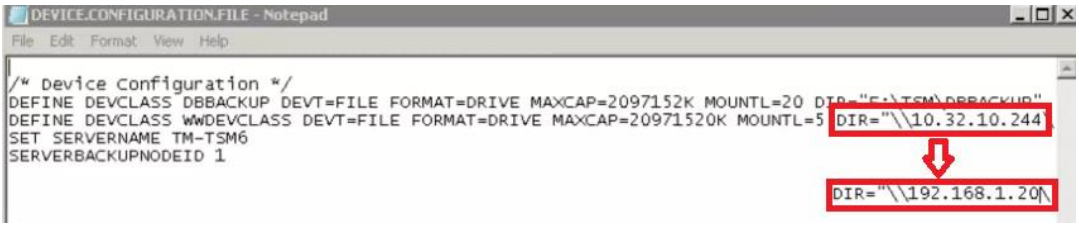
Parameter	Description
Num-days <number of days>	Filters the data retrieved by number of last-modified days.
Pattern <pattern>	Filters the data retrieved by the pattern you specify.
Recursive	Enables the data to be prepopulated in subdirectories under a given directory.
dryrun	AltaVault calculates the 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: 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 handle, then the recovery process might fail. AltaVault AVA v8, 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 Spectrum Protect media server.

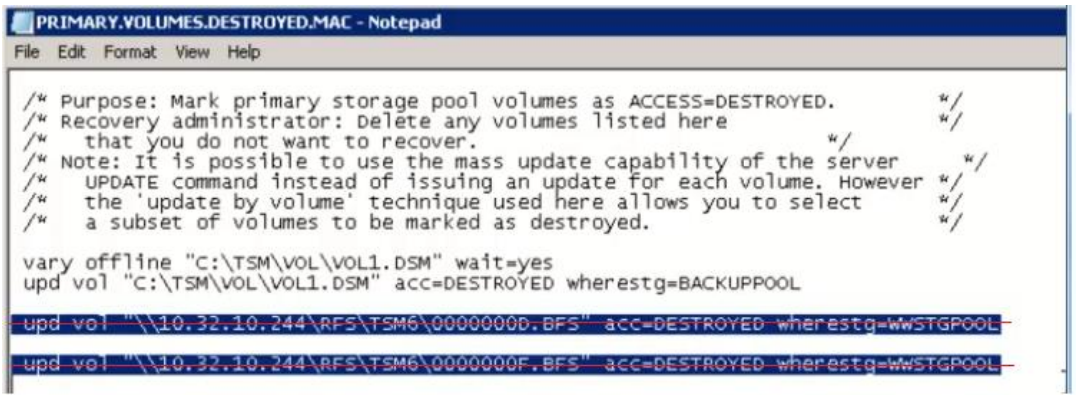
5.3 Spectrum Protect Recovery

After the AltaVault appliance has been recovered, you need to install and configure the Spectrum Protect server. The following procedures assume that you are using Spectrum Protect Disaster Recovery Manager (DRM) and have taken appropriate Spectrum Protect server database backups. See the TSM Disaster Recovery redbook available at http://redbooks.ibm.com for further details.

1. Install Spectrum Protect server to a new host system at the DR site. Make sure that the installation and configuration of the Spectrum Protect server db, log, and disk volumes are the same as in the previous production site and that the DRM files are split up in preparation for disaster recovery. Several of the DRM files can help you identify the paths for each of the preceding items.
2. Edit the DRM file DEVICE.CONFIGURATION.FILE using a text editor and adjust the AltaVault device class name to reflect the new IP addressing of the AltaVault data interfaces available at the DR site.



3. If the AltaVault appliance at the production site was used as a primary storage pool with Spectrum Protect, edit the DRM file PRIMARY.VOLUMES.DESTROYED.MAC and remove lines that refer to the volumes based on AltaVault. Because the AltaVault appliance at the DR site recovers the data from the cloud storage provider, there are no destroyed volumes that DRM must report to Spectrum Protect, and they are available when Spectrum Protect is brought up.



4. If the AltaVault appliance at the production site was used as a copy storage pool with Spectrum Protect, edit the DRM file COPYSTGPOOL.VOLUMES.AVAILABLE.MAC and adjust the AltaVault copy storage pool volume directory path to reflect the new IP addressing of the AltaVault interfaces available at the DR site. Because the AltaVault appliance at the DR site recovers the data from the cloud provider, there are no unavailable volumes that DRM must report to Spectrum Protect, and they are available when Spectrum Protect is brought up to recover the primary storage pool.
5. Run the DRM executable command file RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.CMD to begin the process of restoring the Spectrum Protect server to the last database backup state.

6. When the restore procedure is complete, update the device class definition that corresponds to the AltaVault device class to reflect the new network configuration of AltaVault at the DR site. This step is similar to step 2 earlier, but stores the change within the Spectrum Protect database.
   Use the UPDATE DEVCLASS command to make the modification to the network path to AltaVault:

```
UPDATE DEVCLASS <devclassname> DIRECTORY=\\<AltaVaultDataInterface>\<sharename>
```

   - **<devclassname>.** Provide a new device class name. It cannot match an existing device class name.
   - **DIRECTORY=\\<AltaVaultDataInterface>\<sharename>.** Enter a fully qualified domain name SMB share path value that corresponds to the AltaVault SMB share.

5.4 Production Systems Recovery

From this point forward, the AltaVault appliance and Spectrum Protect are configured as they were prior to the disaster, and you can now begin system restores of any production systems that need to be recovered at the DR site using normal Spectrum Protect recovery strategies such as intelligent disaster recovery. See Spectrum Protect 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 1.0a	Sept 2015	Minor corrections for clarity
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, dropped Simpana name
Version 1.4	January 2017	Updated for 4.3 release
Version 1.5	April 2017	Updated for 4.3.1 release
Version 1.6	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-4407-0117