NetApp® AltaVault® Cloud Integrated Storage 4.2.1

User's Guide

NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089
U.S.

Telephone: +1 (408) 822-6000
Fax: + 1 (408) 822-4501
Support telephone: +1(888) 463-8277
Web: www.netapp.com
Feedback: doccomments@netapp.com

Part number: 215-11344_A0
August 2016

Contents

Chapter 1 - Introduction of NetApp AltaVault Cloud Integrated Storage 9

Overview of AltaVault 9
AutoSupport 10
Supported backup applications 10
Interoperability Matrix Tool 10

System requirements and specifications 11

Using the management console 11
Connecting to the management console 11
Home page 12
Getting help 13

Documentation and release notes 14

Chapter 2 - Using the AltaVault configuration wizard 15

Using the wizard dashboard 16

Using the system settings wizard 16

Using the cloud settings wizard 17

Using the import configuration wizard 46

Using the export configuration wizard 48

Chapter 3 - Configuring storage settings 49

Configuring cloud settings 49
Configuring cloud provider settings 50
Configuring encryption 50
Configuring replication 50
Configuring bandwidth limits 51

Configuring SMB 52

Configuring NFS 57
Configuration tasks 57
Editing an NFS configuration 58
Troubleshooting NFS exports to AIX 60

Configuring OST 60

Restoring data from the cloud using the prepopulation page 62

Viewing offline file system check page 63

Viewing online file system check page 64

Viewing the verify tool diagnostics 65

Chapter 4 - Modifying networking settings 67

Modifying general host settings 67

Modifying management interfaces 69

Modifying data interfaces 71

Modifying virtual interfaces 73

Modifying VLANs 73

Chapter 5 - Managing the AltaVault appliance 75

Starting and stopping the AltaVault appliance 75

Configuring scheduled jobs 76

Managing licenses 77

- Managing POC licenses 78
- Managing licenses using the command-line 78
- Adding a new license using management console 78
- 90-day evaluation period 79
- AltaVault-v licenses 79
- Specifying license limits 79
- Model upgrades on the virtual AltaVault appliances 80

Upgrading your software 80

Rebooting and shutting down AltaVault appliance 82

Viewing the current user settings 82

Managing configuration files 83

Chapter 6 - Configuring system administrator settings 85

Setting announcements 85

Configuring alarm settings 86

Configuring date and time 91

Configuring SNMP basic settings 94

- Configuring SNMP v3 96
- SNMP authentication and access control 98

Configuring email settings 101

Configuring log settings 102

Chapter 7 - Configuring security settings 105

Configuring general security settings 105

Managing user permissions 107

- Configuring user permissions 109
- Unlocking an account 110
- Configuring password policy settings 111

Setting RADIUS servers 111

Configuring TACACS+ access 113
Unlocking the secure vault 114
Configuring Web settings 115
Managing web SSL certificates 115
Configuring KMIP 117
Using the management console to configure KMIP 118
Using CLI to configure KMIP 120
Configuring appliance monitoring 122
Configuring a management ACL 123
Configuring SSH Access 125

Chapter 8 - Viewing reports and logs 127

About reports 128
Viewing the storage optimization report 131
Viewing the front-end throughput report 132
Viewing the back-end throughput report 134
Viewing the eviction report 135
Viewing the replication report 136
Viewing the cloud operations report 137
Viewing schedule reports 138
Viewing per share utilization reports 139
Viewing the alarm status report 140
Viewing the CPU utilization report 144
Viewing the memory paging report 145
Viewing the interface counters report 146
Viewing the disk throughput report 147
Viewing the disk IOPS report 148
Viewing the disk utilization report 148
Viewing logs 149
Viewing system logs 150
Viewing user logs 150
Downloading log files 151
Generating system dumps 152
Viewing process dumps 153
Capturing and uploading TCP dumps 153
Viewing a TCP dump 158
Viewing the appliance monitoring report 159
Viewing the shelf details 161

Viewing the storage RAID group 162

Chapter 9 - Configuring AltaVault appliances for FIPS-compliant cryptography 163

What is FIPS? 163

Understanding FIPS on AltaVault 163

NetApp cryptographic security module 164

Compliant FIPS cryptography features 164

Noncompliant FIPS cryptography features 164

Basic steps for configuring FIPS compliance 165

Configuring AltaVault appliances for FIPS-compliant cryptography 165

Enabling FIPS mode 166

Verifying that your system uses FIPS-compliant encryption 167

Working with features to maintain FIPS compliance 167

Account passwords 167

Cipher requirements 168

Key size requirements 168

NTP 169

RADIUS and TACACS+ 169

SNMP 170

SSH 170

Telnet server 171

Web proxy 171

Disabling FIPS mode 171

Viewing reports and logs 172

Viewing user logs 172

Viewing system logs 172

Downloading user log files 172

Downloading system log files 172

Verifying FIPS mode in system logs 173

Verifying that file transfers operate in FIPS mode 173

Verifying that NTP operates in FIPS mode 173

Verifying that secure vault operates in FIPS mode 173

Verifying that SNMP operates in FIPS mode 173

Verifying that the web interface operates in FIPS mode 173

FIPS CLI 174

Chapter 10 - Deploying Kerberos-based environments 175

Chapter 11 - Migrating data from a SteelStore appliance to an AltaVault appliance 179

Overview of physical or virtual SteelStore appliance to physical AltaVault appliance 179

Data migration connection diagrams 180

Data migration process 182

Prerequisites 182

Prerequisites for the source appliance 182
Prerequisites for the target appliance 183
Performing appliance data migration 184
Post-data migration procedure....185

Appendix A - AltaVault appliance MIB 187
Accessing AltaVault appliance MIB....187
SNMP traps....187

Appendix B - Amazon AWS IAM and S3 bucket policies 199
Typical AltaVault setup....199
IAM policies for AltaVault 199
Sample of IAM policy 200
Bucket policies for AltaVault 201
Sample of bucket policy 201

Appendix C - Root certificates 203

Appendix D - Installing and configuring NetApp AltaVault OST Plug-in 211
Installing and configuring AltaVault OST Plug-in on Windows....211
Installing and configuring AltaVault OST Plug-in on Linux 212
Next steps for AltaVault OST Plug-in 213
Upgrading AltaVault OST Plug-in 214

Copyright Information....215

Trademark Information....217

How to Send Your Comments 219

Index 221

Contents

CHAPTER 1 Introduction of NetApp AltaVault Cloud Integrated Storage

This section provides an introduction of the AltaVault Management Console (Management Console). It includes the following sections:

- "Overview of AltaVault" on page 9
- "System requirements and specifications" on page 11
- "Using the management console" on page 11
- "Documentation and release notes" on page 14

Overview of AltaVault

AltaVault appliance is a disk-to-disk data storage optimization system with unique cloud storage integration.

Note: To access the management console of Azure cloud appliances, specify the https protocol explicitly.

There are three types of AltaVault deployments:

- Physical Hardware Appliance - AltaVault appliance is available on AVA400 and AVA800 models.
- Virtual Appliance - AltaVault virtual appliance (AltaVault-v) is a virtual machine hosted package that allows you to try it out as an evaluation version that lasts for 90 days, allowing you to optimize your storage backups.

  You can use VMware ESXi servers, Linux KVM, or Microsoft Hyper-V, to create a virtual machine (VM) and install the AltaVault-v software on the VM.

  AltaVault-v is available in the following models for VMware, Linux KVM, or Microsoft Hyper-V: AVA-v2, AVA-v8, AVA-v16, AVA-v32.
- Cloud-Based Virtual Appliance - The following AltaVault cloud-based appliances are available for Amazon: AVA-c4, AVA-c8, AVA-c16. For Azure, the following AltaVault cloud-based appliance is available: AVA-c4.

Note: Downgrades are not supported in this release.

AutoSupport

AltaVault supports user-triggered and daily AutoSupports (ASUPs). ASUP functionality is supported on all AltaVault models.

For more information on ASUP CLI commands, see the *NetApp AltaVault Cloud Integrated Storage Command-Line Interface Reference Guide*.

Supported backup applications

AltaVault works with a wide range of enterprise grade backup applications. For a current list of supported backup applications and versions, refer to the Interoperability Matrix Tool.

Interoperability Matrix Tool

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.

Benefits

The AltaVault appliance provides the following benefits:

- Ease of use - You manage the AltaVault appliance with the appliance that you can access directly using a Web browser.
- Interoperability - The AltaVault appliance easily integrates into your existing backup infrastructure. It acts as a disk target at the front end and can write directly to cloud storage. You do not need to change your existing backup products to deploy the AltaVault appliance.
- WAN optimization - Using the NetApp compression and deduplication technologies, WAN optimization provides performance gains when replicating data to the cloud.
- Security - The AltaVault appliance provides robust security. It encrypts data from the backup server using AES-256 encryption. It protects data both at rest and in transit.
- Stateless appliance - The appliance can rebuild recent backups locally that can all be retrieved from the cloud.
- Scalability - Even large enterprises can achieve off-site data protection for all their data with just a few appliances.
- Cost-effective - The AltaVault appliance enables you to outsource your storage infrastructure to the cloud and use a “pay as you use” model to reduce costs. It reduces cloud storage requirements, thereby reducing the total cost of cloud storage.
- Reliability - By backing up data directly to the cloud, the AltaVault appliance eliminates the need for tape storage that is less reliable than cloud storage.
- Disaster recovery - AltaVault appliance is also available as a virtual machine. You can use AltaVault-v during disaster recovery if the hardware appliance fails.

System requirements and specifications

This section specifies the hardware and software requirements.

For system requirements for virtual appliances, see the *NetApp AltaVault Cloud Integrated Storage Installation and Service Guide for Virtual Appliances.*

For system requirements for physical appliances, see the *NetApp AltaVault Cloud Integrated Storage Installation and Service Guide for Physical Appliances.*

For system requirements for cloud, see the *NetApp AltaVault Cloud Integrated Storage Installation and Service Guide for Cloud Appliances.*

Using the management console

The following section describes how to connect to and navigate in the Management Console. It includes the following sections:

- "Connecting to the management console" on page 11
- "Home page" on page 12
- "Navigating in the management console" on page 12

Connecting to the management console

To connect to the Management Console, you must know the URL and administrator password that you assigned in the configuration wizard when you installed the AltaVault.

To connect to the AltaVault management console

1. Enter the URL for the Management Console in the location box of your Web browser:

   ```
   <protocol>://<host>.<domain>
   ```

   The <*protocol*> variable is http or https. HTTPS uses the SSL/TLS protocol to ensure a secure environment. When you connect using HTTPS, you are prompted to inspect and verify the SSL certificate. The SSL certificate is a self-signed certificate used to provide encrypted Web connections to the Management Console. It is re-created when the appliance hostname is changed and when the certificate has expired.

   The <*host*> variable is the hostname you assigned to the AltaVault primary interface in the configuration wizard. If your DNS server maps that IP address to a name, you can specify the DNS name.

   The <*domain*> variable is the full domain name for the appliance.

   You can also specify the IP address instead of the host and domain name.

   The Management Console appears, displaying the Login page.

2. In the Username text box, specify the user login: admin, monitor, a login from a RADIUS or TACACS+ database, or any local accounts created using the Role-Based Accounts feature. The default login is admin.

   Users with administrator (admin) privileges can configure and administer the AltaVault. Users with monitor privileges can view the AltaVault reports, user logs, and change their own password. A monitor user cannot make configuration changes.

3. In the Password text box, specify the password you assigned in the CLI configuration wizard of the AltaVault. The password cannot be "password." To change your password, see "Viewing the current user settings" on page 82.

4. Click **Log In** to display the AltaVault configuration wizard (when you log in for the first time) or the Home page (for subsequent logins).

   When you log in to the AltaVault for the first time, the configuration wizard appears.

Home page

The Home page displays the following parameters:

- Cloud and Disk Storage Allocation - The outer circle represents the cloud storage and the inner circle represents the local AltaVault cache storage. This section also lists the used storage, free storage, and total storage on the cloud and the disk.
- Optimization Service - Specifies whether the storage optimization service is running or has stopped and the status of the service (such as ready).

  If the Status displays replaying, it indicates that the storage optimization service has been terminated during backup replication, either due to loss of power or a crash. During this replay process, the AltaVault verifies data consistency from its transaction logs.

  The amount of time it takes to replay process to complete will depend on the amount of data in flight at the time the AltaVault appliance was abnormally stopped.
- Cloud Storage Reclamation - Provides the status of the cloud storage reclamation service (garbage collection). This service runs automatically when needed to clean up fragmented disk and cloud space. If the cloud storage reclamation status is "Running," then the status color changes from red to black.
- Alarms Triggered - Displays the appliance health status and software update. To view the alarms triggered, choose Reports > Alarm Status.
- System Status - Displays details about the AltaVault system such as the AltaVault time, system up time, and optimization service up time.
- Appliance Information - Provides the appliance hostname and its model number.
- Replicated Data - Displays the status of the data replication. Replication is the process of copying data and metadata from the AltaVault to the cloud. The AltaVault replicates data to the cloud asynchronously. Replication provides an extra measure of redundancy that can be invaluable if the main storage backup system fails. Immediate access to the replicated data minimizes downtime and its associated costs. Replication streamlines disaster recovery processes by generating duplicate copies of all backed-up files on a continuous basis. It can also simplify recovery from all types of disasters, including fire, flood, hurricane, virus, or worm.
- Storage Optimization - Displays the expanded data, deduplicated data, and deduplication factor. Expanded data is the data that has been backed up locally by the AltaVault. Deduplicated data reflects data that has been optimized through the use of deduplication and compression. Deduplication is a method of reducing storage space by eliminating redundant data. It replaces redundant data with a pointer to the unique data copy. Deduplication factor is the ratio of the expanded data and total optimized data. The total optimized data includes both deduplication and compression savings.
- Cloud Information - Displays the status of the cloud connection and the cloud provided that the appliance is connected to the WAN.

Navigating in the management console

You navigate to the tools and reports available to you in the Management Console using cascading menus.

To display cascading menus

1. Select the Reports menus to display their submenus. The menu item that is currently active is highlighted.
2. To go to a page, slide your mouse down to the submenu item you want to display and select the menu name. For example, under Reports select Disk IOPS to display the Disk IOPS page.

Saving your configuration

As you apply page settings, the values are applied to the running configuration. Most Management Console configuration pages include an Apply button for you to commit your changes. When you click **Apply**, the Management Console updates the running configuration. Your changes are written to disk only when you save your configuration.

NetApp recommends that you save your configuration after every change.

The Save icon on the menu bar alerts you if the changes you have made require saving them to disk.

To save your changes, click Save to save the changes to disk. The system displays a message that your configuration is saved and that you should export your new configuration.

A red asterisk next to a control indicates that the field is required. You must specify a valid entry for all of the required controls on a page before saving the changes.

Restarting AltaVault appliance service

The AltaVault service is a daemon that executes in the background, performing required operations.

Some configuration settings apply to the AltaVault service. When you change settings for features that depend on the AltaVault service, you must restart the service for the changes to take effect.

To restart the service, click **Restart** to display the Service page or go to Storage Optimization Service page and restart the service.

Printing pages and reports

You can print Management Console pages and reports using the print option on your Web browser.

To print pages and reports

- Choose File > Print in your Web browser to open the Print dialog box.

Getting help

The Help page provides the following options:

- Online Help - View browser-based online help.
- Technical Support - View links and contact information for NetApp Support.
- Appliance Details - View appliance information such as the model number, hardware revision type, serial number, and software version currently installed on the appliance.
- MIB Files - View NetApp and appliance MIB files in text format.

Displaying online help

The Management Console provides page-level help for the appliance.

To display online help

- Click the question mark icon next to the page title. The help for the page appears in a new browser window.

Logging out

In the menu bar, click **Sign out** to end your session.

Documentation and release notes

To obtain the most current version of all NetApp documentation, go to the NetApp Support site at https://mysupport.netapp.com.

The following documents are provided in this release:

- *NetApp AltaVault Cloud Integrated Storage Deployment Guide*
- *NetApp AltaVault Cloud Integrated Storage User's Guide*
- *NetApp AltaVault Cloud Integrated Storage Command-Line Reference Guide*
- *NetApp AltaVault Cloud Integrated Storage Installation and Service Guide for Cloud Appliances*
- *NetApp AltaVault Cloud Integrated Storage Installation and Service Guide for Physical Appliances*
- *NetApp AltaVault Cloud Integrated Storage Installation and Service Guide for Virtual Appliances*

If you need more information, see the NetApp Knowledge Base for any known issues, how-to documents, system requirements, and common error messages. You can browse titles or search for keywords and strings. For more information, see the NetApp Support site at https://mysupport.netapp.com.

CHAPTER 2 Using the AltaVault configuration wizard

The AltaVault configuration wizard appears only after you log in to the appliance the first time. It enables you to access other configuration wizards, so that you can configure your own system settings, configure cloud settings, and import and export settings.

This section includes the following:

- "Using the wizard dashboard" on page 16
- "Using the system settings wizard" on page 16
- "Using the cloud settings wizard" on page 17
- "Using the import configuration wizard" on page 46
- "Using the export configuration wizard" on page 48

Use the Wizard Dashboard page to configure AltaVault after you log in to the appliance for the first time. The wizard does not appear for subsequent logins.

Using the wizard dashboard

The Wizard Dashboard is the first page of the wizard. You can access the System Settings wizard, Cloud Settings wizard, Import Configuration wizard, and Export Configuration wizard from this page.

To access the AltaVault configuration wizard dashboard

1. Log in to the AltaVault Management Console.
2. If you are logging in to the management console for the first time, the wizard appears, displaying the Welcome page. For subsequent logins, log in to AltaVault and choose Configure > Setup Wizard.

Based on your configuration requirements, you can use different wizards from the dashboard.

Task	Reference
Configure networking settings and time zone, use the System Settings wizard.	"Using the system settings wizard" on page 16
Configure cloud settings, licenses, and encryption key, use the Cloud Settings wizard.	"Using the cloud settings wizard" on page 17
Import a previously saved configuration, use the Import Configuration wizard.	"Using the import configuration wizard" on page 46
Export the current configuration from the system, use the Export Configuration wizard.	"Using the export configuration wizard" on page 48

Using the system settings wizard

Use the System Settings wizard to configure networking settings and time zone.

To use the System Settings wizard

1. Select System Settings in the Wizard Dashboard.

   The System Settings wizard displays the hostname and DNS server IP address for the AltaVault.

2. In the System Settings wizard, complete the configuration as described in this table.

Control	Description
Obtain IPv4 Address Automatically	Specify this option to automatically obtain the IPv4 address from a DHCP server. A DHCP server must be available so that the system can request the IP address from it. • Enable IPv4 Dynamic DNS - Select this option to enable IPv4 dynamic DNS on the primary interface. Dynamic DNS is a method, protocol, or network service that enables a network device, such as a router or computer system using the Internet Protocol Suite, to notify a Domain Name System (DNS) name server to change, in real time, the active DNS configuration of its configured hostnames, addresses, or other information.
Specify IPv4 Address Manually	Specify this option if you do not use a DHCP server to set the IP address. Specify the following settings: • IPv4 Address - Specify an IPv4 address. • IPv4 Subnet Mask - Specify an IPv4 subnet mask. • Default IPv4 Gateway - Specify the default primary gateway IPv4 address. The primary gateway must be in the same network as the primary interface. You must set the primary gateway for interface configurations.
Time Zone	Specify the country and time zone in which the AltaVault is located.
Enable Analytics	Select Yes or No from the drop-down list. Enabling this feature will send system dumps to NetApp to help diagnose and troubleshoot issues.

3. Click **Next** to display the Confirmation page.

4. Click **Save and Apply** to display the System Settings Wizard Finish page.

5. Click **Exit** to close the System Settings Wizard and go back to the dashboard.

6. Click **Cloud Settings** in the Wizard Dashboard to display the cloud settings. For more information, see "Using the cloud settings wizard" on page 17.

Using the cloud settings wizard

Use the Cloud Settings wizard to configure cloud settings, licensing, and the encryption key.

To use the cloud settings wizard

1. Select Cloud Settings in the Wizard Dashboard.

   Check that the data store is empty. If the data store is not empty, you cannot change the cloud provider, region, hostname, and bucket name.

2. Under Provider, select and configure one of the following cloud service providers from the drop-down list:
   - "Amazon Glacier" on page 19
   - "Amazon S3" on page 23
   - "AT&T Synaptic Storage" on page 24
   - "Cleversafe Cloud Storage" on page 25

- "Cloudian Cloud Storage" on page 26
- "Cloudwatt Object Storage" on page 27
- "Customizing a private cloud" on page 28
- "Dunkel Cloud Storage" on page 29
- "EMC Atmos" on page 30
- "EVault LTS2 Cloud Storage" on page 31
- "Google Cloud Storage" on page 32
- "Internet Initiative Japan (IIJ)" on page 33
- "Microsoft Windows Azure Storage" on page 34
- "NetApp StorageGRID Webscale" on page 35
- "OpenStack Object Storage (Swift)" on page 36
- "Oracle Storage Cloud Service - Object Storage" on page 38
- "Outscale On-Demand Storage" on page 39
- "Rackspace Cloud Files" on page 40
- "Scality RING" on page 41
- "SoftLayer Object Storage (Swift)" on page 41
- "Swisscom Dynamic Storage" on page 43
- "Telefonica Cloud Storage" on page 44
- "Verizon Cloud Storage" on page 45

3. Select Encryption Settings in the Wizard Dashboard. This page is only available to users with Read-Only Security Settings permissions or Read and Write Security Settings permissions.

4. Specify the following:

Control	Description
Create New Datastore Encryption Key	Select this option to establish a new AES-256 bit encryption key that AltaVault uses to secure data. Optionally, provide a passphrase that will be used to encrypt the datastore encryption key. The key passphrase must be provided whenever importing this datastore encryption key, such as for disaster recovery. It is not stored within a configuration archive and must be kept in a secure location. Set Key Passphrase - Specify a passphrase that will be used to secure the encryption key on AltaVault. This passphrase will be required when importing the encryption key or AltaVault configuration onto a new AltaVault appliance. Confirm Key Passphrase - Confirm the passphrase.
Import Key from File	Select this option to import the key from a file. Select the file to import it onto the appliance. The key must be the key that was generated or exported from an AltaVault appliance.
Import Key from Text	Select this option to import the key from text. The key must be the key that was generated or exported from an AltaVault appliance.
Next	Click Next to display the Confirmation page.

5. On the Confirmation page verify the information, and click Save and Apply.

6. On the Finish page verify that the settings were successfully applied. A Cloud Connection Check Successful message displays if the AltaVault is able to connect to the cloud provider and establish ownership of the cloud storage container.

Amazon Glacier

1. Select Amazon Glacier.

2. Select yes or no to use keys from KMIP server from the drop-down list. When configuring the KMIP server, you must:
   - Use the same username and password as created in KMS.
   - Upload the same certificate as downloaded from KMS after signing it.
   - Add a symmetric key (KMIP key) as the encryption key.
   - Add a secret data key (KMIP key) for each of the authentication fields.

3. Specify the following settings:
   - Region - Select an Amazon Glacier region from the drop-down list. You can choose to store your data in the Amazon Glacier Region that meets your regulatory, throughput, and geographic redundancy criteria. You can select one of the following regions:
   - Asia Pacific (Tokyo)
   - Asia Pacific (Sydney)
   - EU (Ireland)
   - EU (Frankfurt)
   - GovCloud (US)
   - US Standard
   - US-West (Northern California)
   - US-West (Oregon)

4. Custom Region - Optionally, specify the custom region for your cloud service provider account. This field is not required when the AWS region already exists in the Region drop-down menu.

5. Authentication Method - Specify one of the following authentication methods from the drop-down list:
   - Standard - Specify selections for the "Standard authentication" on page 20.
   - STS - Specify selections for the "STS authentication" on page 21.

Note: If user files are not cached on AltaVault, they should be pre-populated before reads are performed. The reason is, restores from Amazon Glacier have a latency of 4-5 hours. For more information, see AWS documentation.

Standard authentication

Note: When S3 or Glacier is configured and Storage Optimization Service fails to start, the logs may contain the error "BucketAlreadyExists: The requested bucket name is not available. The bucket namespace is shared by all users of the system. Please select a different name and try again." This indicates that the chosen bucket name is not available. You can resolve this by selecting a different bucket name. This error may also be encountered after a cloud migration or changing of the cloud settings. One possible reason may be that the cloud credentials do not belong to the account that owns the bucket. Double-check the credentials and ensure that the correct credentials are entered on the Cloud Settings page.

For the Standard authentication type, make selections for the following:

1. Access Key - Specify the access key for your Amazon S3 (AWS) account.

2. Secret Key - Specify the secret key for your cloud service provider account.

3. Enable Cloud Deduplication (Displayed only for Amazon Glacier selections) - Select this check box to specify that the AltaVault must check the incoming data for deduplication against the entire data set, both in the Glacier cloud and in the local disk cache. This is the same procedure that the AltaVault uses for other (non-Glacier) cloud providers.

4. Hostname - Verify the hostname of the cloud provider on which AltaVault stores the replicated data. For example, s3.amazonaws.com.

5. Bucket Name - Specify the bucket name associated with your cloud service provider account. Buckets are the basic containers that store deduplicated data sent from the AltaVault. Everything that you store in the cloud provider storage must be contained in a bucket. You can use buckets to organize your data and control access to your data, but unlike directories and folders, you cannot nest buckets. If the bucket name does not exist, the bucket is created during initial AltaVault replication.

   For Amazon S3 in the US Standard region only, the bucket names must conform to the following rules:

   - Bucket names can contain only lowercase letters, numbers, periods, hyphens, and underscores.
   - Bucket names must start with a number or letter.
   - Bucket names must be from 3 to 255 characters.

   For Amazon S3, in all regions (except US Standard) bucket names must comply with the following rules. These rules result in a DNS-compliant bucket name.

   - Bucket names must be from 3 to 63 characters.
   - If the region is not US Standard, the bucket names cannot contain underscores and they must be from 3 to 63 characters.
   - Bucket names must be a series of one or more labels separated by a period, and each label:

   – must start with a lowercase letter or a number.

   – must end with a lowercase letter or a number.

   – can contain lowercase letters, numbers, and hyphens.

6. Port - Specify the port through which replication occurs. Amazon uses port 80, which is an unsecured port, or port 443, which is a secure port and the default port.

7. In the Enable Archiving drop-down list select Yes to enable or No to disable it. Enable this option if you are using the AltaVault for cold storage mode. If you enable this option, it increases the AltaVault cloud capacity for archive

workloads. For more information about cold storage mode, see the section *Deployment guidelines* in the *NetApp AltaVault Cloud Integrated Storage Deployment Guide*.

8. Enable Cloud CA Certificate - Optionally, specify a cloud CA certificate that will be used to validate the server certificate of cloud provider. This must be .pem extension file.

9. Enable Proxy - Select the enable proxy check box to enable proxy server settings. A proxy server acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting service such as a file, connection, Web page, or other resource available on a different server, and the proxy server evaluates the request as a way to simplify and control their complexity.

   After you select the check box, specify the following settings:

   - Hostname/IP address - Specify the hostname or the IP address of the proxy server.
   - Port - Specify the port numbers to access the proxy server.
   - Username - Specify the name of the user who has access to the proxy server.
   - Password - Specify the password to authenticate the user.

STS authentication

For the STS authentication type, make selections for the following:

1. Identity Provider URL: Specify the URL of the provider.

   The identity provider is a server that performs two roles: 1) authenticating users and machines wishing to access Amazon AWS services, and 2) providing temporary security credentials with which to access those services. AltaVault makes a call to the identity provider, which in turn makes a call to Amazon STS using the AssumeRole API call to generate temporary security credentials, and then passes these credentials back to AltaVault.

   AltaVault uses the following specification for communication with the Identity Provider:

   Identity Provider Request

   When AltaVault requires a set of temporary security credentials, it will make a request to the identity provider. This request is a HTTP GET or POST request to the configured URL over a mutually-authenticated SSL/TLS connection. A mutually-authenticated connection is one where the client and server validate each other's SSL certificates. If the identity provider requires GET or POST parameters to be passed as part of the request, these can be specified when STS is configured.

   Identity Provider Response

   The response from the identity provider should be the exact same response that it receives from the AssumeRole API call in JSON format. The identity provider should not modify the response in any way, except possibly to convert it into JSON format.

2. Parameters - Specify the parameters for the https request that the provider expects to authenticate the AltaVault appliance.

3. Response Type - JSON is the default response type.

4. Method - Select the method GET or POST from the drop-down list.

5. CA Certificate - Specify the certificate that will be used to validate the server certificate of the identity provider. Ensure that the file has the required .pem extension.

6. Select the Web Settings page link.

- Select the Replace tab.
- Certificate - Upload the client certificate.
- Separate Private Key - Upload the Private Key.
- To replace the certificate and private key, click Import Certificate and Key.
- To go back to the Cloud Settings page, click the back button.

7. For Glacier only: Enable Cloud Deduplication - Select this check box to specify that the AltaVault must check the incoming data for deduplication against the entire data set, both in the Glacier cloud and in the local disk cache. This is the same procedure that the AltaVault uses for other (non-Glacier) cloud providers.

8. Hostname - Verify the hostname of the cloud provider on which AltaVault stores the replicated data. For example, s3.amazonaws.com.

9. Bucket Name - Specify the bucket name associated with your cloud service provider account. Buckets are the basic containers that store deduplicated data sent from the AltaVault. Everything that you store in the cloud provider storage must be contained in a bucket. You can use buckets to organize your data and control access to your data, but unlike directories and folders, you cannot nest buckets. If the bucket name does not exist, the bucket is created during initial AltaVault replication.

For Amazon S3 in the US Standard region only, the bucket names must conform to the following rules:

- Bucket names can contain only lowercase letters, numbers, periods, hyphens, and underscores.
- Bucket names must start with a number or letter.
- Bucket names must be from 3 to 255 characters.

For Amazon S3, in all regions (except US Standard) a bucket names must comply with the following rules. These rules result in a DNS-compliant bucket name.

- Bucket names must be from 3 to 63 characters.
- If the region is not US Standard, the bucket names cannot contain underscores and they must be from 3 to 63 characters.
- Bucket names must be a series of one or more labels separated by a period, and each label:

– must start with a lowercase letter or a number.

– must end with a lowercase letter or a number.

– can contain lowercase letters, numbers, and hyphens.

10. Port - Specify the port through which replication occurs. Amazon uses port 80, which is an unsecured port, or port 443, which is a secure port and the default port.

11. In the Enable Archiving drop-down list select Yes to enable or No to disable it. Enable this option if you are using the AltaVault for cold storage mode. If you enable this option, it increases the AltaVault cloud capacity for archive workloads. For more information about cold storage mode, see the section *Deployment guidelines* in the *NetApp AltaVault Could Integrated Storage Deployment Guide*.

12. Enable Cloud CA Certificate - Optionally, specify a cloud CA certificate that will be used to validate the server certificate of cloud provider. This must be .pem extension file.

13. Enable Proxy - Select the enable proxy check box to enable proxy server settings. A proxy server acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server,

requesting service such as a file, connection, Web page, or other resource available on a different server, and the proxy server evaluates the request as a way to simplify and control their complexity.

After you select the check box, specify the following settings:

- Hostname/IP address - Specify the hostname or the IP address of the proxy server.
- Ports - Specify the port numbers to access the proxy server.
- Username - Specify the name of the user who has access to the proxy server.
- Password - Specify the password to authenticate the user.

