Technical Report

NetApp AltaVault Cloud-Integrated Storage Appliances

Performance Tuning Guide

Christopher Wong, NetApp
December 2017 | TR-4416

Abstract

This solution guide outlines the considerations and best practices for optimizing NetApp® AltaVault™ cloud-integrated storage appliance performance. AltaVault appliances provide a simple, efficient, and secure way to off-site 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 FIGURES

1 AltaVault Overview

This chapter is an overview of the AltaVault appliance.

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.

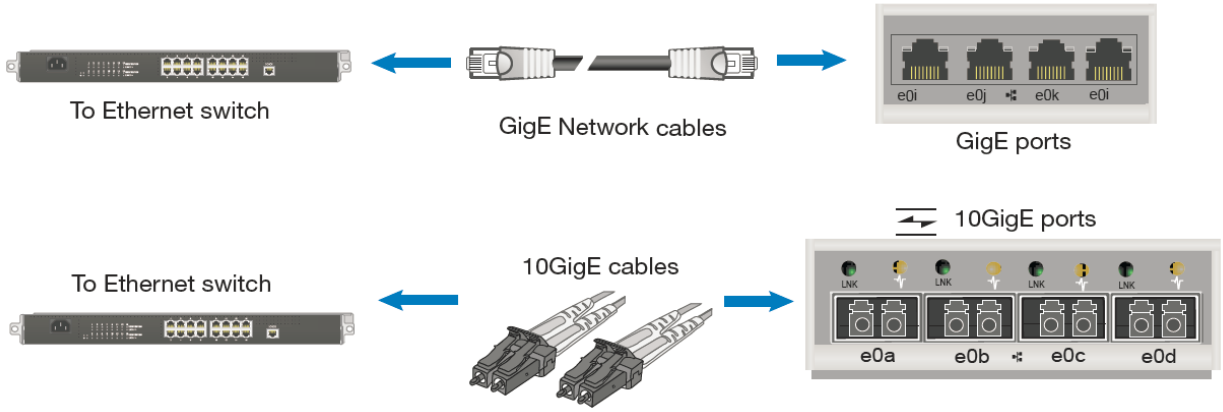
Security is provided by encrypting data on site or in flight, as well as in the cloud, using 256-bit AES encryption and SSL v3/TLS v1. AltaVault appliances provide a dual layer of encryption, which means that any data moved into the cloud is not compromised, and it creates a complete end-to-end security solution for cloud storage.

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

1.2 AltaVault Appliance Connectivity Overview

AltaVault appliances are high-performing cloud-integrated storage appliances capable of receiving data from multiple 1GbE and 10GbE Ethernet connections. As shown in the following diagram, AltaVault appliances have a total of four 1GbE interfaces, labeled e0i through e0l, and four 10GbE ports, labeled e0a through e0d. These ports can be connected to the network to receive data from backup servers and to send data to the cloud storage provider of your choice.

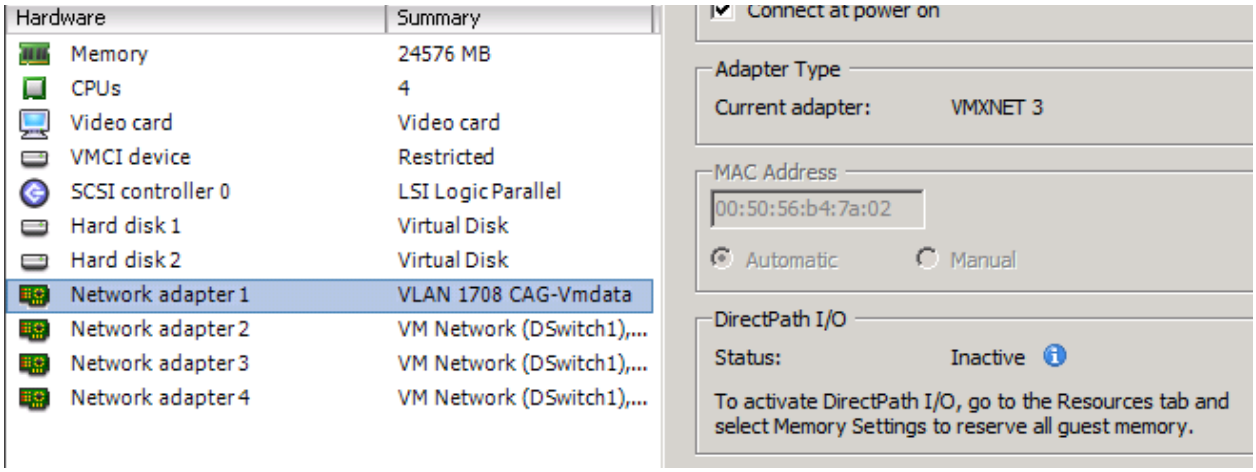
Figure 1) Cabling diagram.



In addition to these data interfaces, AltaVault appliances provide a management interface, known as the wrench port, to manage the appliance through a web browser–based GUI or SSH session. They also provide a serial port to perform the initial configuration of the appliance.

Virtual AltaVault appliances on VMware offer four VMXNET3 connections, as shown below. Similar to the physical appliance data interfaces, these network interfaces can be used to provide either 1GbE or 10GbE network connectivity to backup servers and to the cloud storage provider.

Figure 2) VMware network.



1.3 AltaVault Performance Overview

AltaVault appliances are high-performing cloud-integrated storage appliances designed to receiving data from backup and archive applications. Performance is optimized for workloads in which the backup or archive application sends large volumes of sequential data. AltaVault is not intended for use as a primary disk storage target and random I/O activity such as a general NAS filer. The AltaVault datasheets provide the ingest performance specification for moving data onto the appliance as follows:

Figure 3) Physical AltaVault performance.

