



Technical FAQ

NetApp AltaVault Cloud-Integrated Storage

Christopher Wong, Technical Marketing, NetApp

Mike Braden, Technical Marketing, NetApp

April 2017

Abstract

This document is a technical FAQ for NetApp customers, sales engineers, partners, and solution providers that answers questions about how to setup and implement, manage, and monitor the NetApp® AltaVault® appliance.

TABLE OF CONTENTS

1 General	5
What is AltaVault?	5
What new features are available in the current AltaVault release?	5
Which public and private cloud storage providers does AltaVault support?	5
What backup applications does AltaVault support?	5
What type of deduplication, compression, and encryption technologies does AltaVault implement?	6
Does all the data that goes through AltaVault go to the cloud?	6
Does AltaVault support methods to reduce the initial seeding time to the cloud?	6
2 Setup	6
What are the prerequisites for getting a virtual AltaVault appliance set up for proof of concept?	6
What are the basic steps for getting a virtual AltaVault appliance running?	7
How do I troubleshoot and correct initial cloud configuration problems?	7
Can a virtual AltaVault appliance use more than one virtual disk for storing data?	8
How do I set up a cloud-based AltaVault appliance within Amazon Elastic Compute Cloud (Amazon EC2 Marketplace) or Azure Marketplace?	8
3 Upgrades	8
I have a customer using SteelStore, can they upgrade to AltaVault?	8
Is it possible to do a headswap from an AVA400 to an AVA800? Does that require downtime?	8
Will adding a new disk shelf or upgrading firmware require downtime?	8
If I add a new shelf and want to increase my cache, will the disk pool grow automatically or will I need to do manual steps for "restriping"?	8
Is it possible to do a swap from a smaller virtual instance to a large virtual instance?	8
Can I downgrade an AltaVault appliance?	9
4 Usability	9
Can an AltaVault appliance be configured to use two cloud storage providers simultaneously?	9
Can an AltaVault appliance be used in a multi-tenant environment?	9
If a customer's cloud provider eliminates service, can the contents of a cloud storage container created and used by an AltaVault appliance be transferred to another cloud storage provider?	9
Does AltaVault have a maximum amount of data that it can write to a cloud storage provider?	9
Can AltaVault appliances be used with any backup (or without backup) applications?	9
Does AltaVault work with NetApp SnapVault® or SnapManager® software?	9
What data ingest protocols does AltaVault support?	10
What versions of Server Message Block (SMB, also known as CIFS) and Network File System (NFS) are supported with the AltaVault appliance?	10
What changes have occurred with SMB starting in AltaVault v4.2?	10
When I map a share or mount an export, why is the reported space available so high?	10
What minimum storage technology does a virtual AltaVault appliance require?	10
Why does usable cache space appear to be lower than what is consumed from RAW capacity by RAID?	10

Can AltaVault guarantee a certain number of versions of backup can be maintained on cache?	10
My customer has 10GbE to the cloud. Can the AltaVault appliance use a 10GbE connection to talk to a cloud storage provider?	10
Can my customer use the AltaVault data interfaces in link aggregation (also referred to as a virtual interface, or VIF)?	11
Does the AltaVault appliance support VLAN tagging?	11
How do I troubleshoot performance problems with an AltaVault appliance?	11
What happens if there is a WAN outage or cloud storage provider outage?	11
What's the difference between AltaVault Backup mode and Cold Storage mode?	12
If my customers set up an AltaVault appliance in Cold Storage mode, can they switch to Backup mode? Or can an AltaVault appliance run in both modes simultaneously?	12
The data that is being sent to AltaVault isn't being deduplicated. How can this problem be fixed?	12
My customer has compressed or encrypted data. Can the customer elect to have AltaVault skip processing of this data?	12
Does the AltaVault appliance maintain logging and auditing or provide automated reporting and high-level summary information about the appliance state?	12
Amazon Glacier storage is cheap, but is that a good use case for AltaVault appliances given the 3- to 5-hour wait time for data?	12
Can I implement my own data usage policy using Amazon's interface tools?	13
Can multiple AltaVault appliances be managed from a central administration console?	13
Can data backed up from one AltaVault appliance be read back by another AltaVault appliance?	13
What is the maximum number of SMB/NFS mounts allowed?	13
Can AltaVault use the storage tiering capabilities offered by the Amazon S3 to Glacier API to selectively store data on S3 for a default period that is longer than 24 hours?	13
Can AltaVault take advantage of Glacier lock?	13
Does AltaVault support the use of Bulk or Expedited retrieval for Glacier recovery?	13
Can AltaVault use IPv6?	13
Does AltaVault have REST API support?	14
AltaVault is reporting that the cloud capacity is almost exhausted – what do I do?	14
What is the maximum writable limit I can send to Microsoft Azure blob storage today?	14
Does AltaVault support batch data import methods to reduce the initial seeding time to the cloud?	14
Can I write to multiple Amazon Snowballs?	14
Does AltaVault support receiving data from an AmazonSnowball?	14
Amazon Snowball Edge and Snowmobile are available – Does AltaVault support these devices?	14

5 Security.....14

Is there a security paper for AltaVault?	14
How secure are the contents of an AltaVault appliance?	14
What government security compliance certifications has the AltaVault appliance passed?	15
If the cloud credentials are compromised, is the data that AltaVault has stored at risk?	15
My customer's AltaVault administrator has left. How does my customer secure the appliance and cloud storage contents against unauthorized access?	15
Can an AltaVault appliance join more than one Windows Active Directory domain?	15
Are file permissions secured if my customer simply drags and drops files onto a SMB share on AltaVault?	15