Amazon S3

1. Select Amazon S3.
2. Select yes or no to use keys from KMIP server from the drop-down list. When configuring the KMIP server, you must:
   - Use the same username and password as created in KMS.
   - Upload the same certificate as downloaded from KMS after signing it.
   - Add a symmetric key (KMIP key) as the encryption key.
   - Add a secret data key (KMIP key) for each of the authentication fields.
3. Specify the following settings:
   - Region - Select an Amazon S3 region from the drop-down list. You can choose a region to optimize for latency, minimize costs, or address regulatory requirements. You can select one of the following regions:
   - Asia Pacific (Singapore)
   - Asia Pacific (Sydney)
   - Asia Pacific (Tokyo)
   - EU (Frankfurt)
   - EU (Ireland)
   - GovCloud (US)
   - GovCloud (US) (FIPS 140-2)
   - South America (Sao Paulo)
   - US Standard
   - US West (Northern California)
   - US West (Oregon)
4. Custom Region - Optionally, specify the custom region for your cloud service provider account. This field is not required when the AWS region already exists in the Region drop-down menu.
5. Storage Class - Specify a storage class from the drop-down list:
   - Standard (Standard storage class)
   - Standard-IA (Standard Infrequent Access)

- RRS (Reduced Redundancy Service)

6. Authentication Type - Specify one of the following authentication types from the drop-down list:
   - Standard - Specify selections for the "Standard authentication" on page 20.
   - STS - Specify selections for the "STS authentication" on page 21.

AT&T Synaptic Storage

1. Select AT&T Synaptic Storage.

2. Select yes or no to use keys from KMIP server from the drop-down list. When configuring the KMIP server, you must:
   - Use the same username and password as created in KMS.
   - Upload the same certificate as downloaded from KMS after signing it.
   - Add a symmetric key (KMIP key) as the encryption key.
   - Add a secret data key (KMIP key) for each of the authentication fields.

3. Specify the following settings:

   Storage Policy - Select one of the following storage policies from the drop-down list:
   - Local Replication - Stores data stored in one location and protects it using erasure coding (which is a software-based data protection scheme that allows for data recovery in the event of hardware failures).
   - Remote Replication - Stores data in two locations maintains a copy in one data center and replicates it to a geographically remote data center.

4. Specify the subtenant ID.

5. Specify the user ID that AT&T Synaptic Storage uses to authenticate each request.

6. Specify the shared secret that AT&T Synaptic Storage uses to authenticate each request. When the client application builds a Web service request, AT&T Synaptic Storage uses the shared secret to create a signature entry as a part of the request. The shared secret must be associated with the tenant ID and application ID created by AT&T Synaptic Storage.

7. Specify the hostname of the cloud provider on which AltaVault stores the replicated data. For example, storage.synaptic.att.com.

8. Specify the bucket name associated with your cloud service provider account. Buckets are the basic containers that store deduplicated data sent from the AltaVault. Everything that you store in the cloud provider storage must be contained in a bucket. You can use buckets to organize your data and control access to your data, but unlike directories and folders, you cannot nest buckets. If the bucket name does not exist, the bucket is created during initial AltaVault replication.

   For AT&T Synaptic Storage, the bucket names must conform to the following rules:
   - Bucket names can contains only lowercase letters, numbers, periods, hyphens, and underscores.
   - Bucket names must start with a number or letter.
   - Bucket names must be from 3 to 255 characters.

9. Specify the port through which replication occurs. The default value is 443 for AT&T Synaptic Storage.

10. In the Enable Archiving drop-down list select Yes to enable or No to disable it. Enable this option if you are using the AltaVault for cold storage mode. If you enable this option, it increases the AltaVault cloud capacity for archive workloads. For more information about cold storage mode, see the section *Deployment guidelines* in the *NetApp AltaVault Could Integrated Storage Deployment Guide*.

11. Enable Cloud CA Certificate - Optionally, specify a cloud CA certificate that will be used to validate the server certificate of cloud provider. This must be .pem extension file.

12. Select the Enable Proxy check box to enable proxy server settings. A proxy server acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting service such as a file, connection, Web page, or other resource available on a different server, and the proxy server evaluates the request as a way to simplify and control their complexity.

    After you select the check box, specify the following settings:

    - Hostname/IP address - Specify the hostname or the IP address of the proxy server.
    - Ports - Specify the port numbers to access the proxy server.
    - Username - Specify the name of the user who has access to the proxy server.
    - Password - Specify the password to authenticate the user.

Cleversafe Cloud Storage

1. Select Cleversafe Cloud Storage.

2. Select yes or no to use keys from KMIP server from the drop-down list. When configuring the KMIP server, you must:

    – Use the same username and password as created in KMS.

    – Upload the same certificate as downloaded from KMS after signing it.

    – Add a symmetric key (KMIP key) as the encryption key.

    – Add a secret data key (KMIP key) for each of the authentication fields.

3. Specify the following settings:

    - Access Key - Specify the access key (same as the username) for your Cleversafe Cloud Storage account.
    - Secret Key - Specify the secret key (password) for your cloud service provider account.

4. Specify the hostname.

5. Specify the bucket name associated with your cloud service provider account. Buckets are the basic containers that store deduplicated data sent from the AltaVault. Everything that you store in the cloud provider storage must be contained in a bucket. You can use buckets to organize your data and control access to your data, but unlike directories and folders, you cannot nest buckets. If the bucket name does not exist, the bucket is created during initial AltaVault replication.

    You can use bucket names that:

    - are from 3 to 63 characters.
    - start with lower-case letters or numbers, hyphens (-), and periods (.).

6. Specify the port number.

7. In the Enable Archiving drop-down list select Yes to enable or No to disable it. Enable this option if you are using the AltaVault for cold storage mode. If you enable this option, it increases the AltaVault cloud capacity for archive workloads. For more information about cold storage mode, see the section *Deployment guidelines* in the *NetApp AltaVault Could Integrated Storage Deployment Guide*.

8. Enable Cloud CA Certificate - Optionally, specify a cloud CA certificate that will be used to validate the server certificate of cloud provider. This must be .pem extension file.

9. Select the Enable Proxy check box to enable proxy server settings. A proxy server acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting service such as a file, connection, Web page, or other resource available on a different server, and the proxy server evaluates the request as a way to simplify and control their complexity.

   After you select the check box, specify the following settings:

   - Hostname/IP Address - Specify the hostname or IP address of the proxy.
   - Port - Specify the port number.
   - Username - Specify the username.
   - Password - Specify the password.

Cloudian Cloud Storage

1. Select Cloudian Cloud Storage.

2. Select yes or no to use keys from KMIP server from the drop-down list. When configuring the KMIP server, you must:

   – Use the same username and password as created in KMS.

   – Upload the same certificate as downloaded from KMS after signing it.

   – Add a symmetric key (KMIP key) as the encryption key.

   – Add a secret data key (KMIP key) for each of the authentication fields.

3. Specify the following settings:

   - Access Key - Specify the access key (same as the username) for your Cloudian Cloud Storage account.
   - Secret Key - Specify the secret key (password) for your cloud service provider account.

4. Specify the hostname.

5. Specify the bucket name associated with your cloud service provider account. Buckets are the basic containers that store deduplicated data sent from the AltaVault. Everything that you store in the cloud provider storage must be contained in a bucket. You can use buckets to organize your data and control access to your data, but unlike directories and folders, you cannot nest buckets. If the bucket name does not exist, the bucket is created during initial AltaVault replication.

   You can use bucket names that:

   - are from 3 to 63 characters.
   - are a series of one or more labels separated by a period.

- start and end with lower-case letters or numbers.

6. Specify the port number.

7. In the Enable Archiving drop-down list select Yes to enable or No to disable it. Enable this option if you are using the AltaVault for cold storage mode. If you enable this option, it increases the AltaVault cloud capacity for archive workloads. For more information about cold storage mode, see the section *Deployment guidelines* in the *NetApp AltaVault Could Integrated Storage Deployment Guide*.

8. Enable Cloud CA Certificate - Optionally, specify a cloud CA certificate that will be used to validate the server certificate of cloud provider. This must be .pem extension file.

9. Select the Enable Proxy check box to enable proxy server settings. A proxy server acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting service such as a file, connection, Web page, or other resource available on a different server, and the proxy server evaluates the request as a way to simplify and control their complexity.

   After you select the check box, specify the following settings:

   - Hostname/IP Address - Specify the hostname or IP address of the proxy.
   - Port - Specify the port number.
   - Username - Specify the username.
   - Password - Specify the password.

Cloudwatt Object Storage

1. Select Cloudwatt Object Storage.

2. Select yes or no to use keys from KMIP server from the drop-down list. When configuring the KMIP server, you must:

   – Use the same username and password as created in KMS.
   – Upload the same certificate as downloaded from KMS after signing it.
   – Add a symmetric key (KMIP key) as the encryption key.
   – Add a secret data key (KMIP key) for each of the authentication fields.

3. Specify the following settings:

   - Authentication - Specify one of the following methods that Cloudwatt Object Storage uses to authenticate each request:

     Access Key ID/Secret Key- Specify the access key ID, secret key, and tenant ID for your Cloudwatt Object Storage account.

     Username/Password - Specify the username, password, and tenant ID of your Cloudwatt Object Storage account.

     Username/API Access Key - Specify the username and the API Access key for your Cloudwatt Object Storage account.

   - Authentication URL Path - Specify the cloud server API URL for Cloudwatt Object Storage to authenticate the request. For example, /auth/v1.0 or /auth/v2.0.

- Web Protocol - Specify whether to use the HTTP or HTTPS protocol. HTTPS is the secure version of the HTTP protocol, where packets are encrypted before they are transmitted. It uses the SSL protocol to ensure a secure environment.

4. Specify the hostname of the cloud provider on which AltaVault stores the replicated data.

5. Specify the bucket name associated with your cloud service provider account. Buckets are the basic containers that store deduplicated data sent from the AltaVault. Everything that you store in the cloud provider storage must be contained in a bucket. You can use buckets to organize your data and control access to your data, but unlike directories and folders, you cannot nest buckets. If the bucket name does not exist, the bucket is created during initial AltaVault replication.

   You can use bucket names that are alphanumeric and contain period, dash, underscore, and tilde.

6. Specify the port through which replication occurs. The default value is 443.

7. In the Enable Archiving drop-down list select Yes to enable or No to disable it. Enable this option if you are using the AltaVault for cold storage mode. If you enable this option, it increases the AltaVault cloud capacity for archive workloads. For more information about cold storage mode, see the section *Deployment guidelines* in the *NetApp AltaVault Could Integrated Storage Deployment Guide*.

8. Enable Cloud CA Certificate - Optionally, specify a cloud CA certificate that will be used to validate the server certificate of cloud provider. This must be .pem extension file.

9. Select the Enable Proxy check box to enable proxy server settings. A proxy server acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting service such as a file, connection, Web page, or other resource available on a different server, and the proxy server evaluates the request as a way to simplify and control their complexity.

   After you select the check box, specify the following settings:

   - Hostname/IP address - Specify the hostname or the IP address of the proxy server.
   - Ports - Specify the port numbers to access the proxy server.
   - Username - Specify the name of the user who has access to the proxy server.
   - Password - Specify the password to authenticate the user.

Customizing a private cloud

You need to contact NetApp Support to configure a private cloud. After you configure a private cloud, the cloud appears as the cloud provider in the cloud settings page.

To customize a private cloud

1. Contact NetApp Support to convert a cloud to a private cloud.

2. After you configure a private cloud using the CLI, it appears in the Cloud Settings page and the dashboard in the Cloud Information section as the Provider. For more information on CLI, see the *NetApp AltaVault Cloud Integrated Storage Command-Line Interface Reference Guide*.

3. Choose Configure > Cloud Settings.

4. Select the Cloud tab.

5. Under Cloud Provider Settings, complete the configuration as necessary. Refer to your private cloud configuration for the required authentication credentials needed to communicate with this cloud.

Dunkel Cloud Storage

1. Select Dunkel Cloud Storage.

2. Select yes or no to use keys from KMIP server from the drop-down list. When configuring the KMIP server, you must:
   - Use the same username and password as created in KMS.
   - Upload the same certificate as downloaded from KMS after signing it.
   - Add a symmetric key (KMIP key) as the encryption key.
   - Add a secret data key (KMIP key) for each of the authentication fields.

3. Specify the following settings:
   - Access Key - Specify the access key (same as the username) for your Dunkel Cloud Storage account.
   - Secret Key - Specify the secret key (password) for your cloud service provider account.

4. Specify the hostname.

5. Specify the bucket name associated with your cloud service provider account. Buckets are the basic containers that store deduplicated data sent from the AltaVault. Everything that you store in the cloud provider storage must be contained in a bucket. You can use buckets to organize your data and control access to your data, but unlike directories and folders, you cannot nest buckets. If the bucket name does not exist, the bucket is created during initial AltaVault replication.

   You can use bucket names that:
   - are from 3 to 63 characters.
   - start with lower-case letters or numbers, hyphens (-), and periods (.).

6. Specify the port number.

7. In the Enable Archiving drop-down list select Yes to enable or select No to disable it. Enable this option if you are using the AltaVault for cold storage mode or writing compressed or encrypted backup data. If you enable this option, it increases the cloud capacity for such workloads.

8. Enable Cloud CA Certificate - Optionally, specify a cloud CA certificate that will be used to validate the server certificate of cloud provider. This must be .pem extension file.

9. Select the Enable Proxy check box to enable proxy server settings. A proxy server acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting service such as a file, connection, Web page, or other resource available on a different server, and the proxy server evaluates the request as a way to simplify and control their complexity.

   After you select the check box, specify the following settings:
   - Hostname/IP Address - Specify the hostname or IP address of the proxy.
   - Port - Specify the port number.
   - Username - Specify the username.

- Password - Specify the password.

10. Click **Apply** to apply your changes to the running configuration.

11. Click **Save** to save your configuration.

EMC Atmos

1. Select EMC Atmos.

2. Select yes or no to use keys from KMIP server from the drop-down list. When configuring the KMIP server, you must:
   - Use the same username and password as created in KMS.
   - Upload the same certificate as downloaded from KMS after signing it.
   - Add a symmetric key (KMIP key) as the encryption key.
   - Add a secret data key (KMIP key) for each of the authentication fields.

3. Specify the following settings:
   - Subtenant ID - Specify the subtenant ID that EMC Atmos uses to authenticate each request.
   - UID - Specify the user ID that EMC Atmos uses to authenticate each request.
   - Shared Secret - Specify the shared secret that EMC Atmos uses to authenticate each request. When the client application builds a Web service request, EMC Atmos uses the shared secret to create a signature entry as a part of the request. The shared secret must be associated with the subtenant ID and application ID created by the EMC Atmos-based storage provider.

4. Specify the hostname of the cloud provider on which AltaVault stores the replicated data.

5. Leave the bucket name field as is. This field is the top-level namespace directory that the AltaVault creates to store deduplicated data in the cloud.

6. Specify the port through which replication occurs. The default value is 443.

7. In the Enable Archiving drop-down list select Yes to enable or No to disable it. Enable this option if you are using the AltaVault for cold storage mode. If you enable this option, it increases the AltaVault cloud capacity for archive workloads. For more information about cold storage mode, see the section *Deployment guidelines* in the *NetApp AltaVault Could Integrated Storage Deployment Guide*.

8. Enable Cloud CA Certificate - Optionally, specify a cloud CA certificate that will be used to validate the server certificate of cloud provider. This must be .pem extension file.

9. Select the Enable Proxy check box to enable proxy server settings. A proxy server acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting service such as a file, connection, Web page, or other resource available on a different server, and the proxy server evaluates the request as a way to simplify and control their complexity.

   After you select the check box, specify the following settings:
   - Hostname/IP address - Specify the hostname or the IP address of the proxy server.
   - Ports - Specify the port numbers to access the proxy server.

- Username - Specify the name of the user who has access to the proxy server.
- Password - Specify the password to authenticate the user.

EVault LTS2 Cloud Storage

1. Select EVault LTS2 Cloud Storage.
2. Select yes or no to use keys from KMIP server from the drop-down list. When configuring the KMIP server, you must:
   - Use the same username and password as created in KMS.
   - Upload the same certificate as downloaded from KMS after signing it.
   - Add a symmetric key (KMIP key) as the encryption key.
   - Add a secret data key (KMIP key) for the authentication fields.
3. Specify the following settings:
   - Username - Specify the username.
   - Password - Specify the password.
   - Tenant ID - Specify the tenant ID.
4. Specify the hostname.
5. Specify the bucket name associated with your cloud service provider account. Buckets are the basic containers that store deduplicated data sent from the AltaVault. Everything that you store in the cloud provider storage must be contained in a bucket. You can use buckets to organize your data and control access to your data, but unlike directories and folders, you cannot nest buckets. If the bucket name does not exist, the bucket is created during initial AltaVault replication.

   You can use bucket names that:
   - are from 3 to 63 characters.
   - start with lower-case letters or numbers, hyphens (-), and periods (.).
6. Specify the port number.
7. In the Enable Archiving drop-down list select Yes to enable or No to disable it. Enable this option if you are using the AltaVault for cold storage mode. If you enable this option, it increases the AltaVault cloud capacity for archive workloads. For more information about cold storage mode, see the section *Deployment guidelines* in the *NetApp AltaVault Could Integrated Storage Deployment Guide*.
8. Enable Cloud CA Certificate - Optionally, specify a cloud CA certificate that will be used to validate the server certificate of cloud provider. This must be .pem extension file.
9. Select the Enable Proxy check box to enable proxy server settings. A proxy server acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting service such as a file, connection, Web page, or other resource available on a different server, and the proxy server evaluates the request as a way to simplify and control their complexity.

   After you select the check box, specify the following settings:
   - Hostname/IP Address - Specify the hostname or IP address of the proxy.

- Port - Specify the port number.
- Username - Specify the username.
- Password - Specify the password.

10. Click **Apply** to apply your changes to the running configuration.

11. Click **Save** to save your configuration.

Google Cloud Storage

1. Select Google Cloud Storage.

2. Select yes or no to use keys from KMIP server from the drop-down list. When configuring the KMIP server, you must:
   - Use the same username and password as created in KMS.
   - Upload the same certificate as downloaded from KMS after signing it.
   - Add a symmetric key (KMIP key) as the encryption key.
   - Add a secret data key (KMIP key) for each of the authentication fields.

3. Specify the following settings:
   - Location - Select your location from the drop-down list. The choices are:
   - EU- Specifies Europe as the location.
   - US - Specifies the United States of America as the location.
   - Asia - Specifies Asia as the location.

4. Storage Class - Specify the storage class from the drop-down list:
   - Standard (Standard storage class)
   - Nearline
   - Project ID - Specify the project ID associated with the bucket. The project ID tells Google Cloud Storage which project you want to create a bucket in or which project to list buckets for. Each project is identified by its unique project ID. Since it is possible to have multiple projects, this ensures that the request is properly completed in the right project.
   - Client email - Specify the service account email address value from the API Manager > Credentials page of the Google developers console. For example, 12345@developer.gserviceaccount.com.
   - Private Key - Select Browse to specify the private key for your Google Cloud Storage service provider account.

     Google provides the private key in JSON and PKCS12 format. The AVA cloud credentials page requires a private key with a required extension of .pem or .json. You can read the client email and project ID from the .json file.

5. Verify the hostname of the cloud provider on which AltaVault stores the replicated data.

6. Specify the bucket name associated with your cloud service provider account. If Nearline is selected as Storage Class, the bucket should not be created through Google Developers Console. The Nearline bucket will

automatically be created by AltaVault. Buckets are the basic containers that store deduplicated data sent from the AltaVault. Everything that you store in the cloud provider storage must be contained in a bucket. You can use buckets to organize your data and control access to your data, but unlike directories and folders, you cannot nest buckets.

For more information on bucket name restrictions, see Google documentation.

- Bucket names must contain only lowercase letters, numbers, periods, hyphens, and underscores. Names containing periods require verification.
- Bucket names must start and end with a number or letter.
- Bucket names must contain from 3 to 63 characters. Names containing periods can contain up to 222 characters, but each period-separated component can be no longer than 63 characters.
- Bucket names cannot be represented as an IP address in dotted-decimal notation (for example, 192.168.5.4).
- Bucket names cannot begin with the "goog" prefix.

7. Specify the port through which replication occurs. Use port 443 for replication. Port 80 is not supported.

8. In the Enable Archiving drop-down list select Yes to enable or No to disable it. Enable this option if you are using the AltaVault for cold storage mode. If you enable this option, it increases the AltaVault cloud capacity for archive workloads. For more information about cold storage mode, see the section *Deployment guidelines* in the *NetApp AltaVault Could Integrated Storage Deployment Guide*.

9. Enable Cloud CA Certificate - Specify a cloud CA certificate that will be used to validate the server certificate of cloud provider. This must be a .pem or .json extension file.

10. Select the Enable Proxy check box to enable proxy server settings. A proxy server acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting service such as a file, connection, Web page, or other resource available on a different server, and the proxy server evaluates the request as a way to simplify and control their complexity.

After you select the check box, specify the following settings:

- Username/IP address - Specify the username or the IP address of the proxy server.
- Ports - Specify the port numbers to access the proxy server.
- Username - Specify the name of the user who has access to the proxy server.
- Password - Specify the password to authenticate the user.

Internet Initiative Japan (IIJ)

1. Select IIJ.

2. Select yes or no to use keys from KMIP server from the drop-down list. When configuring the KMIP server, you must:

- Use the same username and password as created in KMS.
- Upload the same certificate as downloaded from KMS after signing it.
- Add a symmetric key (KMIP key) as the encryption key.
- Add a secret data key (KMIP key) for each of the authentication fields.

3. Specify the following settings:

- Access Key - Specify the access key ID for your IIJ account.
- Secret Key - Specify the secret key for your IIJ account.

4. Specify the hostname of the cloud provider on which AltaVault stores the replicated data.

5. Specify the bucket name associated with your cloud service provider account. Buckets are the basic containers that store deduplicated data sent from the AltaVault. Everything that you store in the cloud provider storage must be contained in a bucket. You can use buckets to organize your data and control access to your data, but unlike directories and folders, you cannot nest buckets. If the bucket name does not exist, the bucket is created during initial AltaVault replication.

   You can use bucket names that are alphanumeric and contains period, dash, underscore, and tilde.

6. Specify the port number through which replication occurs.

7. In the Enable Archiving drop-down list select Yes to enable or No to disable it. Enable this option if you are using the AltaVault for cold storage mode. If you enable this option, it increases the AltaVault cloud capacity for archive workloads. For more information about cold storage mode, see the section *Deployment guidelines* in the *NetApp AltaVault Could Integrated Storage Deployment Guide*.

8. Enable Cloud CA Certificate - Optionally, specify a cloud CA certificate that will be used to validate the server certificate of cloud provider. This must be .pem extension file.

Microsoft Windows Azure Storage

1. Select Microsoft Windows Azure Storage

2. Select yes or no to use keys from KMIP server from the drop-down list. When configuring the KMIP server, you must:
   - Use the same username and password as created in KMS.
   - Upload the same certificate as downloaded from KMS after signing it.
   - Add a symmetric key (KMIP key) as the encryption key.
   - Add a secret data key (KMIP key) for each of the authentication fields.

3. Specify the following settings:
   - Cloud Type - Select your option from the drop-down list. The options are Azure Government or Azure Public.
   - Storage Account - Specify the Microsoft Azure Storage account name. AltaVault supports storage accounts belonging to either the Hot or Cool access tier.
   - Primary or Secondary Access Key - Specify the primary or secondary Microsoft Azure Storage access key that you generated when you created your Microsoft Azure Storage account. The secondary key provides the same access as the primary key and is used for backup purposes. You can regenerate each key in case either one is compromised.

4. Specify the hostname of the cloud provider on which AltaVault stores the replicated data.

5. Specify the port through which replication occurs. The default value is 443.

6. In the Enable Archiving drop-down list select Yes to enable or No to disable it. Enable this option if you are using the AltaVault for cold storage mode. If you enable this option, it increases the AltaVault cloud capacity for archive workloads. For more information about cold storage mode, see the section *Deployment guidelines* in the *NetApp AltaVault Could Integrated Storage Deployment Guide*.

7. Enable Cloud CA Certificate - Optionally, specify a cloud CA certificate that will be used to validate the server certificate of cloud provider. This must be .pem extension file.

8. Specify the container name associated with your cloud service provider account. Containers are the basic containers that store deduplicated data sent from the AltaVault. Everything that you store in the cloud provider storage must be contained in a container. You can use container to organize your data and control access to your data, but unlike directories and folders, you cannot nest containers. If the container name does not exist, the container is created during initial AltaVault replication.

   For Azure, the bucket names must be a valid DNS name, conforming to the following naming rules:

   - Container names must start with a letter or number and can contain only letters, numbers, and hyphens.
   - Every hyphen must be immediately preceded and followed by a letter or number. You cannot use consecutive hyphens.
   - All letters in a bucket names must be lowercase.
   - Container names must be from 3 to 63 characters.

9. Select the Enable Proxy check box to enable proxy server settings. A proxy server acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting service such as a file, connection, Web page, or other resource available on a different server, and the proxy server evaluates the request as a way to simplify and control their complexity.

   After you select the check box, specify the following settings:

   - Hostname/IP address - Specify the hostname or the IP address of the proxy server.
   - Ports - Specify the port numbers to access the proxy server.
   - Username - Specify the name of the user who has access to the proxy server.
   - Password - Specify the password to authenticate the user.

NetApp StorageGRID Webscale

1. Select NetApp StorageGRID Webscale

2. Select yes or no to use keys from KMIP server from the drop-down list. When configuring the KMIP server, you must:

   – Use the same username and password as created in KMS.
   – Upload the same certificate as downloaded from KMS after signing it.
   – Add a symmetric key (KMIP key) as the encryption key.
   – Add a secret data key (KMIP key) for each of the authentication fields.

3. Specify the following settings:

   - Account Access Key Identifier - Specify the access key (same as the username) for your NetApp StorageGRID Webscale account.

- Account Secret Access Key - Specify the secret key (password) for your cloud service provider account.
- Web Protocol - Select the Web protocol from the drop-down list.

4. Specify the hostname.

5. Specify the bucket name associated with your cloud service provider account. Buckets are the basic containers that store deduplicated data sent from the AltaVault. Everything that you store in the cloud provider storage must be contained in a bucket. You can use buckets to organize your data and control access to your data, but unlike directories and folders, you cannot nest buckets. If the bucket name does not exist, the bucket is created during initial AltaVault replication.

   You can use bucket names that:

   - are from 3 to 63 characters.
   - start with lower-case letters or numbers, hyphens (-), and periods (.).

6. Specify the port number.

   The default port is 8082. If you are using a StorageGRID Webscale single storage Node or a third party load balancer, the default port is 18082.

7. In the Enable Archiving drop-down list select Yes to enable or No to disable it. Enable this option if you are using the AltaVault for cold storage mode. If you enable this option, it increases the AltaVault cloud capacity for archive workloads. For more information about cold storage mode, see the section *Deployment guidelines* in the *NetApp AltaVault Could Integrated Storage Deployment Guide*.

8. Enable Cloud CA Certificate - Optionally, specify a cloud CA certificate that will be used to validate the server certificate of cloud provider. This must be .pem extension file.

9. Select the Enable Proxy check box to enable proxy server settings. A proxy server acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting service such as a file, connection, Web page, or other resource available on a different server, and the proxy server evaluates the request as a way to simplify and control their complexity.

   After you select the check box, specify the following settings:

   - Hostname/IP Address - Specify the hostname or IP address of the proxy.
   - Port - Specify the port number.
   - Username - Specify the username.
   - Password - Specify the password.

10. Click **Apply** to apply your changes to the running configuration.

11. Click **Save** to save your configuration.

OpenStack Object Storage (Swift)

1. Select OpenStack Object Storage (Swift).

2. Select yes or no to use keys from KMIP server from the drop-down list. When configuring the KMIP server, you must:

   – Use the same username and password as created in KMS.

- Upload the same certificate as downloaded from KMS after signing it.
- Add a symmetric key (KMIP key) as the encryption key.
- Add a secret data key (KMIP key) for the authentication fields.

3. Specify the following settings:

- Authentication - Specify one of the following methods that OpenStack Object Storage uses to authenticate each request:

  Access Key ID/Secret Key- Specify the access key ID, secret key, and tenant ID for your OpenStack Object Storage account.

  Username/Password - Specify the username, password, and tenant ID of your OpenStack Object Storage account.

  Username/API Access Key - Specify the username and the API Access key for your OpenStack Object Storage account.
- Authentication URL Path - Specify the cloud server API URL for OpenStack Object Storage to authenticate the request. For example, /auth/v1.0 or /auth/v2.0.
- Web Protocol - Specify whether to use the HTTP or HTTPS protocol. HTTPS is the secure version of the HTTP protocol, where packets are encrypted before they are transmitted. It uses the SSL protocol to ensure a secure environment.

4. Specify the hostname of the cloud provider on which AltaVault stores the replicated data.

5. Specify the bucket name associated with your cloud service provider account. Buckets are the basic containers that store deduplicated data sent from the AltaVault. Everything that you store in the cloud provider storage must be contained in a bucket. You can use buckets to organize your data and control access to your data, but unlike directories and folders, you cannot nest buckets. If the bucket name does not exist, the bucket is created during initial AltaVault replication.

You can use bucket names that are alphanumeric and contain period, dash, underscore, and tilde.

6. Specify the port through which replication occurs. The default value is 443.

7. In the Enable Archiving drop-down list select Yes to enable or No to disable it. Enable this option if you are using the AltaVault for cold storage mode. If you enable this option, it increases the AltaVault cloud capacity for archive workloads. For more information about cold storage mode, see the section *Deployment guidelines* in the *NetApp AltaVault Could Integrated Storage Deployment Guide*.

8. Enable Cloud CA Certificate - Optionally, specify a cloud CA certificate that will be used to validate the server certificate of cloud provider. This must be .pem extension file.

9. Select the Enable Proxy check box to enable proxy server settings. A proxy server acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting service such as a file, connection, Web page, or other resource available on a different server, and the proxy server evaluates the request as a way to simplify and control their complexity.

After you select the check box, specify the following settings:

- Hostname/IP address - Specify the hostname or the IP address of the proxy server.
- Ports - Specify the port numbers to access the proxy server.
- Username - Specify the name of the user who has access to the proxy server.
- Password - Specify the password to authenticate the user.

Oracle Storage Cloud Service - Object Storage

1. Select Oracle Storage Cloud Service - Object Storage.

2. Select yes or no to use keys from KMIP server from the drop-down list. When configuring the KMIP server, you must:
   - Use the same username and password as created in KMS.
   - Upload the same certificate as downloaded from KMS after signing it.
   - Add a symmetric key (KMIP key) as the encryption key.
   - Add a secret data key (KMIP key) for the authentication fields.

3. Specify the following settings:
   - Storage Class - By default, Storage Class is set to Standard.
   - Authentication - Specify one of the following methods that Oracle Storage Cloud uses to authenticate each request:

     Access Key ID/Secret Key- Specify the access key ID, secret key, and tenant ID for your Oracle Storage Cloud account.

     Username/Password - Specify the username, password, and tenant ID of your Oracle Storage Cloud.

     Username/API Access Key - Specify the username and the API Access key for your Oracle Storage Cloud account.
   - Authentication URL Path - Specify the cloud server API URL for Oracle Storage Cloud to authenticate the request. For example, /auth/v1.0 or /auth/v2.0.
   - Web Protocol - Specify whether to use the HTTP or HTTPS protocol. HTTPS is the secure version of the HTTP protocol, where packets are encrypted before they are transmitted. It uses the SSL protocol to ensure a secure environment.

4. Specify the hostname of the cloud provider on which AltaVault stores the replicated data.

5. Specify the bucket name associated with your cloud service provider account. Buckets are the basic containers that store deduplicated data sent from the AltaVault. Everything that you store in the cloud provider storage must be contained in a bucket. You can use buckets to organize your data and control access to your data, but unlike directories and folders, you cannot nest buckets. If the bucket name does not exist, the bucket is created during initial AltaVault replication.

   You can use bucket names that are alphanumeric and contain period, dash, underscore, and tilde.

6. Specify the port through which replication occurs. The default value is 443.

7. In the Enable Archiving drop-down list select Yes to enable or No to disable it. Enable this option if you are using the AltaVault for cold storage mode. If you enable this option, it increases the AltaVault cloud capacity for archive workloads. For more information about cold storage mode, see the section *Deployment guidelines* in the *NetApp AltaVault Could Integrated Storage Deployment Guide*.