CATEGORY	ATTRIBUTES[1]	PHYSICAL APPLIANCES		
		Backup Mode		Cold Storage Mode
		AVA400	AVA800	AVA400
Performance	Backup throughput (maximum)[2]	9.8TB/hr	14.1TB/hr	350GB/hr

Figure 4) Virtual AltaVault performance.

CATEGORY	ATTRIBUTES[1]	VIRTUAL APPLIANCES							
		Backup Mode				Cold Storage Mode			
		AVA-v2	AVA-v8	AVA-v16	AVA-v32	AVA-v2	AVA-v8	AVA-v16	AVA-v32
Performance	Backup throughput (maximum)	500GB/hr	1TB/hr	2TB/hr	3TB/hr	350GB/hr	350GB/hr	350GB/hr	350GB/hr

Figure 5) Cloud-based AltaVault performance.

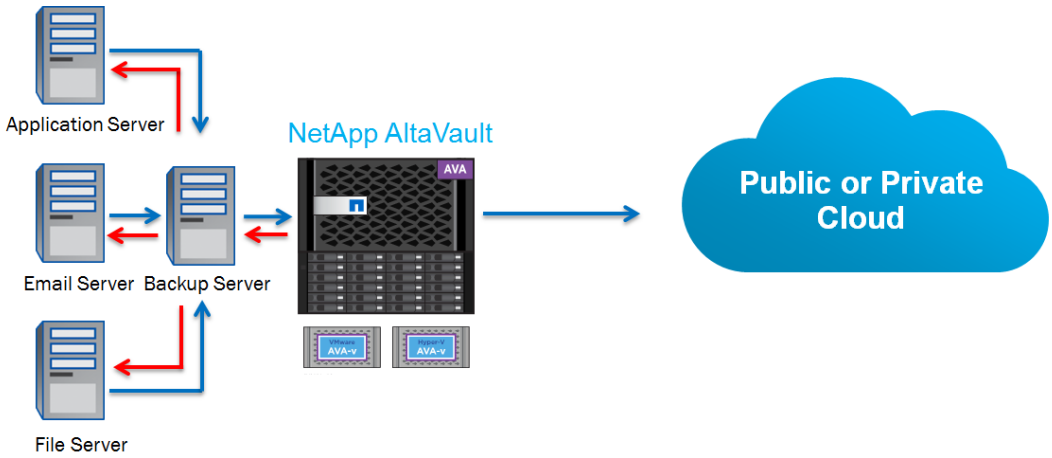
CATEGORY	ATTRIBUTES[1]	CLOUD APPLIANCES[4]					
		Backup Mode			Cold Storage Mode		
		AVA-c4	AVA-c8	AVA-c16	AVA-c4	AVA-c8	AVA-c16
Performance	Backup throughput (maximum)	345GB/hr	400GB/hr	3TB/hr	175GB/hr	225GB/hr	350GB/hr

For example, the AltaVault AVA400 appliance offers a maximum ingest rate of 9.8 TB/hr. AltaVault appliances achieve maximum performance when using multiple 10GbE interfaces. Virtual AltaVault models are restricted to the performance of the virtual host environments, and thus they deliver lower performance than their physical counterparts. You can find a full list of virtual AltaVault installation requirements in the NetApp AltaVault Cloud-Integrated Storage Installation and Service Guide for Virtual Appliances.

1.4 Network Overview

Typical network environments are relatively flat, meaning that each network interface of an AltaVault appliance connects to the same network segment as the rest of the infrastructure, including backup servers.

Figure 6) Typical backup infrastructure.



However, there are also environments in which multiple network segments might exist. AltaVault interfaces can be configured in either topology, allowing you to maximize throughput regardless of the network configuration. Understanding the network topology can be helpful in troubleshooting environments in which operations to AltaVault appliances are affected for some backup applications but not others.

1.5 Backup Application Overview

Backup applications feeding data to an AltaVault appliance vary in their performance because of a variety of factors, including:

- Backup client capability to feed data to the backup server (client disk type and speed, CPU/memory utilization, and so on)
- Backup server ability to write large streams of sequential data to AltaVault appliances (AltaVault does not work well with random I/O operations, such as synthetic fulls, direct incremental forever backups, large volumes of small log file backups, health checks or verify operations, etc)

- Backup server host resources to write large streams of sequential data to AltaVault appliances (server disk type and speed, RAID configuration if configured, CPU/memory utilization, and so on)
- Backup application write buffer size
- Network congestion and topology

Depending on these factors, backup throughput to AltaVault appliances can vary greatly, between 30MB/sec with one backup job, full line speed on a gigabit link, and upward of 2–3gb/sec using a 10-gigabit link. In the next sections, we discuss how to optimize backup throughput and be aware of performance bottlenecks.

2 Performance Tuning

It can be challenging to tune backup applications, networks, and AltaVault appliances, so it is best to establish the baseline performance of a single backup job that is representative of the environment and then expand performance by adding additional backup jobs. AltaVault is tuned to perform best when receiving large datasets, such as from backup applications.