Can an AltaVault appliance use my customer's existing CA-signed security certificate?	15
Can role-based permissions be established for users on the AltaVault appliance?.....	15
Does AltaVault support multi-factor authentication, or LDAP authentication for management?	16
Does the AltaVault appliance expose the operating system shell to users or administrators?	16
Does AltaVault support the Key Management Interoperability Protocol (KMIP)?	16
Which KMIP compliant are supported with AltaVault?	16
Can I import a public CA certificate for my private object storage target such as StorageGRID?	16
Can replication be configured across a specific interface?	16
Why was the peer replication capability removed from AltaVault?	16
6 Disaster Recovery	16
How do customers perform disaster recovery with a virtual AltaVault appliance?	16
Can AltaVault be used at a secondary site to test disaster recovery without affecting the data on the primary AltaVault appliance or cloud?	16
Can customers recover a destroyed AltaVault appliance in a data center by using an Amazon or Azure cloud-based AltaVault appliance?	17
Are AltaVault appliances offered in high-availability (HA) mode?	17
7 Data Fabric Solution for Cloud Backup	17
What is the Data Fabric Solution for Cloud Backup?	17
8 Services and Support	17
Is installation included in any of the support offerings?	17
When will SupportEdge Secure for Government be available on the AltaVault product?	18
Are there support limitations from NetApp for AltaVault?	18
Where can partners find enablement and training for AltaVault products?	18
9 Resources	18
Where can I find additional information or documentation?	18
I didn't see a feature my customer wants listed in documentation or this FAQ - where can I find additional information about future AltaVault features?	18

LIST OF FIGURES

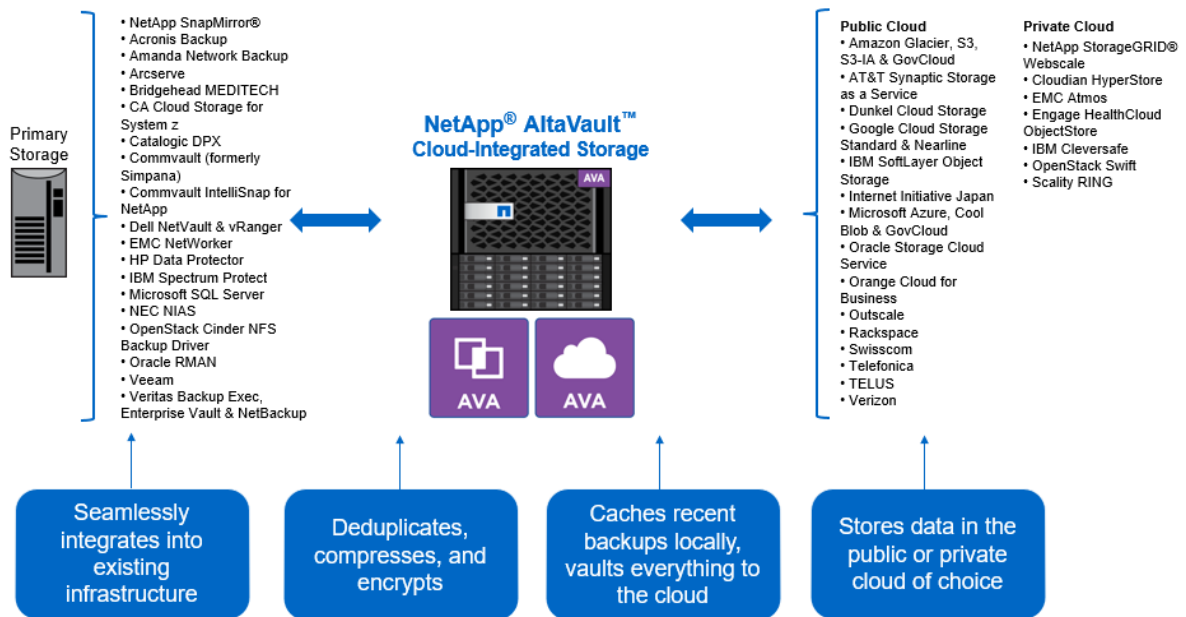
Figure 1) How AltaVault works.	5
-------------------------------------	---

1 General

What is AltaVault?

Answer: NetApp AltaVault is an enterprise-class cloud-integrated storage appliance that enables customers to securely and efficiently leverage public and private cloud as part of their backup and recovery strategy. AltaVault seamlessly integrates with existing backup software, and it compresses, deduplicates, encrypts, and streams data to the cloud provider of the customer's choosing. AltaVault intelligently caches recent backups locally while vaulting older versions to the cloud, allowing rapid local restores with off-site protection.

Figure 1) How AltaVault works.



What new features are available in the current AltaVault release?

Answer: Refer to the [current product release notes](#) to learn about the newest features available in AltaVault. As of version 4.3.1, the new features available include support for SnapMirror snapshots from ONTAP, support for Amazon Snowball seeding appliances, and support for Glacier expedited and bulk retrieval methods. In addition, AltaVault is now formally supported with OST operations from NetBackup appliances.

Which public and private cloud storage providers does AltaVault support?

Answer: AltaVault currently supports the following public cloud storage providers: Amazon (Glacier, S3, S3 Standard- Infrequent Access, and GovCloud), Dunkel Cloud Storage, Google Cloud Platform (Standard and Nearline), IBM SoftLayer and Bluemix Object Storage, IJ, Microsoft Azure (Cool, Blob, and GovCloud), Oracle Storage Cloud, Orange Cloud for Business, Outscale, Rackspace, Swisscom, Telefonica, TELUS, and Verizon. In addition, AltaVault supports private cloud storage built on NetApp StorageGRID Webscale, Cloudian HyperStore, EMC Atmos, IBM Cleversafe and OpenStack Swift, and Scalify RING. Always refer to the [Interoperability matrix \(IMT\)](#) for current support.

What backup applications does AltaVault support?

Answer: AltaVault supports the following backup applications: NetApp SnapProtect and SnapMirror; Amanda Network Backup; Arcserve; Acronis Backup; Catalogic DPX, Commvault and Commvault

Intellisnap for NetApp; Dell NetVault and vRanger; EMC NetWorker; HP Data Protector; IBM Spectrum Protect (Tivoli Storage Manager); NEC NIAS; OpenStack Cinder; Veeam; and Veritas (Symantec) Backup Exec, Enterprise Vault, and NetBackup. In addition, AltaVault also supports database backups performed by Microsoft SQL Server and Oracle RMAN. Always refer to the [Interoperability matrix \(IMT\)](#) for current support.

What type of deduplication, compression, and encryption technologies does AltaVault implement?