8. Enable Cloud CA Certificate - Optionally, specify a cloud CA certificate that will be used to validate the server certificate of cloud provider. This must be .pem extension file.

9. Select the Enable Proxy check box to enable proxy server settings. A proxy server acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting service

such as a file, connection, Web page, or other resource available on a different server, and the proxy server evaluates the request as a way to simplify and control their complexity.

After you select the check box, specify the following settings:

- Hostname/IP address - Specify the hostname or the IP address of the proxy server.
- Ports - Specify the port numbers to access the proxy server.
- Username - Specify the name of the user who has access to the proxy server.
- Password - Specify the password to authenticate the user.

Outscale On-Demand Storage

1. Select Outscale On-Demand Storage.
2. Select yes or no to use keys from KMIP server from the drop-down list. When configuring the KMIP server, you must:
   - Use the same username and password as created in KMS.
   - Upload the same certificate as downloaded from KMS after signing it.
   - Add a symmetric key (KMIP key) as the encryption key.
   - Add a secret data key (KMIP key) for each of the authentication fields.
3. Specify the following settings:
   - Access Key - Specify the access key ID for your Outscale On-Demand Storage account.
   - Secret Key - Specify the secret key for your Outscale On-Demand Storage account.
4. Specify the hostname of the cloud provider on which AltaVault stores the replicated data.
5. Specify the bucket name associated with your cloud service provider account. Buckets are the basic containers that store deduplicated data sent from the AltaVault. Everything that you store in the cloud provider storage must be contained in a bucket. You can use buckets to organize your data and control access to your data, but unlike directories and folders, you cannot nest buckets. If the bucket name does not exist, the bucket is created during initial AltaVault replication.

   You can use bucket names that are alphanumeric and contains period, dash, underscore, and tilde.
6. Specify the port number through which replication occurs.
7. In the Enable Archiving drop-down list select Yes to enable or select No to disable it. Enable this option if you are using the AltaVault for cold storage mode or writing compressed or encrypted backup data. If you enable this option, it increases the AltaVault cloud capacity for such workloads.
8. Enable Cloud CA Certificate - Optionally, specify a cloud CA certificate that will be used to validate the server certificate of cloud provider. This must be .pem extension file.
9. Select the Enable Proxy check box to enable proxy server settings. A proxy server acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting service such as a file, connection, Web page, or other resource available on a different server, and the proxy server evaluates the request as a way to simplify and control their complexity.

   After you select the check box, specify the following settings:

- Hostname/IP address - Specify the hostname or the IP address of the proxy server.
- Ports - Specify the port numbers to access the proxy server.
- Username - Specify the name of the user who has access to the proxy server.
- Password - Specify the password to authenticate the user.

Rackspace Cloud Files

1. Select Rackspace Cloud Files.
2. Select yes or no to Use Keys from KMIP Server from the drop-down list. When configuring the KMIP server, you must:
   - Use the same username and password as created in KMS.
   - Upload the same certificate as downloaded from KMS after signing it.
   - Add a symmetric key (KMIP key) as the encryption key.
   - Add a secret data key (KMIP key) for the authentication fields.
3. Specify the following settings:
   - Region - Select the region from the drop-down list:
   - US-based
   - UK-based
- Username - Specify the username that Rackspace uses to authenticate each request.
- API Access Key - Specify the API access key for your Rackspace account.

4. Specify the hostname of the cloud provider on which AltaVault stores the replicated data.
5. Specify the bucket name associated with your cloud service provider account. Buckets are the basic containers that store deduplicated data sent from the AltaVault. Everything that you store in the cloud provider storage must be contained in a bucket. You can use buckets to organize your data and control access to your data, but unlike directories and folders, you cannot nest buckets. If the bucket name does not exist, the bucket is created during initial AltaVault replication.

   You can use bucket names that are alphanumeric and contain period, dash, underscore, and tilde.

   For Rackspace, the bucket names must not be longer than 256 characters.
6. Specify the port through which replication occurs. The default value is 443.
7. In the Enable Archiving drop-down list select Yes to enable or select No to disable it.Enable this option if you are using the AltaVault for cold storage mode or writing compressed or encrypted backup data. If you enable this option, it increases the AltaVault cloud capacity for such workloads.
8. Enable Cloud CA Certificate - Optionally, specify a cloud CA certificate that will be used to validate the server certificate of cloud provider. This must be .pem extension file.
9. Select the Enable Proxy check box to enable proxy server settings. A proxy server acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting service

such as a file, connection, Web page, or other resource available on a different server, and the proxy server evaluates the request as a way to simplify and control their complexity.

After you select the check box, specify the following settings:

- Hostname/IP address - Specify the hostname or the IP address of the proxy server.
- Ports - Specify the port numbers to access the proxy server.
- Username - Specify the name of the user who has access to the proxy server.
- Password - Specify the password to authenticate the user.

Scality RING

1. Select the provider as Scality RING.
2. Select yes or no to use keys from KMIP server from the drop-down list. When configuring the KMIP server, you must:
   - Use the same username and password as created in KMS.
   - Upload the same certificate as downloaded from KMS after signing it.
   - Add a symmetric key (KMIP key) as the encryption key.
   - Add a secret data key (KMIP key) for each of the authentication fields.
3. Specify the following settings:
   - Access Key - Specify the access key ID for your Scality RING account.
   - Secret Key - Specify the secret key for your Scality RING account.
4. Specify the hostname of the cloud provider on which AltaVault stores the replicated data.
5. Specify the bucket name associated with your cloud service provider account. Buckets are the basic containers that store deduplicated data sent from the AltaVault. Everything that you store in the cloud provider storage must be contained in a bucket. You can use buckets to organize your data and control access to your data, but unlike directories and folders, you cannot nest buckets. If the bucket name does not exist, the bucket is created during initial AltaVault replication.

   You can use bucket names that are alphanumeric and contain period, dash, underscore, and tilde characters.
6. Specify the port number through which replication occurs.
7. In the Enable Archiving drop-down list select Yes to enable or select No to disable it. Enable this option if you are using the AltaVault for cold storage mode or writing compressed or encrypted backup data. If you enable this option, it increases the AltaVault cloud capacity for such workloads.
8. Enable Cloud CA Certificate - check this box and specify a cloud CA certificate that will be used to validate the server certificate of cloud provider. This must be .pem extension file.

SoftLayer Object Storage (Swift)

1. Select SoftLayer Object Storage (Swift).

2. Select yes or no to Use Keys from KMIP Server from the drop-down list. When configuring the KMIP server, you must:
   - Use the same username and password as created in KMS.
   - Upload the same certificate as downloaded from KMS after signing it.
   - Add a symmetric key (KMIP key) as the encryption key.
   - Add a secret data key (KMIP key) for each of the authentication fields.
3. Specify the following settings:

- Region - Select the region from the drop-down list:
  - San Jose 1
  - Amsterdam 1
  - Dallas 5
  - Hong Kong 2
  - London 2
  - Singapore 1
  - Toronto 1
- Username - Specify the username that SoftLayer Object Storage (Swift) uses to authenticate each request.
- API Access Key - Specify the API access key for your SoftLayer Object Storage (Swift) account.

4. Specify the hostname of the cloud provider on which AltaVault stores the replicated data.
5. Specify the bucket name associated with your cloud service provider account. Buckets are the basic containers that store deduplicated data sent from the AltaVault. Everything that you store in the cloud provider storage must be contained in a bucket. You can use buckets to organize your data and control access to your data, but unlike directories and folders, you cannot nest buckets. If the bucket name does not exist, the bucket is created during initial AltaVault replication.

   You can use bucket names that are alphanumeric and contain period, dash, underscore, and tilde.

   For SoftLayer Object Storage (Swift), the bucket names must not be longer than 256 characters.
6. Specify the port through which replication occurs. The default value is 443.
7. In the Enable Archiving drop-down list select Yes to enable or No to disable it. Enable this option if you are using the AltaVault for cold storage mode. If you enable this option, it increases the AltaVault cloud capacity for archive workloads. For more information about cold storage mode, see the section *Deployment guidelines* in the *NetApp AltaVault Could Integrated Storage Deployment Guide*.
8. Enable Cloud CA Certificate - Optionally, specify a cloud CA certificate that will be used to validate the server certificate of cloud provider. This must be .pem extension file.
9. Select the Enable Proxy check box to enable proxy server settings. A proxy server acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting service such as a file, connection, Web page, or other resource available on a different server, and the proxy server evaluates the request as a way to simplify and control their complexity.

   After you select the check box, specify the following settings:

   - Username/IP address - Specify the username or the IP address of the proxy server.

- Ports - Specify the port numbers to access the proxy server.
- Username - Specify the name of the user who has access to the proxy server.
- Password - Specify the password to authenticate the user.

Swisscom Dynamic Storage

1. Select Swisscom Dynamic Storage.
2. Select yes or no to use keys from KMIP server from the drop-down list. When configuring the KMIP server, you must:
   - Use the same username and password as created in KMS.
   - Upload the same certificate as downloaded from KMS after signing it.
   - Add a symmetric key (KMIP key) as the encryption key.
   - Add a secret data key (KMIP key) for each of the authentication fields.
3. Specify the following settings:
   - Subtenant ID - Specify the subtenant ID that Swisscom Dynamic Storage uses to authenticate each request.
   - UID - Specify the user ID that Swisscom Dynamic Storage uses to authenticate each request.
   - Shared Secret - Specify the shared secret that Swisscom Dynamic Storage uses to authenticate each request. When the client application builds a Web service request, Swisscom Dynamic Storage uses the shared secret to create a signature entry as a part of the request. The shared secret must be associated with the tenant ID and application ID created by Swisscom Dynamic Storage.
4. Specify the hostname.
5. Specify the bucket name associated with your cloud service provider account. Buckets are the basic containers that store deduplicated data sent from the AltaVault. Everything that you store in the cloud provider storage must be contained in a bucket. You can use buckets to organize your data and control access to your data, but unlike directories and folders, you cannot nest buckets. If the bucket name does not exist, the bucket is created during initial AltaVault replication.

   You can use bucket names that:
   - are from 3 to 255 characters.
   - are a series of one or more labels separated by a period, dash, and underscore.
   - start with alphanumeric character.
6. Specify the port number.
7. In the Enable Archiving drop-down list select Yes to enable or No to disable it. Enable this option if you are using the AltaVault for cold storage mode. If you enable this option, it increases the AltaVault cloud capacity for archive workloads. For more information about cold storage mode, see the section *Deployment guidelines* in the *NetApp AltaVault Could Integrated Storage Deployment Guide*.
8. Enable Cloud CA Certificate - Optionally, specify a cloud CA certificate that will be used to validate the server certificate of cloud provider. This must be .pem extension file.

9. Select the Enable Proxy check box to enable proxy server settings. A proxy server acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting service such as a file, connection, Web page, or other resource available on a different server, and the proxy server evaluates the request as a way to simplify and control their complexity.

   After you select the check box, specify the following settings:

   - Hostname/IP Address - Specify the hostname or IP address of the proxy.
   - Port - Specify the port number.
   - Username - Specify the username.
   - Password - Specify the password.

Telefonica Cloud Storage

1. Select Telefonica Cloud Storage.

2. Select yes or no to use keys from KMIP server from the drop-down list. When configuring the KMIP server, you must:

   – Use the same username and password as created in KMS.

   – Upload the same certificate as downloaded from KMS after signing it.

   – Add a symmetric key (KMIP key) as the encryption key.

   – Add a secret data key (KMIP key) for each of the authentication fields.

3. Specify the following settings:

   - Access Key - Specify the access key (same as the username) for your Telefonica Cloud Storage account.
   - Secret Key - Specify the secret key (password) for your cloud service provider account.

4. Specify the hostname.

5. Specify the bucket name associated with your cloud service provider account. Buckets are the basic containers that store deduplicated data sent from the AltaVault. Everything that you store in the cloud provider storage must be contained in a bucket. You can use buckets to organize your data and control access to your data, but unlike directories and folders, you cannot nest buckets. If the bucket name does not exist, the bucket is created during initial AltaVault replication.

   You can use bucket names that:

   - are from 3 to 30 characters.
   - start with lower-case letters or numbers.

6. Specify the port number.

7. In the Enable Archiving drop-down list select Yes to enable or No to disable it. Enable this option if you are using the AltaVault for cold storage mode. If you enable this option, it increases the AltaVault cloud capacity for archive workloads. For more information about cold storage mode, see the section *Deployment guidelines* in the *NetApp AltaVault Could Integrated Storage Deployment Guide*.

8. Enable Cloud CA Certificate - Optionally, specify a cloud CA certificate that will be used to validate the server certificate of cloud provider. This must be .pem extension file.

9. Select the Enable Proxy check box to enable proxy server settings. A proxy server acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting service such as a file, connection, Web page, or other resource available on a different server, and the proxy server evaluates the request as a way to simplify and control their complexity.

   After you select the check box, specify the following settings:

   - Hostname/IP Address - Specify the hostname or IP address of the proxy.
   - Port - Specify the port number.
   - Username - Specify the username.
   - Password - Specify the password.

Verizon Cloud Storage

1. Select Verizon Cloud Storage.

2. Select yes or no to use keys from KMIP server from the drop-down list. When configuring the KMIP server, you must:

   – Use the same username and password as created in KMS.

   – Upload the same certificate as downloaded from KMS after signing it.

   – Add a symmetric key (KMIP key) as the encryption key.

   – Add a secret data key (KMIP key) for each of the authentication fields.

3. Specify the following settings:

   - Region - Select an Verizon Cloud Storage region from the drop-down list. You can choose a region to optimize for latency, minimize costs, or address regulatory requirements. You can select one of the following regions:

   – US (East Coast)

   – US (3 Data Center Spread)

   – EU (Netherlands)

   - Access Key - Specify the access key (same as the username) for your Version Cloud Storage account.
   - Secret Key - Specify the secret key (password) for your cloud service provider account.

4. Specify the hostname.

5. Specify the bucket name associated with your cloud service provider account. Buckets are the basic containers that store deduplicated data sent from the AltaVault. Everything that you store in the cloud provider storage must be contained in a bucket. You can use buckets to organize your data and control access to your data, but unlike directories and folders, you cannot nest buckets. If the bucket name does not exist, the bucket is created during initial AltaVault replication.

   You can use bucket names that:

   - are from 3 to 63 characters.
   - are a series of one or more labels separated by a period.
   - start and end with lower-case letters or numbers.

6. Specify the port number.

7. In the Enable Archiving drop-down list select Yes to enable or No to disable it. Enable this option if you are using the AltaVault for cold storage mode. If you enable this option, it increases the AltaVault cloud capacity for archive workloads. For more information about cold storage mode, see the section *Deployment guidelines* in the *NetApp AltaVault Could Integrated Storage Deployment Guide*.

8. Enable Cloud CA Certificate - Optionally, specify a cloud CA certificate that will be used to validate the server certificate of cloud provider. This must be .pem extension file.

9. Select the Enable Proxy check box to enable proxy server settings. A proxy server acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting service such as a file, connection, Web page, or other resource available on a different server, and the proxy server evaluates the request as a way to simplify and control their complexity.

   After you select the check box, specify the following settings:

   - Hostname/IP Address - Specify the hostname or IP address of the proxy.
   - Port - Specify the port number.
   - Username - Specify the username.
   - Password - Specify the password.

Using the import configuration wizard

Use the Import Configuration wizard to import a previously saved configuration into the AltaVault. The Import Configuration Wizard fails if the AltaVault already has an encryption key set.

It is recommended to run the System Settings Wizard first to properly set the AltaVault's time zone to the same time zone as previously configured in the AltaVault configuration being imported.

To use the import configuration wizard

1. Select Import Configuration in the Wizard Dashboard.

2. Select one of the following options:

   - Select Local File and click **Browse** to select a local configuration file from your computer.

     -or-

   - Select URL and specify the URL of an appliance whose configuration you want to import.

3. Leave the Import Shared Data Only check box selected to import only the following common settings (the system does not automatically copy the other settings):

   - Cloud settings
   - Email settings
   - Logging
   - NTP settings
   - SNMP settings
   - Statistics or Alarms settings

- Time zone settings
- Web and CLI preferences
- SMB, NFS, and OST configuration

When you select the Import Shared Data Only check box, the following settings are not imported:

- General Security Settings
- Static host configuration
- Appliance licenses
- Interface configuration, IP configuration, static routes, and virtual interfaces.
- Radius protocol settings
- Name server settings and domains
- Scheduled Jobs
- SSH server settings and public or private keys
- Hostname, Message of the Day (MOTD), and Fully Qualified Domain Name (FQDN)
- TACACS protocol settings
- Telnet server settings

4. Select the Key Passphrase protect the Encryption Key check box to specify a password for the encryption key. If you select this option, you must enter the same password when you import or export the encryption key.

5. Click **Import Configuration**.

6. Click **Exit**.

Using the export configuration wizard

Use the Export Configuration wizard to export the current AltaVault configuration.

To use the export configuration wizard

1. Select Export Configuration in the dashboard.
2. Specify the password for the encryption key in the password field. The password field appears only if you specified a password for your encryption key when you generated it in the Cloud Settings Wizard page.
3. Click **Export Configuration** to download the current AltaVault configuration file AltaVault_config_(HOSTNAME)_(DATETIME).tgz.
4. Click **Exit** to close the Export Configuration Wizard page and go back to the dashboard.

CHAPTER 3 Configuring storage settings

This section describes how to configure storage settings. It includes the following sections:

- "Configuring cloud settings" on page 49
- "Configuring SMB" on page 52
- "Configuring NFS" on page 57
- "Configuring OST" on page 60
- "Restoring data from the cloud using the prepopulation page" on page 62
- "Viewing offline file system check page" on page 63
- "Viewing online file system check page" on page 64
- "Viewing the verify tool diagnostics" on page 65

Configuring cloud settings

You can specify cloud settings, encryption settings, replication scheduling, and bandwidth limit settings in the Configure > Cloud Settings page.

Before you configure cloud settings, you must configure DNS settings to access the cloud service provider host machine on the Configure > Host Settings page.

This section includes the following topics:

- "Configuring cloud provider settings" on page 50
- "Configuring encryption" on page 50
- "Configuring replication" on page 50
- "Configuring bandwidth limits" on page 51

To transition cloud credentials and the encryption key from the AltaVault to a Key Management Server (KMS), refer to the section "Configuring KMIP" on page 117.

Configuring cloud provider settings

The cloud provider is a service provider that offers customers storage or software services available through a private (internal) or public network (cloud). This setting enables you to access the storage and software through the Internet. For more details on cloud provider settings, see "Using the cloud settings wizard" on page 17.

Only users who have Read-Only Replication Settings permission or Read and Write Replication Settings permission can access and configure the Cloud Settings Page.

Configuring encryption

The new datastore encryption key can be generated or imported from an existing one.

To secure the encryption key, protect it using a key passphrase. This passphrase will be used to encrypt the datastore encryption key, and must be provided whenever importing this datastore encryption key, such as for disaster recovery. It is not stored within a configuration archive and must be kept in a secure location.

For more information on encryption, see "Using the cloud settings wizard" on page 17.

Configuring replication

Replication is the process of copying data and metadata from the AltaVault to the cloud. The AltaVault replicates data to the cloud asynchronously. Replication provides an extra measure of redundancy that can be invaluable if the main storage backup system fails. Immediate access to the replicated data minimizes downtime and its associated costs. This access can be invaluable if the AltaVault disk cache or if the entire AltaVault fails.

Replication streamlines disaster recovery processes by generating duplicate copies of all backed-up files on a continuous basis. It can also simplify recovery from all types of disasters, including fire, flood, hurricane, virus, or worm.

Only users who have Read-Only Replication Settings permission or Read and Write Replication Settings permission can access and configure the Replication Settings Page.

To configure replication

1. Choose Configure > Cloud Settings.
2. Select the Replication tab.
3. Under Replication Settings, complete the configuration as described in this table.

Control	Description
Pause Replication at	Specify the time (in HH:MM:SS format) at which you want replication to pause.
Resume Replication at	Specify the time (in HH:MM:SS format) at which you want replication to resume.
Bytes pending replication alert limit	Displays an alarm if the number of bytes pending replication to the cloud exceeds the value you specify. The default value is 500 GiB.
Bytes pending replication clear limit	Specify the lower clear so that, if the number of bytes pending replication to the cloud rises above the alert limit (and generates a notification), and later falls below this value, the notification is cleared. The default value is 450 GiB.
Suspend Replication	Click to temporarily stop replication. This step might require restarting the storage optimization service. In this case, the AltaVault prompts you to restart service.

4. Click **Apply** to apply your changes to the running configuration.

5. Click **Save** to save your configuration.

Configuring bandwidth limits

You can limit the bandwidth that the AltaVault uses to replicate data as well as restore data in the bandwidth limit settings page.

Only users who have Read-Only Replication Settings permission or Read and Write Replication Settings permission can access and configure the Bandwidth Limit Settings Page.

To configure bandwidth limits

1. Choose Configure > Cloud Settings.
2. Select the Bandwidth tab.
3. Under Bandwidth Limit Settings, complete the configuration as described in this table.

Control	Description
Cloud Replication Interface	Select either primary or default from the drop-down list. Use this parameter to limit the number of bits per second transmitted through this interface. The AltaVault can use different interfaces to send data to the cloud, to restore data. To configure the bandwidth for each interface, select the interface in the drop-down list and then specify the bandwidth limits and scheduling. You must specify the cloud replication interface to enable bandwidth limiting. You can force data replication or restoration using this interface. It is useful if the appliance can connect to the cloud on more than one interface, and you want to specify which interface to use for the cloud connection.
Replication Limit Rate	Specify a rate to limit the data transmitted to the cloud storage provider in kilobits per seconds (kbps).
Restore Limit Rate	Specify a rate to limit the data restored to the front-end SMB share, NFS export, or OST share, in kilobits per second (kbps).
Enable Bandwidth Limit Scheduling	Before you select this option, you must specify the replication/restore interface above. Select the check box and specify the following bandwidth limit schedule parameters: • Start Time - Specify the time at which the bandwidth limit should start. • End Time - Specify the time at which the bandwidth limit should end. • Replication Limit Rate - Specify a secondary rate to limit the data transmitted in kilobits per second during the scheduled start and end times. The bandwidth reverts to the normal replication limit rate outside the scheduled times. • Restore Limit Rate - Specify the limit rate. • Include Weekends - Click to include weekends in the schedule.

4. Click **Apply** to apply your changes to the running configuration.
5. Click **Save** to save your configuration.

   After you apply your settings, you can verify whether changes have had the desired effect by reviewing related reports. When you have verified appropriate changes, you can write the active configuration that is stored in memory to the active configuration file (or you can save it using any filename you choose).

Configuring SMB

One of the primary AltaVault NAS protocols that is used to perform data protection movement from backup application servers to AltaVault is SMB. This Windows-based protocol allows Windows servers to communicate with other SMB-enabled systems, such as AltaVault. SMB is sometimes referred to as *CIFS*, but CIFS is the predecessor to SMB and is now considered as obsolete.

SMB is currently enabled in two versions: SMBv2 and SMBv3. SMBv2 is the default protocol that is used with Windows 2000 and Windows 2008 systems, and SMBv3 is the default protocol that is used with Windows 2012 systems.NetApp AltaVault supports SMB2 and SMB3. The SMB protocol that AltaVault uses has been redesigned to take advantage of the latest technology features that are available with SMBv3, such as SMB multichannel.You can configure SMB access for Microsoft Windows based clients to the AltaVault in the Configure > SMB page. SMB is a protocol that allows programs to make requests for files and services on remote computers on the Internet.

Note: If you are upgrading to AVA4.2 or later releases, migration of your CIFS configuration from earlier AVA releases to AVA SMB is supported. For detailed CIFS to SMB upgrade considerations and information about connecting to the SMB share from Windows environments, see the *NetApp AltaVault Could Integrated Storage Deployment Guide*.

When configuring SMB, you perform the following tasks:

- "To configure an Active Directory domain" on page 52
- "To add an SMB share" on page 53
- "To add a local user to access the share" on page 54
- "To edit local user permission to access the share" on page 55
- "To add local SMB user" on page 55
- "To edit SMB local user" on page 56
- "To edit multichannel settings" on page 56

To configure an Active Directory domain

1. The SMB page does not appear until the storage optimization service is started. If needed, choose Maintenance > Service and click Start to initialize the service.

2. If your network has an Active Directory (AD) domain, you can add the AltaVault to the domain and enable domain users to access AltaVault SMB shares.

   You can add the AltaVault only to one domain, you cannot add it to multiple domains.

   Ensure that you have permissions to join appliances to the domain and add users who can access the domain.

   To join the AltaVault to an AD domain, go to the Domain section of the page and complete the configuration as described in this table.

Control	Description
Domain Name	Specify the fully qualified domain name of the AD that the AltaVault must join. If your system has an AD domain, then you can add the AltaVault to your AD domain and create share permissions for AD users and groups.

Control	Description
Username	Specify the username of a user to access the AD domain. The username must be a part of the AD and the user must have permissions to add computers to the domain.
Password	Specify the domain password to authenticate the user.

3. Click Show Advanced Settings to display Advanced Settings to (optionally) configure the domain. Complete the configuration as described in this table.

Control	Description
Hostname	Optionally, specify the hostname that the AltaVault must use to join the domain. AltaVault then appears as the specified hostname in the AD.
Domain Controller Name	Optionally, specify the fully qualified domain name of the domain controller AltaVault will use for joining the domain. **Note:** Remember this value and for later use when leaving the domain.
Join Domain	Select to add the AltaVault to your AD domain.

4. After you join a domain, the Domain section of the SMB page changes to reflect the domain that the AltaVault has joined.

   When you leave a domain, specify the following information:.

Control	Description
Username	Optionally, specify the username of a user to access the AD domain. The username must be a part of the AD and the user must have permissions to add computers to the domain.
Password	Optionally, specify the domain password to authenticate the user.
Domain Controller Name	Optionally, if a specific domain controller was used to join the domain, specify the fully qualified domain name of the domain controller AltaVault originally used for joining the domain.
Leave Domain	Select Leave for the AltaVault to leave the AD domain.

   Reboot all client machines that were used to connect to the AltaVault to delete cached domain credentials.

To add an SMB share

1. The SMB page does not appear until the storage optimization service is started. If needed, choose Maintenance > Service and click Start to initialize the service.

2. Optionally, under Pinned Data Information, slide the thermometer to select the bytes allowed for share pinning. Share pinning enables the share to always contain data that is available to the AltaVault locally, without fetching it from the cloud.

3. To add an SMB share, complete the configuration as described in this table.

Control	Description
Add SMB Share	Displays the controls to add a new SMB share.
Share Name	Specify the name of the share to be added.

Control	Description
Pin Share	Select yes or no from the drop-down list to specify whether or not the SMB share should be pinned. Share pinning enables the share to always contain data that is available to the AltaVault locally, without fetching it from the cloud. You cannot remove a pinned share if it contains data. Once a share is pinned, unpinning of that share can be performed via CLI and requires optimization service to be offline. Unpinning a share can be a time-consuming operation. Unpinning a share does not result in erasing the previously pinned data. Only the previously pinned data is available for eviction, if applicable becomes full.
Early Eviction	Select yes or no from the drop-down list to specify whether or not data from this share should be assigned a higher priority for eviction. If you select yes, data written to this share is eligible for eviction earlier than other data. If you select no, data written to this share is evicted using the default method.
Disable Dedupe	Select yes or no from the drop-down list to specify whether or not data written to this share should be checked for duplication. If you select no, then the AltaVault checks if there is duplication of the data written to the share, and deduplicates the data. If you select yes, then the AltaVault does not check if there is duplication of the data written to the share and does not does perform deduplication.
Disable Compression	Select yes or no from the drop-down list to specify whether or not data from this share should be checked for compression. Select yes if your data set is already in a precompressed format. Select no if you data set is not precompressed.
Local Path	Specify the internal pathname on the AltaVault to which this SMB share writes data.
Comment	Specify a comment about the share. You use only alphanumeric characters, underscores, hyphens, and spaces.
Read Only	Select this check box if you want the share to be a read-only share.
Allow Everyone Access	Select this check box to enable all clients connected to the AltaVault system to access the SMB share. Clear this check box if you want to enable individual authentication, such as through Windows AD users or groups. **Note:** If AltaVault is configured in a domain environment, NetApp recommends that you leave the option Allow Everyone Access selected. Leaving it selected allows initial administration access to the share. After you connect to the share and set the share ownership, you can remove the Everyone account when you configure domain users and groups from your Windows settings. If AltaVault is not configured in a domain, the Allow Everyone Access option is not required.
Remove Selected	Deletes the selected SMB share.
Add Share	Adds the SMB share to the AltaVault.

The share you configured appears in the list of shares on the page along with the option to add a local user.

To add a local user to access the share

SMB share security and access can be administered in AD domains via Windows Explorer. If AltaVault is not within an AD domain, use a local user account to gain access to a share.

1. To add a local user to access the share that you created, expand the share name to complete the configuration as described in the following table.

Note: A local SMB user must first be created as described in the "To add local SMB user" on page 55 before you can add the user to a share.

Control	Description
Add a User	Displays the controls to add a user to the SMB share.
User	Select the user from t he drop-down list.
Access	Select one of the following options from the drop-down list: Allow - Allows the user read and write privileges of a file or folder. Attributes are defined by NTFS. Deny - Denies the user read and write privileges of a file or folder. Attributes are defined by NTFS.
Remove Selected	Deletes the selected user from the SMB server.
Add User	Adds the SMB user.

2. Click Save to apply your changes.

To edit local user permission to access the share

After adding local user access to the share, you can edit access permissions for each user.

1. Expand the user name to change permissions as described in the following table.

Control	Description
Edit Permissions	Select the following options: Allow - Allows the user Read, Write, or Modify permission for the share. Deny - Denies the user Read, Write, or Modify permission for the share. **Note:** Permission settings are hierarchical; that is, Read permission provides read-only access to the share. Write permission provides read and write access to the share. Modify permission provides read, write, and modify access to the share, as well as allowing full control of the share. For example, Modify provides read, write, and modify permission to a user even if you specifically deny write permission to that user.
Apply	Applies the changes to the SMB share users.

To add local SMB user

1. To add SMB user to access the share that you created, complete the configuration as described in this table.

Control	Description
Add SMB User	Displays the controls to add a user to the SMB share.
User Name	Specify the user name of a local user to access the SMB share. The user name is case sensitive.
Password	Specify the password for the new user.

Control	Description
Password Confirm	Confirm the new password of the new user.
Admin	Select one of the following options from the drop-down list: • Yes - Provides Administrator privileges to user • No - Disables Administrator privileges to user
Account	Select one of the following options from the drop-down list: • Enabled - Enables local user account for accessing SMB share • Disabled - Disables local user account from accessing SMB share
Remove Selected	Removes local SMB user configuration.
Add	Adds local SMB user.

To edit SMB local user

1. Extend the user name to complete the configuration as described in this table.

Control	Description
Change Password	Select the check box to change the password.
Password	Specify the new password for the user.
Password Confirm	Confirm the new password of the user.
Admin	Select one of the following options from the drop-down list: • Yes - Provides Administrator privileges to user • No - Disables Administrator privileges to user
Account	Select one of the following options from the drop-down list: • Enabled - Enables local user account for accessing SMB share • Disabled - Disables local user account from accessing SMB share
Remove Selected	Deletes the selected user from the SMB server.
Apply	Applies the changes to the SMB share users.

To edit multichannel settings

SMB multichannel is a feature allows SMB v3 shares to be accessed via multiple network interfaces from Windows hosts that support SMB v3.

1. Multichannel support is enabled for all interfaces by default. To disable an interface (e0a, e0b, e0c), select the checkbox for the interface and click **Disable**.

Note: To choose all interfaces simultaneously, select the Physical interfaces checkbox.

2. To enable an interface, click the checkbox for the interface and click **Enable**.

Configuring NFS

You can configure Network File System (NFS) for Unix and Linux based clients in the Configure > NFS page. NFS is a protocol that enables a user on a Unix or Linux based client computer to access files over a network in a manner similar to how local storage is accessed. Before you configure NFS, choose Reports > Storage Optimization and click **Stop** to stop the storage optimization service.