2.1 Backup Application Best Practices

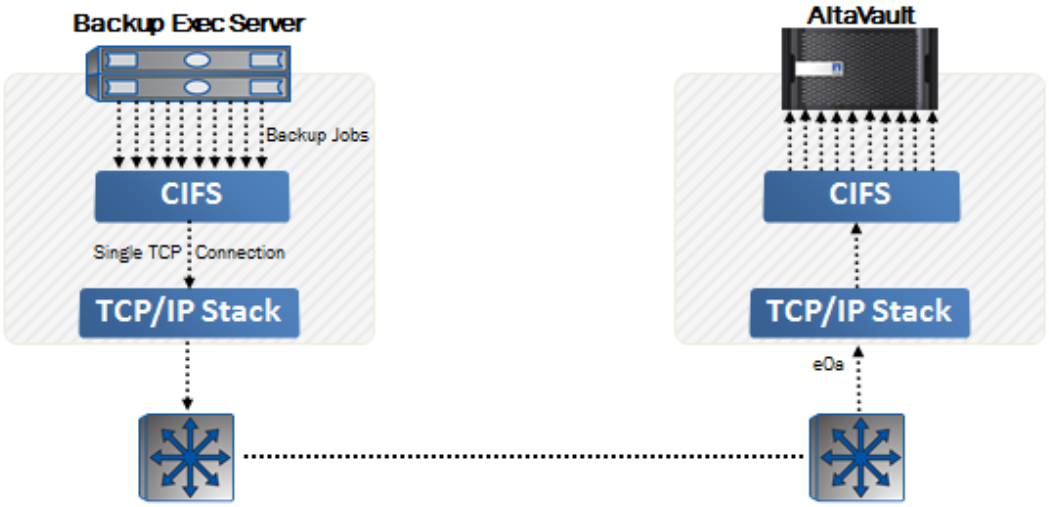
Before tuning the AltaVault appliance, NetApp highly recommends configuring the backup application. Implementing the best practices helps improve performance from the backup application and allows you to focus on AltaVault appliance tuning without being as concerned about backup application performance. Contact NetApp to obtain access to the AltaVault Best Practices Guide for Backup Applications and Technical Report Solution Deployment Guides for each particular backup application.

2.2 Single AltaVault Network Interface Tuning

Backup clients send data to a backup server through backup sessions, also commonly known as backup jobs. To begin using an AltaVault appliance with the backup application, test a single backup job from the backup application server or media server to the AltaVault appliance. Select a backup job that is representative of the type of workload most backup jobs will send to AltaVault. This establishes the typical backup job profile, which is measured in throughput rate (MB/sec). If the single backup job performs slower than expected, then refer to the “Troubleshooting” section to examine potential causes.

For example, say that the backup application is Backup Exec 2015 on Windows Server 2008, and the typical backup job performance is measured at roughly 50MB/sec. This means, assuming that the Backup Exec server is capable of maintaining this performance for additional jobs, that a single AltaVault 10GbE interface can handle roughly 10 to 15 backup jobs simultaneously before saturating 1 of its 4 10GbE interfaces.

Figure 7) Saturating a single AltaVault interface with backup jobs.



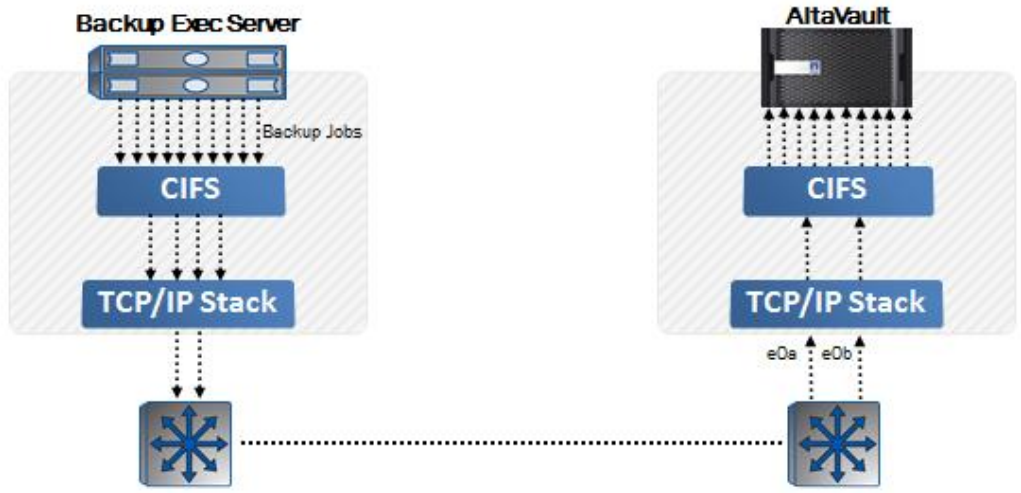
2.3 Multiple AltaVault Network Interfaces Tuning

Configuring the maximum throughput of an AltaVault appliance using multiple data interfaces from a backup application requires more design effort. This is because each AltaVault network interface card (NIC) needs to be configured onto a different network subnet such that the backup jobs can be configured to travel (be routed) across the network to one of the four NICs available. It is also important to ensure that when multiple ingest interfaces are available, enough bandwidth and WAN capacity are available to replicate data so that the AltaVault cache does not fill with new data. If this outcome occurs, AltaVault stops accepting writes because of insufficient free space, which can lead to failed backups.

Note: The AltaVault NIC tuning procedures below might not apply if you have multiple backup application servers in the environment. This is because each backup application server can be routed specifically to a single IP on the AltaVault appliance to achieve overall performance.

Continuing the example of Backup Exec 2016, a general diagram of the configuration might look similar to the following. Note that in this example, multiple 10GbE interfaces are also available on the backup server host.

Figure 8) Saturating multiple AltaVault interfaces with backup jobs.