Answer: AltaVault implements variable-block-length, inline deduplication using a strong SHA-256 bit hash to eliminate the need for redundant blocks to be stored and sent to cloud storage. In addition, AltaVault implements LZ compression and encrypts data by using AES 256-bit encryption.

Does all the data that goes through AltaVault go to the cloud?

Answer: Yes, all the data that AltaVault ingests must go to either a public or a private cloud. AltaVault does not support non-cloud replicating scenarios, such as “local storage only” mode or “selective cloud replication” mode. Implement AltaVault with a private cloud such as StorageGRID Webscale or OpenStack if the solution requires the backup data remain on premise. StorageGRID Webscale offers tiering to Amazon S3, so you can implement a tiered local and cloud storage solution using this object storage solution.

Does AltaVault support methods to reduce the initial seeding time to the cloud?

Answer: There is no general physical media seeding capability (also known as bulk ingest) available but AltaVault now supports Amazon Snowball to seed data to Amazon S3 storage. In general, if customers have minimal bandwidth, they are not going to be happy cloud customers. However, if their bandwidth is good enough but they don't want to wait for seeding, there is an easy way to migrate the data quickly. Customers can sign up for a burstable pipe to the Internet and set the value higher for the first few weeks to get the massive data transferred.

Answer: The other option is to ship the AltaVault appliance to an Equinix site (or a local VAR with fast Internet access) where the customer can buy a 10GbE link to Amazon directly and do the first seed there. After that step, the box can be moved back on-premises where the customer has a more modest pipe and be successfully connected to the cloud data again.

2 Setup

What are the prerequisites for getting a virtual AltaVault appliance set up for proof of concept?

Answer: You must have the following prepared for an installation. Refer to the NetApp AltaVault Cloud-Integrated Storage [Installation and Service Guide for Virtual Appliances](#) for a complete list of requirements.

1. A supported VMware, Microsoft Hyper-V, or Linux KVM hypervisor.
2. Confirmation that the hypervisor can allocate a minimum of 6GB of RAM and 4 virtual CPU for an AVA-v2. Higher virtual AltaVault models require further resources.
3. A minimum of two IP addresses (NetApp highly recommends that they be static IPs in different subnets) to manage and send data from the appliance. One of the two IP addresses must be WAN accessible with DNS resolution to the cloud storage provider that you plan to use.
4. A cloud storage account and related authentication credentials.

Note: The appliance cannot initialize until these credentials are provided.

5. One manually added disk volume, beyond the one deployed with the virtual AltaVault appliance, for the AltaVault cache. It is recommended to deploy the volume as recommended in the AltaVault Virtual Install Guide using a thick-provisioned volume of appropriate size for the version being used.

What are the basic steps for getting a virtual AltaVault appliance running?

Answer: There are six steps for setting up a virtual AltaVault appliance. These steps are fully documented in the NetApp AltaVault Cloud-Integrated Storage [Installation and Service Guide for Virtual Appliances](#), but are provided in abbreviated form here:

1. Deploy the VM onto your chosen hypervisor as outlined in the Installation and Service Guide for Virtual Appliances. Ensure the VM meets the virtual CPU, memory, and disk requirements of the model being deployed.
2. Add the second disk which represents the cache to the VM. This needs to be done prior to powering on the VM.
3. Power on the AltaVault appliance and connect to it through the hypervisor console. Step through the command-line wizard to provide initial management networking for the appliance.
4. Log in to the AltaVault appliance GUI by using a web browser. On new installations, the Setup wizard automatically appears. If it does not appear, you can access the Setup wizard by using the Configure > Setup Wizard menu. Follow the steps in the first two Setup wizards (System Settings and Cloud Settings). Use the System Settings wizard to verify the DNS and time zone of the appliance. Use the Cloud Settings wizard to provide the cloud credentials and configure encryption,. If you provide the information correctly, you receive a cloud connection check successful message.

Note: If there is a configuration problem, you receive an error message or no messages at all. Refer to the following troubleshooting section for tips.

5. Exit the Setup wizard and configure SMB shares, NFS exports, or OST shares from the Configure menu. Fill out the appropriate information to add a share or export. For Windows environments, you can add the AltaVault appliance to an Active Directory domain and configure access control through Active Directory credentials. For Linux environments, you can add NFSv4 Kerberos authentication.
6. Configure at least one data interface through the Configure > Data Interfaces menu. This interface connects to your backup infrastructure to receive backup data.

How do I troubleshoot and correct initial cloud configuration problems?

Answer: There are common problems that can cause initial AltaVault cloud configuration to fail:

- **A second disk was not added before booting the virtual AltaVault appliance.**
Deploying the virtual AltaVault appliance by using the template does not provide a second disk. The second disk must be associated with the VM before you start the appliance.
- **The time or date is too far out of sync with the intended cloud storage provider.** Temporarily resolve this problem by manually configuring the date and time from Configure > Date and Time. If you are using a private cloud storage provider, also make sure that your cloud provider time and time zone settings are correct.
- **Cloud storage credentials are incorrect.** NetApp recommends copying and pasting the authentication values from your cloud provider to prevent typos from manual entries. Make sure that there are no leading or trailing spaces in any of the authentication values provided. Also make sure that the correct cloud provider target, port, storage class, and region are being used. For StorageGRID Webscale you can import the required certificate to AltaVault, or disable certificate checks on AltaVault using the CLI command `no replication ssl verify-certs`.
- **The encryption key is missing.** If this step was not performed by using the Cloud Settings wizard, use the Configure > Cloud Settings page and use the Encryption tab to create an encryption key.
- Additional troubleshooting tips can be reviewed in support kbase article [2024963](#).

Can a virtual AltaVault appliance use more than one virtual disk for storing data?

Answer: A virtual AltaVault appliance can use only one LUN or volume as the target for data. The size of the volume can be expanded, however, to the maximum size allowed by the given appliance license and does not need to be fully allocated initially. If the appliance will be converted from a proof of concept (POC) to a paid unit, size the appliance disk appropriately at initial deployment for the target license that will be applied.