This section includes the following topics:

- "Configuration tasks" on page 57
- "Editing an NFS configuration" on page 58
- "Troubleshooting NFS exports to AIX" on page 60

Configuration tasks

You can configure NFS on the Configure > NFS page.

To configure NFS protocol

1. The NFS page does not appear until the storage optimization service is started. If needed, choose Maintenance > Service and click Start to initialize the service.

2. Under Pinned Data Information, slide the thermometer to select the maximum bytes allowed for share pinning. Share pinning enables the share to always contain data that is available to the AltaVault locally, without fetching it from the cloud. You can pin NFS exports only when you create the share.

3. To configure Kerberos, see "Deploying Kerberos-based environments".

4. Under Add an Export, complete the configuration as described in this table.

Control	Description
Add an Export	Displays the controls to export an NFS share.
Name	Specify the name of the export share.
Export as NFSv4	Select yes or no from the drop-down list to specify the type of NFS export. If you select yes, the export will be configured as NFSv4 export. If you select no, the export will be configured as NFSv3 export.
Pin Export	Select Yes or No from the drop-down list to specify whether the NFS export should be pinned. Share pinning enables the share to always contain data that is available to the AltaVault locally without fetching it from the cloud. You cannot change this option after the NFS export is created.
Early Eviction	Select yes or no from the drop-down list to specify whether or not data from this share should be assigned a higher priority for eviction. If you select yes, data written to this share is eligible for eviction earlier than other data. If you select no, data written to this share is evicted using the default method.
Disable Dedupe	Select yes or no from the drop-down list to specify whether or not data written to this share should be checked for duplication. If you select no, then the AltaVault checks if there is duplication of the data written to the share, and deduplicates the data. If you select yes, then the AltaVault does not check if there is duplication of the data written to the share and does not does perform deduplication.

Control	Description
Disable Compression	Select yes or no from the drop-down list to specify whether or not data from this share should be checked for compression. Select yes if your data set is already in a precompressed format. Select no if you data set is not precompressed.
Local Path	Specify the export file pathname. It starts with a forward slash (/).
Comment	Specify a comment about the NFS share. You use only alphanumeric, underscore (_), hyphen (-) characters and space in this field.
Export Asynchronously	Select the check box to export the NFS share asynchronously. Click the icon i for the following information: Exporting NFS asynchronously forces the server to drop all fsync requests from the client. This is a feature of the NFS protocol. It is required to obtain good performance with NFS clients that issue frequent NFS COMMIT operations, which might degrade the AltaVault performance significantly. Many UNIX clients often execute NFS COMMIT operations when low on memory. To understand the circumstances that cause this behavior and to detect and prevent it, contact your client operating system vendor. The AltaVault automatically synchronizes any file that is idle for a configurable amount of time. The default value is 10 seconds. Although there is a window of time (after the server responds with success for an fsync request, and before the data is written to disk), this window is small and performance benefits are large. NetApp recommends exporting NFS asynchronously.
Allow Specified Clients	Enables only the clients that you specify to connect to the AltaVault to access the NFS share. If you select this option, you must specify the client's IP address and subnet mask in the text field below it. To enable all clients to access the NFS share, specify 0.0.0.0/0 in the Client IP/Network field IP/Network field. This is the default.
Allow All Clients	Enables all clients connected to the AltaVault system to access the NFS share. When selected, the following warning displays: WARNING: Enabling all clients to access the NFS share is not recommended.
Add	Adds the export path and client IP address to the AltaVault NFS server.
Remove Selected	Select the check box next to the name and click **Remove Selected**.

The share you configure and its parameters appear in the list of shares on the page.

5. Click **Add** to apply your changes to the running configuration.

Editing an NFS configuration

You can edit and change most of the parameters of an exported NFS share.

To edit an existing configuration

1. Choose Configure > NFS and click the share name at the bottom of the page.

2. Select the NFS share name, and complete the configuration as described in this table.

Control	Description
Edit Export	Select this tab to edit the NFS share.
Local Path	Change the export file pathname, which starts with a forward slash (/).
Comment	Specify or change the comment about the NFS share.

Control	Description
Export as NFSv4	Select yes or no from the drop-down list to specify the type of NFS export. If you select yes, the export will be configured as NFSv4 export. If you select no, the export will be configured as NFSv3 export.
Kerberos Authentication	Select yes or no from the drop-down list to specify whether or not the export has to be configured with Kerberos authentication. If you select yes, the export will have to be accessed with Kerberos credentials. If you select no, the export will not be configured with Kerberos.
Pinned	Select yes or no from the drop-down list to specify whether or not the data from this share should never be evicted. If you select yes, data written to this share will not be eligible for eviction. If you select no, normal data written to this share is evicted using the default method.
Early Eviction	Select yes or no from the drop-down list to specify whether or not data from this share should be assigned a higher priority for eviction. If you select yes, data written to this share is eligible for eviction earlier than other data. If you select no, data written to this share is evicted using the default method.
Disable Dedupe	Select yes or no from the drop-down list to specify whether or not data written to this share should be checked for duplication. If you select no, then the AltaVault checks if there is duplication of the data written to the share, and deduplicates the data. If you select yes, then the AltaVault does not check if there is duplication of the data written to the share and does not does perform deduplication.
Disable Compression	Select yes or no from the drop-down list to specify whether or not data from this share should be checked for compression. Select yes if your data set is already in a precompressed format. Select no if you data set is not precompressed.
Export Asynchronously	Select the check box to export the NFS share asynchronously. Click the icon i for the following information: Exporting NFS asynchronously forces the server to drop all fsync requests from the client. This is a feature of the NFS protocol. It is required to obtain good performance with NFS clients that issue frequent NFS COMMIT operations, which might degrade the AltaVault performance significantly. Many UNIX clients often execute NFS COMMIT operations when low on memory. To understand the circumstances that cause this behavior and to detect and prevent it, contact your client operating system vendor. The AltaVault automatically synchronizes any file that is idle for a configurable amount of time. The default value is 10 seconds. Although there is a window of time (after the server responds with success for an fsync request and before the data is written to disk), this window is small and performance benefits are large. NetApp recommends exporting NFS asynchronously.
Allow All Clients	Enables all clients connected to the AltaVault system to access the NFS share.
Allow Specified Clients	Enables only the clients that you specify to connect to the AltaVault system to access the NFS share. If you select this option, you must specify the client's IP address and subnet mask in the Client IP/Network text field below it. To enable all clients to access the NFS share, specify 0.0.0.0/0 in the Client IP/Network field.
Mount Commands	Select this tab to display the Linux and UNIX NFS mount commands. You configure the mount commands through the command-line. These commands are for your reference. If the AltaVault is a secondary appliance, the mount commands enable only read permissions and not write permissions.

3. Click **Apply** to apply your changes to the running configuration.

Troubleshooting NFS exports to AIX

If an AIX command using an AltaVault export fails, you may need to issue the following command:

```
nfso -p -o nfs_use_reserved_ports=1
```

Configuring OST

OpenStorage (OST) is a proprietary protocol created by Veritas for ingesting backup data streams to (third-party) disk-like storage devices. It can be treated as a customized NFS- or SMB-like protocol but optimized for backup application ingest workflows. In addition, it provides advanced features that are not possible when ingesting to an appliance over an NFS or SMB share. Typically, OST is implemented as a plug-in (shared object/DLL) running in NetBackup media server process address space and streaming data to the OST server running on the AltaVault.

You can perform the following tasks:

- "To configure OST share" on page 60
- "To add OST user to access the share" on page 61
- "To edit OST user" on page 61

To configure OST share

1. The OST page does not appear until the storage optimization service is started. If needed, choose Maintenance > Service and click Start to initialize the service

2. Optionally, under Pinned Data Information, slide the thermometer to select the maximum bytes allowed for share pinning. Share pinning enables the share to always contain data that is available to the AltaVault locally, without fetching it from the cloud.

3. Click **Apply** to apply your changes.

4. To add an OST share, click **Add OST Share**, and complete the configuration as described in this table.

Control	Description
Share Name	Specify the name of the share to be added.
Type	Select regular or cloud. Regular shares treat incoming data by AltaVault the same as traditional SMB shares or NFS exports by writing the data on cache, and replicating the data to the cloud. Cloud shares are used to create an optimized duplicate of data in regular shares replicated in the cloud that are managed via NetBackup storage lifecycle policies (SLP).
Pin Share	Select yes or no from the drop-down list to specify whether or not the OST share should be pinned. Share pinning enables the share to always contain data that is available to the AltaVault locally, without fetching it from the cloud. You cannot remove a pinned share if it contains data. Once a share is pinned, unpinning of that share can be performed via CLI and requires optimization service to be offline. Unpinning a share can be a time-consuming operation. Unpinning a share does not result in erasing the previously pinned data. Only the previously pinned data is available for eviction, if applicable becomes full.

Control	Description
Early Eviction	Select yes or no from the drop-down list to specify whether or not data from this share should be assigned a higher priority for eviction. If you select yes, data written to this share is eligible for eviction earlier than other data. If you select no, data written to this share is evicted using the default method.
Disable Dedupe	Select yes or no from the drop-down list to specify whether or not data written to this share should be checked for duplication. If you select no, then the AltaVault checks if there is duplication of the data written to the share, and deduplicates the data. If you select yes, then the AltaVault does not check if there is duplication of the data written to the share and does not does perform deduplication.
Disable Compression	Select yes or no from the drop-down list to specify whether or not data from this share should be checked for compression. Select yes if your data set is already in a precompressed format. Select no if you data set is not precompressed.
Add Share	Adds the OST share to the AltaVault.

5. Optionally, to remove an OST share, select the OST share from the table and click **Remove Selected**

6. Optionally, to enable SSL communication between the AltaVault OST Plug-in and the AltaVault, select the checkbox, **Enable SSL,** in the Global OST Settings section, and click **Apply**. AltaVault will receive secure connections from the AltaVault OST Plug-in using secure port 8085.

To add OST user to access the share

1. To add a user to access the share that you created, select the share and complete the configuration as described in the following table.

Note: OST shares must have an associated user to be used by NetBackup storage server. Multiple users per OST share are allowed.

Control	Description
Add OST User	Displays the controls to add a user to the OST share.
User Name	Type the user name that you would use for authenticating the share from NetBackup.
Password	Choose an appropriate strength password for authentication.
Password confirm	Retype the password.
Add User	Adds the OST user.

To edit OST user

1. Extend the user name to complete the configuration as described in this table.

Control	Description
Change Password	Select the check box to change the password.
Password	Specify the new password for the user.
Password Confirm	Confirm the new password of the user.

Control	Description
Account	Select one of the following options from the drop-down list: • Enabled - Enables local user account for accessing OST share • Disabled - Disables local user account from accessing OST share
Apply	Applies the changes to the OST share users.

Restoring data from the cloud using the prepopulation page

Use the prepopulation feature to restore data from the cloud to the AltaVault cache in batch mode. If an application accesses the data after you restore it, there is no WAN latency because the data is already in the AltaVault cache.

The Prepopulation page displays the status of the prepopulation tasks that were started using the Management Console or the command-line interface. For each task, you can also view the list of files that are being restored by the task. The prepopulation page provides a granular status of all prepopulation requests.

To restore data from the cloud using the prepopulation page

1. Ensure that you have permissions to use the prepopulation feature in the AltaVault. Only users with specific Prepopulation Settings permissions can use the prepopulation feature.

2. Choose Configure > Prepopulation.

3. Click the **Select File** tab to display the Prepopulation File Browser that contains a list of files that can be prepopulated.

   The Prepopulation File Browser enables you to browse the files on the AltaVault shares. For each file, it displays the file size, modification time (appears when you hover the cursor over a specific file), and its estimated size on disk.

   Select a file or a list of files, and click **Fetch Percent Locally Cached for selected files** to obtain the locally cached percent in the AltaVault cache. This process might be slow for large files.

   -or-

   Optionally, specify a list of complete path names, separated by the pipe (|) character, to the files that you want in the List of files to be prepopulated. Refer to the following examples:

   To prepopulate the file /nfs/dir_1/dir_2/test-2.txt, enter the following path name:

   /nfs/dir_1/dir_2/test-2.slab

   To prepopulate the files /nfs/dir_1/test-1.txt and /nfsv4/dir_1/dir_2/test-2.txt, enter the following path names:

   /nfs/dir_1/test-1.slab|/nfsv4/dir_1/dir_2/test-2.slab

   To prepopulate all the files under /nfs, enter the following path name:

   /nfs/*

   To prepopulate the files /smb/app_1/test_file.txt and /smb/app_2/test_file.txt, enter the following path names:

   /smb/app_1/test_file.txt|/smb/app_2/test_file.txt

   To prepopulate all the files under /smb/app_1/, enter the following path name:

   /smb/app_1/*

4. Select the check box next to the file (displayed in the list) name you want to prepopulate.

5. Click **Prepopulate Selected Files** to prepopulate the files that you selected and display the Prepopulation Report Status page.

   The Prepopulation Report Status page displays the status of the prepopulation task. The various states are:

Status	Description
Enqueued	The prepopulation task is just recorded. The AltaVault has not started processing it. You do not usually see this status (unless there are a large number of prepopulation tasks) because the prepopulation process is very fast and it quickly moves to the next step in the process.
Processing	The AltaVault is identifying data that must be restored from the cloud.
Requested	The system has requested all of the data required for the prepopulation request from the cloud.
Downloading	The system has started downloading the data for the prepopulation request. When the cloud provider is Amazon Glacier, it usually takes about five hours for this state to appear.
Completed	This state indicates that the prepopulation task is complete. The completion time also appears in a separate column.
Failed	This state indicates that the AltaVault did not restore all of the data and the prepopulation task failed. View the logs to determine the reason for failure.
Canceled	Cancels the process.

After a prepopulation job is complete, the system sends an email notification to the email recipients configured to receive email notifications.

If the prepopulation job is successful, the email notification contains the following information:

```
For a successful prepop:
Subject: Prepopulation Job Completed
Body: Prepopulation job #[job id] has completed successfully.
```

If the prepopulation job fails, the email notification contains the following information:

```
Subject: Prepopulation Job Failed
Body: Prepopulation job #[job id] has failed. Please check the system log for more information.
```

6. To add users who should receive email notifications, choose Configure > Email.

Viewing offline file system check page

The Offline File System Check page checks the integrity of the local file system and provides the diagnosis. You cannot run the Offline File System Check if the storage optimization service is running. Before you perform the Offline File System Check, choose Maintenance > Service and click **Stop** to stop the storage optimization service.

To view the offline file system check page

1. Choose Maintenance > Offline File System Check.

2. Click the filename to open an Offline File System Check log file or save the file to disk.

3. To remove an entry, select the box next to the name and click **Remove Selected**.

4. Under Offline File System Check Actions, complete the configuration as described in this table.

Control	Description
Status	Displays the status of the Offline File System Check report such as, running or not running.
Check type	Select the type of diagnosis from the drop-down list: • Internal Data Consistency - Checks only the internal consistency of the data. This is the fast mode. • Complete - Checks the data completely from end to end. This is the slow mode.
Repair errors	Click this option to repair errors from which the system can recover.
Replay log after a crash	Click this option to replay log after a crash.
Start Mfsck	Starts the Offline File System Check tool.
Stop Mfsck	Stops the Offline File System Check tool.

5. Open and check the Offline File System Check log file that you downloaded. If your configuration is accurate, under File verification summary, it displays File check result: Volume consistent and under Label verification summary, it displays Label check result: Volume consistent. Otherwise, the log file displays an error message.

Viewing online file system check page

The Online File System Check is a file system check that the AltaVault performs online as it writes data to the cloud, it checks the data. The Online File System Check report displays the log files that contain the integrity check data, the date and time up to which AltaVault performed the integrity check, and the file size.

You can perform the Online File System Check only if the storage optimization service is running. You can stop the check at any time, but NetApp recommends that you keep it running.

Field	Description
Download Link	Displays a link that you can click to download a specific log file.
Integrity Check done up to	Displays the date and time up to which the AltaVault has performed the Online File System Check.
Size	Displays the size of the log file.

To view the Online File System Check page

1. Choose Maintenance > Online File System Check.

2. Under Online File System Check Actions, click **Start Data Integrity Check** to start the data integrity check as the AltaVault writes data to the cloud.

   -or-

   Click **Stop Data Integrity Check** to stop the check.

3. Optionally, selected the check box next to the link and click **Remove Selected**.

Viewing the verify tool diagnostics

The Verify page provides the diagnosis of the Verify tool. Verify is a tool for checking cloud replication consistency. Start the Verify operation only after all pending replication has completed successfully and the value of Replication Bytes Pending is zero.

You cannot run the Verify tool if the storage optimization service is running.

To view the Verify tool diagnostics

1. Choose Maintenance > Replication Verify Check.
2. Click the filename to open a Verify log file or save the file to disk.
3. To remove an entry, select the box next to the name and click **Remove Selected**.
4. Under Actions, complete the configuration as described in this table.

Control	Description
Status	Displays the status of the Offline File System Check report, such as running or not running.
Only validate checksums	Click this option to verify only the checksums (a computed value that enables you to check the validity of data).
Start	Starts the Verify tool.
Stop	Stops the Verify tool.

5. Open and check the Verify log file. If all data in the local disk is replicated in the cloud, the file displays the following result:

   ```
   Verification complete: collection is properly replicated.
   ```

   Otherwise, the log file displays an error message.

   Optionally, select the check box next to the link and click **Remove Selected**.

CHAPTER 4 Modifying networking settings

You initially set these properties when you ran the AltaVault installation wizard (CLI or GUI). This section describes how you can view and modify these settings, if needed. It includes the following sections:

- "Modifying general host settings" on page 67
- "Modifying management interfaces" on page 69
- "Modifying data interfaces" on page 71
- "Modifying virtual interfaces" on page 73
- "Modifying VLANs" on page 73

Modifying general host settings

You can view and modify general host settings in the Configure > Host Settings page.

When you initially ran the installation wizard, you set required network host settings for the AltaVault. Use the following groups of controls on this page only if modifications or additional configuration is required:

- Name - Modify the hostname only if your deployment requires it.
- DNS Settings - NetApp recommends that you use DNS resolution.
- Hosts - If you do not use DNS resolution, or if the host does not have a DNS entry, you can create a host-IP address resolution map.
- Web/FTP Proxy - Configure proxy addresses for Web or FTP proxy access to the AltaVault. The proxy settings do not affect cloud connections originating from the AltaVault.

To view general host settings

- Choose Configure > Host Settings.

To change the hostname

1. Choose Configure > Host Settings.
2. Under Name, modify the value in the Hostname field.
3. Click **Apply** to apply your changes to the running configuration.

4. Click **Save** to save your settings permanently.

To specify DNS settings

Before joining a domain name, verify that you can ping the domain name.

1. Choose Configure > Host Settings.

2. Under DNS Settings, complete the configuration as described in this table.

Control	Description
Primary DNS Server	Specify the IP address for the primary name server.
Secondary DNS Server	Optionally, specify the IP address for the secondary name server.
Tertiary DNS Server	Optionally, specify the IP address for the tertiary name server.
DNS Domain List	Specify an ordered list of domain names. If you specify domains, the system automatically finds the appropriate domain for each of the hosts that you specify in the system.

3. Click **Apply** to apply your changes to the running configuration.

4. Click **Save** to save your settings permanently.

To add a new host

1. Choose Configure > Host Settings.

2. Under Hosts, complete the configuration as described in this table.

Control	Description
Add a New Host	Displays the controls for adding a new host.
IP Address	Specify the IP address for the host.
Hostname	Specify a hostname.
Add	Adds the host.
Remove Selected	Select the check box next to the name and click **Remove Selected**.

3. Click **Apply** to apply your changes to the running configuration.

4. Click **Save** to save your settings permanently.

To set a Web/FTP proxy

1. Choose Configure > Host Settings.

2. Under Web/FTP Proxy, complete the configuration as described in this table.

Control	Description
Enable Web Proxy	Enables the appliance to use a Web proxy to contact the NetApp licensing portal and fetch licenses in a secure environment. You can optionally require user credentials to communicate with the proxy, and you can specify the method used to authenticate and negotiate user credentials. Web proxy access is disabled by default.
Web/FTP Proxy	Specify the IP address for the Web or FTP proxy.
Port	Optionally, specify the port for the Web or FTP proxy. The default port is 1080.
Enable Authentication	Optionally, select to require user credentials for use with Web or FTP proxy traffic. Specify the following settings to authenticate the users: • User Name - Specify a username. • Password - Specify a password. • Authentication Type - Select an authentication method from the drop-down list: – Basic - Authenticates user credentials by requesting a valid username and password. This is the default setting. – NTLM - Authenticates user credentials based on an authentication challenge and response. – Digest - Provides the same functionality as Basic authentication; however, Digest authentication improves security because the system sends the user credentials across the network as a Message Digest 5 (MD5) hash.

3. Click **Apply** to apply your changes to the running configuration.

4. Click **Save** to save your settings permanently.

   The proxy settings do not affect cloud connections originating from the AltaVault.

Modifying management interfaces

You can view and modify settings for the appliance interfaces in the Management Interfaces page.

When you initially ran the installation wizard, you set required settings for the management interfaces for the AltaVault. Use the following groups of controls on this page only if you require modifications or additional configuration:

- Primary Interface - On the appliance, the primary interface is the port you use for replication traffic. This is default port used for replication.
- Main IPv4 Routing Table - Displays a summary of the main routing table for the appliance. If necessary, you can add static routes that might be required for some device management subnets.

To display and modify the configuration for management interfaces

1. Choose Configure > Management Interfaces.

2. Under Primary Interface, complete the configuration as described in this table.

Control	Description
Enable Primary Interface	Enables a primary interface for the AltaVault. NetApp recommends that you use the primary interface for replication traffic. However, if only one interface (the primary, by default) is set up, then the same interface is used for both replication traffic and appliance management.
Obtain IPv4 Address Automatically	Specify this option to automatically obtain the IPv4 address from a DHCP server. A DHCP server must be available so that the system can request the IP address from it. • Enable IPv4 Dynamic DNS - Select this option to enable IPv4 dynamic DNS on the primary interface. Dynamic DNS is a method, protocol, or network service that enables a network device, such as a router or computer system using the Internet Protocol Suite, to notify a Domain Name System (DNS) name server to change, in real time, the active DNS configuration of its configured hostnames, addresses, or other information.
Specify IPv4 Address Manually	Specify this option if you do not use a DHCP server to set the IP address. Specify the following settings: • IPv4 Address - Specify an IPv4 address. • IPv4 Subnet Mask - Specify an IPv4 subnet mask. • Default IPv4 Gateway - Specify the default primary gateway IPv4 address. The primary gateway must be in the same network as the primary interface. You must set the primary gateway for interface configurations.
MTU	Specify the Maximum Transmission Unit (MTU) value. The MTU is the largest physical packet size, measured in bytes, that a network can send. The default value is 1500.

3. Click **Apply** to apply your changes to the running configuration.

4. Click **Save** to save your changes permanently.

To modify main IPv4 routing table

1. Choose Configure > Management Interfaces.

2. Under Main IPv4 Routing Table, complete the configuration as described in following table.

Control	Description
Add a New Route	Displays the controls for adding a new route.
Destination IPv4 Address	Specify the destination IPv4 address for the appliance.
IPv4 Subnet Mask	Specify the IPv4 subnet mask.
Gateway IPv4 Address	Specify the IPv4 address for the gateway. The gateway must be in the same network as the primary you are configuring.
Interface	Select the interface from the drop-down list.
Add	Adds the route to the table list.
Remove Selected	Select the check box next to the name and click **Remove Selected**.

3. Click **Apply**.

The Management Console writes your configuration changes to memory.

You can verify whether changes have had the desired effect by reviewing related reports. When you have verified appropriate changes, you can write the active configuration that is stored in memory to the active configuration file (or you can save it as any filename you choose).

Modifying data interfaces

You can view and modify settings for the data interfaces in the Configure > Data Interfaces page.

To display and modify the configuration for data interfaces

1. Choose Configure > Data Interfaces.

2. Under Physical Interface, click the arrow next to the name of the interface and complete the configuration as described in this table.

Control	Description
Enable Data Interface	Select the check box to enable the data interface and specify the following settings: • IPv4 Address - Specify an IPv4 address. • IPv4 Subnet Mask - Specify a subnet mask. • IPv4 Gateway - Specify the data gateway IP address. The data gateway must be in the same network as the data interface. • MTU - Specify the MTU value. The MTU is the largest physical packet size, measured in bytes, that a network can send. The default value is 1500.

If an interface is a member of a virtual interface, you can only enable it by editing the virtual interface.

3. Under Routing Table for <physical interface>, you can configure a static routing in the routing table if your device management network requires static routes.

   You can add or remove routes from the table as described in following table.

Control	Description
Add a New Route	Displays the controls for adding a new route.
Destination IP Address	Specify the destination IP address for the appliance.
Subnet Mask	Specify the subnet mask.
Gateway IP Address	Specify the IP address for the gateway. The gateway must be in the same network as the network interface you are configuring.
Add	Adds the route to the table list.
Remove Selected	Select the check box next to the name and click **Remove Selected**.

4. Under Virtual Interface, you can configure the IP address for the virtual interface created from the Configure > VIFs page. You can enable and configure the VIF networking configuration as described in this table.

Control	Description
Virtual Interface	Displays the controls to add a virtual network interface. Click the magnifying glass icon next to an interface to display the controls to configure the interface.
IP Configuration	Displays the IP address of the network interface.
Enabled	Displays if it is enabled.
Members	Specify a comma-separated list of the data interfaces that are members of this VIF.
Status	Displays the status.
Enable Data Interface	Select this check box to enable the data interface and specify the following settings: • IPv4 Address - Specify an IPv4 address. • IPv4 Subnet Mask - Specify a subnet mask. • MTU - Specify the MTU value. The MTU is the largest physical packet size, measured in bytes, that a network can send. The default value is 1500.

5. Under VLAN Interface, click the arrow next to the name of the interface and complete the configuration as described in this table.

Control	Description
Enable Interface	Select the check box to enable the data interface and specify the following settings: • IPv4 Address - Specify an IPv4 address. • IPv4 Subnet Mask - Specify a subnet mask. • IPv4 Gateway - Specify the data gateway IP address. The data gateway must be in the same network as the data interface. • MTU - Specify the MTU value. The MTU is the largest physical packet size, measured in bytes, that a network can send. The default value is 1500.

If an interface is a member of a virtual interface, you can only enable it by editing the virtual interface.

6. Under Routing Table for <VLAN interface>, you can configure a static routing in the routing table if your device management network requires static routes.

   You can add or remove routes from the table as described in following table.

Control	Description
Add a New Route	Displays the controls for adding a new route.
Destination IP Address	Specify the destination IP address for the appliance.
Subnet Mask	Specify the subnet mask.
Gateway IP Address	Specify the IP address for the gateway. The gateway must be in the same network as the network interface you are configuring.
Add	Adds the route to the table list.
Remove Selected	Select the check box next to the name and click **Remove Selected**.

7. Click **Apply** to apply your changes to the running configuration.

8. Click **Save** to save your changes permanently.

Modifying virtual interfaces

You can view, add and modify virtual interfaces (VIFS) in the Configure > VIFs page. VIF is a logical bonded interface created by aggregating multiple physical interfaces. Just like a physical Ethernet interface, you can assign an IP address to each VIF.

To display, add, and modify the VIF configuration

1. Choose Configure > VIFs.

2. Click Add a Virtual Interface and complete the configuration as described in this table.

Control	Description
Enable VIF	Enables VIF feature.
Virtual Interface Name	Specify a name for the virtual interface.
Member Interfaces	Specify a comma-separated list of the data interfaces that are members of this VIF.
Mode	Select one of the following modes: • **802.3ad** - Enables IEEE 802.3ad Dynamic Link Aggregation. This mode enables you to bundle or aggregate multiple physical interfaces into a single VIF and enables load balancing between the interfaces. It conforms to clause 43 of IEEE 802.3 standard (802.3ad). Most switches require some type of configuration to enable the 802.3ad mode. • **Transmit/Receive Load Balance** - Provides both transmit and receive load balancing. You can use this mode to deploy VIFs for both HA and load balancing. • **Transmit Load Balance** - Provides adaptive-transmit load balancing. The AltaVault distributes the outgoing traffic based on the current load on each member interface. One of the member interfaces of the VIF receives the incoming traffic.
Monitoring interval	Specifies the Media Independent Interface (MII) link monitoring frequency in milliseconds. This determines how often the link state of each slave is inspected for link failures. A value of zero disables MII link monitoring. A value of 50 is a good starting point.
Add	Adds the VIF to your configuration.
Remove Selected	Select the check box next to the existing VIF to remove, and click Remove Selected.

Modifying VLANs

You can view, add and modify VLANs in the VLANs page. VLAN tagging enables AltaVault to direct network packets to specific virtual local area networks (VLANs) in order to segment data traffic.

To display, add, or modify a VLAN configuration

1. Stop the storage optimization service before adding or removing a VLAN. If needed, choose Maintenance > Service and click **Stop** to terminate the service.

2. Choose Configure > VLANs.

3. Click Add a VLAN Interface and complete the configuration as described in this table.

Control	Description
VLAN ID	Specify the VLAN tag identifier. This can be a number from 2 to 4094.
Interface Type	Select from Data Interface or Virtual Interface (VIF).
Data Interfaces	Select from the drop-down list.
VIFs	Select from the drop-down list.
Add	Adds the VLAN interface to your configuration.
Remove Selected	Select the check box next to the name and click **Remove Selected**. **Note:** A restart of the AltaVault is required before performing any further networking changes.

CHAPTER 5 Managing the AltaVault appliance

This section describes tasks you perform for routine management of the AltaVault appliance. It includes the following sections:

- "Starting and stopping the AltaVault appliance" on page 75
- "Configuring scheduled jobs" on page 76
- "Managing licenses" on page 77
- "Upgrading your software" on page 80
- "Rebooting and shutting down AltaVault appliance" on page 82
- "Viewing the current user settings" on page 82
- "Managing configuration files" on page 83

Starting and stopping the AltaVault appliance

You can start, stop, and restart AltaVault storage optimization service in the Maintenance > Service page. You can also use this page to reset the service alarm after it has been triggered.

The AltaVault storage optimization service is a daemon that executes in the background, performing operations when required.

Restarting AltaVault service disrupts front-end sessions (such as SMB, NFS, and OST) established with the AltaVault. This has the following impact:

- All shares (SMB, NFS, and OST) will go down, and cloud connections will fail until the service initializes again.
- Active backup jobs will fail and will need to be restarted after AltaVault storage optimization service is running again.

To start, stop, or restart the storage optimization service

1. Choose Maintenance > Service.
2. Click **Stop**, **Start**, or **Restart**.

If Status displays Replaying, the storage optimization service has been terminated during backup replication, either due to loss of power or a crash. During this replay process, the AltaVault is verifying data consistency from its transaction logs and, if needed, restoring data slabs (file chunks and references) from the cloud to the local AltaVault. This might take a long time, depending on your WAN bandwidth and disk size.

If the replay process is very slow or seems to be stuck, contact NetApp Support at https://mysupport.netapp.com.

3. To verify that the service is running again, go to Home > Optimization Service. You should see that Service is running and Status is ready.

   To check the service status from the command line interface, run the `show service` command. When Storage Optimization Service shows ready, the service is running.

Configuring scheduled jobs

You can view completed, pending, and inactive jobs, as well as jobs that were not completed because of an error, in the Scheduled Jobs page. You can also delete a job, change its status, or modify its properties.

Jobs are commands that are scheduled to execute at a time you specify.

You can use the Management Console to:

- schedule a software upgrade.
- generate multiple TCP trace dumps on a specific date and time.

To schedule all other jobs, you must use the NetApp CLI.

For details about scheduling jobs using the CLI, see the *NetApp AltaVault Cloud Integrated Storage Command-Line Reference Guide*.