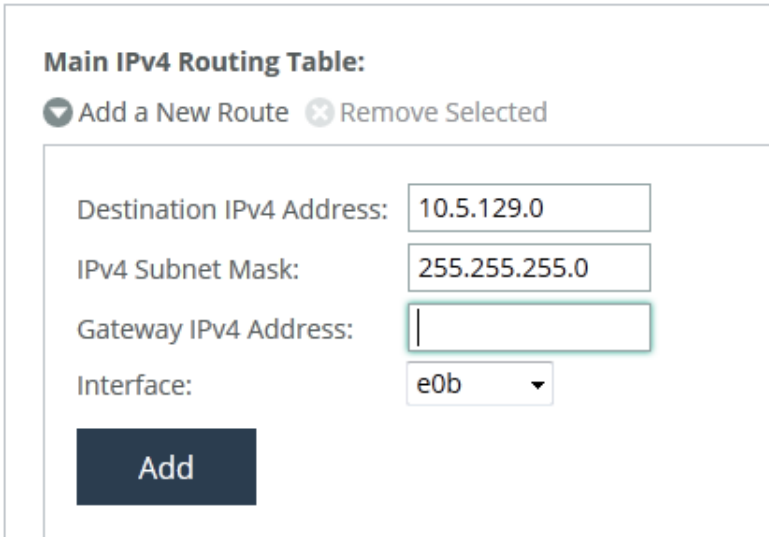
1. To implement a configuration similar to the one above, the first thing you need to do is design the interface mappings between the Backup Exec server host and the AltaVault appliance. For example, you might create this configuration mapping:
   - backupserverNIC1 (10.5.129.99) > AltaVault Eth0_0 (10.5.129.89)
   - backupserverNIC2 (10.5.130.106) > AltaVault Eth0_1 (10.5.130.91)
2. Configure the routing table (on the Backup Exec server host) so that traffic to the specific AltaVault IPs above is routed through the correct NIC on the Backup Exec server host. Use the `route -4 print` and `route – p add` commands from a Windows command prompt. For example, route -4 print might display:

```
C:\Users\Administrator>route -4 print
===========================================================================
Interface List
 12...00 0e b6 46 d3 a9 ......NVIDIA nForce Networking Controller #2
 13...00 0e b6 9a 25 c7 ......Intel(R) PRO/1000 PT Dual Port Server Adapter
 14...00 0e b6 9a 25 c6 ......Intel(R) PRO/1000 PT Dual Port Server Adapter #2
 17...00 0e b6 9a 25 c4 ......Intel(R) PRO/1000 PT Dual Port Server Adapter #4
 16...00 0e b6 9a 25 c5 ......Intel(R) PRO/1000 PT Dual Port Server Adapter #3
 10...00 0e b6 46 d3 a8 ......NVIDIA nForce Networking Controller
===========================================================================
```

   Assuming that you select interfaces 10 and 17 from the list above to use for backups to the AltaVault appliance, enter the following four `route –p add` commands:

```
route -p add 10.5.129.89 mask 255.255.255.0 10.5.129.99 metric 1 if 10
route -p add 10.5.130.91 mask 255.255.255.0 10.5.130.106 metric 1 if 17
```

   This creates the routes to the destination AltaVault IP addresses from the Backup Exec server host NICs. You can verify it if you rerun the `route -4 print` command.
3. To make sure that the routing is also configured correctly on the AltaVault appliance, equivalent routes need to be established. In the AltaVault GUI, choose Configure → Management Interfaces. Add the routes using the Add a New Route configuration under the Main IPv4 Routing Table section.



4. With the routing complete, configure the AltaVault SMB shares, one to be provided to each Backup-to-Disk folder. Do this from the Configure > SMB page of the AltaVault GUI.

5. Next, configure the four Backup-to-Disk folders on Backup Exec. Each Backup-to-Disk folder should refer to the correct DNS name or IP address as designated by the interface mappings in step 1, above.
6. Finally, test the configuration by assigning backup jobs to each of the four Backup-to-Disk folders. Monitor the backup activity to confirm that the appropriate routes are being used to send traffic to each of the AltaVault data interfaces.

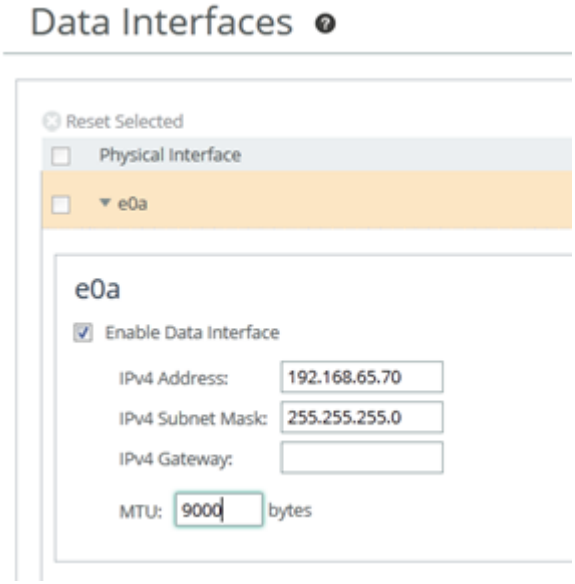
2.4 MTU Tuning (Jumbo Frames)

Performance over a 10-gigabit link can be further increased by allowing bigger Ethernet frames to flow across the network. Jumbo frames increase the data payload size from 1,500 bytes to 9,000 bytes, allowing more data to be sent per frame. This can yield a performance increase of up to an additional 1TB/hr. Not all environments support jumbo frames, so ensure that all equipment along the path is configured properly to support this feature.

To implement jumbo frames, configure all the network interfaces, switches, and other network equipment across the path between the backup server and the AltaVault appliance to use the same jumbo frame value, which typically is 9,000. Refer to your vendor's documentation regarding configuration and support for jumbo frames.

To configure jumbo frames on AltaVault appliances, go to Configure → Data Interfaces and select your interface from the list. In the MTU field, adjust the size to 9,000 bytes and click Apply to save the change.

Figure 9) Set MTU size.



You can verify that jumbo frames are enabled by performing the following:

- Windows: `ping -f -l 9000 <destination IP address>`
- Linux: `ping -M do -s 8972 <destination IP address>`

2.5 Enabling Virtual Interfaces

AltaVault appliances enable two or more of their data interfaces to be aggregated as a Virtual Interfaces (VIF). This is also commonly referred to as link aggregation, or 802.3AD.

Note: Using a VIF does not improve the performance of an AltaVault appliance versus using the individual network interfaces. However, there are passive advantages to using a VIF:

- Backup applications need to point to only one IP address that represents the VIF and the VIF automatically distributes traffic across the physical interfaces.
- It provides a failover path if one of the NICs in the bonded pairing fails.
- It enables you to configure and manage the appliance easily.