How do I set up a cloud-based AltaVault appliance within Amazon Elastic Compute Cloud (Amazon EC2 Marketplace) or Azure Marketplace?

Answer: Refer to the NetApp AltaVault Cloud-Integrated Storage [Installation and Service Guide for Cloud Appliances](#) manual. Also refer to the video demonstrations ([AWS AMI](#)) ([Azure AVM](#)) on configuring the cloud-based AltaVault appliance.

3 Upgrades

I have a customer using SteelStore, can they upgrade to AltaVault?

Answer: AltaVault provides support for SteelStore users who wish to upgrade to AltaVault. Learn the general upgrade paths available in this [Powerpoint](#) presentation, then refer to the following resources for each migration scenario:

1. Physical SteelStore 3.2.3 to Physical AltaVault 4.0.1 or higher: [AltaVault Administration Guide](#), Ch 13, [migration video](#)

Answer: 2. Virtual SteelStore 3.x to Virtual AltaVault 4.x: [Installation and Service Guide for Virtual Appliances](#), Appendix B

Answer: 3. Cloud-based SteelStore 3.x to Cloud-based AltaVault 4.x: [Installation and Service Guide for Cloud Appliances](#), Appendix A

Is it possible to do a headswap from an AVA400 to an AVA800? Does that require downtime?

Answer: AltaVault appliance controllers cannot be swapped for a larger model, due to the fact that they rely on specifically sized disks within attached disk shelves. AVA400 controllers will only work with DS4246 shelves with 4TB disks, and AVA800 controllers will only work with DS4246 shelves with 6TB disks.

Will adding a new disk shelf or upgrading firmware require downtime?

Answer: Yes, AltaVault requires downtime to perform these maintenance activities. Ensure that AltaVault cleanly shuts down to avoid possible data consistency issues. Refer to the Installation and Service Guide for Physical Appliances for details.

If I add a new shelf and want to increase my cache, will the disk pool grow automatically or will I need to do manual steps for “restripping”?

Answer: AltaVault, when brought up after a new shelf is added, will recognize and automatically increase its usable cache space.

Is it possible to do a swap from a smaller virtual instance to a large virtual instance?

Answer: Answer: Yes, virtual instance licenses can be upgraded to a similar hypervisor platform. Refer to the [Installation and Service Guide for Virtual Appliances](#), Appendix A. for details. Note that your existing virtual license will not be used when the larger virtual license is installed.

Can I downgrade an AltaVault appliance?

Answer: Answer: AltaVault does not currently support downgrades of software nor downgrades of the version of virtual AltaVault appliance.

4 Usability

Can an AltaVault appliance be configured to use two cloud storage providers simultaneously?

Answer: An AltaVault appliance can be associated with only a single cloud storage provider (which is performed at setup). Customers who wish to change cloud storage providers can use the AltaVault Cloud Agility feature to change from one cloud provider to another. Refer to the next question for details.

Can an AltaVault appliance be used in a multi-tenant environment?

Answer: An AltaVault appliance does not support multitenancy scenarios where multiple customers use the same appliance. Data deduplication and compression is performed across all data received by AltaVault, and is not measured by each share to determine per tenant charge back or capacity utilization.

If a customer's cloud provider eliminates service, can the contents of a cloud storage container created and used by an AltaVault appliance be transferred to another cloud storage provider?

Answer: Data stored by an AltaVault appliance can be migrated to another cloud provider at any time by using the AltaVault interface. Data is recalled from the first cloud storage provider to the appliance and is directly uploaded to the second cloud storage provider. No AltaVault local cache space is consumed by the operation, and writes can resume after the migration completes. Refer to the [AltaVault Administration Guide](#) for details and [this video](#) for a demonstration of the feature.

Does AltaVault have a maximum amount of data that it can write to a cloud storage provider?

Answer: Each AltaVault appliance starts off with a preset allocated amount of space, which depends on the model selected. For physical appliances, this amount can be expanded by adding shelves. The cloud capacity granted is 5 times the appliance cache size. The overall amount of user data that can be written depends on the deduplication rate achieved by the AltaVault appliance. Refer to the [NetApp AltaVault technical specifications](#) for more details.

Can AltaVault appliances be used with any backup (or without backup) applications?

Answer: AltaVault appliances have been qualified and tested with the backup applications documented, and only those backup applications are officially supported. A mix of supported applications can send data to a single appliance, but NetApp highly recommends that each backup application write to its own share or mount point on the AltaVault appliance. Backup applications not specifically listed in the Interoperability Matrix are not supported by NetApp.

Sending data to AltaVault without a backup application can also be accomplished, but overall performance and data policy management vary depending on the makeup of the dataset and which tool is used to copy the data to AltaVault. Refer to the [IMT](#) for current details about interoperability support.

Does AltaVault work with NetApp SnapVault® or SnapManager® software?

Answer: AltaVault version 4.3 and higher now supports SnapMirror capability as a component of the Data Fabric Solution for Cloud Backup. Refer to section 7 *Data Fabric Solution for Cloud Backup* below and the [Data Fabric Solution for Cloud Backup FAQ](#) for further details about the features and capabilities supported in this solution.

What data ingest protocols does AltaVault support?

Answer: AltaVault supports Server Message Block (SMB), Network File System (NFS), and Veritas OpenStorage (OST) protocols. These protocols are supported by a vast majority of the backup applications available on the market. In addition, AltaVault v4.3 and higher now supports the ability to directly receive ONTAP® Snapshot™ backups using SnapMirror, NetApp's snapshot replication engine.

What versions of Server Message Block (SMB, also known as CIFS) and Network File System (NFS) are supported with the AltaVault appliance?

Answer: AltaVault appliances currently support SMBv2 and v3 and NFSv3 and v4 protocols. Veritas OST support is enabled starting with NetBackup 6.5 and 7.7.

What changes have occurred with SMB starting in AltaVault v4.2?

Answer: AltaVault appliances starting at version 4.2 have updated SMB support, which can now support SMBv3 connections from Windows 2012/2012 R2 servers, and SMB multi channel connections. However, it is advised to carefully review [TR-4511](#) if you are considering an upgrade of an AltaVault that has SMB shares and is being upgraded from a version prior to 4.2 to version 4.2 or higher.