To view scheduled jobs

1. Choose Reports > View Scheduled Jobs.

2. Click the Job ID number to display details about the job.

3. Under Details for Job <#>, complete the configuration as described in this table.

Control	Description
ID	Specify the job ID number.
Name	Specify a name for the job.
Comment	Specify a comment.
Interval	For recurring jobs, specify the interval in seconds
Executes On	Specify the date on which the job runs.
Created	Specify the date and time at which the job was created.
Last Run	Specify the last date and time at which the job was run.
Enable/Disable Job	Enables the job.
Apply Changes	Applies the changes to the current configuration.
Cancel This Job	Cancels the job.
Execute Now	Runs the job.
Remove Selected Jobs	Select the check box next to the name and click **Remove Selected Jobs**.

4. Click **Save** to save your settings permanently.

Managing licenses

You can configure your license on the Licenses page.

There are four types of license keys, one for each capacity (AVA-v2, AVA-v8, AVA-v16, AVA-v32). License keys are required only for the AltaVault-v models. RAM, disk, and cloud capacity enforcement is based on license capacity.

Note: You can install only one license key at a time.

To add or remove a license requires the optimization service to be shutdown. This enables the optimization service to perform capacity and usage checks at the time of starting up. Choose Maintenance > Service to shut down the service.

If an attempt is made to configure license while service is running the following message will appear in the CLI:

```
Cannot configure license while optimization service is running
```

Manging licenses includes the following sections:

- “Managing POC licenses” on page 78
- “Managing licenses using the command-line” on page 78
- “Adding a new license using management console” on page 78
- “90-day evaluation period” on page 79
- “AltaVault-v licenses” on page 79
- “Specifying license limits” on page 79

- "Model upgrades on the virtual AltaVault appliances" on page 80

Managing POC licenses

When upgrading an AltaVault 4.1 or earlier model that is not licensed (proof-of-concept [POC] or trial model) to version 4.2 or higher, the model will be reset to AVA-v2 from whichever cache configuration it previously had. Service will not start but there is no data loss either. To change the model back to its previous configuration, use the following CLI command (AVA-v8 is used as an example):

```
CLI (config)> license virtual-model v8
```

Reboot the appliance for changes to take effect:

```
CLI (config)>reload
```

Managing licenses using the command-line

You can install, delete, or view an existing licenses using the command-line.

To install a license

- Use the following command to install a license:

  ```
  CLI> license install <license-key>
  ```

  If a license already exists, the `license install <license-key>` command fails and it warns the user of any unintended license installs of a lower capacity.

To delete a license

- Use the following command to delete a license that already exists:

  ```
  CLI> no license install <license-key>
  ```

  This enable users to switch a license that is already installed on a system with a different capacity.

To view existing licenses

- Use the following command to view existing licenses:

  ```
  CLI> show licenses
  Key: <license-key>
  Capacity: <capacity in TB>
  Version: <software version>
  Type: Capacity"
  Installation: <date/time>
  Expiration: <date>
  ```

  This command does not require the optimization service to be shutdown.

  If there is no license, the following command displays:

  ```
  No license found
  ```

Adding a new license using management console

You can add a new license using the Management Console.

To add a new license using the Management Console

1. Choose Maintenance > Licenses.
2. Select Add a New License.
3. Enter or paste the licenses into the text box, and click **Add**.
4. Click **Save**.

90-day evaluation period

When a virtual machine is brought up for the first time, it enters a 90-day evaluation period. During this evaluation period, the full functionality of the product is available without a license requirement, with full capacity as supported by the model. Once the 90-day evaluation expires, the virtual machine will only allow read-only access to the data ingested into the appliance. The virtual machine cannot ingest new data. Once a valid license is installed, the full functionality of the virtual machine returns, with capacity as enforced by the installed license.

When a valid license is installed on the virtual machine, then the virtual machine permanently exits out of evaluation mode, and cannot be returned to evaluation mode at any future point.

AltaVault-v licenses

The AltaVault-v is packaged into a deployment file available on the NetApp Support site at https://mysupport.netapp.com. You can download it for free, try it, and then choose to purchase a license for it. For details about the file and installing the AltaVault-v, see *NetApp AltaVault Cloud Integrated Storage Installation and Service Guide for Virtual Appliances*.

The following applies to AltaVault virtual licensing:

- AltaVault-v has a 90 day free evaluation period.
- A license key has to be installed to use the appliance past the 90 day evaluation period.
- The license key enforces the memory and maximum disk space that can be allocated to the AltaVault-v appliance as well as the amount of cloud storage which can be used by the appliance.
- License keys for AltaVault-v provide three capacity options: 2TB, 8TB, 16TB and 32TB.

Specifying license limits

The AltaVault license limit controls the amount of data you can back up to the cloud from the AltaVault. The license limit varies for each AltaVault model. For details, see the *NetApp AltaVault Cloud Integrated Storage Installation and Service Guide for Virtual Appliances.*

The AltaVault lets you exceed the license limit by 10 percent before triggering the over_capacity alarm. When you exceed 110 percent of the limit, the AltaVault pauses all replication activity and does not upload any additional data to the cloud until you increase the licensed capacity or reclaim the space by deleting files.

Restore operations are not affected by the over_capacity alarm and all files, whether stored locally or in the cloud, remain available through the SMB, NFS, or OST share(s). Any new files written to the AltaVault are queued pending replication to the cloud during the over_capacity alarm.

The over_capacity alarm is triggered when the total data in the cloud is under the license limit, but the data pending replication to the cloud pushes the total over the limit. You can find the pending data to be replicated in the Replication Optimization report by choosing Reports > Replication.

Model upgrades on the virtual AltaVault appliances

The following applies when you are upgrading on the virtual AltaVault appliances:

- The default model is AVA-v2 when virtual AltaVault appliance is deployed.
- A model can be upgraded by installing new license key.
- License keys can be installed using the CLI command "license install <license-key>"
- License keys can be removed using the CLI command "no license install <license-key>"
- Only one license key can be present on the appliance at any time.
- Must reboot appliance after provisioning more RAM and disk.
- In evaluation mode, a model can be upgraded using "license virtual-model <model-name>" CLI command, where the model-name is one of the following: AVA-v2, AVA-v8, AVA-v16, or AVA-v32.
- The appliance needs to be rebooted after running the "license virtual-model" command for the changes to take effect.
- Model downgrade is not supported for the virtual AltaVault appliances.

For details, see the *NetApp AltaVault Cloud Integrated Storage Installation and Service Guide for Virtual Appliances*.

Upgrading your software

You can upgrade your AltaVault software in the Maintenance > Software Upgrade page.

Note: To migrate from an AltaVault 3.x physical or virtual appliance to an AltaVault 4.x physical appliance, see "Migrating data from a SteelStore appliance to an AltaVault appliance" on page 179. To migrate from an AltaVault 3.x virtual appliance to an AltaVault 4.x virtual appliance refer to Appendix A of the *NetApp AltaVault Installation and Service Guide for Virtual Appliances*.

The bottom of the page displays the AltaVault software version history, which includes the version number and the software installation date.

Review the following installation notes before proceeding with the upgrade:

- AltaVault software upgrades cannot be reversed once applied. In addition, downgrades to previous AltaVault software versions are not supported.
- AltaVault 4.2 and later releases do not support hidden SMB shares. During the upgrade, hidden shares are converted to regular shares, and share permissions are truncated to either read, write, or modify. The shares will be visible in the management console, and they will be available to users provided they have permissions.
- AltaVault 4.2 and later releases do not support guest access to the SMB shares. If prior to the upgrade, guest access was used for the SMB shares, the same should be replaced by a local user or a domain user. See "Configuring SMB" on page 52. If local user is used, the same user credentials need to be provisioned on both the client and AltaVault.
- If you are planning to upgrade from AltaVault 4.2, 4.2P, or 4.2D to AltaVault 4.2.1 or later, and this AltaVault appliance configuration was imported from a different AltaVault appliance that was upgraded from AltaVault 4.0x or 4.1x, you must manually set the domain user permissions on the shares. Contact technical support for assistance.

To upgrade software versions

1. Choose Maintenance > Software Upgrade.
2. Under Install Upgrade, complete the configuration as described in this table.

Control	Description
From URL	Select this option and type the URL. If you specify a URL in the URL text box, the image is uploaded and installed and the system is rebooted at the time you specify. Use the image.img file for upgrades, found on the NetApp support site.
From Local File	Select this option and type the path, or click **Browse** to go to the local file directory. If you specify a file to upload in the From Local File text box, the image is uploaded immediately; however, the image is installed and the system is rebooted at the time you specify.
Schedule Upgrade for Later	Schedules the upgrade process. Specify the date and time to run the upgrade: • Date and Time - Use the following format: YYYY/MM/DD, HH:MM:SS.
Install	Installs the software upgrade on your system.

3. Choose Maintenance > Reboot/Shutdown, and click Reboot.
4. If you do not use SMB, stop here. The upgrade is complete.
5. If you use SMB, check if you must manually migrate share-level access control lists (ACLs). Use SSH to log in to the AltaVault and check the migration status:

   ```
   CLI (config)# show smb migrate domain-acls status
   ```

   Based on the migration status message, take the appropriate action:

If the migration status is...	Take the following action...
• Migration not required • Auto migration completed • Manual migration completed	Stop here. The upgrade is complete.
• Manual migration allowed but not migrated	Go to step 6 to complete the ACL migration for a share.
• Migration failed with errors • Failed to initialize migration state • Auto migration required	Contact technical support for assistance.

6. If you are migrating individual shares, use the following command for each share you will migrate:

   ```
   CLI (config)> smb migrate domain_acls name <sharename> force [override]
   ```

   If you are migrating all shares, use the following command:

   ```
   CLI (config)> smb migrate domain_acls all [override]
   ```

   Use the `name` parameter to specify a share name. Use the `all` parameter to specify all SMB shares on the AltaVault. The optional `override` parameter overwrites any existing share-level ACLs.

For detailed SMB deployment information, see the *NetApp AltaVault (Formerly SteelStore) Cloud-Integrated Storage Appliances SMB Deployment Guide (Technical Report 4511)* for detailed deployment instructions.

Note: After successfully upgrading the AltaVault software, the appliance does not support start up from the alternate boot partition containing the previous version of software. The alternate boot partition exists to applied software upgrades, without affecting the current running AltaVault software version. If the software upgrade process fails or experiences an error, then the current running version of AltaVault software is not affected.

Rebooting and shutting down AltaVault appliance

You can reboot or shut down the system in the Maintenance > Reboot/Shutdown page.

Rebooting the system disrupts existing network connections. Rebooting can take a few minutes.

When you shut down the system, connections are broken and optimization ceases. Shutdown can take a few minutes.

To restart the system, you must manually turn on the AltaVault.

You must mount all NFS shares again after a reboot or a service restart.

Rebooting the AltaVault physical appliances does not reboot the attached add-on shelves. You do not need to power off the add-on shelves, even if the AltaVault is rebooting. The add-on shelves should always be powered on before the AltaVault boots and starts running the storage optimization service.

To reboot or shut down the system

1. Choose Maintenance > Reboot/Shutdown.
2. Click **Reboot**. After you click Reboot, you are logged out of the system and it is rebooted.
3. Click **Shutdown** to shut down the system. After you click Shutdown, the system is turned off. To restart the system, you must manually turn on the AltaVault.

   Reboot or shutdown operations can take a few minutes.

Viewing the current user settings

You can change your login password, reset your user preferences, and view your role-based permissions in the My Account page.

To display system permissions

1. Choose Configure > My Account.

2. To change the password of the currently logged in user, complete the configuration as described in this table.

Control	Description
Change Password	Select the check box to change the password for the currently logged in user.
New Password/Confirm New Password	Type a password in the text box. Retype the password in the Confirm New Password text box. The password cannot be “password.”
Apply	Click to confirm the password change.

To restore user preferences

1. To restore the default user preferences for the currently logged in user, click the **Restore Defaults** button.

   The user preferences are used to remember the state of the Management Console across sessions on a per-user basis. They do not affect the configuration of the appliance.

Managing configuration files

You can save, activate, import, and revert configurations in the Configure > Configurations page.

Each AltaVault has an active, running configuration and a written, saved configuration.

Only the Admin account can manage configurations. Role-based accounts cannot manage configuration files

When you apply your settings in the Management Console, the values are applied to the active running configuration, but the values are not written to disk and saved permanently.

When you save your configuration settings, the values are written to disk and saved permanently. Some settings take effect after you restart the AltaVault service.

Each time you save your configuration settings, they are written to the current running configuration, and a backup is created.

The Configuration Manager is a utility that enables you to save configurations as backups or active configuration backups.

The Configuration Manager also includes an Import Configuration utility to support these common use cases:

- Replacing the AltaVault - If you are replacing one AltaVault with another, you can import all of the network information (except the licenses) and disconnect the old AltaVault before you switch configurations on the new AltaVault.

  Contact NetApp Support to help you migrate your data from the old appliance to the new one in the case of an upgrade or failure.

- Configuration template for a large deployment - You can avoid entering the complete AltaVault configuration for every appliance in a large deployment by setting up a template AltaVault configuration and importing template settings to the configuration list.

The default configurations are as follows:

Configuration	Description
initial	This is the initial configuration.
initial.bak	This is the backup of the initial configuration.

To manage configurations

1. Choose Configure > Configurations.

2. Under Current Configuration: <filename>, complete the configuration as described in this table.

Control	Description
Current Configuration: <configuration name>	View Running Config - Displays the running configuration settings in a new browser window. Save - Saves settings that have been applied to the running configuration. Revert - Reverts your settings to the running configuration.
Save Current Configuration	Specify a new filename to save settings that have been applied to the running configuration as a new file, and then click **Save As**.

3. To import a configuration from another appliance, complete the configuration as described in this table.

Control	Description
Import a New Configuration	Displays the controls to import a configuration from another appliance.
IP/Hostname	Specify the IP address or hostname of the AltaVault from which you want to import the configuration.
Remote Admin Password	Specify the administrator password for the remote AltaVault.
Remote Config Name	Specify the name of the configuration that you want to import from the remote AltaVault.
New Config Name	Specify a new, local configuration name.
Import Shared Data Only	This value is enabled by default. Copies only the following common settings: interface, protocols, CLI and Web, statistics, NTP, SNMP, cloud settings, and alarm settings. The system does not automatically copy other settings.
Import	Imports the configuration. The imported configuration appears in the Configuration list but does not become the active configuration until you click **Activate**.
Remove Selected	Select the check box next to the name and click **Remove Selected**.
Change Active Configuration	Select the configuration to activate from the drop-down list.

4. Click **Activate** to change the active configuration to the configuration you select.

5. Restart the AltaVault service on the Maintenance > Service page.

   Click the configuration name to display the configuration settings in a new browser window.

CHAPTER 6 Configuring system administrator settings

This section describes how to configure features to assist you in system administration. It includes the following sections:

- "Setting announcements" on page 85
- "Configuring alarm settings" on page 86
- "Configuring date and time" on page 91
- "Configuring SNMP basic settings" on page 94
- "Configuring email settings" on page 101
- "Configuring log settings" on page 102

Setting announcements

You can create or modify a login message or a message of the day. The login message appears in the Management Console Login page. The message of the day appears in the Home page and when you first log in to the CLI.

To set an announcement

1. Choose Configure > Announcements.
2. Use the controls to complete the configuration as described in this table.

Control	Description
Login Message	Type a message in the text box to appear on the Login page.
MOTD	Type a message in the text box to appear on the Home page as the message of the day.

3. Click **Apply** to view the message before saving.
4. Click **Save** to save your settings permanently.

Configuring alarm settings

You can set alarms in Configure > Alarms page.

Enabling alarms is *optional*.

AltaVault uses hierarchical alarms. The system groups certain alarms into top-level categories, such as the SSL Settings alarm. When an alarm triggers, its parent expands to provide more information. As an example, the Disk Full top-level parent alarm aggregates over multiple partitions. If a specific partition is full, the Disk Full parent alarm triggers, and the System Status report displays more information regarding which partition caused the alarm to trigger.

Disabling a parent alarm disables its children. You can enable a parent alarm and disable any of its child alarms. You cannot enable a child alarm without first enabling its parent.

The child alarm of a disabled parent appear on the System Status report with a suppressed status. Disabled children alarm of an enabled parent appear on the System Status report with a disabled status.

To set alarm parameters

1. Choose Configure > Alarms.

2. Under Enable Alarms, complete the configuration as described in this table.

Alarm	Description
Admission Control	Enables an alarm if the AltaVault reaches admission control, which limits the number of connections made to the AltaVault so that you do not over-consume resources on your system. By default, this alarm is enabled.
Cloud Bucket Consistency	Enables an alarm if there is data in the cloud, although the AltaVault data store is empty. To clear this alarm, enable replication and recovery to ensure that the cloud storage is synchronized with the data store. This alarm occurs when you perform disaster recovery without specifying the correct parameters.
Cloud Bucket Disparity	Enables an alarm when the cloud bucket that the AltaVault is trying to connect to is not its own. This alarm prevents corruption of the files in the cloud.
Cloud Bucket Over Capacity	Enables an alarm when the cloud bucket that the AltaVault connects to has exceeded the licensed cloud capacity.
CPU Utilization	Enables an alarm if the average and peak thresholds for the CPU utilization are exceeded. When an alarm reaches the rising threshold, it is activated; when it reaches the lowest or reset threshold, it is reset. After an alarm is triggered, it is not triggered again until it has fallen below the reset threshold. If the CPU utilization alarm triggers when the AltaVault is under a heavy load, you can ignore it. By default, this alarm is enabled, with a rising threshold of 95% and a reset threshold of 70%.
	Rising Threshold - Specify the rising threshold. When an alarm reaches the rising threshold, it is activated. The default value is 95%.
	Reset Threshold - Specify the reset threshold. When an alarm reaches the lowest or reset threshold, it is reset. After an alarm is triggered, it is not triggered again until it has fallen below the reset threshold. The default value is 70%.
Data Integrity Error	Enables an alarm when inconsistency in the data stored on the disk is detected.
Datastore Eviction	Indicates that the system has detected an issue with datastore eviction. The alarm triggers when the appliance starts evicting data from the local disk cache and the age of the evicted data is relatively young. AltaVault has disk space much smaller than the total addressable space on the cloud, and if disk space runs low, the appliance starts evicting data from disk that has not been used recently. This keeps only fresh and frequently accessed data in cache. The AltaVault keeps statistics about how old the evicted data is (this is the average evicted age). Usually, only old data is evicted. This behavior is generally not a problem and does not trigger an alarm. However, the appliance might be experiencing such a huge workload that more and more recent data needs to be evicted from the appliance to make space for incoming data. This causes the average evicted age to decrease, and when it goes below a certain threshold, the average evicted age alarm triggers. This alarm is an anomalous event, signaling that the appliance is handling a much larger workload than expected. This alarm is useful in detecting whether the appliance is undersized relative to your normal workload. If the alarm is constantly triggered, then you should consider moving your data to a AltaVault model with a larger disk cache.
Datastore Low Space	Indicates that the local data store (disk cache on the AltaVault) is running out of space and the eviction process on the AltaVault is unable to run at a sufficient pace to create space on the disk cache. This alarm might trigger when replication is too slow. View the Eviction Optimization report (choose Reports > Eviction) to determine how much disk cache is available.

Alarm	Description
Disk Full	Enables an alarm if the system partitions (not the AltaVault data store) are full or almost full. For example, AltaVault monitors the available space used to hold logs, statistics, system dumps, and TCP dumps. By default, this alarm is enabled. This alarm monitors the following system partitions: • /boot Full • /bootmgr Full • /config Full • /tmp Full • /var Full
Hardware	Fan Error - Enables an alarm when an appliance fan error is detected (the fan is either missing or running at a low speed). Fans for many systems can be replaced. Contact NetApp Support at https://mysupport.netapp.com and file a trouble ticket to order a replacement fan.
	Flash Error - Enables an alarm if the flash disk is unresponsive and needs to be reloaded. This alarm is specific to xx10 appliances.
	Battery Backup Unit - Enables an alarm when battery backup unit is detected.
	IPMI - Indicates that there has been a physical security intrusion, triggering an Intelligent Platform Management Interface (IPMI) error. The following events trigger the IPMI alarm: • Chassis intrusion (physical opening and closing of the appliance case) • Memory errors (ECC memory errors that can or cannot be corrected) • Hard drive faults or predictive failures • Power supply status or predictive failures The option to reset the alarm appears only after the service triggers the IPMI alarm. To reset the alarm, click **Clear the IPMI alarm now**.
	Memory Error - Enables an alarm when there is a memory error in one or more memory modules. A system memory stick might be failing. Unplug the power cords from the power supply and try reseating the memory. If the problem persists, contact NetApp Support for an RMA replacement soon.
	Power Supply - Enables an alarm when an inserted power supply cord does not have power, as opposed to a power supply slot with no power supply cord inserted. By default, this alarm is enabled.
	RAID - Indicates that the system has encountered RAID errors (for example, missing drives, pulled drives, drive failures, and drive rebuilds). For drive rebuilds, if a drive is removed and then reinserted, the alarm continues to be triggered until the rebuild is complete. **Important**: Rebuilding a disk drive can take four to six hours. By default, this alarm is enabled. You can enable or disable the alarm for a specific RAID disk. To enable or disable an alarm, choose Settings > Alarms and select or clear the check box next to the RAID disk name. This alarm monitors and displays the status of the RAID disks.
	RAID Integrity Check - Enables an alarm when RAID integrity check is needed.
	Shelf Power Supply - Enables an alarm when shelf power supply is needed.
Inconsistent Cloud Connectivity	Enables an alarm when the connection to the cloud provider is inconsistent that leads to larger number connection errors.
Inconsistent Cloud Data	Enables an alarm when inconsistency in the data stored in the cloud is detected.

Alarm	Description
Licensing	Enables an alarm and sends an email notification if a license on the AltaVault is removed, is about to expire, has expired, or is invalid. This alarm triggers if the AltaVault has no MSPEC license installed for its currently configured model. The licenses expiring and licenses expired alarms are triggered per feature. For example, if you install two license keys for a feature, WW1-FOO-xxx (expired) and WW1-FOO-yyy (not expired), the alarms do not trigger, because the feature has one valid license. By default, this alarm is enabled.
Link Duplex	Enables an alarm and sends an email notification when an interface is not configured for half-duplex negotiation but has negotiated half-duplex mode. Half-duplex significantly limits the optimization service results. The alarm displays which interface is triggering the duplex alarm. By default, this alarm is enabled.
Link I/O Errors	Enables an alarm and sends an email notification when the link error rate exceeds 0.1% while either sending or receiving packets. This threshold is based on the observation that even a small link error rate reduces TCP throughput significantly. A properly configured LAN connection should experience very few errors. The alarm clears when the rate drops below 0.05%. You can change the default alarm thresholds by entering the **alarm link_errors err-threshold xxxxx** CLI command at the system prompt. For details, see the *NetApp AltaVault Cloud Integrated Storage Command-Line Interface Reference Guide*. By default, this alarm is enabled. You can enable or disable the alarm for a specific interface. For example, you can disable the alarm for a link where you have decided to tolerate the errors. To enable or disable an alarm, choose Settings > Alarms and select or clear the check box next to one or more of the link names.
Link State	Enables an alarm and sends an email notification if an Ethernet link is lost due to an unplugged cable or dead switch port. Depending on which link is down, the system might no longer be optimizing and a network outage could occur. This is often caused by surrounding devices, like routers or switches, interface transitioning. This alarm also accompanies service or system restarts on the AltaVault. By default, this alarm is disabled. You can enable or disable the alarm for a specific interface. To enable or disable an alarm, choose Settings > Alarms and select or clear the check box next to one or more link names.
Low Memory	Enables an alarm when there is not enough memory in the system to start the storage optimization service.
Max inodes limit	Enables an alarm when the maximum number of files that can be stored has been reached.
Max Pinnable Limit	Enables an alarm when the share has reached the maximum pinnable limit. If you configure a share to be pinned, it always has data available locally in the AltaVault; data need not be fetched from the cloud.
Memory Paging	Enables an alarm when the system has reached the memory paging threshold. If 100 pages are swapped approximately every two hours, the AltaVault is functioning properly. If thousands of pages are swapped every few minutes, then reboot the AltaVault from the Maintenance > Reboot/Shutdown page to clear this alarm. If rebooting does not solve the problem, contact NetApp Support at https://mysupport.netapp.com. If the memory paging alarm triggers when the AltaVault is under a heavy load, you can ignore it.
Metadata Space Full	Enables an alarm when the data reserved for storing system metadata has filled up and leading to reduced deduplication.

Alarm	Description
Process Dump Creation Error	Enables an alarm and sends an email notification if the system detects an error while trying to create a process dump. This alarm indicates an abnormal condition in which the AltaVault cannot collect the core file after three retries. It can be caused when the directory used to hold the process dumps is reaching capacity, or by other conditions. When the alarm is raised, the directory is blacklisted. By default, this alarm is enabled.
Restore Throttling	The restore throttling alarm is applicable only when the cloud storage used is AWS Glacier. AWS Glacier documentation specifies a monthly limit up to which no restore costs are charged for retrieving data from Glacier. Once this limit is crossed, data retrieval costs can be substantial. For details, see AWS Glacier documentation. By default, the AltaVault has a restore throttle for data retrieved from Glacier. This throttle keeps retrievals below the no-cost limit. The default value of this restore throttle is 5%. Therefore, you can use the AltaVault to restore 5% of total cloud usage in a month. The throttle is enforced on an hourly basis. Hourly data retrieval is limited to (5% of the total cloud use)/(hours per month). You can increase the 5% restore throttle limit up to 100% or completely disable it by setting the limit to 0. You might incur data retrieval charges when you make this change. For details about how to change the restore throttle limit, see the *NetApp AltaVault Cloud Integrated Storage Command-Line Interface Reference Guide*.
Secure Vault	Enables an alarm and sends an email notification if the system encounters a problem with the secure vault: • Secure Vault Locked - Indicates that the secure vault is locked. To optimize SSL connections or to use data store encryption, the secure vault must be unlocked. Go to Configure > Secure Vault and unlock the secure vault.
SMB	Enables an alarm when AltaVault detects the Domain Controller is not reachable. • Domain Controller Network Status - Indicates the Domain Controller is unreachable. The alarm is cleared when network connectivity to the Domain Controller is restored. If the alarm is not cleared after the network connectivity is restored, you can clear the alarm manually using **alarm smb_alarms clear** command.
Software update available	Enables an alarm when a new version of the software is available.
Shelf Error	Shelf Missing - This alarm is applicable only to the AltaVault models. The AltaVault Expansion Shelf is missing or cannot be accessed.
	Shelf <shelf name> • Shelf Inconsistent - The AltaVault Expansion Shelf is not consistent with the stored configuration. • Shelf Not Empty - You have added a new AltaVault Expansion Shelf that is not empty. A new AltaVault Expansion Shelf must be empty before you add it to AltaVault appliance. • Shelf Not Valid - The AltaVault Expansion Shelf is not a valid shelf. For details, choose Reports > Storage RAID Groups and click the serial number of the shelf.

Alarm	Description
Storage Optimization Service	• Storage Optimization Service Down - Enables an alarm and sends an email notification if the storage optimization service encounters a service condition. By default, this alarm is enabled. The message indicates the reason for the condition. The following conditions trigger this alarm: • Configuration errors: examples include no encryption key set, incorrect appliance time, or incorrect cloud credentials. • An AltaVault appliance reboot for example, during an appliance software update. • A system crash for example, due to a power failure • A storage optimization service restart for example, due to a cloud storage provider change. • A user enters the CLI command **no service enable** or shuts down the storage optimization service from the Management Console • A user restarts the optimization service from either the Management Console or CLI • Storage Optimization Service Error - Enables an alarm and sends an email notification if the storage optimization service encounters a condition that might degrade optimization performance. By default, this alarm is enabled. Go to the Maintenance > Service page and restart the optimization service.
Storage Optimization Service Replication	• Replication Error - Enables an alarm when the replication to the cloud encounters an error. Displays an error message that indicates the type of error such as, a file cannot be replicated to the cloud. • Replication Paused - Enables an alarm when the replication to the cloud pauses, because there is a cloud connection error, or you entered the CLI command no replication enable, or because you are using replication scheduling (nonbandwidth limit type). This alarm warns you that the AltaVault is not replicating data in the cloud. By default, this alarm is enabled.
System Reserved Space Full	Indicates that the space used for internal data structures is full. If you write more data to the appliance, it reduces deduplication performance.
Temperature	• Critical Temperature - Enables an alarm and sends an email notification if the CPU temperature exceeds the rising threshold. When the CPU returns to the reset threshold, the critical alarm is cleared. The default value for the rising threshold temperature is 80º C; the default reset threshold temperature is 67º C. • Warning Temperature - Enables an alarm and sends an email notification if the CPU temperature approaches the rising threshold. When the CPU returns to the reset threshold, the warning alarm is cleared. • Rising Threshold - Specifies the rising threshold. The alarm activates when the temperature exceeds the rising threshold. The default value is 80%. • Reset Threshold - Specifies the reset threshold. The alarm clears when the temperature falls below the reset threshold. The default value is 67%. After the alarm triggers, it cannot trigger again until after the temperature falls below the reset threshold and then exceeds the rising threshold again.
Upgrade Status	Indicates the status of the upgrade. By default, this alarm is enabled.

3. Click **Apply** to apply your changes to the running configuration.

4. Click **Save** to save your settings permanently.

Configuring date and time

You set the system date and time in the Configure > Date and Time page.

You can either set the system date and time by entering it manually, or by assigning an NTP server to the AltaVault. By default, the appliance uses the NetApp-provided NTP server.

To set the date and time manually

1. Choose Configure > Date and Time.
2. Complete the configuration as described in this table.

Control	Description
Time Zone	Select a time zone from the drop-down list. If you change the time zone, log messages retain the previous time zone until you reboot the AltaVault.
Set Time Manually	Change Date - Specify the date in this format: YYYY/MM/DD. Change Time - Specify military time in this format: HH:MM:SS.

3. Click **Apply** to apply your changes to the running configuration.
4. Click **Save** to save your settings permanently.

To use Network Time Protocol (NTP) time synchronization

1. Choose Configure > Date and Time.
2. Under Date and Time, select Use NTP Time Synchronization.
3. As a best practice, configure your own internal NTP servers.

Current NTP status

Brief status information appears just below the Use NTP Time Synchronization button. The label Current NTP server is followed by either a server name or nothing if no NTP server is active.

This information appears after an NTP server name:

- Authentication information; “unauthenticated” appears after the server name when it is not using authentication.
- When the system has no NTP information about the current server, nothing appears.

When you configure an NTP server pool, the current NTP server that appears after the label Current NTP server never matches the hostname of the server pool.

NTP MD5-based authentication

NTP authentication verifies the identity of the NTP server sending timing information to the AltaVault. The system supports MD5-based Message-Digest Algorithm symmetric keys for NTP authentication. MD5 is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value.

NTP authentication is *optional*.

Configuring NTP authentication involves these steps that you can perform in any order:

- Configure a key ID and a secret pair.

- Configure the NTP server with the key ID.

NTP servers

NetApp recommends synchronizing the AltaVault to an NTP server of your choice.

To add an NTP server

1. Choose Configure > Date and Time.
2. Under Requested NTP Servers, complete the configuration as described in this table.

Control	Description
Add a New NTP Server	Displays the controls to add a server.
Hostname or IP Address	Specify the hostname or IP address for the NTP server.
Version	Select the NTP server version from the drop-down list: 3 or 4.
Enabled/Disabled	Select Enabled from the drop-down list to connect to the NTP server. Select Disabled from the drop-down list to disconnect from the NTP server.
Key ID	Specify the MD5 key identifier to use to authenticate the NTP server. The valid range is 1 to 65534. The key ID must appear on the trusted keys list.
Add	Adds the NTP server to the server list.
Remove Selected	Select the check box next to the name and click **Remove Selected**.

3. Click **Save** to save your settings permanently.

NTP authentication keys

NTP authentication uses a key and a shared secret to verify the identity of the NTP server sending timing information to the AltaVault. The system encrypts the shared secret text using MD5, and uses the authentication key to access the secret.