A VIF does not allow a single backup server connection to distribute packets across multiple NICs of the VIF. This means that a backup server host must have multiple NICs if you want to transmit multiple lines of traffic to the VIF. Also, multiple VIFs must be configured on the AltaVault appliance using the methodology described in the previous section to allow traffic to be received.

Note: Use VIFs if you want to improve reliability of multiple file sharing protocols (SMB, NFS, OST) being used simultaneously.

2.6 SMB Multichannel Tuning

AltaVault version 4.2 implements updated SMB protocol support, including support for the SMB 3.0 protocol and SMB multichannel.

- SMBv3 is the network file transfer protocol provided with Windows Server 2012 and higher.
- SMB multichannel is a feature of SMBv3 which allows Windows Server 2012 systems to take advantage of multiple network interfaces to transfer data between systems and improve resiliency of data transfers.

By leveraging multiple network interfaces on the Windows host system as well as on AltaVault, data throughput and path resiliency can be automatically improved without any configuration requirements at the network level, such as through VIFs as discussed in the previous section.

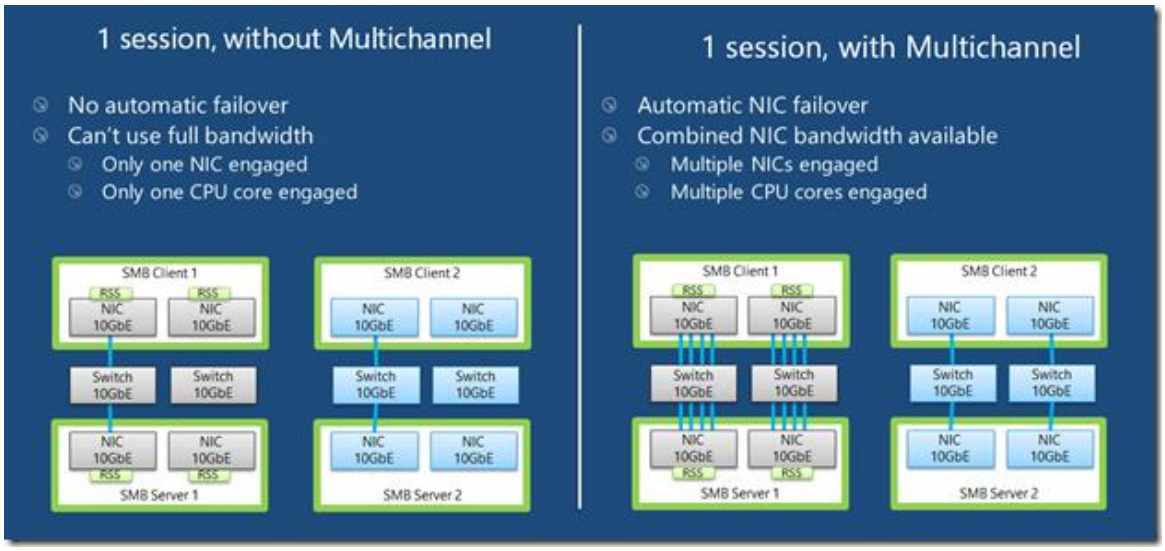
Note: VIFs are recommended for best stability in multi-network configurations. VIFs should not be configured for backup application network traffic if you intend to deploy AltaVault with SMB multichannel. VIFs should only be used for AltaVault cloud replication network traffic.

Microsoft states that network interfaces on the Windows 2012 server must meet one of the following configurations below:

- Multiple network adapters
- One or more network adapters that support RSS (Receive Side Scaling)
- One or more network adapters configured with NIC Teaming
- One or more network adapters that support RDMA (Remote Direct Memory Access NFS Tuning)

However, the only supported configuration AltaVault supports is with the multiple network adapters configuration above. Each of the network interfaces must be equivalent (1GbE or 10GbE) in order for SMB multichannel to use more than one path. In addition, SMB multichannel favors stability over performance, meaning that two 1GbE network interfaces and one 10GbE network interface will result in a multichannel configuration that utilizes the two 1GbE interfaces.

Figure 10) SMB MultiChannel comparison with multiple NICs.



Source: The basics of SMB Multichannel, a feature of Windows Server 2012 and SMB 3.0, Jose Barreto, Microsoft Technet Blog, 2012.

SMB multichannel on the Windows 2012 server is enabled by default, and no features, roles, or services are required to begin using this functionality. SMB will automatically detect and use multiple network connections if a proper configuration is available. If the SMB multichannel feature is disabled, you can re-enable the feature by using the PowerShell command:

```
Set-SmbClientConfiguration -EnableMultiChannel $true
```

Note: SMB multichannel on the AltaVault system will automatically be enabled for data interfaces that have properly set IP configuration information. If interfaces are not enabled, you can enable them from the Configure > SMB page. Section 2.3 describes how to create multiple paths between the backup application NICs and the AltaVault appliance NICs to perform parallel operations. With AltaVault 4.2 and higher, SMB multichannel makes defining multiple network paths unnecessary. Simply enable two or more of the same speed NICs, and SMB multichannel will automatically enable link aggregation. Be aware that after an upgrade to 4.2 or higher, an SMB share in the AltaVault will automatically be enabled to use multichannel mode. Performance may be non-optimal if multiple SMB shares are used with multichannel, so NetApp recommends either simplifying operations to 1 SMB share, or disabling multichannel mode on the appliance.

2.7 NFS Tuning

Operations with NFS to AltaVault appliances use either NFSv3 or NFSv4. By default, AltaVault suggests that you use the following mount commands:

Linux:

```
mount -t nfs -o rw,nolock,hard,intr,nfsvers=3,tcp,rsize=131072,wsize=131072,bg <IP of data
interface>:/rfs/nfs <mount-point>
```

Solaris:

```
mount -F nfs -o
rw,setuid,devices,llock,hard,intr,vers=3,proto=tcp,rsize=131072,wsize=131072,
bg,xattr <IP of data interface>:/rfs/nfs <mount-point>
```

However, depending on the environment, NetApp recommends increasing the mount read/write size to 1024kb from the default of 128k for high-speed, low-latency networks. This reduces the number of RPC calls needed to transfer the data.