When I map a share or mount an export, why is the reported space available so high?

Answer: AltaVault reports a large available size to ensure a backup application does not run into a low space condition when using a share or export. Because AltaVault deduplicates, compresses, and encrypts the data, the actual storage consumed on AltaVault will be much less than the data received by the backup application share or export.

What minimum storage technology does a virtual AltaVault appliance require?

Answer: Virtual AltaVault appliances should be placed on storage array disk subsystems that have at least RAID-1 disk protection. It is recommended to have RAID-5 or higher protection and high performing disk to reduce performance impacts to AltaVault within a virtualized environment.

Why does usable cache space appear to be lower than what is consumed from RAW capacity by RAID?

Answer: AltaVault appliances reserve portions of the cache space to hold supporting structures, such as metadata and hash tables. These are not counted towards the usable cache space, but consume space from the disk after RAID is performed. The usable cache space represents the amount of data that a user can store onto the appliance, independent of the supporting structures that consume the additional space.

Can AltaVault guarantee a certain number of versions of backup can be maintained on cache?

Answer: To ensure that you maintain the current backups on cache for quick restore, you can configure the cloud provider setting "Enable cloud deduplication" to ensure that the data is always on cache for the most recent backups. This prevents the situation where a current backup may deduplicate against data only in the cloud, and therefore require data from the cloud for restore. Because AltaVault appliances use least recently used (LRU) eviction mechanism to remove data that has not been accessed recently, it is also important to size the solution correctly so that the backups can be maintained on cache without impacting other backups in the range you wish to maintain locally.

My customer has 10GbE to the cloud. Can the AltaVault appliance use a 10GbE connection to talk to a cloud storage provider?

Answer: Yes, an AltaVault appliance can use 10GbE to communicate with a cloud storage provider at 10GbE speed. Note, however, that performance will peak at the stated rates documented in the [AltaVault Specification Sheet](#). Refer to [TR-4416 AltaVault Performance Tuning Guide](#) for further details on 10GbE deployment.

Can my customer use the AltaVault data interfaces in link aggregation (also referred to as a virtual interface, or VIF)?

Answer: Yes, your customers can aggregate the interfaces together (NetApp recommends using 802.3ad mode), assuming that their network switch has the ability to support link aggregation. Watch the [VIF overview video](#) to get an overview and understand considerations for setting up a VIF.

Note: AltaVault VIF is used primarily for redundancy and ease of management. However, your customers might gain additional performance benefits if data is being sent from multiple backup sources. Refer to the [TR-4416 AltaVault Performance Tuning Guide](#) for additional details.

Does the AltaVault appliance support VLAN tagging?

Answer: Yes, AltaVault appliances version 4.2 and higher provide the capability to support VLAN tagging. Users will need to configure networking and AltaVault appropriately to allow the AltaVault appliance to communicate with the proper subnets based on the VLAN tags.

How do I troubleshoot performance problems with an AltaVault appliance?

Answer: Because AltaVault represents a connection point along the backup chain, troubleshooting performance related to backups can be tricky. Review the following to help isolate performance problems:

1. Ensure that AltaVault is not performing other activities other than receiving data from the backup application. Random I/O requests or heavy amounts of read activity can disrupt the performance profile of reading long backup streams, reducing performance. Common causes for performance degradation can include but are not limited to the following types of activities:

- Backup applications performing verification or restore operations.
- Backup applications performing synthetic full or reverse full operations.
- Anti-virus applications reading back the data during file system scans. Media servers should not have anti-virus scanning being performed of backup data.
- AltaVault eviction running while backups are in flight

2. Try to baseline network performance without backup applications or complex networks (i.e. VIFs/LACP) as a first step.

3. Use single session actions to measure per session throughput.

4. Try operations with a different AltaVault share or protocol type, or within the context of a different backup application.

5. Check the NIC (client, master/media server) and switch adapter settings for all devices in the data path to AltaVault and ensure that they are all configured for equivalent MTU size.

6. If performance measures 100MB/s when using 10Gbe interfaces look for signs of a 1gb/s network link.

7. Check that the backup infrastructure is able to sustain backup speeds to other types of storage.

8. Check for signs of source based bottlenecks. Typical throttles include limited disk resources or I/O, high CPU utilization, and incorrect network interface configurations.

9. Check AltaVault reports to confirm if there are multiple concurrent operation types being executed. Multiple operations can impact disk I/O. For example, simultaneous backups and cloud restores, or backups and cache eviction and cache restores can be impactful to ingest performance.

10. Refer to the [AltaVault Performance Tuning Guide](#) for further troubleshooting information and how to properly configure the appliance for ingest performance with backup applications. Guidance is also provided about expected capabilities AltaVault can achieve under certain controlled workloads.

What happens if there is a WAN outage or cloud storage provider outage?

Answer: AltaVault appliances communicate regularly with the cloud provider to verify the link state. In the absence of a connection, AltaVault stores and logs all uncommitted cloud storage data and related transactions in local storage until the cloud storage connection has been reestablished. If the WAN outage lasts long enough for the AltaVault local storage to fill completely, AltaVault notifies applications by denying write attempts of data.

What's the difference between AltaVault Backup mode and Cold Storage mode?

Answer: Backup mode is optimized for repeating datasets and rapid backups and recoveries. In Backup mode, the AltaVault appliance keeps recent copies of regularly recurring backups in cache for quick recoveries, while also vaulting data out to the cloud. Dedupe rates typically are higher in backup mode. Cloud capacity is limited to 5 times that of the cache (i.e. AVA-v32 with 32TB usable cache can manage a cloud capacity of 160TB).

Cold Storage, or archive, mode enables customers to efficiently use the cloud for infrequently accessed and non-recurring data for archives. Examples of archive use cases include but are not limited to storing data for regulatory compliance or legal retention. In this mode, the AltaVault appliance uses the local cache largely for metadata, and it maintains only a minimum amount of cache for recent data, increasing the cloud storage scalability of the solution by more than 5 times. Cold storage mode will typically see much lower deduplication and performance rates because of the smaller cache for files, the nature of archive data being non-repeating, optimized (i.e. jpg, mp4, zip) file types, and due to AltaVault eviction removing deduplication hashes with the data when space is needed for new data.