To add an NTP authentication key

1. Choose Configure > Date and Time.

2. Under NTP Authentication Keys, complete the configuration as described in this table.

Control	Description
Add a New NTP Authentication Key	Displays the controls to add an authentication key to the key list. Both trusted and untrusted keys appear on the list.
Key ID	Optionally, specify the secret MD5 key identifier for the NTP server. The valid range is 1 to 65534.
Key Type	Select MD5 or SHA1 option.
Secret (Text)	Specify the shared secret. You must configure the same shared secret for both the NTP server and the NTP client to use MD5-based cryptography. The shared secret: • is limited to 16 characters or fewer • cannot include white space or #s • cannot be empty • is case sensitive The secret appears in the key list as its MD5 hash value.
Add	Adds the authentication key to the trusted keys list.
Remove Selected	Select the check box next to the name and click **Remove Selected**.

3. Click **Save** to save your settings permanently.

NTP key information

NTP keys appear in a list that includes the key ID, type, secret (displays as the MD5 hash value), and whether the system trusts the key for authentication.

Configuring SNMP basic settings

You configure Simple Network Management Protocol (SNMP) contact and trap receiver settings to enable event reporting to an SNMP entity in the Configure > SNMP Basic page.

Traps are messages sent by an SNMP entity that indicate the occurrence of an event. The default system configuration does not include SNMP traps.

AltaVault supports the following SNMP Basic settings:

- SNMP Version 1
- SNMP Version 2c
- SNMP Version 3, which provides authentication through the User-based Security Model (USM)
- View-Based Access Control Mechanism (VACM), which provides richer access control
- Enterprise Management Information Base (MIB)
- ACLs (Access Control Lists) for users (v1 and v2c only)

To set general SNMP basic parameters

1. Choose Configure > SNMP Basic.
2. Under SNMP Server Settings, complete the configuration as described in this table.

Control	Description
Enable SNMP Traps	Enables event reporting to an SNMP entity.
System Contact	Specify the username for the SNMP contact.
System Location	Specify the physical location of the SNMP system.
Read-Only Community String	Specify a password-like string to identify the read-only community. For example, public. This community string overrides any VACM settings. Community strings do not allow non-printable 7-bit ASCII characters, except for white spaces. Also, the community strings cannot begin with '#' and '-'.

3. Click **Apply** to apply your changes to the running configuration.
4. Click **Save** to save your settings permanently.

To add or remove a trap receiver

1. Under Trap Receivers, complete the configuration as described in this table.

Control	Description
Add a New Trap Receiver	Displays the controls to add a new trap receiver.
Receiver	Specify the destination IP address or hostname for the SNMP trap.
Destination Port	Specify the destination port.
Receiver Type	Select SNMP version v1, v2c, or v3 (user-based security model). **Note:** SNMP v1 and v2c are less secure, v3 is recommended.
Remote User	(Appears only when you select v3). Specify a remote username.
Authentication	(Appears only when you select v3). Optionally, select either Supply a Password or Supply a Key to use while authenticating users.
Authentication Protocol	(Appears only when you select v3). Select an authentication method from the drop-down list: • MD5 - Specifies the Message-Digest 5 algorithm, a widely used cryptographic hash function with a 128-bit hash value. This is the default value. • SHA - Specifies the Secure Hash Algorithm, a set of related cryptographic hash functions. SHA is considered to be the successor to MD5.
Password/Password Confirm	(Appears only when you select v3 and Supply a Password). Specify a password. The password must have a minimum of eight characters. Confirm the password in the Password Confirm text box.

Control	Description
Security Level	(Appears only when you select v3).Determines whether a single atomic message exchange is authenticated. Select one of the following settings from the drop-down list: • No Auth - Does not authenticate packets and does not use privacy. This is the default setting. • Auth - Authenticates packets but does not use privacy. • AuthPriv - Authenticates packets using AES 128 and DES to encrypt messages for privacy. A security level applies to a group, not to an individual user.
Community	For v1 or v2 trap receivers, specify the SNMP community name. For example, public or private v3 trap receivers need a remote user with an authentication protocol, a password, and a security level.
Enable Receiver	Select to enable the new trap receiver. Clear to disable the receiver.
Add	Adds a new trap receiver to the list.
Remove Selected	Select the check box next to the name and click **Remove Selected**.

2. Click **Save** to save your settings permanently.

After upgrade, all previous traps and community string intact are visible.

To test an SNMP trap

1. Choose Configure > SNMP Basic.
2. Under SNMP Trap Test, click **Run**.

Configuring SNMP v3

SNMP v3 provides additional authentication and access control for message security. For example, you can verify the identity of the SNMP entity (manager or agent) sending the message.

Using SNMP v3 is more secure than SNMP v1 or v2; however, it requires more configuration steps to provide the additional security features.

Basic steps

1. Create the SNMP-server users. Users can be authenticated using either a password or a key.
2. Configure SNMP-server views to define which part of the SNMP MIB tree are visible.
3. Configure SNMP-server groups, which map users to views, allowing you to control who can view what SNMP information.
4. Configure the SNMP-server access policies that contain a set of rules defining access rights. Based on these rules, the entity decides how to process a given request.

To create users for SNMP v3

1. Choose Configure > SNMP v3.

2. Under Users, complete the configuration as described in this table.

Control	Description
Add a New User	Displays the controls to add a new user.
User Name	Specify the username.
Authentication Protocol	Select an authentication method from the drop-down list: • MD5 - Specifies the Message-Digest 5 algorithm, a widely used cryptographic hash function with a 128-bit hash value. This is the default value. • SHA - Specifies the Secure Hash Algorithm, a set of related cryptographic hash functions. SHA is considered to be the successor to MD5.
Authentication	Optionally, select either Supply a Password or Supply a Key to use while authenticating users.
Password/Password Confirm	Specify a password. The password must have a minimum of eight characters. Confirm the password in the Password Confirm text box. The password cannot be “password.”
MD5 Key	(Appears only when you select Supply A Key). Specify a unique authentication key. The key is a MD5 or SHA-1 digest created using md5sum or sha1sum.
Privacy MD5/SHA Key	(Appears only when you select v3 and Privacy as Supply a Key). Specify the privacy authentication key. The key is either a 32-hexadecimal digit MD5 or a 40-hexadecimal digit SHA digest created using md5sum or sha1sum.
Use Privacy Option	Privacy Protocol - Select the privacy protocol from the drop-down list. Choose AES or DES. Privacy - Select the privacy option from the drop-down list. Choose Same as Authentication, Supply a Password, or Supply a Key.
Add	Adds the user.
Remove Selected	Select the check box next to the name and click **Remove Selected**.

3. Click **Apply** to apply your changes to the running configuration.

4. Click **Save** to save your settings permanently.

SNMP authentication and access control

The features on this page apply to SNMP v1, v2c, and v3 unless noted otherwise:

- Security Names - Identify an individual user (v1 or v2c only).
- Secure Groups - Identify a security-name, security model by a group, and referred to by a group-name.
- Secure Views - Create a custom view using the View-based Access Control Model (VACM) that controls who can access which MIB objects under agent management by including or excluding specific Object Identifiers (OIDs). For example, some users have access to critical read-write control data, while some users have access only to read-only data.
- Security Models - A security model identifies the SNMP version associated with a user for the group in which the user resides.
- Secure Access Policies - Defines who gets access to which type of information. An access policy contains <group-name, security-model, security-level, read-view-name>:
  - read-view-name is a preconfigured view that applies to read requests by this security-name.
  - write-view-name is a preconfigured view that applies to write requests by this security-name.
  - notify-view-name is a preconfigured view that applies to write requests to this security-name.

An access policy is the configurable set of rules, based on which the entity decides how to process a given request.

To set secure usernames

1. Choose Configure > SNMP ACLs.

2. Under Security Names, complete the configuration as described in this table.

Control	Description
Add a New Security Name	Displays the controls to add a security name.
Security Name	Specify a name to identify a requestor allowed to issue gets and sets (v1 and v2c only). The specified requestor can make changes to the view-based access-control model (VACM) security name configuration. Community strings do not allow printable 7-bit ASCII characters, except for white spaces. Also, community strings cannot begin with '#' or '-' (hash or hyphen). This control does not apply to SNMPv3 queries. To restrict v3 USM users from polling a particular subnet, use the Management ACL feature. Traps for v1 and v2c are independent of the security name.
Community String	Specify the password-like community string to control access. Use a combination of uppercase, lowercase, and numerical characters to reduce the chance of unauthorized access to the AltaVault. Community strings do not allow printable 7-bit ASCII characters, except for white spaces. Also, the community strings cannot begin with '#' and '-'. If you specify a read-only community string (located in the SNMP Basic page under SNMP Server Settings), it takes precedence over this community name and allows users to access the entire MIB tree from any source host. If this is not desired, delete the read-only community string. To create multiple SNMP community strings on a AltaVault, leave the default public community string and then create a second read-only community string with a different security name. Or, you can delete the default public string and create two new SNMP ACLs with unique names.
Source IP Address and Mask Bits	Specify the host IP address and mask bits to which you permit access using the security name and community string.
Add	Adds the security name.
Remove Selected	Select the check box next to the name and click **Remove Selected**.

3. Click **Apply** to apply your changes to the running configuration.

4. Click **Save** to save your settings permanently.

To set secure groups

1. Choose Configure > SNMP ACLs.

2. Under Groups, complete the configuration as described in this table.

Control	Description
Add a New Group	Displays the controls to add a new group
Group Name	Specify a group name.
Security Model and Name Pairs	Click the + button and select a security model from the drop-down list: • v1 or v2c - displays another drop-down list; select a security name. • v3 (usm) - displays another drop-down list, select a user. To add another Security Model and Name pair, click the plus sign (+).

Control	Description
Add	Adds the group name and security model and name pairs.
Remove Selected	Select the check box next to the name and click **Remove Selected**.

3. Click **Apply** to apply your changes to the running configuration.

4. Click **Save** to save your settings permanently.

To set secure views

1. Choose Configure > SNMP ACLs.

2. Under Views, complete the configuration as described in this table.

Control	Description
Add a New View	Displays the controls to add a new view.
View Name	Specify a descriptive view name to facilitate administration.
Includes	Specify the object identifiers (OIDs) to include in the view, separated by commas. For example, .1.3.6.1.4.1. By default, the view excludes all OIDs. You can specify .iso or any subtree or subtree branch. You can specify an OID number or use its string form. For example, .iso.org.dod.internet.private.enterprises.xxx.products.AltaVault.system.model
Excludes	Specify the OIDs to exclude in the view, separated by commas. By default, the view excludes all OIDs.
Add	Adds the view.
Remove Selected	Select the check box next to the name and click **Remove Selected**.

3. Click **Apply** to apply your changes to the running configuration.

4. Click **Save** to save your settings permanently.

To add an access policy

1. Choose Configure > SNMP ACLs.

2. Under Access Policies, complete the configuration as described in this table.

Control	Description
Add a New Access Policy	Displays the controls to add a new access policy.
Group Name	Select a group name from the drop-down list.

Control	Description
Security Level	Determines whether a single atomic message exchange is authenticated. Select one of the following from the drop-down list: • **No Auth** - Does not authenticate packets and does not use privacy. This is the default setting. • **Auth** - Authenticates packets but does not use privacy. • **AuthPriv** - Authenticates packets using AES or DES to encrypt messages for privacy. A security level applies to a group, not to an individual user.
Read View	Select a view from the drop-down list.
Add	Adds the policy to the policy list.
Remove Selected	Select the check box next to the name and click **Remove Selected**.

3. Click **Apply** to apply your changes to the running configuration.

4. Click **Save** to save your settings permanently.

Configuring email settings

You can set email notification parameters for events and failures in the Configure > Email page.

By default, email addresses are not specified for event and failure notification.

To set event and failure email notification

1. Choose Configure > Email.

2. Under Email Notification, complete the configuration as described in this table.

Control	Description
SMTP Server	Specify the SMTP server. You must have external DNS and external access for SMTP traffic for this feature to function. Make sure you provide a valid SMTP server to ensure that the users you specify receive email notifications for events and failures.
SMTP Port	Specify the port number for the SMTP server.
Report Events via Email	Specify this option to report events through email. Specify a list of email addresses to receive the notification messages. Separate addresses by spaces, semicolons, commas, or vertical bars.
Report Failures via Email	Specify this option to report failures through email. Specify a list of email addresses to receive the notification messages. Separate addresses by spaces, semicolons, commas, or vertical bars.
Override Default Sender's Address	Select this option to configure the SMTP protocol for outgoing server messages for errors or events. Specify a list of email addresses to receive the notification messages. Separate addresses by commas. You can also configure the outgoing email address sent to the client recipients. The default outgoing address is do-not-reply@hostname.domain. If you do not specify a domain the default outgoing email is do-not-reply@hostname.

3. Click **Apply** to apply your changes to the running configuration.

4. Click **Save** to save your settings permanently.

Configuring log settings

You set up local and remote logging in the Configure > Logging page.

By default, the system rotates each log file every 24-hours or if the file size reaches one Gigabyte uncompressed. You can change this to rotate every week or month and you can rotate the files based on file size.

The automatic rotation of system logs deletes your oldest log file, labeled as Archived log #10, pushes the current log to Archived log # 1, and starts a new current-day log file.

To set up logging

1. Choose Configure > Logging.

2. To rotate the logs immediately, under Log Actions at the bottom of the page, click **Rotate Logs**. After the logs are rotated, the following message appears:

   ```
   logs have been successfully rotated
   ```

   You can also schedule a log rotation based on time or the amount of disk space the log uses, described next.

3. Under Logging Configuration, complete the configuration as described in this table.

Control	Description
Minimum Severity	Select the minimum severity level for the system log messages. The log contains all messages with this severity level or higher. Select one of the following levels from the drop-down list: • Emergency - Emergency, the system is unusable. • Alert - Action must be taken immediately. • Critical - Conditions that affect the functionality of the AltaVault. • Error - Conditions that probably affect the functionality of the AltaVault. • Warning - Conditions that could affect the functionality of the AltaVault, such as authentication failures. • Notice - Normal but significant conditions, such as a configuration change. • Info - Informational messages that provide general information about system operations. This is the default setting. This control applies to the system log only. It does not apply to the user log.
Maximum Number of Log Files	Specify the maximum number of logs to store. The default value is 10.
Lines Per Log Page	Specify the number of lines displayed per page when viewing the logs. The default value is 100.
Rotate Based On	Specifies the rotation option: • Time - Select Day, Week, or Month from the drop-down list. The default setting is Day. • Disk Space - Specify how much disk space, in megabytes, the log uses before it rotates. The default value is 16 MB. The log file size is checked at 10-minute intervals. If there is an unusually large amount of logging activity, it is possible for a log file to grow larger than the set disk space limit in that period of time.

4. Click **Apply** to apply your changes to the running configuration.

5. Click **Save** to save your settings permanently.

To add or remove a log server

1. Under Remote Log Servers, complete the configuration as described in this table.

Control	Description
Add a New Log Server	Displays the controls for configuring new log servers.
Server IP	Specify the server IP address.
Minimum Severity	Select the minimum severity level for the log messages. The log contains all messages with this severity level or higher. Select one of the following levels from the drop-down list: • Emergency - Emergency, the system is unusable. • Alert - Action must be taken immediately. • Critical - Conditions that affect the functionality of the AltaVault. • Error - Conditions that probably affect the functionality of the AltaVault. • Warning - Conditions that could affect the functionality of the AltaVault, such as authentication failures. • Notice - Normal but significant conditions, such as a configuration change. This is the default setting. • Info - Informational messages that provide general information about system operations.
Add	Adds the server to the list.
Remove Selected	Select the check box next to the name and click **Remove Selected**.

2. Click **Apply** to apply your changes to the running configuration.

3. Click **Save** to save your settings permanently.

Filtering logs by application or process

You can filter a log by one or more applications or one or more processes. This is particularly useful when capturing data at a lower severity level at which the AltaVault might not be able to sustain the flow of logging data that the service is committing to disk.

Log filters enable you to specify the logging level of individual processes independently.

To filter a log

1. Choose Configure > Logging.

2. Under Per-Process Logging, complete the configuration as described in this table.

Control	Description
Add a New Process Logging Filter	Displays the controls for adding a process-level logging filter.
Process	Select a process to include in the log from the drop-down list: • alarmd - Alarm Manager. • cli - Command Line Interface. • hald - Hardware abstraction daemon, which handles access to the hardware. • Isiraidd - LSI raid daemon. • mgmtd - Device control and management, which directs the entire device management system. It handles message passing between various management daemons, managing system configuration and general application of system configuration on the hardware underneath through the hardware abstraction layer daemon (HALD). • pm - Process Manager, which handles launching of internal system daemons and keeps them running. • sched - Process Scheduler that handles one-time scheduled events. • statsd - Statistics Collector that handles the statistics. • wdt - Watchdog Timer, the motherboard watchdog daemon. • webasd - Web Application Process, which handles the Web user interface.
Minimum Severity	Select the minimum severity level for the log messages. The log contains all messages with this severity level or higher. Select one of the following levels from the drop-down list: • Emergency - Emergency, the system is unusable. This is the default setting. • Alert - Action must be taken immediately. • Critical - Conditions that affect the functionality of the AltaVault. • Error - Conditions that probably affect the functionality of the AltaVault. • Warning - Conditions that could affect the functionality of the AltaVault, such authentication failures. • Notice - Normal but significant conditions, such as a configuration change. • Info - Informational messages that provide general information about system operations.
Add	Adds the filter to the list, after which it logs at the selected severity and higher.
Remove Selected	Select the check box next to the name and click **Remove Selected** to remove the filter.

3. Click **Apply** to apply your changes to the running configuration.

4. Click **Save** to save your settings permanently.

CHAPTER 7 Configuring security settings

This section describes how to configure the AltaVault security features. It includes the following sections:

- "Configuring general security settings" on page 105
- "Managing user permissions" on page 107
- "Setting RADIUS servers" on page 111
- "Configuring TACACS+ access" on page 113
- "Unlocking the secure vault" on page 114
- "Configuring Web settings" on page 115
- "Configuring KMIP" on page 117
- "Configuring appliance monitoring" on page 122
- "Configuring a management ACL" on page 123
- "Configuring SSH Access" on page 125

Configuring general security settings

You can prioritize local, RADIUS, and TACACS+ authentication methods for the system and set the authorization policy and default user for RADIUS and TACACS+ authorization systems in the Configure > General Settings page.

Make sure to put the authentication methods in the order in which you want authentication to occur. If authorization fails on the first method, the next method is attempted, and so on, until all of the methods have been attempted.

To set TACACS+ authorization levels (admin or read-only) to allow certain members of a group to log in, add the following attribute to users on the TACACS+ server:

```
service = rbt-exec {
      local-user-name = "monitor"
}
```

Replace `monitor` with `admin` for write access.

To set general security settings

1. Choose Configure > General Settings.

2. Under Authentication Methods, complete the configuration as described in this table.

Control	Description
Authentication Methods	Specifies the authentication method. Select an authentication method from the drop-down list. The methods are listed in the order in which they occur. If authorization fails on the first method, the next method is attempted, and so on, until all of the methods have been attempted.
For RADIUS/TACACS+, fallback only when servers are unavailable	Specifies that the AltaVault uses a RADIUS or TACACS+ server only when all other servers do not respond. This is the default setting. When this feature is disabled, the system does not use the RADIUS or TACACS+ servers. If the system exhausts the other servers and does not get a response, it returns a server failure.
Authorization Policy	Appears only for some Authentication Methods. Optionally, select one of the following policies from the drop-down list: • Remote First - Checks for an authentication policy on the remote server first, and only checks locally if the remote server does not have a policy set. This is the default behavior. • Remote Only - Checks only the remote server. • Local Only - Checks only the local server. All remote users are mapped to the user specified. Any vendor attributes received by an authentication server are ignored.
Default User	Optionally, select Admin or Monitor from the drop-down list to define the default authentication policy.

3. Click **Apply** to apply your changes to the running configuration.

4. Click **Save** to save your settings permanently.

Managing user permissions

You can change the administrator or monitor passwords and define role-based users in the Configure > User Permissions page.

There are two types of accounts:

- "Capability-based accounts" on page 107
- "Role-based accounts" on page 107

Capability-based accounts

The system has two accounts, based on what actions you can take:

- Admin - The administrator user has full privileges. For example, as an administrator you can set and modify configuration settings, add and delete users, restart the AltaVault service, reboot the AltaVault, and create and view performance and system reports.
- Monitor - Monitor users can view reports and user logs and change their own password. A monitor user cannot make configuration changes.

Role-based accounts

Use the role-based management feature in the AltaVault to specify who can configure what on the appliance and also assign read-only or read and write permissions for the feature.

You can specify role-based accounts for general settings, prepop settings, replication settings, report settings, security settings, and storage settings in the AltaVault.

You can create users, assign passwords to the user, and assign varying configuration roles to the user. Available menu items reflect the privileges of the user. For example, any menu items that you do not have permission to use are unavailable. When you click an unavailable link, the User Permissions page appears.

A role-based account cannot modify another role-based or capability-based account. Only the Admin account can create and modify role-based accounts.

This section describes the roles that you can assign for specific features.

General settings

You can assign users permissions to configure the following General Settings:

- Software upgrades
- Licenses
- Email, SNMP settings, and Web settings.
- Hardware RAID settings
- Shelf settings
- Starting and stopping the storage optimization service

You can assign users permissions to configure the following network-related General Settings:

- All Networking Settings
- All Maintenance Settings
- All System Settings

You can assign users permissions to configure the following actionable diagnostic General Settings:

- System logs
- Accessing system dumps and process dumps
- Debugging commands such as the alarm command
- Tcpdumps

Prepop settings

You can assign users permissions to start a new prepopulation task and to view an existing prepopulation task.

Replication settings

You can assign users permissions to configure the following Replication Settings:

- Cloud configuration
- Replication settings
- Starting and stopping the storage optimization service

Report settings

You can assign users permissions to configure the following read-only Report Settings:

- Interface statistics
- Alarm Status
- View report graphs and statistics

Security settings

You can assign users permissions to configure the following Security Settings:

- RADIUS
- TACACS
- FIPS
- Secure vault
- Import, export, generate, and reset encryption key
- Import
- Export
- Reboot/Shutdown
- Appliance Monitoring
- Alarm
- User Log

Storage settings

You can assign users permissions to configure the following Storage Settings:

- SMB

- NFS
- OST

Configuring user permissions

You can specify the following permissions for the feature:

- Deny - You cannot view settings or make configuration changes for a feature.
- Read-Only - You can view current configuration settings but not change them.
- Read/Write - You can view settings and make configuration changes for a feature.

To configure user permissions

1. Choose Configure > User Permissions.
2. Under Capability-Based Accounts, complete the configuration as described in this table.

Control	Description
admin/monitor	Click the magnifying glass icon to change the administrator or monitor password.
	Enable Account - Select or clear the check box to enable or disable the administrator or monitor account.
	Change Password - Select the check box to change password protection. • New Password - Specify a password in the text box. The password cannot be “password” or any case combination of “password” for any user including admin and root. You will be prompted with the following message: Password “password” and its case combinations are not allowed. The password must be at least 6 characters long. • New Password Confirm - Confirm the new administrator password.

3. Under Role-Based Accounts, complete the configuration as described in this table.

Control	Description
Add a New User	Click to display the controls for creating a new role-based account.
Account Name	Specify a name for the role-based account.
Password	Specify the new password. The password cannot be “password” or any case combination of “password” for any user including admin and root and must be at least 6 characters long. You will be prompted with the following message: Password “password” and its case combinations are not allowed. The password must be at least 6 characters long.
New Password Confirm	Confirm the new password.
Enable Account	Select the check box to enable the new role-based account.
Roles and Permissions	Identify the desired permissions for the account being created. Click **Select All** to choose the given access level for all feature settings.
Add	Adds your settings to the system.
Remove Selected Users	Select the check box next to the name and click **Remove Selected**.

4. Click **Save** to save your settings permanently.

Unlocking an account

AltaVault Operating System temporarily locks out an account after a user exceeds the configured number of login attempts. Account lockout information appears on the Configure > User Permissions page.

When an account is locked out, the lockout ends after:

- The configured lockout time elapses.

  —*or*—

- The administrator unlocks the account. AltaVault never locks out administrator accounts.

To unlock an account

1. Log in as an administrator (admin).
2. Choose Configure > User Permissions.
3. Select the user to display Edit User section.
4. Click **Clear Login Failure Details** to unlock the user account.

When you log in to your account successfully, AltaVault resets the login failure count.

Configuring password policy settings

You configure password complexity and lockout requirements for management logins using Password Policy settings.

To configure password policy

1. Choose Configure > User Permissions.
2. Click **Password Policy** at the bottom of the page.
3. Specify values for each of the following settings:
   - Login attempts before lockout
   - Timeout for user login after lockout (seconds)
   - Days before password expires
   - Days to warn user of an expiring password
   - Days to keep account active after password expires
   - Days between password changes
   - Minimum Interval for password reuse
   - Minimum password length
   - Minimum uppercase characters
   - Minimum lowercase characters
   - Minimum numerical characters
   - Minimum special characters
   - Minimum character difference between passwords
   - Maximum consecutively repeating characters
   - Choose whether to prevent dictionary words
4. Click Apply to save your settings.

Setting RADIUS servers

You configure Remote Authentication Dial-in User Server (RADIUS) server authentication in the Configure > RADIUS page.

RADIUS is an access control protocol that uses a challenge and response method for authenticating users. Configuring RADIUS server authentication is optional.

To configure RADIUS server authentication

1. Choose Configure > RADIUS.

2. Under Default RADIUS Settings, complete the configuration as described in this table.

Control	Description
Set a Global Default Key	Enables a global server key for the RADIUS server.
Global Key	Specify the global server key.
Confirm Global Key	Confirm the global server key.
Timeout (seconds)	Specify the time-out period in seconds (1 to 60). The default value is 3.
Retries	Specify the number of times that you want to allow the user to retry authentication. The default value is 1.

3. Click **Apply** to apply your changes to the running configuration.

4. To add a new RADIUS server, complete the configuration as described in this table.

Control	Description
Add a RADIUS Server	Displays the controls for defining a new RADIUS server.
Hostname or IP Address	Specify the hostname or IP address.
Authentication Port	Specify the port for the server.
Authentication Type	Select one of these authentication types: • PAP - Password authentication protocol (PAP), which validates users before allowing them access to the RADIUS server resources. PAP is the most flexible protocol but is less secure than CHAP. • CHAP - Challenge-Handshake Authentication Protocol (CHAP), which provides better security than PAP. CHAP validates the identity of remote clients by periodically verifying the identity of the client using a three-way handshake. This happens at the time of establishing the initial link and might happen again at any time afterwards. CHAP bases verification on a user password and transmits an MD5 sum of the password from the client to the server.
Override the Global Default Key	Select this check box to override the global server key for the server and specify the following: • Server Key - Specify the override server key. • Confirm Server Key - Confirm the override server key.
Timeout (seconds)	Specify the time-out period in seconds (1 to 60). The default value is 3.
Retries	Specify the number of times that you want to allow the user to retry authentication. Valid values are 0 to 5. The default value is 1.
Enabled	Select the check box to enable the new server.
Add	Adds the RADIUS server to the list.
Remove Selected	Select the check box next to the name and click **Remove Selected**.

If you add a new server to your network and you do not specify these fields at that time, the global settings are applied automatically.

5. Click **Save** to save your settings permanently.

Configuring TACACS+ access

You set up TACACS+ (Terminal Access Controller Access-Control System) server authentication in the Configure > TACACS+ page.

TACACS+ is an authentication protocol that allows a remote access server to forward a login password for a user to an authentication server to determine whether access is allowed to a given system.

Enabling this feature is *optional*.

You can prioritize local, RADIUS, and TACACS+ authentication methods for the system and set the authorization policy and default user for RADIUS and TACACS+ authorization systems in the General Settings page.

To configure a TACACS+ server

1. Choose Configure > TACACS+.

2. Under Default TACACS+ Settings, complete the configuration as described in this table.

Control	Description
Set a Global Default Key	Enables a global server key for the server.
Global Key	Specify the global server key.
Confirm Global Key	Confirms the global server key.
Timeout (seconds)	Specify the time-out period in seconds (1 to 60). The default value is 3.
Retries	Specify the number of times you want to allow the user to retry authentication. Valid values are 0 to 5. The default is 1.

3. Click **Apply** to apply your changes to the running configuration.

4. To add or remove a TACACS+ server, complete the configuration as described in this table.

Control	Description
Add a TACACS+ Server	Displays the controls for defining a new TACACS+ server.
Hostname or IP Address	Specify the hostname or server IP address.
Authentication Port	Specify the port for the server. The default value is 49.
Authentication Type	Select either PAP or ASCII as the authentication type. The default value is PAP.
Override the Global Default Key	Specify this option to override the global server key for the server.
Server Key	Specify the override server key.
Confirm Server Key	Confirm the override server key.
Timeout (seconds)	Specify the time-out period in seconds (1 to 60). The default is 3.
Retries	Specify the number of times you want to allow the user to retry authentication. Valid values are 0 to 5. The default is 1.
Enabled	Enables the new server.

Control	Description
Add	Adds the TACACS+ server to the list.
Remove Selected	Select the check box next to the name and click **Remove Selected**.

If you add a new server to your network and you do not specify these fields, the system automatically applies the default settings.

5. Click **Save** to save your settings permanently.

Unlocking the secure vault

You can unlock and change the password for the secure vault in the Secure Vault page.

The secure vault contains sensitive information from your AltaVault configuration, including the encryption key. These configuration settings are encrypted on the disk at all times, using 256-bit AES encryption.

Initially, the secure vault is keyed with a default password known only to the AltaVault software. This allows the AltaVault to automatically unlock the vault during system startup. You can change the password, but the secure vault does not automatically unlock on startup. To use encryption, the secure vault must be unlocked.

To unlock or change the password of the secure vault

1. Choose Configure > Secure Vault.

2. Under Unlock Secure Vault, complete the configuration as described in this table.

Control	Description
Password	Type a password and click Unlock Secure Vault. Initially, the secure vault is keyed with a default password known only to the AltaVault software. This allows the system to automatically unlock the vault during system startup. You can change the password, but the secure vault does not automatically unlock on startup.
Unlock Secure Vault	Unlocks the vault.

3. Under Change Password, complete the configuration as described in this table.

Control	Description
Current Password	Specify the current password. If you are changing the password that ships with the product, leave the text box blank.
New Password	Specify a new password for the secure vault.
New Password Confirm	Confirm the new password for the secure vault.
Change Password	Changes the password for the secure vault.

4. Click **Save** to save your settings permanently.

Configuring Web settings

You can modify Management Console Web user interface settings in the Configure > Web Settings page. For information on managing Web SSL certificates, see "Managing web SSL certificates" on page 115.

To modify web settings

1. Choose Configure > Web Settings.
2. Under Web Settings, complete the configuration as described in this table.

Control	Description
Default Web Login ID	Specify the username that appears in the authentication page. The default value is admin.
Web Inactivity Timeout (minutes)	Specify the number of idle minutes before time-out. The default value is 15. A value of 0 disables time-out.
Allow Session Timeouts When Viewing Auto-Refreshing Pages	By default, session time-out is enabled, which stops the automatic updating of the report pages when the session times out. Clear the Allow box to disable the session time-out, remain logged-in indefinitely, and automatically refresh the report pages. Disabling this feature poses a security risk.

3. Click **Apply** to apply your changes to the running configuration.
4. Click **Save** to save your settings permanently.

Managing web SSL certificates

The AltaVault provides the following additional security features to manage SSL certificates used by the AltaVault Management Console Web user interface using HTTPS.

- Generate the certificate and key pairs on the AltaVault. This overwrites the existing certificate and key pair regardless of whether the previous certificate and key pair was self-signed or user added. The new self-signed certificate lasts for one year (365 days).
- Create certificate signing requests from the certificate and key pairs.
- Replace a signed certificate with one created by an administrator or generated by a third-party certificate authority.

For information on root certificates, see "Root certificates" on page 203.