Linux:

```
mount -t nfs -o rw,nolock,hard,intr,nfsvers=3,tcp,rsize= 1048576,wsize= 1048576,bg <IP of data interface>:/rfs/nfs <mount-point>
```

Solaris:

```
mount -F nfs -o rw,setuid,devices,llock,hard,intr,vers=3,proto=tcp,rsize= 1048576,wsize= 1048576,bg,xattr <IP of data interface>:/rfs/nfs <mount-point>
```

Depending on the version of Linux and the NFS version used, the operating system can potentially negotiate a larger value for the read/write size if no default rsize/wsize option is provided with the mount command. However, it is suggested to specify the size as suggested in the commands above in order to manually control the size selected. If you use Oracle RMAN to perform backups, it is recommended to use Oracle NFS for best performance.

2.8 OST Tuning

Veritas OpenStorage (OST) is a storage network protocol designed specifically to enhance performance of operations between Veritas NetBackup and supported storage devices such as AltaVault. As a file transfer protocol, it leverages design capabilities to optimize file data transmission with smaller overhead than existing protocols such as NFS and SMB. Configuring OST for use with AltaVault does not require any specific tuning to be performed, as OST automatically optimizes performance for operations to AltaVault.

2.9 Replication Performance Tuning

AltaVault appliances replicate data between the appliance and the cloud storage. Replication of data to cloud storage occurs over one of the data interfaces on an AltaVault appliance, and is internally tuned for best performance depending on the speed of your connection to the cloud storage provider. No tuning is required to reach optimal performance. If needed, bandwidth scheduling and throttling of AltaVault replication can be performed to reduce the network traffic to the cloud. For details, refer to chapter 4 of the AltaVault Administration Guide for details on configuring scheduling and bandwidth limiting.

2.10 Cloud-Based AltaVault Tuning

Cloud-based AltaVault appliances use high-speed interconnects to communicate between other compute instances and with cloud storage.

Amazon: When configuring a backup server located in the Amazon compute environment, use the private IP address of the AltaVault appliance. To enable the use of 10GbE on AVA-c16, the AltaVault and backup server compute instances must be in the same placement group.

Azure: When configuring a backup server located in the Azure compute environment, use the private IP address of the AltaVault appliance. The AltaVault and backup server compute instances must be connected to the same virtual switch to perform data movement.

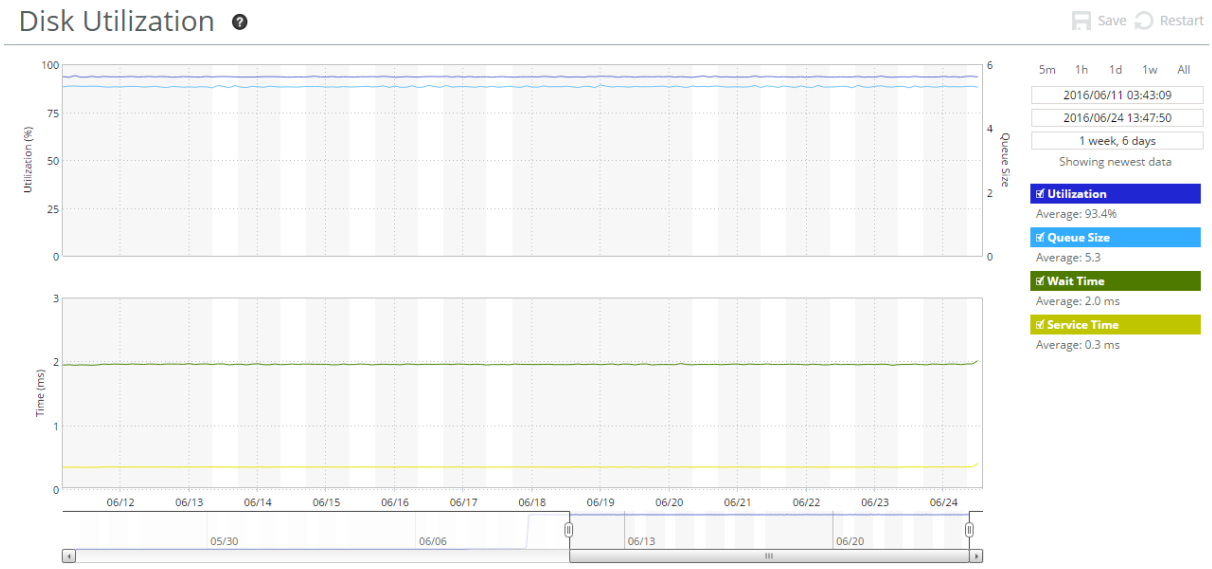
2.11 AltaVault Resource Tuning

In general, AltaVault is designed to handle a high number of concurrent backup operations. NetApp does not recommend using more than 128 concurrent sessions at any time to a single appliance. In most properly tuned backup application environments, performance will typically peak between 16 to 40 concurrent sessions.

In addition to backup connections, AltaVault can also support multiple replication connections to the cloud storage provider. AltaVault by default will begin replication with up to 16 sessions, and can increase this to 36 sessions depending on WAN bandwidth available.

Additional operations such as restores, eviction of least recently used data segments, garbage collection of eligible cloud data segments, and disk system checks can impact performance. Performing multiple operations simultaneously can increase network utilization, disk utilization, CPU utilization, and/or memory utilization. Examining AltaVault report graphs when operations appear to be performing slowly can help to isolate causes of conflict or identify bottlenecks in specific resources.

Figure 11) Example of a disk bottleneck.



If known concurrent operations could occur to create a resource bottleneck, such as eviction during backup time frames, it is suggested to adjust or modify operations to ensure that overlap does not occur. Separating operations will minimize potential resource contention of resources.