In most circumstances, backup mode should be selected for AltaVault solutions.

If my customers set up an AltaVault appliance in Cold Storage mode, can they switch to Backup mode? Or can an AltaVault appliance run in both modes simultaneously?

Answer: During the initial setup of an AltaVault appliance, customers can select only one mode or the other. After customers set the mode, they cannot change it. To change the mode, they must delete the entire contents of the AltaVault appliance cache and rerun the setup to configure the appliance anew.

Note: This action effectively orphans all the data that AltaVault previously sent to cloud storage, unless the customer instructs the AltaVault appliance to delete cloud data as well.

The data that is being sent to AltaVault isn't being deduplicated. How can this problem be fixed?

Answer: Data should be transmitted from the backup application to the data interfaces on AltaVault. Review the SMB, OST or NFS mount being used by the backup application and make sure that it is addressing the DNS or IP address of a data interface on AltaVault. Make sure that the SMB, OST or NFS export is not enabled with the Disable Dedupe or Disable Compression options. Confirm the data file type being sent to AltaVault and make sure that it is not encrypted or already in an optimized file format as this will lower both deduplication and ingest performance of AltaVault.

My customer has compressed or encrypted data. Can the customer elect to have AltaVault skip processing of this data?

Answer: AltaVault can disable its own deduplication and compression operations for incoming data streams that are already deduplicated or compressed. This action is performed at the SMB share or NFS mount point level when exposed to the backup system. Encryption is always performed to protect data that will reside in cloud storage, and encryption cannot be disabled.

Does the AltaVault appliance maintain logging and auditing or provide automated reporting and high-level summary information about the appliance state?

Answer: Yes. AltaVault has complete logging and auditing capabilities, with varying levels of reporting capability available, depending on what administrators require. In addition, high-level executive summary reports can be scheduled and e-mailed, as well as alerts about any warning or critical errors that an AltaVault appliance encounters.

Amazon Glacier storage is cheap, but is that a good use case for AltaVault appliances given the 3- to 5-hour wait time for data?

Answer: By default, AltaVault appliances send all data to cloud storage but maintain a hot cache of the most frequently accessed data for quick restore. When an AltaVault appliance in backup mode is coupled

with Amazon Glacier, AltaVault can provide local availability for many days or weeks of data while storing the unused data in inexpensive but highly durable Glacier storage. This however incurs a significant recovery time cost for backups that are not available on the AltaVault cache. For backup workloads, it is highly recommended to have AltaVault use either S3 or S3-IA as the cloud storage target instead. When storing infrequently accessed data, such as for archives, using an AltaVault appliance in cold storage mode coupled with Amazon Glacier can reduce costs while greatly increasing accessible capacity, but at the cost of cache space for most restores. Refer to the [AltaVault Administration Guide](#) for considerations on using AltaVault with Amazon Glacier.

Can I implement my own data usage policy using Amazon's interface tools?

Answer: AltaVault will manage the data location and lifecycle policies for you, and you should not attempt to use Amazon tools to manage the data policy lifecycles of the data.

Can multiple AltaVault appliances be managed from a central administration console?

Answer: AltaVault provides a feature called peer monitoring, which allows an AltaVault appliance to provide single-pane-of-glass monitoring of additional AltaVault appliances in the environment. Refer to the [AltaVault Administration Guide](#) for details on configuring peer monitoring.

Can data backed up from one AltaVault appliance be read back by another AltaVault appliance?

Answer: An AltaVault appliance at a secondary location can provide limited read-only access to data written by a primary AltaVault appliance. To accomplish this access, the primary AltaVault appliance must have completed (or paused) replication, which then allows the secondary AltaVault appliance read-only access to the data, such as for disaster recovery testing. AltaVault is not supported as a multisite, multiuser collaboration appliance, and it cannot perform multisite reads of data when replication from the primary appliance is in flight. Refer to [TR-4420 AltaVault DR best practices](#) and [this video](#) on performing DR testing.

What is the maximum number of SMB/NFS mounts allowed?

Answer: AltaVault appliances can create up to 256 SMB shares or NFS mounts.

Can AltaVault use the storage tiering capabilities offered by the Amazon S3 to Glacier API to selectively store data on S3 for a default period that is longer than 24 hours?

Answer: AltaVault supports the migration delay of data from Amazon S3 to Glacier beyond the default period, which is up to 24 hours. However, it is important to understand that using this migration delay does not guarantee the data will be recalled from S3, due to the API functionality which control data migration. This can still result in delayed restores even if the backup is recent. Further development by both engineering at NetApp and Amazon is required to fully integrate this feature into AltaVault.

Can AltaVault take advantage of Glacier lock?

Answer: AltaVault does not currently support the use of Glacier lock to protect files for long term locking.

Does AltaVault support the use of Bulk or Expedited retrieval for Glacier recovery?

Answer: AltaVault supports the standard retrieval method for Glacier today, and is investigating support for the two other modes of Glacier retrieval.

Can AltaVault use IPv6?

Answer: IPv4 is the only TCP/IP protocol that is supported with AltaVault. IPv6 is not supported at this time.

Does AltaVault have REST API support?

Answer: AltaVault has limited REST API support, which will be enhanced with future versions of the appliance. At this time, the REST API does not have any deployment or manageability features that service providers would require to create scripted solutions. Instead, users can create scripted actions using the AltaVault CLI, as discussed in this [AltaVault scripting guide](#).

AltaVault is reporting that the cloud capacity is almost exhausted – what do I do?

Answer: AltaVault can write up to the limit provided by the appliance type, plus a grace of 10 percent. For example, a fully loaded AVA800 appliance with 4 shelves can protect 1.92PB + 10%, or 2.11PB in the cloud. As AltaVault nears the cloud capacity, it will trigger alarms indicating cloud capacity is almost reached, and email notifications if configured on AltaVault. To address cloud capacity, you can either reduce consumption by expiring older backups via the backup application policy, or expand capacity in AltaVault physical models by adding additional shelves and disk packs. Each disk pack will allow AltaVault to address additional cloud capacity.