To modify web SSL certificates

1. Choose Configure > Web Settings.
2. Under Web Certificate, select the Details tab.

The AltaVault identity certificate details appear, as described in this table.

Control	Description
Issued To/Issued By	Common Name - Specifies the common name of the certificate authority.
	Email - Specifies the email address of the contact person.
	Organization - Specifies the organization name (for example, the company).
	Locality - Specifies the city.
	State - Specifies the state.
	Country - Specifies the country.
Validity	Issued On - Specifies the date the certificate was issued.
	Expires On - Specifies the date the certificate expires.
Fingerprint	SHA1 - Specifies the SSL fingerprint.
Key	Type - Specifies the key type.
	Size - Specifies the size in bytes.

3. To import certificate and private key, under Web Certificate, select the Replace tab and complete the configuration as described in this table.

Control	Description
Import Certificate and Private Key	Select this option to import certificate and private key. Upload (PKCS-12, PEM or DER formats) - Select this option if the existing private key and CA-signed certificate are located in one file. The page displays a Private Key and CA-Signed Public Certificate control for browsing to the key and certificate files or a text box for copying and pasting the key and certificate. Paste it here (PEM only) - Select this option to paste the private key. Private Key - Select an option from the following: • This private is in a separate file (below) • This file includes the certificate and Private Key • The Private Key for this certificate was created with a CSR generated on this appliance
Separate Private Key	Upload (PEM or DER formats) - Select this option if the existing private key and CA-signed certificate are located in one file. The page displays a Private Key and CA-Signed Public Certificate control for browsing to the key and certificate files or a text box for copying and pasting the key and certificate. Click Browse to navigate to the file. Paste it here (PEM only) - Select this option to paste the private key. Decryption password - Specify the decryption password. It is required for PKCS-12 files.
Import Certificate and Key	Imports the new private key and self-signed public certificate.

4. To generate self-signed certificate and new private key, under Web Certificates, select the Replaces tab and complete the configuration as described in this table.

Control	Description
Organization Name	Specify the organization name (for example, the company).
Organization Unit Name	Specify the organization unit name (for example, the section or department).

Control	Description
Locality	Specify the city.
State	Specify the state. Do not abbreviate.
Country	Specify the country (2-letter code only).
Email Address	Specify the email address of the contact person.
Validity Period	Specify the validity period. You can select from 60 to 3650 days.
Cipher:RSA	Select the cipher from the drop-down list.
Generate CSR	Generates the Certificate Signing Request.

5. To generate a CSR, under Web Certificate, select the Generate CSR tab and complete the configuration as described in this table.

Control	Description
Common Name	Specify the common name.
Organization Name	Specify the organization name (for example, the company).
Organization Unit Name	Specify the organization unit name (for example, the section or department).
Locality	Specify the city.
State	Specify the state. Do not abbreviate.
Country	Specify the country (2-letter code only).
Email Address	Specify the email address of the contact person.
Generate CSR	Generates the Certificate Signing Request.

6. Click **Apply** to apply your changes to the running configuration.

7. Click **Save** to save your settings permanently.

8. To view PEM information, under Web Certificate, select the PEM tab.

Configuring KMIP

Key Management Interoperability Protocol (KMIP) is a standard describing communication between key management servers and their clients. AltaVault manages several important pieces of information that must be kept secure. These pieces include the datastore encryption key that encrypts user data and cloud credentials, which allow AltaVault to authenticate itself to the cloud provider. Without KMIP, these pieces of information are stored on a disk in an encrypted partition called the Secure Vault. They can also be exported in configuration archives. It is up to the user to keep these archives secure.

A user's environment may be running multiple AltaVault and other appliances or services which also require own encryption keys and other sensitive information. If each appliance or service manages their keys in an ad-hoc fashion, key management for the customer can become troublesome. This has led to development of key management servers (KMS), which can manage keys and other sensitive information in one place.

In order to support as many KMS vendors as possible, and to prevent being tied down to one or more proprietary protocols, AltaVault communicates with key management servers using an open protocol called KMIP.

During setup, the administrator specifies an external KMS to manage AltaVault's keys and cloud authentication parameters. The datastore encryption key and/or cloud authentication parameters will then be managed by the KMS.

AltaVault implements the following KMIP functionality:

- Registering keys with a KMS
- Fetching previously registered keys from a KMS

For other key management functionality, for example, searching for keys, deleting keys, and modifying properties on keys use the GUI provided by the Key Management Servers.

Note: Keys retrieved from a key server are never stored on a disk, only in memory. You cannot export keys from a key server.

Note: Note: If AltaVault uses KMIP, the KMS must be up in order for AltaVault to come up successfully.

This section includes:

- "Using the management console to configure KMIP"
- "Using CLI to configure KMIP"
- "Troubleshooting CLI"

Using the management console to configure KMIP

You can configure KMIP using the management console.

It includes the following sections:

- "To add a KMIP server" on page 118
- "To add KMIP keys" on page 119
- "To configure cloud settings" on page 119
- "To configure the encryption key" on page 120

To add a KMIP server

Before you add a KMIP server, check Web Settings page to verify that you have a certificate under the PEM tab.

1. Choose Configure > KMIP.
2. Under KMIP Servers, select Add a New Server and complete as described in the table.

Control	Description
Key Server Name	Specify the key server name.
Hostname	Specify the hostname of the server.
Port	Specify the port number.
Protocol Version	Select the protocol version from the drop-down list.
Username	Specify the username.

Control	Description
Password	Specify the password.
Upload CA Certificate	Select Browse to navigate to the CA certificate. The certificate must be a .pem file.
Add	Adds the KMIP server to the AltaVault. The KMIP server displays in the table below.
Remove Selected	Select a KMIP server and click **Remove Selected** to delete.This will result in AltaVault not using the key any longer. But the key will remain on the KMS. Deleting the key from the KMS has to be done through the UI provided by the KMS

3. Click Save.

To add KMIP keys

1. Under KMIP Keys, select Add a New Key and complete as described in the table.

Control	Description
Key Server Name	Select the key server name that was added earlier from the drop-down. If the server is not available, you must add the KMIP server.
Key Name	Specify the key name of the server.
Type	Select the type from the drop-down. **Secret Data** - Select this option to manage cloud authentication. **Symmetric Key** - Select this option to manage datastore encryption key. The selected key must be an AES-256 key.
Register Key	Select yes or no from the drop-down list. **Note:** Select yes only if this key does not exist on the server. Select no if the key already exists.
Key Data	Specify the cloud authentication parameters. This field displays only when the Register Key is set to Yes, and the Type is set to Secret Data.
UUID	Specify the UUID from your server. The UUID field displays only if the Register Key is set to No.
Add	Adds the KMIP keys to the AltaVault. The KMIP key displays in the table below.
Remove Selected	Select a KMIP key and click **Remove Selected** to delete.

2. Click Save.

To configure cloud settings

1. Choose Configure > Cloud Settings.
2. Select Cloud tab.
3. Select your cloud provider.
4. Select Yes from the Use Keys from KMIP Server drop-down list.
5. Select the correct secret data object names for each cloud authentication parameter (Access Key and Secret Key).

6. Click Save.

7. Select Maintenance > Service, and select Start to start the storage optimization service.

To configure the encryption key

1. Choose Configure > Cloud Settings.

2. Select Encryption tab.

3. Select yes from the drop-down list.

4. Select the symmetric key name that corresponds to the AES-256 key.

Using CLI to configure KMIP

You can use CLI to configure KMIP. For more information, see the *NetApp AltaVault Cloud Integrated Storage Command-Line Reference Guide* available on the NetApp Support at https://mysupport.netapp.com under the Documentation tab.

Troubleshooting CLI

KMIP CLI commands are executed in two situations: when the service comes up (most common) and when an object is registered with the server. When either one happens, there will be KMIP logs in the syslogs.

Example of a successful command

```
[mgmtd.INFO]: Executing KMIP command
[mgmtd.INFO]: KMIP request:
[mgmtd.INFO]: Tag: REQUEST_MESSAGE (0x420078), Type: STRUCTURE (0x01), Data:
[mgmtd.INFO]:   Tag: REQUEST_HEADER (0x420077), Type: STRUCTURE (0x01), Data:
[mgmtd.INFO]:     Tag: PROTOCOL_VERSION (0x420069), Type: STRUCTURE (0x01), Data:
[mgmtd.INFO]:       Tag: PROTOCOL_VERSION_MAJOR (0x42006a), Type: INTEGER (0x02), Data: 0x00000001
[mgmtd.INFO]:       Tag: PROTOCOL_VERSION_MINOR (0x42006b), Type: INTEGER (0x02), Data: 0x00000000
[mgmtd.INFO]:     Tag: AUTHENTICATION (0x42000c), Type: STRUCTURE (0x01), Data: null
[mgmtd.INFO]:       Tag: CREDENTIAL (0x420023), Type: STRUCTURE (0x01), Data: null
[mgmtd.INFO]:         Tag: CREDENTIAL_TYPE (0x420024), Type: ENUMERATION (0x05), Data: 0x00000001 (USERNAME_AND_PASSWC
[mgmtd.INFO]:         Tag: CREDENTIAL_VALUE (0x420025), Type: STRUCTURE (0x01), Data: null
[mgmtd.INFO]:           Tag: USERNAME (0x420099), Type: TEXT_STRING (0x07), Data: testuser
[mgmtd.INFO]:           Tag: PASSWORD (0x4200a1), Type: TEXT_STRING (0x07), Data: *********
[mgmtd.INFO]:     Tag: BATCH_COUNT (0x42000d), Type: INTEGER (0x02), Data: 0x00000001
[mgmtd.INFO]:   Tag: BATCH_ITEM (0x42000f), Type: STRUCTURE (0x01), Data:
[mgmtd.INFO]:     Tag: OPERATION (0x42005c), Type: ENUMERATION (0x05), Data: 0x0000000a (GET)
[mgmtd.INFO]:     Tag: REQUEST_PAYLOAD (0x420079), Type: STRUCTURE (0x01), Data:
[mgmtd.INFO]:       Tag: UNIQUE_IDENTIFIER (0x420094), Type: TEXT_STRING (0x07), Data: E39C6A6BF0E74E52DCA3CE1ABFBCD7C
4B2153F24041439E4A0C4EA5A0A
[mgmtd.INFO]:       Tag: KEY_FORMAT_TYPE (0x420042), Type: ENUMERATION (0x05), Data: 0x00000002 (OPAQUE)
[mgmtd.INFO]: KMIP response:
[mgmtd.INFO]: Tag: RESPONSE_MESSAGE (0x42007b), Type: STRUCTURE (0x01), Data:
[mgmtd.INFO]:   Tag: RESPONSE_HEADER (0x42007a), Type: STRUCTURE (0x01), Data:
[mgmtd.INFO]:     Tag: PROTOCOL_VERSION (0x420069), Type: STRUCTURE (0x01), Data:
[mgmtd.INFO]:       Tag: PROTOCOL_VERSION_MAJOR (0x42006a), Type: INTEGER (0x02), Data: 0x00000001
[mgmtd.INFO]:       Tag: PROTOCOL_VERSION_MINOR (0x42006b), Type: INTEGER (0x02), Data: 0x00000000
[mgmtd.INFO]:     Tag: TIME_STAMP (0x420092), Type: DATE_TIME (0x09), Data: 0x00000000560b08d1 Tue Sep 29 21:55:29 201
[mgmtd.INFO]:     Tag: BATCH_COUNT (0x42000d), Type: INTEGER (0x02), Data: 0x00000001
[mgmtd.INFO]:   Tag: BATCH_ITEM (0x42000f), Type: STRUCTURE (0x01), Data:
[mgmtd.INFO]:     Tag: OPERATION (0x42005c), Type: ENUMERATION (0x05), Data: 0x0000000a (GET)
[mgmtd.INFO]:     Tag: RESULT_STATUS (0x42007f), Type: ENUMERATION (0x05), Data: 0x00000000 (SUCCESS)
[mgmtd.INFO]:     Tag: RESPONSE_PAYLOAD (0x42007c), Type: STRUCTURE (0x01), Data:
[mgmtd.INFO]:       Tag: OBJECT_TYPE (0x420057), Type: ENUMERATION (0x05), Data: 0x00000007 (SECRET_DATA)
[mgmtd.INFO]:       Tag: UNIQUE_IDENTIFIER (0x420094), Type: TEXT_STRING (0x07), Data: E39C6A6BF0E74E52DCA3CE1ABFBCD7C
```

Example of an unsuccessful command

```
[mgmtd.INFO]: KMIP request:
[mgmtd.INFO]: Tag: REQUEST_MESSAGE (0x420078), Type: STRUCTURE (0x01), Data:
[mgmtd.INFO]:   Tag: REQUEST_HEADER (0x420077), Type: STRUCTURE (0x01), Data:
[mgmtd.INFO]:     Tag: PROTOCOL_VERSION (0x420069), Type: STRUCTURE (0x01), Data:
[mgmtd.INFO]:       Tag: PROTOCOL_VERSION_MAJOR (0x42006a), Type: INTEGER (0x02), Data: 0x00000001
[mgmtd.INFO]:       Tag: PROTOCOL_VERSION_MINOR (0x42006b), Type: INTEGER (0x02), Data: 0x00000000
[mgmtd.INFO]:     Tag: AUTHENTICATION (0x42000c), Type: STRUCTURE (0x01), Data: null
[mgmtd.INFO]:       Tag: CREDENTIAL (0x420023), Type: STRUCTURE (0x01), Data: null
[mgmtd.INFO]:         Tag: CREDENTIAL_TYPE (0x420024), Type: ENUMERATION (0x05), Data: 0x00000001 (USERNAME_AND_PASSWC
[mgmtd.INFO]:         Tag: CREDENTIAL_VALUE (0x420025), Type: STRUCTURE (0x01), Data: null
[mgmtd.INFO]:           Tag: USERNAME (0x420099), Type: TEXT_STRING (0x07), Data: testuser
[mgmtd.INFO]:           Tag: PASSWORD (0x4200a1), Type: TEXT_STRING (0x07), Data: ********
[mgmtd.INFO]:     Tag: BATCH_COUNT (0x42000d), Type: INTEGER (0x02), Data: 0x00000001
[mgmtd.INFO]:   Tag: BATCH_ITEM (0x42000f), Type: STRUCTURE (0x01), Data:
[mgmtd.INFO]:     Tag: OPERATION (0x42005c), Type: ENUMERATION (0x05), Data: 0x0000000a (GET)
[mgmtd.INFO]:     Tag: REQUEST_PAYLOAD (0x420079), Type: STRUCTURE (0x01), Data:
[mgmtd.INFO]:       Tag: UNIQUE_IDENTIFIER (0x420094), Type: TEXT_STRING (0x07), Data: asdf2
[mgmtd.INFO]:       Tag: KEY_FORMAT_TYPE (0x420042), Type: ENUMERATION (0x05), Data: 0x00000002 (OPAQUE)
[mgmtd.INFO]: KMIP response:
[mgmtd.INFO]: Tag: RESPONSE_MESSAGE (0x42007b), Type: STRUCTURE (0x01), Data:
[mgmtd.INFO]:   Tag: RESPONSE_HEADER (0x42007a), Type: STRUCTURE (0x01), Data:
[mgmtd.INFO]:     Tag: PROTOCOL_VERSION (0x420069), Type: STRUCTURE (0x01), Data:
[mgmtd.INFO]:       Tag: PROTOCOL_VERSION_MAJOR (0x42006a), Type: INTEGER (0x02), Data: 0x00000001
[mgmtd.INFO]:       Tag: PROTOCOL_VERSION_MINOR (0x42006b), Type: INTEGER (0x02), Data: 0x00000000
[mgmtd.INFO]:     Tag: TIME_STAMP (0x420092), Type: DATE_TIME (0x09), Data: 0x00000000561d66a2 Tue Oct 13 13:16:34 201
[mgmtd.INFO]:     Tag: BATCH_COUNT (0x42000d), Type: INTEGER (0x02), Data: 0x00000001
[mgmtd.INFO]:   Tag: BATCH_ITEM (0x42000f), Type: STRUCTURE (0x01), Data:
[mgmtd.INFO]:     Tag: OPERATION (0x42005c), Type: ENUMERATION (0x05), Data: 0x00000018 (QUERY)
[mgmtd.INFO]:     Tag: RESULT_STATUS (0x42007f), Type: ENUMERATION (0x05), Data: 0x00000001 (OPERATION_FAILED)
[mgmtd.INFO]:     Tag: RESULT_REASON (0x42007e), Type: ENUMERATION (0x05), Data: 0x00000003 (AUTHENTICATION_NOT_SUCCES
[mgmtd.INFO]:     Tag: RESULT_MESSAGE (0x42007d), Type: TEXT_STRING (0x07), Data: Authentication failed
[mgmtd.WARNING]: KMIP command returned OPERATION_FAILED, reason: AUTHENTICATION_NOT_SUCCESSFUL, message: Authenticatic
```

Example of an unsuccessful command (failure to connect)

```
[mgmtd.INFO]: [SSL_connect:before/connect initialization]
[mgmtd.INFO]: [SSL_connect:error in SSLv2/v3 write client hello B]
[mgmtd.INFO]: 140013611939528:error:2006A066:BIO routines:BIO_get_host_ip:bad hostname lookup:b_sock.c:146:host=null
[mgmtd.WARNING]: KMIP command returned IO, message: I/O Error
```

Common Errors

An authentication error could be caused the following:

- Incorrect username or password
- Incorrect client certificate.
- Misconfigured certificates.

Configuring appliance monitoring

You can set up any AltaVault as the monitoring master appliance that monitors peer AltaVaults. The AltaVault uses REST APIs that you can access to set up peer appliance monitoring.

After you configure REST API access and add the API access code for the monitored appliance, the Appliance Monitoring report enables you to view the health status, disk space, and cloud service status of the AltaVault.

The monitoring appliance probes the monitored peer appliances every 60 seconds by default.

To configure REST API Access

When you add an appliance to be monitored by the AltaVault, you must generate an API access code to enable authenticated communication between the monitoring master appliance and the monitored peer appliance.

1. Log in to the monitored AltaVault appliance.
2. Choose Configure > REST API Access.
3. To enable access to the REST APIs, under REST API Access Settings, select the Enable REST API Access check box.
4. Click **Apply**.
5. Complete the configuration as described in the table.

Control	Description
Add Access Code	Displays the controls to generate the API access code.
Description of Use	Specify a clear description of the monitoring appliance such as the hostname or IP address of the monitoring master appliance and a description such as “monitoring appliance.”
Generate New Access Code	Generates the new access code.
Use Existing Access Code	Select to use an existing REST API access code. When you are monitoring multiple appliances, you can use the same access code instead of creating a new one for each appliance.
Add	Adds the API access code to the AltaVault.
Remove Selected	Select an access code description from the table below and click **Remove Selected** to delete the selected REST API access code.

   The added access code description appears in the Access Code Description table, along with the name of the user who created it.

6. Click the **Access Code Description**.
7. Copy the Access Code from the text field into a text editor, such as Notepad.

To specify the API access code in the monitoring appliance

1. Log in to the monitoring AltaVault appliance.
2. Choose Reports > Appliance Monitoring.
3. Complete the configuration as described in this table.

Control	Description
Add Monitored Peer	Displays the controls to add a monitored appliance.
Hostname or IP address	Specify a valid hostname or IP address for the monitored appliance.
API Access Code	Specify the API access code that you obtained from the monitored appliance as specified in "To configure REST API Access" on page 122.
Add	Adds the API access code to the AltaVault appliance.
Remove Selected Appliances	Select an access code from the table below and click **Remove Selected Appliances** to delete the selected REST API access code.

4. Click **Save**.

Configuring a management ACL

You can secure access to the AltaVault using an internal management Access Control List (ACL) in the Configure > Management ACL page. For information on the ACL rules, see "ACL Management Rules" on page 124.

AltaVaults are subject to the network policies defined by a corporate security policy, particularly in large networks.

Using an internal management ACL, you can:

- restrict access to certain interfaces or protocols of an appliance.
- restrict inbound IP access to the AltaVault, protecting it from access by hosts that do not have permission without using a separate device (such as a router or firewall).
- specify which hosts or groups of hosts can access and manage the AltaVault by IP address, simplifying the integration of AltaVaults into your network.

The Management ACL provides the following safeguards to prevent accidental disconnection from the AltaVault:

- It detects the IP address you are connecting from and displays a warning if you add a rule that denies connections to that address.
- It converts well-known port and protocol combinations such as SSH, Telnet, HTTP, HTTPS, SNMP, and SOAP into their default management service and protects these services from disconnection. For example, if you specify protocol 6 (TCP) and port 22, the management ACL converts this port and protocol combination into SSH and protects it from denial.
- It tracks changes to default service ports and automatically updates any references to changed ports in the access rules.

To set up a management ACL

1. Choose Configure > Management ACL.

2. Under Management ACL Settings, complete the configuration as described in this table.

Control	Description
Enable Management ACL	Select the check box to secure access to a AltaVault using a management ACL.

3. Click **Apply** to apply your changes to the running configuration.

4. Click **Save** to save your settings permanently.

   If you add, delete, edit, or move a rule that could disconnect connections to the AltaVault, a warning message appears. Click **Confirm** to override the warning and allow the rule definition anyway. Use caution when overriding a disconnect warning.

ACL Management Rules

The management ACL contains rules that define a match condition for an inbound IP packet. You set a rule to allow or deny access to a matching inbound IP packet. When you add a rule on a AltaVault, the destination specifies the AltaVault itself, and the source specifies a remote host.

To add an ACL management rule

1. Choose Configure > Management ACL.

2. Under Add a new rule, complete the configuration as described in this table.

Control	Description
Add a New Rule	Displays the controls for adding a new rule.
Action	Select one of the following rule types from the drop-down list: • **Allow** - Allows a matching packet access to the AltaVault. This is the default action. • **Deny** - Denies access to any matching packets.
Service	Optionally, select Specify Protocol, or HTTP, HTTPS, SOAP, SNMP, SSH, Telnet. When specified, the Destination Port is dimmed and unavailable.
Protocol	(Appears only when Service is set to Specify Protocol.) Optionally, select All, TCP, UDP, or ICMP from the drop-down list. The default setting is All. When set to All or ICMP, the Service and Destination Ports are dimmed and unavailable.
Source Network	Optionally, specify the source subnet of the inbound packet. For example, 1.2.3.0/24.
Destination Port	Optionally, specify the destination port of the inbound packet, either a single port value or a port range of port1-port2, where port1 must be less than port2. Leave it blank to specify all ports.
Interface	Optionally, select an interface name from the drop-down list. Select All to specify all interfaces.
Description	Optionally, describe the rule to facilitate administration.
Rule Number	Optionally, select a rule number from the drop-down list. By default, the rule goes to the end of the table (just above the default rule). AltaVaults evaluate rules in numerical order starting with rule **1**. If the conditions set in the rule match, then the rule is applied, and the system moves on to the next packet. If the conditions set in the rule do not match, the system consults the next rule. For example, if the conditions of rule 1 do not match, rule 2 is consulted. If rule 2 matches the conditions, it is applied, and no further rules are consulted. The default rule, Allow, which allows all remaining traffic from everywhere that has not been selected by another rule, cannot be removed and is always listed last.
Log Packets	Tracks denied packets in the log. By default, packet logging is enabled.
Add	Adds the rule to the list. The Management Console redisplays the Rules table and applies your modifications to the running configuration, which is stored in memory.
Remove Selected	Select the check box next to the name and click **Remove Selected**.
Move Selected	Moves the selected rules. Click the arrow next to the desired rule position; the rule moves to the new position.

3. Click **Save** to save your settings permanently.

Configuring SSH Access

AltaVault supports SSH access to the management port of the appliance. SSH access can be done using either user credentials (username/password) or the client public key. This section describes how to use AltaVault CLI commands to the configure SSH access using public keys.

To enable SSH access via public key

1. Log in to the AltaVault with the login name and password.
2. At the user prompt, enter the enable command:

```
> enable
```

3. At the enable mode prompt, enter the configuration mode command:

```
# configure terminal
```

4. At the configuration mode prompt, enter following SSH command:

```
(config)# ssh server user <username> authorized-key <authorized-key>
```

For example:

```
config) # ssh server user admin authorized-key "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC7ZCATT6tD3t5JmS276WzIJpVoPn+0ReCbRThpyh/2Glsv346
XV3Odz1954gd2n1kpeMckt7iSv6EgF2oGWMPE1h9tiCY5PKumZsT7bwQ94Y8IML+ZsldggVDOqRXRyXsInAm0hLCOFp3Ux
g4SUxjcTwJM82ZP6jTSMLVjxWJhZKqJLzQpsUgv0BuAaQWdeS6vyNmgxfm+Fpv4Ov2o376sPSmnEPodkyGnXTnn1JoQPH0
ICrrwt8of6IxObKH9HEBUaO94qZ+XLT+7SM6s9j4uR53KON8DnHNkntpGFDmR9hL6Krg9KWVCOb7Z0amNDk1p4y4bOkcMk
AXMm+v6ldT user@example.com"
```

To disable SSH access using public key

To delete an authorized public key (disabling SSH access for a given user), enter the index number of the public key. For example, the first key added would have index value 1.

```
CLI (config) # no ssh server user admin authorized-key 1
```

CHAPTER 8 Viewing reports and logs

This section describes how to display and view reports and logs. It includes the following sections:

- "About reports" on page 128
- "Viewing the storage optimization report" on page 131
- "Viewing the front-end throughput report" on page 132
- "Viewing the back-end throughput report" on page 134
- "Viewing the eviction report" on page 135
- "Viewing the replication report" on page 136
- "Viewing the cloud operations report" on page 137
- "Viewing schedule reports" on page 138
- "Viewing per share utilization reports" on page 139
- "Viewing the alarm status report" on page 140
- "Viewing the CPU utilization report" on page 144
- "Viewing the memory paging report" on page 145
- "Viewing the interface counters report" on page 146
- "Viewing the disk throughput report" on page 147
- "Viewing the disk IOPS report" on page 148
- "Viewing the disk utilization report" on page 148
- "Viewing logs" on page 149
- "Downloading log files" on page 151
- "Generating system dumps" on page 152
- "Viewing process dumps" on page 153
- "Capturing and uploading TCP dumps" on page 153
- "Viewing the appliance monitoring report" on page 159
- "Viewing the shelf details" on page 161
- "Viewing the storage RAID group" on page 162

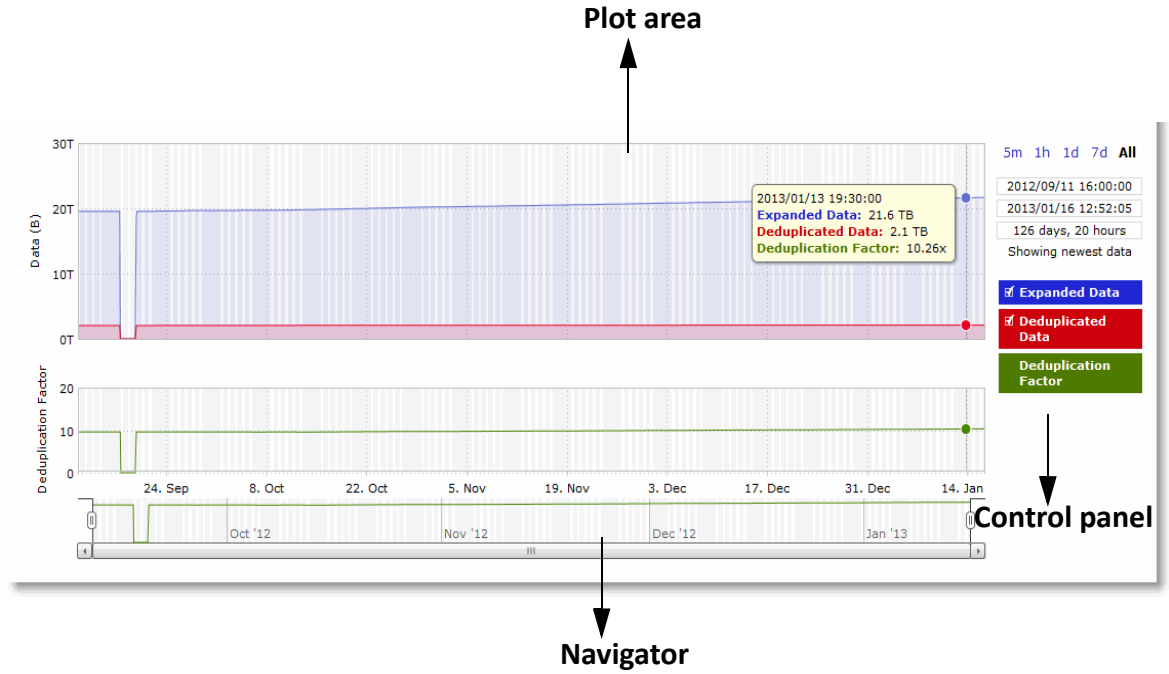
About reports

In AltaVault all of the time-series reports have a look and feel that is clear, interactive, and easy to navigate. The statistics presented in this improved report format are readily accessible, and all updates to the report window appear in real time. This section describes the new report format in detail.

Navigating the report layout

The AltaVault report format not only makes data easily accessible, but also enhances your ability to explore data in context. An example of a typical report is shown in Figure 8-1, with the key areas labeled. For details about individual reports, see the report description.

Figure 8-1. Report layout



The report sections, going counter-clockwise from the top-left of the report window shown in Figure 8-1, are:

- Plot area
- Navigator
- Control panel

The summary tables, which appeared under the graphs in the legacy report style, have been removed. The summary statistics appear in the control panel legend.

Plot area

The plot area is where data visualization occurs. Reports can display either a single-pane or dual-pane layout. In a dual-pane layout, both panes remain synchronized with respect to the x-axis. Each pane is capable of having two y-axes (a primary one on the left and a secondary one on the right).

The reports present the majority of data series as simple line series graphs, but some reports display area series graphs where appropriate. The types of area series graphs are:

- **Layered series**, which appear on top of each other in the z direction. These are identified by transparent colors.
- **Stacked area series**, which appear on top of each other in the y direction. The AltaVault uses stacked area graphs to depict an aggregate broken down by its constituent parts. In this type of graph, each series is a mutually exclusive partition of some aggregate data set, identified by opaque colors. A stacked series is appropriate when the sum of all the series is meaningful.

The report format enables you to hover over individual data points to view this information, obviating the need to display a peak line or arrows over peaks.

To view the timestamp and value of each data series at that time

- Place the mouse pointer over the plot area.

A tool tip displays the timestamp and the value of each data series at that time. The plot area colors the series names appropriately, and the data values have their associated units.

The plot area also displays subtle shading to denote work hours (white background) and nonwork hours (gray background). The AltaVault defines work hours as 8:00 AM to 5:00 PM on weekdays. You cannot configure the work hours.

To zoom the plot area

- Place the mouse pointer over the plot area, and then turn the mouse wheel. Scroll forward to zoom in and scroll backward to zoom out.

The plot area reflects the changing chart window, as do the associated controls in the control panel.

To pan the plot area

1. Place the mouse pointer over the plot area, and then click and hold the left mouse button.
2. Move the mouse left or right to slide the window of visible data left or right.

The navigator reflects the changing chart window as do the associated controls in the control panel.

Navigator

Directly above the scroll bar is the navigator, which shows a much smaller and simpler display of the data in the plot area. The navigator displays only one data series.

Use the navigator to navigate the entire range of chart data. The scroll bar at the bottom displays which portion of the total data range is currently displayed in the plot area.

The navigator display can appear very different than the plot area display when an interesting or eye-catching series in the plot area is not the series in the navigator.

To resize the current chart window

- Move the handles on either side of the chart window in the navigator.

The charts have a minimum chart window size (currently five minutes), so if you try to resize the chart window to something smaller, the chart window springs back to the minimum size.

You can also click the data display portion of the navigator (not the scroll bar) and the chart window moves to wherever you clicked.

Control panel

Use the control panel to control how much data the chart displays, to see chart properties, and to view or hide the summary statistics.