In the above example, AltaVault has a default eviction threshold of 90%. Eviction of least recently used data will occur if total disk cache consumption exceeds 90%, and will cease when the utilization moves back under 90%. This can cause cyclical performance impacts during backup windows, since fewer disk IOPS will be available when eviction is running. To address this problem, eviction can be scheduled to a manually configured threshold of 70% during non-backup periods, and then set back to 90% during backup windows, to provide backups sufficient cache space for writing the new data from the backups to cache.

2.12 Virtual AltaVault Tuning

Tuning virtual AltaVault appliances tends to be more difficult than tuning physical AltaVault appliances, because of the nature of the hypervisor layer serving resources across multiple virtual machines (VMs) at the same time. To ensure that AltaVault has sufficient resources, it is always recommended to reserve resources, as discussed in the best practices section of the AltaVault Install Guide for Virtual Appliances.

3 Troubleshooting AltaVault Performance

It can be difficult to narrow down the reason for slow backup to an AltaVault appliance because there are many components in the backup stream that occurs before data travels across the network to the AltaVault appliance. The following are typical troubleshooting methods:

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. Do not perform these types of operations with AltaVault.
- Backup applications performing synthetic full or reverse full operations. Do not perform these types of operations with AltaVault.
- 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. Perform scheduled eviction using the "datastore eviction threshold" command during non-backup windows.
- AltaVault replication running with many threads. Control replication throughput via the Cloud Settings page, Replication and Bandwidth tabs.

2. Verify the backup performance to a non AltaVault appliance local disk target. Assuming that the local disk target is sufficiently powerful to not be a bottleneck, does the backup performance change significantly?
3. Verify the backup performance to a non AltaVault appliance network disk target of a similar type. If backups are run to an NFS export on AltaVault, test a backup to an NFS export on a network disk system. Assuming that the network disk target is sufficiently powerful to not be a bottleneck, does the backup performance change significantly?
4. Compare the performance of a normal (non-backup application) data transfer to an AltaVault appliance to that of a backup application data transfer to the same AltaVault appliance. For example, drag and drop a sufficiently large file using Windows Explorer to the AltaVault SMB share and measure throughput performance. Assuming that the source disk is sufficiently powerful to not be a bottleneck, does the performance change significantly versus when using a backup application to send the same object?
5. Ensure that a sufficient number of jobs are run to maximize the line utilization to the AltaVault appliance. The AltaVault solution guides for each backup application typically recommend starting with five backup jobs per AltaVault NIC. However, in some cases more backup jobs or streams might be required to maximize throughput because of the design of the backup application.
6. Confirm the write buffer size used by the backup application. To verify this, take a transmission control protocol (TCP) trace of a backup application operation to the AltaVault appliance and look at the transport protocol (for example, SMB2). Small write buffer sizes can limit the throughput of a backup job.
7. Confirm the time between write requests and write response times with a TCP trace of the backup application operation to the AltaVault appliance and examine the transport protocol (for example, SMB2). If write request to write response times are significant (in excess of 1ms), it might indicate an AltaVault appliance performance problem.
8. Test network performance using a tool such as Iperf to verify network throughput and to rule out any protocol bottlenecks. Iperf is an open-source network performance measurement tool for verifying maximum TCP and user datagram protocol (UDP) bandwidth performance. To use Iperf, contact NetApp Support to gain access to and diagnose network performance with this tool.
9. Review the resource graphs of AltaVault, and if running virtual AltaVault review the hypervisor resource graphs, to see if a particular resource (memory, disk, network) is being fully utilized during the operation time frame of the performance problem.
10. Review the system log of AltaVault to examine whether AltaVault is performing retries of operations (such as for replicating data due to inconsistent WAN connectivity), or is experiencing resource shortages that are reported to this log.
11. On AltaVault releases prior to 4.3, consider disabling TCP Offload on AltaVault. Identifying this feature as a possible performance bottleneck and changing the option state requires NetApp support involvement.
12. If you upgrade to 4.3.1 from 4.2.2 or lower and have restore bandwidth throttling set, AltaVault may use that throttling speed for all connections, resulting in slower performance. Review the following KB article to determine if you are impacted, and how to resolve this problem until AltaVault is updated to

address this problem:
https://kb.netapp.com/support/s/article/ka11A0000001a5hQAA/AltaVault-4-3-1-Changes-to-Network-Rate-Limiting