What is the maximum writable limit I can send to Microsoft Azure blob storage today?

Answer: AltaVault can write up to 500TB of cloud data to Microsoft Azure blob storage due to storage limits imposed by Azure. If you require more space than is provisioned for this blob storage target, use a second AltaVault writing to a second blob storage target in Azure storage.

Does AltaVault support batch data import methods to reduce the initial seeding time to the cloud?

Answer: Starting with version 4.3, AltaVault supports Amazon Snowball to perform onsite batch data import. When shipped back to Amazon, Snowball will seed S3 object storage with the AltaVault data.

Can I write to multiple Amazon Snowballs?

Answer: AltaVault can only write to one Snowball at a time. Fill a Snowball before beginning data transfer to the next Snowball.

Does AltaVault support receiving data from an AmazonSnowball?

Answer: Snowball operations are currently enabled to assist users in seeding their S3 cloud with AltaVault data. Future functionality may make restore using Snowball a possibility. Refer to the NDA sharepoint to review future Snowball features being considered for inclusion.

Amazon Snowball Edge and Snowmobile are available – Does AltaVault support these devices?

Answer: AltaVault qualification has been completed only with 50TB and 80TB Snowball devices, and not with Snowball Edge or Snowmobile. Support for these devices is being considered for a future release.

5 Security

Is there a security paper for AltaVault?

Answer: Yes, refer to the [AltaVault security paper](#) for details about how AltaVault secures data, interfaces, and access.

How secure are the contents of an AltaVault appliance?

Answer: AltaVault appliances receive and process data within internal memory as it is received over the LAN. That data is then encrypted with AES 256-bit encryption before being written to the disks and to the cloud by using an TLSv1.1/1.2 connection. The data is always stored in encrypted format, whether it is on the appliance or in cloud storage.

The encryption key can be managed with role-based administration and can be protected by using a rotating passphrase that prevents unauthorized access to the encrypted data. AltaVault appliances secure the encryption key and other pertinent security information such as cloud credentials within the secure vault. This secure vault is an on-disk security space that is unlocked (and read into nonpersistent memory) at boot time by using a secure AES 256-bit password that can be changed or set only by an administrator. Optionally, the encryption key and cloud credentials can be stored on a key management server (KMS) using the KMIP protocol.

What government security compliance certifications has the AltaVault appliance passed?

Answer: AltaVault partners with cloud storage providers to deliver overall security of data during its lifecycle. Providers such as Amazon, AT&T, HP, Google, and others each have their own compliance certifications, such as FIPS, SOX, and HIPAA compliance. AltaVault offers data-at-rest and in-flight encryption using FIPS 140-2 level 1 validated encryption using the NetApp Cryptographic Security Module (NCSM). See the Cryptographic Module Validation Program (CMVP) [FIPS 140-2 Modules in Process List](#) for current NCSM status.

If the cloud credentials are compromised, is the data that AltaVault has stored at risk?

Answer: No. Because AltaVault encrypts all data before sending it to the cloud storage provider, the exposure to security risks is minimal. Customers can simply rotate the cloud credentials to resecure their cloud storage, and enter those new credentials into the AltaVault appliance page (located under Storage, Cloud Settings).

My customer's AltaVault administrator has left. How does my customer secure the appliance and cloud storage contents against unauthorized access?

Answer: Remove the former administrator's credentials from the AltaVault appliance and rotate the encryption key password (Storage, Cloud Settings, Encryption). NetApp also recommends rotating the cloud storage provider authentication credentials and updating the AltaVault appliance with the new credentials. Your customer should be sure to save and reexport the updated AltaVault configuration for safekeeping.

Can an AltaVault appliance join more than one Windows Active Directory domain?

Answer: No, an AltaVault appliance can be a member of only one Windows Active Directory domain at a time. To switch domains, leave the first Active Directory domain and then add AltaVault to the second Active Directory domain. AltaVault can be directed to speak to a specific set of Windows domain controllers.

Are file permissions secured if my customer simply drags and drops files onto a SMB share on AltaVault?

Answer: Yes. If your customer has added the AltaVault appliance to a Windows Active Directory domain, all files managed by the appliance maintain the ACL permissions when stored on the appliance.

Can an AltaVault appliance use my customer's existing CA-signed security certificate?

Answer: AltaVault appliances can accept PEM, PKCS12, or DER-formatted web certificates, generated by a CA-signed public authority. AltaVault appliances can also generate private key and self-signed public certificates.

Can role-based permissions be established for users on the AltaVault appliance?

Answer: Yes. AltaVault provides role-based permissions for a variety of users, including reporting, administration, security, replication, and storage roles. AltaVault administrators can create and set up roles for these various groups according to business requirements.

Does AltaVault support multi-factor authentication, or LDAP authentication for management?

Answer: AltaVault does not have support for either of these features today. Supported authentication methods include using TACACS+ and RADIUS.

Does the AltaVault appliance expose the operating system shell to users or administrators?

Answer: No. AltaVault provides a command line for users to administer the appliance, but, for security purposes, does not expose the operating system shell. Shell access is restricted to support use only, and it requires authentication to enable.

Does AltaVault support the Key Management Interoperability Protocol (KMIP)?

Answer: As of version 4.1, AltaVault appliances supports KMIP for managing encryption keys and cloud credentials. Refer to the [AltaVault Administration Guide](#) for more details on configuration of a Key Management Server (KMS). If configuring a new AltaVault appliance with KMS, refer to [this video](#). If configuring an existing AltaVault for use with KMS, refer to [this video](#).

Which KMIP compliant are supported with AltaVault?

Answer: Key managers that are currently supported with AltaVault include SafeNet and Vormetric Virtual Key Manager. Refer to the [IMT](#) for current details about interoperability support.

Can I import a public CA certificate for my private object storage target such as StorageGRID?

Answer: Yes. As of version 4.1.1 you can import a CA certificate for use with your private cloud storage provider. The file must be provided in .PEM format.

Can replication be configured across a specific interface?

Answer: Yes. Customers can select the cloud replication interface in the Configure > Cloud Settings page. Alternatively, customers can force all traffic across a specific interface by removing the default routing entry and specifying the data gateway entry on a specific data interface. Refer to the [AltaVault Performance Tuning Guide](#) for further details.

Why was the peer replication capability removed from AltaVault?

Answer: Peer replication was an infrequently used feature by installed customers, and architecturally did not meet the requirements of customers. AltaVault will be enhanced to deliver improved replication capabilities in the future. AltaVault relies on its core strengths which are efficient and secure cloud replication, use of the cloud to provide DR capabilities, reduced management and overall reduced TCO.

6 Disaster Recovery

How do customers perform disaster recovery with a virtual AltaVault appliance?

Answer: If the AltaVault appliance has a populated and available local cache, most or all of the disaster recovery can be performed from the local cache by using the most recent backups. If the primary site has been lost, a replacement virtual or physical AltaVault appliance must be spun up at a secondary site and used to restore the data. Refer to the [AltaVault DR Best Practices guide](#) and [overview video of AltaVault DR](#).

Can AltaVault be used at a secondary site to test disaster recovery without affecting the data on the primary AltaVault appliance or cloud?

Answer: Yes, a secondary AltaVault appliance can be used in test DR mode to read data back from the cloud, without affecting any operations from the primary AltaVault appliance or the contents of the cloud.

The primary AltaVault appliance simply delays replicating data to the cloud while the secondary AltaVault appliance reads the data for the DR test. After the DR tests are finished, customers should spin down the secondary AltaVault appliance and resume replication on the primary appliance. Refer to [this video](#) on performing AltaVault DR testing.

Can customers recover a destroyed AltaVault appliance in a data center by using an Amazon or Azure cloud-based AltaVault appliance?

Answer: Yes, customers can use a physical, virtual, or cloud-based AltaVault appliance to recover any lost physical or virtual AltaVault appliance. As long as customers have the exported configuration of the lost appliance, they can recover it onto a new cloud-based AltaVault appliance.

Are AltaVault appliances offered in high-availability (HA) mode?

Answer: No, AltaVault appliances do not currently have the ability to perform automated failover or failback, which is a component of HA design.

7 Data Fabric Solution for Cloud Backup

What is the Data Fabric Solution for Cloud Backup?

Answer: The NetApp Data Fabric Solution for Cloud Backup delivers a comprehensive cloud-integrated data protection solution that streamlines backup operations through array based replication and efficient, automated management. The Data Fabric Solution for Cloud Backup includes the following components:

- NetApp FAS or AFF primary or secondary storage running ONTAP 9.1 RC2 or later with at least one of the following:
 - SnapMirror license (a la carte or with Premium Bundle)
 - SnapVault license (a la carte or with Premium Bundle)
- NetApp AltaVault (physical or virtual) running software version 4.3
- SnapCenter 2.0 with Advanced license
 - Advanced license includes file catalog for file search and restore, AltaVault support, and enhanced automation associated with this solution.

[Sales and technical FAQ](#) for the Data Fabric Solution for Cloud Backup are available to answer specific questions related to this solution. In addition, SnapCenter 2.0 also has a [technical FAQ](#) available.

8 Services and Support

Is installation included in any of the support offerings?

Answer: Answer: Installation service is available separately from NetApp Services or from Professional Services Certified (PSC) partners. SupportEdge Premium (available for AltaVault) includes installation in the offering.. Support Services are available through SupportEdge offerings from NetApp (SupportEdge Standard, Premium, and SESG) or from NetApp reseller or distribution partners.

Answer: Customers who want NetApp assistance with design or configuration reviews, implementation services, or knowledge transfers (similar to the Riverbed legacy JumpStart service) can request a custom quotation from NetApp. They can request assistance on a time-and-materials or SOW basis, or they can work with reseller or distribution partners who can resell NetApp professional and support services.

Answer: What services can partners provide to NetApp customers?

Answer: Answer: All NetApp partners can resell professional and support services from NetApp.

Answer: Professional Services Certified (PSC) partners can provide partner-branded installation, design, and implementation services; Support Services Certified (SSC) Partners can sell partner-branded support services starting in Q3 of calendar year 2015.

When will SupportEdge Secure for Government be available on the AltaVault product?

Answer: Answer: SupportEdge Secure for Government is available for the AltaVault physical appliances.

Are there support limitations from NetApp for AltaVault?

Answer: Answer: NetApp support for AltaVault offers break-fix support on physical and virtual appliances with active support contracts. NetApp takes support calls globally 24/7. Support will be available in English, and support in other languages will be best effort. Support for the cloud-based appliances is community only.

Answer: NetApp Services product management will be available globally, and sales teams will need to contact the local engagement manager, or their local Professional Services Certified partner for activities outside of break-fix.

Where can partners find enablement and training for AltaVault products?

Answer: Answer: For installation, implementation, and configuration of AltaVault, access the [Partner Individual Learning Path \(PILP\)](#) and the “AltaVault Partner Capability” [learning map](#). Additional information can be obtained at the [AltaVault home page](#) on Field Portal.

9 Resources

Where can I find additional information or documentation?

Answer: Answer: A good starting place for anyone looking for AltaVault materials is the [AltaVault home page](#) on Field Portal. The NetApp AltaVault [Technology Overview Guide](#) is available to learn about the technologies built into the AltaVault appliance. Additional AltaVault documentation is available in the [AltaVault Binder in the Field Portal](#) or for Channel Partners in the [Channel Readiness Binder](#). Refer to the Installation Guides for installation information of [physical](#), [virtual](#) and [cloud-based](#) AltaVault, and to the [Administration Guide](#) for how to use AltaVault appliances. Lastly, backup application-specific [solution guides](#) are available for configuring AltaVault appliances.

I didn't see a feature my customer wants listed in documentation or this FAQ - where can I find additional information about future AltaVault features?

Answer: Answer: NetApp sales teams have access to product roadmaps, and AltaVault roadmaps are included. Talk to your NetApp sales team about having a product roadmap discussion.

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.

NetApp provides no representations or warranties regarding the accuracy, reliability, or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer's responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.