4 AltaVault Best Practices for Operating Systems

4.1 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
```

4.2 Solaris Best Practices

Configure NFS networking parameters on Solaris operating systems to optimally send data to AltaVault through configured NFS mounts. In addition to tuning the rsize and wsize mount options appropriately, also tune nfs3_max_transfer_size and nfs3_bsize. They 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 for the configuration changes to take effect.

5 AltaVault Performance Benchmarks

Extensive AltaVault testing is done to ensure that performance specifications are in line with published technical specifications. To measure maximum system performance, AltaVault testing is done under controlled conditions which may not reflect true backup application workloads. In addition, AltaVault is tested as well as under common backup conditions to describe throughput rates that are typical of common backup workloads. This chapter provides some general guidance and information about

configurations used in testing, as well as examples of the type of performance possible with the most common backup configuration using NetBackup. Unless noted, all tests were done using AltaVault AVA800 appliances with 1 or 2 fully populated AVA10S shelves of disk, 10GbE, and the most current version of published AltaVault operating system software. All systems, including AVA800 appliances, Linux clients, NetBackup media servers, and network switch are configured with jumbo frames enabled. Raw data for all ingest tests was optimized with a 3x compression factor with a minimal 1% deduplication factor.

5.1 Performance Definitions

Performance terms used in this chapter consist of the following:

Table 1) Performance definitions.

Item	Description
Ingest performance	The throughput performance of the AltaVault appliance in receiving backup data over the LAN from the backup application.
Egress performance	The throughput performance of the AltaVault appliance in replicating optimized data to the cloud storage target.
Decode performance	The throughput performance of the AltaVault appliance in rehydrating optimized data and sending it over the LAN to the backup application.
Raw data	The source data sent from a backup application over the LAN to AltaVault.
Optimized data	The resulting data that has undergone AltaVault inline deduplication and compression.
Cold performance	The throughput performance of raw data that is received by AltaVault for the first time from a backup application.
Warm performance	The throughput performance of raw data that is received by AltaVault in any subsequent operation after the first time from a backup application.
Synthetic Data	Data that has been artificially created under controlled settings to provide baseline deduplication and compression factors that can be consistently measured.

5.1 Basic Cold Ingest Performance

AltaVault achieved a cold ingest performance throughput rate of 7.0TB/hr (1944MB/s), using 16 NFSv3 sessions spread evenly across the 4x 10GbE interfaces.

Note: NFS shares used rsize=1048576 and wsize=1048576. One (1) Linux x86-64 CentOS 6.5 system using Intel E5-class Xeon CPUs generated synthetic data that was then sent to AltaVault.

5.2 Basic Warm Ingest Performance

AltaVault achieved a warm ingest performance throughput rate of 10.6TB/hr (2944MB/s), using 64 NFSv3 sessions spread evenly across the 4x 10GbE interfaces.

Note: NFS shares used rsize=1048576 and wsize=1048576. One (1) Linux x86-64 CentOS 6.5 system using Intel E5-class Xeon CPUs generated synthetic data that was then sent to AltaVault.

5.3 Basic Decode Performance

AltaVault achieved a decode throughput rate of up to 3.6TB/hr (1000MB/s), using 4 NFSv3 sessions. AltaVault can achieve a decode throughput rate of up to 2TB/hr (556MB/s), using 1 NFSv3 session.

AltaVault can achieve a decode throughput rate of up to 2.6TB/hr (722MB/s) using 128 NFSv3 sessions. The raw data was reconstructed entirely from optimized data stored in AltaVault cache during the decode process, and no cloud data was retrieved to perform the decode.

Note: NFS shares used rsize=1048576 and wsize=1048576. One (1) Linux x86-64 CentOS 6.5 system using Intel E5-class Xeon CPUs received the decoded data.

5.4 NetBackup SMB Warm Ingest Performance

AltaVault achieved an ingest performance throughput rate of 10.5TB/hr (2917MB/s), using 32 SMBv3 sessions to 10GbE. SMBv3 automatically distributes the load across the 4x 10GbE interfaces when multichannel is enabled. One (1) NetBackup storage policy was used.

Note: One (1) Linux x86-64 CentOS 6.5 system using Intel E5-class Xeon CPUs was used to generate synthetic data. One (1) Windows 2012 R2 x86-64 system using Intel E5-class Xeon CPUs was used as NetBackup media server, receiving data from the Linux NetBackup client and then sending to AltaVault.

5.5 NetBackup OST Warm Ingest Performance

AltaVault achieved an ingest performance throughput rate of 14.1TB/hr (3917MB/s), using 16 NetBackup OST sessions to 10GbE. Four (4) NetBackup storage policies were used.

Note: One (1) Linux x86-64 CentOS 6.5 system using Intel E5-class Xeon CPUs was used to generate synthetic data. This system also acted as the NetBackup media server.

5.6 NetBackup SMB Decode Performance

AltaVault achieved a decode performance throughput rate of 2.4TB/hr (667MB/s), using 2 SMBv3 sessions to 10GbE. There were 4x 10GbE interfaces available to SMB multichannel. One (1) NetBackup storage policy was used. The raw data was reconstructed entirely from optimized data stored in AltaVault cache during the decode process, and no cloud data was retrieved to perform the decode.

Note: One (1) Windows 2012 R2 x86-64 system using Intel E5-class Xeon CPUs was used as NetBackup media server, receiving data from AltaVault.

5.7 NetBackup OST Decode Performance

AltaVault achieved a decode performance throughput rate of 8.5TB/hr (2361MB/s), using 96 NetBackup OST sessions to 10GbE. Four (4) NetBackup storage policies were used. The raw data was reconstructed entirely from optimized data stored in AltaVault cache during the decode process, and no cloud data was retrieved to perform the decode.

Note: One (1) Linux x86-64 CentOS 6.5 system using Intel E5-class Xeon CPUs was used as NetBackup media server, receiving data from AltaVault.

5.8 AltaVault Replication Performance

AltaVault achieved an egress performance throughput rate of 117MB/s (936mb/s) using a 1GbE replication interface (Primary). AltaVault achieved an egress performance throughput rate of 536MB/s (4.3gb/s) using a 10GbE replication interface (e0d).

5.9 AltaVault Data Migration Performance

The migration of the full cache of metadata, data, and deduplication index from a SteelStore 3030 head unit with 2 additional shelves to an AltaVault appliance using 10GbE crossover cables between the two 10GbE interfaces achieved a peak throughput rate of 10gb/s. The total time to transfer these contents was approximately 33 hours, for an average throughput rate of ~3TB/hr, or 6.6gb/s.

The migration of the full cache of metadata, data, and deduplication index from a SteelStore 3030 head unit to an AltaVault appliance using 10GbE crossover cables between the two 10GbE interfaces achieved a peak throughput rate of 3gb/s. The total time to transfer these contents was approximately 28 hours, for an average throughput rate of ~1.1TB/hr, or 2.4gb/s.

Where to Find Additional Information

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

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

Version History

Version	Date	Document Version History
Version 1.0	May 2015	Initial version
Version 1.1	August 2015	Updated for 4.0.1 release
Version 1.2	November 2015	Updated for 4.1 release
Version 1.3	April 2016	Updated for 4.2 release
Version 1.4	August 2016	Updated for 4.2.1 release
Version 1.5	January 2017	Updated for 4.3 release
Version 1.6	April 2017	Updated for 4.3.1 release
Version 1.7	December 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-4416-1117