To change the chart interval

- Click a link: 5m (five minutes), 1h (one hour), 1d (one day), 1w (seven days), or All (all data). All includes statistics that have been retained for the last 30 days.

  If the current size of the chart window matches any of the links, the link appears in bold black text; the system ignores any clicks on that link. If the time duration represented by any of the links is greater than the total data range of the chart, those links are dimmed and unavailable.

- **Chart window controls** - More window-related controls appear below the chart window interval links. These controls offer more precise control of the window and also display various window properties. From top to bottom, the controls are:

  - Text field containing the left edge (starting time) of the chart window.
  - Text field containing the right edge (ending time) of the chart window.
  - Text field containing the chart window interval. The chart window interval in this text field is not always exactly correct, but it is correct to two units (with the units being days, hours, minutes, and seconds). For example, if the chart window interval is exactly two days, three hours, four minutes, and five seconds, this text field displays 2 days, 3 hours.
  - Link or static text that represents the chart window state of *attachment* to the end of the chart. When the chart window is attached, the report replaces the link with the static text **Showing newest data**. When the chart is showing newest data, you can see new data points as the system adds them automatically to the chart every 10 seconds. This can be very powerful when you launch a new configuration and need to analyze its impact quickly. You cannot change the 10-second default.

    When the chart window is not attached to the end of the chart, the report replaces the static text with a link that displays **Show newest data**. Click this link to slide the chart window to the end of the chart range of data and attach the window.

All three text fields validate your input; if you enter text in an invalid format, a text field with light red background color displays. If you enter valid text that is logically invalid (for example, an end time that comes before the current start time), a text field with light red background color displays. With all three text fields, if the focus leaves the field (either because you click outside the field or press the Tab key), the chart window updates immediately with the new value. Pressing Enter while in one of these fields removes the focus.

Custom controls

Below the chart window controls is an optional section of custom, report-specific controls. The custom controls vary for each report. In Figure 8-1, the Bandwidth Optimization report displays Port and Direction drop-down lists.

When you change the value of a custom control, the system sends a new request for data to the server. During this time, the control panel is unavailable and an updating message appears on the chart. When the report receives a response, the system replaces the chart, populates it with the new data, and makes the control panel available again.

Chart legend

The chart legend correlates the data series names with line colors and contains a few other features.

You can hide and show individual data series. When a white check box icon appears next to the data series name, you can hide the series from the plot area.

To hide individual series from the plot area

- Clear the check box next to the data series name.

To display individual series in the plot area

- Select the check box next to the data series name.

You cannot toggle the visibility of all series, because it does not always make sense to hide a series (for example, if there is only one data series in the chart). For these series, a white check box does not appear next to the series name. In Figure 8-1, you can hide the LAN Throughput and WAN Throughput series, but you cannot hide the Data Reduction series.

The legend also displays statistics. Each report defines any number of statistics for any of the data series in the chart. The system bases the statistics computation on the subset of each data series that is visible in the current chart window. The statistics display changes as the chart window changes. The reports also support nonseries statistics (for example, composite statistics that incorporate the data from multiple data series); these statistics (not pictured in Figure 8-1) appear at the very bottom of the legend, below all the series.

Setting user preferences

You can change report default settings to match your preferred style. When you customize any report-specific settings, the system immediately writes them to disk on the AltaVault. The system saves all of your custom settings, even after you log out, clear your browsing history, or close the browser. When you view the report again, the custom settings are intact.

The system saves report settings on a per-user basis. A message appears at the top of each page when multiple users are logged in explaining that user preferences might be overwritten.

The system also saves the chart window. Whenever you change the chart window, the next time you view any report, the chart window is set to the last chart window used.

Browser recommendation and printing reports

If your browser is not supported, the login screen displays a message

To print a report, choose File > Print in your Web browser to open the Print dialog box.

Viewing the storage optimization report

The Storage Optimization report is the same report that appears on the home page of the AltaVault Management Console. It summarizes the percentage of the data storage optimized within the time period specified. It includes the following statistics that describe the storage optimization activity for the time period you specify.

Field	Description
Expanded Data	Data that has been backed up locally by the AltaVault.
Deduplicated Data	Current data deduplicated by the AltaVault and sent to the cloud. Deduplication is a method of reducing storage space by eliminating redundant data. It stores only one unique instance of the data. It replaces redundant data with a pointer to the unique data copy.
Deduplication Factor	Ratio of the expanded data and total optimized data. The total optimized data includes both deduplication and compression savings.

The Storage Optimization report answers the following questions:

- What is the latest user data stored?
- What is the latest amount of deduplicated data stored?
- What is the deduplication factor (ratio of user data and deduplicated data)?

To view the Storage Optimization report

1. Choose Reports > Storage Optimization.
2. Use the controls to customize the report as described in this table.

Control	Description
Period	Select the time period from the drop-down list. For Custom, enter the Start Time and End Time and click **Go**. Use the following format: YYYY/MM/DD HH:MM:SS.
Refresh	Select a refresh rate from the drop-down list. To turn refresh off, click **Off**.
Go	Displays the report.

Viewing the front-end throughput report

The Front-End Throughput report summarizes the front-end (SMB/NFS/OST) data read into and written out of the AltaVault within the time period specified. The front-end data is sent from your local servers or backup software to AltaVault.

This report includes the following statistics that describe the storage optimization activity for the time period you specify.

Field	Description
Front-End In	
Average	Average front-end (SMB/NFS/OST) data that the backup server writes to the AltaVault.
Total Data	Total data transferred from the backup server to the AltaVault
Front-End Out	
Average	Average front-end (SMB/NFS/OST) data read by the backup server.
Total Data	Total data transferred from the front-end SM, NFS, or OST system to the backup server.

The Front-End Throughput report answers the following questions:

- What is the average front-end (SMB/NFS/OST) data that the backup server writes to the AltaVault?
- What is the total amount of data transferred from the backup server to the AltaVault?
- What is the average front-end (SMB/NFS/OST) data read by the backup server?
- What was the peak amount of data transmitted?

To view the Front-End Throughput Optimization report

1. Choose Reports > Front-End Throughput.

2. Use the controls in the control panel to customize the report as described in this table.

Control	Description
5m 1h 1d 1w All	Select one of the following report time intervals to filter the display: • 5m - Displays five minutes of data. • 1h - Displays one hour of data. • 1d - Displays one day of data. • 1w - Displays one week of data. • All - Displays all data available for the past 30 days. To type a custom time interval, enter the start time and end time (using the format YYYY/MM/DD HH:MM:SS) in the text field. You can view the newest data and see data points as they are added to the chart dynamically.
Show newest data	Click this option to display only the latest data available. The latest data available depends on the time interval that you specify. For example, if 1h is the specified time interval, then clicking Show newest data displays the last 60 minutes of data.

Viewing the back-end throughput report

The Back-End Throughput report summarizes the back-end cloud data read by and written out of the AltaVault within the time period specified. The back-end data is data that the AltaVault sends to the cloud.

This report includes the following statistics that describe the storage optimization activity for the time period you specify.

Field	Description
Back-End In	
Average	Average back-end data read from the cloud by the AltaVault
Total Data	Total data transferred from the cloud to the AltaVault
Back-End Out	
Average	Average back-end data that the AltaVault writes to the cloud
Total Data	Total data transferred from the AltaVault to the cloud

The Back-End Throughput report answers the following questions:

- What is the average back-end data read from the cloud by the AltaVault?
- What is the total amount of back-end data transferred from the cloud to the AltaVault?
- What is the average back-end data that the AltaVault writes to the cloud?
- What was the peak amount of data transmitted?

To view the Back-End Throughput Optimization report

1. Choose Reports > Back-End Throughput.

2. Use the controls in the control panel to customize the report as described in this table.

Control	Description
5m 1h 1d 1w All	Select one of the following report time intervals to filter the display: • 5m - Displays five minutes of data. • 1h - Displays one hour of data. • 1d - Displays one day of data. • 1w - Displays one week of data. • All - Displays all data available for the past 30 days. To type a custom time interval, enter the start time and end time (using the format YYYY/MM/DD HH:MM:SS) in the text field. You can view the newest data and see data points as they are added to the chart dynamically.
Show newest data	Click this option to display only the latest data available. The latest data available depends on the time interval that you specify. For example, if 1h is the specified time interval, then clicking Show newest data displays the last 60 minutes of data.

Viewing the eviction report

The Eviction report summarizes the evicted bytes and the age of the data leaving the AltaVault local storage disk within the time period specified. The report first displays the available data cache, which is the amount of free space available locally on the AltaVault data store. It also displays the amount of data in bytes that has been evicted from the local AltaVault data store to make space for the new deduplicated data. The second graph shows the average age of data evicted from the AltaVault.

The Eviction reports includes the following statistics that describe the eviction optimization activity for the time period you specify.

Field	Description
Evicted Data	Evicted bytes are the amount of data forced out from the local storage disk because the AltaVault needs to store new deduplicated data on the disk and disk space is insufficient.
Eviction Age	Average value of the data (calculated using the date and time it was created) leaving the AltaVault local storage disk.

The Eviction report answers the following questions:

- How much data is forced out from the AltaVault local disk?
- What is the average of the most recent data (calculated using the date and time it was created) leaving the AltaVault local storage disk?

To view the Eviction report

1. Choose Reports > Eviction.

2. Use the controls in the control panel to customize the report as described in this table.

Control	Description
5m 1h 1d 1w All	Select one of the following report time intervals to filter the display: • 5m - Displays five minutes of data. • 1h - Displays one hour of data. • 1d - Displays one day of data. • 1w - Displays one week of data. • All - Displays all data available for the past 30 days. To type a custom time interval, enter the start time and end time (using the format YYYY/MM/DD HH:MM:SS) in the text field. You can view the newest data and see data points as they are added to the chart dynamically.
Show newest data	Click this option to display only the latest data available. The latest data available depends on the time interval that you specify. For example, if 1h is the specified time interval, then clicking Show newest data displays the last 60 minutes of data.

Viewing the replication report

When you back up data into the AltaVault, it writes data on to its disks and also replicates the data in the cloud. The Replication report shows how much data is currently waiting to be replicated to the cloud and the time and date the cloud was last synchronized.

The Replication report displays the following statistics.

Field	Description
Data Pending Replication	Amount of data that is currently waiting to be replicated to the cloud.
Time to complete replication	Estimated time for replication to complete.
Cloud Synchronized Until	Data ingested up to this time has been replicated to the cloud.

The Replication report answers the following questions:

- How many bytes to be replicated in the cloud are pending?
- What is the estimated time for replication to complete?
- How much data ingested until the specified time is replicated to the cloud?

To view the Replication report

1. Choose Reports > Replication.

2. Use the controls in the control panel to customize the report as described in this table.

Control	Description
5m 1h 1d 1w All	Select one of the following report time intervals to filter the display: • 5m - Displays five minutes of data. • 1h - Displays one hour of data. • 1d - Displays one day of data. • 1w - Displays one week of data. • All - Displays all data available for the past 30 days. To type a custom time interval, enter the start time and end time (using the format YYYY/MM/DD HH:MM:SS) in the text field. You can view the newest data and see data points as they are added to the chart dynamically.
Show newest data	Click this option to display only the latest data available. The latest data available depends on the time interval that you specify. For example, if 1h is the specified time interval, then clicking **Show newest data** displays the last 60 minutes of data.

Viewing the cloud operations report

The Cloud Operations report provides statistics about the total put, head, post, get, and delete operations to and from the cloud.

The Cloud Operations report provides only the main operation statistics and does not completely cover all statistics. Do not use the Cloud Operations report to measure the number of cloud operations issued. Use the cloud provider statistics for cloud cost computations.

The Cloud Operations report displays the following statistics.

Field	Description
Put Operations	The number of HTTP operations to upload a file in the cloud.
Head Operations	The number of HTTP operations that return only the meta-information in the HTTP headers; they do not return a message-body in the response.
Post Operations	The number of HTTP post operations that have been communicated to the cloud.
Get Operations	The number of HTTP get operations performed to download files from the cloud.
Delete Operations	The number of files deleted in the cloud.

The Cloud Operations report answers the following questions:

- What are the total put operations?
- What are the total head operations?
- What are the total post operations?
- What are the total get operations?
- What are the total delete operations?

To view the Cloud Operations report

1. Choose Reports > Cloud Operations.
2. Use the controls in the control panel to customize the report as described in this table.

Control	Description
5m 1h 1d 1w All	Select one of the following report time intervals to filter the display: • 5m - Displays five minutes of data. • 1h - Displays one hour of data. • 1d - Displays one day of data. • 1w - Displays one week of data. • All - Displays all data available for the past 30 days. To type a custom time interval, enter the start time and end time (using the format YYYY/MM/DD HH:MM:SS) in the text field. You can view the newest data and see data points as they are added to the chart dynamically.
Show newest data	Click this option to display only the latest data available. The latest data available depends on the time interval that you specify. For example, if 1h is the specified time interval, then clicking **Show newest data** displays the last 60 minutes of data.

Viewing schedule reports

The AltaVault emails you scheduled reports that contain information such as the hostname, model number, serial number, version, uptime, and statistics related to storage optimization, replicated data, disk storage allocation, and cloud storage allocation that display in the Schedule Reports page.

Use the Schedule Reports page to configure whether the emails should be sent on a weekly or a monthly basis.

The Schedule Reports answer the following questions:

- What is the hostname of the AltaVault?
- What is the model name of the AltaVault?
- What is the AltaVault serial number?
- What is the AltaVault software version?
- What is the date on which the report was sent?
- What is the AltaVault up time?
- What is the expanded data in the AltaVault?
- What is the AltaVault deduplicated data?
- What is the deduplication factor (ratio of the expanded data and the deduplicated data)?
- How much data is replicated to the cloud?
- What is the time to complete replication?
- What are the pending replication bytes?
- How much disk storage is used?
- How much disk storage is free?

- What is the total disk storage?
- How much cloud storage has been used?
- What is the total cloud storage?

To configure Schedule Reports

1. Choose Configure > Schedule Reports.
2. Under Schedule AltaVault Reports via Email, use the controls in the control panel to customize the report as described in this table.

Control	Description
Enable Scheduling	Select this check box for the AltaVault to email scheduled reports.
Weekly	Select this check box to schedule weekly reports and then specify the day of the week on which the AltaVault must email the report.
Monthly	Select this check box to schedule monthly reports and then specify the day of the month and time at which the AltaVault must email the report.

If you do not specify a weekly or monthly schedule, the AltaVault automatically emails reports daily at the selected time.

3. Click **Apply** to apply your changes to the running configuration.
4. Click **Save** to save your configuration.

Viewing per share utilization reports

The AltaVault emails you Share Utilization reports that contain information such as the hostname, model number, serial number, version, date, uptime, and evicted percentage.

The Share Utilization reports answer the following questions:

- What is the hostname of the AltaVault?
- What is the model name of the AltaVault?
- What is the AltaVault serial number?
- What is the AltaVault software version?
- What is the date on which the report was sent?
- What is the AltaVault up time?
- What is the evicted percentage?

To configure and view Share Utilization report

1. Choose Configure > Email.

The system sends an email to all email addresses on the Configure > Email page appearing under Report Events via Email. The email notifies users that the trigger has fired.

2. To generate share statistics, use the following CLI command:

```
share-stats generate
```

Viewing the alarm status report

The Alarm Status report takes a current snapshot of the system to provide a single report you can use to check for any issues with the AltaVault. The report examines key system components. For example, the CPU and memory. Use this report to gather preliminary system information before calling NetApp Support to troubleshoot an issue.

Alarm	Description
Admission Control	Indicates that AltaVault has entered the admission control state. Admission control limits the number of connections made to the AltaVault, so that you do not over-consume resources on your system.
Cloud Bucket Consistency	Indicates that there is data in the cloud, although the AltaVault datastore is empty. Enable replication and recovery to ensure that the cloud storage is synchronized with the datastore.
Cloud Bucket Disparity	Indicates that the cloud bucket that the AltaVault is trying to connect to might be in use by another AltaVault. This prevents corruption of the files in the cloud.
Cloud Bucket Over Capacity	Indicates that the cloud bucket size is greater than the licensed amount of cloud capacity that you are using. You must upgrade to a higher-capacity license.
CPU Utilization	Indicates that the system has reached the CPU threshold for one or more of the CPUs in the AltaVault. If the system has reached the CPU threshold, check and adjust your settings as appropriate. If your alarm thresholds are set appropriately, and the CPU utilization remains high, contact technical support for assistance.
Data Integrity Error	Indicates that there was an inconsistency in the data stored on disk.
Datastore Eviction	Indicates that the system has detected an issue with datastore eviction. The alarm triggers when the appliance has started evicting data from the local disk cache when the age of the evicted data is relatively young. An AltaVault has disk space much smaller than the total addressable space on the cloud, and if disk space runs low, the appliance starts evicting data from disk that has not been used recently. This keeps only fresh and frequently accessed data in cache. The AltaVault keeps statistics about how old the evicting data is (this is the average evicted age). Usually, only old data is evicted. This behavior is generally not a problem and does not trigger an alarm. However, the appliance might be experiencing such a huge workload that more and more recent data needs to be evicted from the appliance to make space for incoming data. This causes the average evicted age to decrease, and when it goes below a certain threshold, the average evicted age alarm triggers. This alarm is an anomalous event because it signals that the appliance is handling a much larger workload than expected. The alarm is useful in detecting whether the appliance is undersized relative to the your normal workload. If the alarm is constantly triggered, then you should consider moving your data to a larger AltaVault model with a larger disk cache.
Datastore Low Space	Indicates that the local data store (disk cache on the AltaVault) is running out of space and the eviction process on the AltaVault is unable to run at a sufficient pace to create space on the disk cache. This alarm might trigger when replication is too slow. View the Eviction Optimization report to determine how much disk cache is available.

Alarm	Description
Disk Full	Enables an alarm if the system partitions (not the AltaVault data store) are full or almost full. For example, AltaVault monitors the available space on the directory that contains logs, statistics, system dumps, and TCP dumps. By default, this alarm is enabled. This alarm monitors the following system partitions: • Directory "/boot" free space • Directory "/bootmgr" free space • Directory "/config" free space • Directory “/tmpFull” • Directory “/var Full”
Hardware	Fan Error - Indicates that the system has detected a problem with the fans. Fans for many systems can be replaced. Contact NetApp Support at https://mysupport.netapp.com and file a trouble ticket to order a replacement fan.
	IPMI - Indicates that there has been a physical security intrusion, triggering an Intelligent Platform Management Interface (IPMI) error. The following events trigger the IPMI alarm: • Chassis intrusion (physical opening and closing of the appliance case) • Memory errors (ECC memory errors that can or cannot be corrected) • Hard drive faults or predictive failures • Power supply status or predictive failures The option to reset the alarm appears only after the service triggers the IPMI alarm. To reset the alarm, click **Clear the IPMI alarm now**.
Inconsistent Cloud Connectivity	Indicates that the connection to the cloud provider is inconsistent, leading to a large number of connection errors.
Inconsistent Cloud Data	Indicates that an inconsistency in the data stored in the cloud was detected.
Licensing	Indicates that your appliance does not have a valid license. • Evaluation Mode Expire - Evaluation mode license expired. • License Expired - A license expired. • License Expiring - A license will expire. • License Missing - A license is missing.
Link Duplex	Indicates that an interface is not configured for half-duplex negotiation but has negotiated half-duplex mode. Half-duplex significantly limits the optimization service results. The alarm displays which interface is triggering the duplex error. Choose Configure > Data Interfaces and examine the AltaVault link configuration. Next, examine the peer switch user interface to check its link configuration. If the configuration on one side is different from the other, traffic is sent at different rates on each side, causing many collisions. To troubleshoot, change both interfaces to automatic duplex negotiation. If the interfaces do not support automatic duplex, configure both ends for full duplex. You can enable or disable the alarm for a specific interface. To disable an alarm, choose Configure > Alarms and select or clear the check box next to the link alarm.

Alarm	Description
Link I/O Errors	Indicates that the error rate on an interface has exceeded 0.1% while either sending or receiving packets. This threshold is based on the observation that even a small link error rate reduces TCP throughput significantly. A properly configured connection experiences very few errors. The alarm clears when the error rate drops below 0.05%. You can change the default alarm thresholds by entering the **alarm link_errors err-threshold *xxxxx*** CLI command at the system prompt. For details, see the *NetApp AltaVault Cloud Integrated Storage Command-Line Interface Reference Guide*. To troubleshoot, try a new cable and a different switch port. Another possible cause is electromagnetic noise nearby. You can enable or disable the alarm for a specific interface. For example, you can disable the alarm for a link after deciding to tolerate the errors. To enable or disable an alarm, choose Configure > Alarms and select or clear the check box next to the link name.
Link State	Indicates that the system has detected a link that is down. You are notified through SNMP traps, email, and alarm status. The system has lost one of its Ethernet links due to an unplugged cable or dead switch port. Check the physical connectivity between the AltaVault and its neighbor device. Investigate this alarm as soon as possible. Depending on what link is down, the system might no longer be optimizing and a network outage could occur. You can enable or disable the alarm for a specific interface. To enable or disable the alarm, choose Configure > Alarms and select or clear the check box next to the link name.
Low Memory	Indicates that low memory exists.
Max inodes limit	Indicates that the maximum number of files that can be stored has been reached.
Max Pinnable Limit	Indicates that the maximum pinnable limit gas been reached.
Memory Paging	Indicates that the system has reached the memory paging threshold. If 100 pages are swapped approximately every two hours, the AltaVault is functioning properly. If thousands of pages are swapped every few minutes, then reboot the AltaVault. If rebooting does not solve the problem, contact NetApp Support at https://mysupport.netapp.com. If the memory paging alarm triggers when the AltaVault is under a heavy load, you can ignore it.
Metadata Space Full	Indicates that the data reserved for storing system metadata has filled up, leading to reduced deduplication.
Process Dump Creation Error	Indicates that the system has detected an error while trying to create a process dump. Contact NetApp Support at https://mysupport.netapp.com to correct the issue.

Alarm	Description
Restore Throttling	The restore throttling alarm is applicable only when the cloud storage used is AWS Glacier. AWS Glacier documentation specifies a monthly limit up to which no restore costs are charged for retrieving data from Glacier. Once this limit is crossed, data retrieval costs can be substantial. For details, see AWS Glacier documentation. By default, the AltaVault has a restore throttle for data retrieved from Glacier. This throttle keeps retrievals below the no-cost limit. The default value of this restore throttle is 5%. Therefore, you can use the AltaVault to restore 5% of total cloud usage in a month. The throttle is enforced on an hourly basis. Hourly data retrieval is limited to (5% of the total cloud use)/(hours per month). You can increase the 5% restore throttle limit up to 100% or completely disable it by setting the limit to 0. You might incur data retrieval charges when you make this change. For details about how to change the restore throttle limit, see the *NetApp AltaVault Cloud Integrated Storage Command-Line Interface Reference Guide*.
Secure Vault	Enables an alarm and sends an email notification if the system encounters a problem with the secure vault: • Secure Vault Locked - Indicates that the secure vault is locked. To optimize SSL connections or to use data store encryption, the secure vault must be unlocked. Go to Configure > Secure Vault and unlock the secure vault.
SMB	Domain Controller Network Status - Indicates the Domain Controller is unreachable. The alarm is cleared when network connectivity to the Domain Controller is restored. If the alarm is not cleared after the network connectivity is restored, you can clear the alarm manually using **alarm smb_alarms clear** command.
Software Update Available	Indicates that a newer version of the software is available. • To disable the alarm enter the following CLI command: `software_upgrade_available_clear`

Storage Optimization Service	• Storage Optimization Service Down - Enables an alarm and sends an email notification if the storage optimization service encounters a service condition. By default, this alarm is enabled. The message indicates the reason for the condition. The following conditions trigger this alarm:
	
	  • Configuration errors: examples include no encryption key set, incorrect appliance time, or incorrect cloud credentials.
	  • An AltaVault appliance reboot for example, during an appliance software update.
	  • A system crash for example, due to a power failure
	  • A storage optimization service restart for example, due to a cloud storage provider change.
	  • A user enters the CLI command no service enable or shuts down the storage optimization service from the Management Console
	  • A user restarts the optimization service from either the Management Console or CLI
	
	• Storage Optimization Service Error - Enables an alarm and sends an email notification if the storage optimization service encounters a condition that might degrade optimization performance. By default, this alarm is enabled.

Alarm	Description
Storage Optimization Service Replication	• Replication Error - Enables an alarm when the replication to the cloud encounters an error. Displays an error message that indicates the type of error such as, a file cannot be replicated to the cloud. • Replication Paused - Enables an alarm when the replication to the cloud pauses, because there is a cloud connection error, or you entered the CLI command no replication enable, or because you are using replication scheduling (nonbandwidth limit type). This alarm warns you that the AltaVault is not replicating data in the cloud. By default, this alarm is enabled.
System Reserved Space Full	Indicates that the space used for internal data structures is full. If you write more data to the appliance, it reduces deduplication performance.
Upgrade Status	Indicates the current AltaVault status.

The Alarm Status report answers the following question:

- What is the current status of the AltaVault?

To view the Alarm Status report

- Choose Reports > Alarm Status. Alternately, you can click the current alarm status that appears in the status box in the upper-right corner of each screen (Healthy, Degraded, or Critical).

Viewing the CPU utilization report

The CPU Utilization report summarizes the percentage of the CPU used within the time period specified.

Typically, the AltaVault operates on approximately 30 to 40 percent CPU capacity during nonpeak hours and approximately 60 to 70 percent capacity during peak hours. No single AltaVault CPU usage should exceed 95 percent.

The CPU Utilization report answers the following questions:

- How much of the CPU is being used?
- What is the average and peak percentage of the CPU being used?

To view the CPU Utilization report

1. Choose Reports > CPU Utilization.

2. Use the controls to customize the report as described in this table.

Control	Description
5m 1h 1d 1w All	Select one of the following report time intervals to filter the display: • 5m - Displays five minutes of data. • 1h - Displays one hour of data. • 1d - Displays one day of data. • 1w - Displays one week of data. • All - Displays all data available for the past 30 days. To type a custom time interval, enter the start time and end time (using the format YYYY/MM/DD HH:MM:SS) in the text field. You can view the newest data and see data points as they are added to the chart dynamically.
Show newest data	Click this option to display only the latest data available. The latest data available depends on the time interval that you specify. For example, if 1h is the specified time interval, then clicking **Show newest data** displays the last 60 minutes of data.

To generate share level expanded bytes report

- To generate the share level expanded bytes report using the CLI command:

  ```
  share-stats generate [num-threads]
  ```

  This command scans all the files in the various shares and exports created and accumulates the statistics. The report contains the following statistics for all the shares in the appliance:

  – Size of the share

  – Number of files in the share

  – Average file size

  – Evicted percentage

  The size of the share is the expanded bytes that is the actual size of the data being written to the appliance.

  When the command is executed, an email containing the report is sent to the administrator. The report will not be display in the Web.

Viewing the memory paging report

The Memory Paging report provides the total number of memory pages, per second, utilized in the time period specified. It includes the following data that describe memory paging activity for the time period you specify.

Field	Description
Page Swap Out Rate	Specifies the rate at which pages swapped. If 100 pages are swapped every couple of hours, the AltaVault is functioning properly. If thousands of pages are swapped every few minutes, contact NetApp Support at https://mysupport.netapp.com.

The Memory Paging report answers the following questions:

- How much memory is being used?
- What is the average and peak number of memory pages swapped?

To view the Memory Paging report

1. Choose Reports > Memory Paging.
2. Use the controls in the control panel to customize the report as described in this table.

Control	Description
5m 1h 1d 1w All	Select one of the following report time intervals to filter the display: • 5m - Displays five minutes of data. • 1h - Displays one hour of data. • 1d - Displays one day of data. • 1w - Displays one week of data. • All - Displays all data available for the past 30 days. To type a custom time interval, enter the start time and end time (using the format YYYY/MM/DD HH:MM:SS) in the text field. You can view the newest data and see data points as they are added to the chart dynamically.
Show newest data	Click this option to display only the latest data available. The latest data available depends on the time interval that you specify. For example, if 1h is the specified time interval, then clicking **Show newest data** displays the last 60 minutes of data.

Viewing the interface counters report

The Interface Statistics report displays information for each AltaVault interface, such as the interface name, its IP address, the Ethernet MAC address settings, the link settings, and the number of packets received and transmitted by the interface.

The Interface Statistics report includes the following statistics.

Field	Description
Interface	Name of the AltaVault interface.
IP	IP address of the network interface.
Ethernet	The MAC address information for the interface. The speed can be Auto, 1000, 100, or 10. The default value is Auto.
Link	Parameter that indicates whether there is an active connection plugged into the interface. Displays true if the interface is connected; otherwise, it displays false.
Receive Packets	Number of packets received by the interface. It also provides details such as the number of packets discarded, packet errors, packet overruns, packet frames, and packets multicast.
Transmit Packets	Number of packets transmitted by the interface. It also provides details such as the number of packets discarded, packet errors, packet overruns, packet frames, and packets multicast.

The Interface Statistics report answers the following questions:

- What is the name, IP address, Ethernet information, and link state of each AltaVault interface?
- What is the number of packets received by the interface? How many of these packets were discarded, and how many had errors, overruns, frames, and multicast?

- What is the number of packets transmitted by the interface? How many of these packets were discarded, and how many had errors, overruns, frames, and multicast?

To view the Interface Counters report

- Choose Reports > Interface Counters.

Viewing the disk throughput report

The Disk Throughput report displays information for each AltaVault disk, such as the average read throughput, and average write throughput.

The Disk Throughput report includes the following statistics.

Field	Description
Read	Average data read from the AltaVault internal disk subsystem.
Write	Average data written to the AltaVault internal disk subsystem.

The Disk Throughput report answers the following questions:

- What is the average read throughput that the AltaVault is experiencing at the specified time?
- What is the average write throughput that the AltaVault is experiencing at the specified time?

The average disk throughput is a measure of performance that help you to discover disk-based bottlenecks.

The rate at which the AltaVault can read from the internal disk subsystem characterizes the performance by which the AltaVault can serve read requests to client machines and transfer data to the cloud storage provider.

The rate at which the AltaVault can write to the internal disk subsystem characterizes the performance by which the AltaVault can serve write requests from the client machines and retrieve data from the cloud storage provider.

To view the Disk Throughput report

1. Choose Reports > Disk Throughput.
2. Use the controls in the control panel to customize the report as described in this table.

Control	Description
5m 1h 1d 1w All	Select one of the following report time intervals to filter the display: • 5m - Displays five minutes of data. • 1h - Displays one hour of data. • 1d - Displays one day of data. • 1w - Displays one week of data. • All - Displays all data available for the past 30 days. To type a custom time interval, enter the start time and end time (using the format YYYY/MM/DD HH:MM:SS) in the text field. You can view the newest data and see data points as they are added to the chart dynamically.
Show newest data	Click this option to display only the latest data available. The latest data available depends on the time interval that you specify. For example, if 1h is the specified time interval, then clicking **Show newest data** displays the last 60 minutes of data.

Viewing the disk IOPS report

The Disk IOPS report displays the average Input/Output Operations Per Second (IOPS) information for each AltaVault disk.

The Disk IOPS report includes the following statistics.

Field	Description
Read	Average value of input/output operations per second for read operations from the AltaVault internal disk subsystem.
Write	Average value of input/output operations per second for write operations to the AltaVault internal disk subsystem.

The Disk IOPS report answers the following questions:

- What is the average read IOPS that the AltaVault is experiencing at the specified time?
- What is the average write IOPS that the AltaVault is experiencing at the specified time?

The average disk IOPS is a measure of performance that help you to discover disk-based bottlenecks.

To view the Disk IOPS report

1. Choose Reports > Disk IOPS.
2. Use the controls in the control panel to customize the report as described in this table.

Control	Description
5m 1h 1d 1w All	Select one of the following report time intervals to filter the display: • 5m - Displays five minutes of data. • 1h - Displays one hour of data. • 1d - Displays one day of data. • 1w - Displays one week of data. • All - Displays all data available for the past 30 days. To type a custom time interval, enter the start time and end time (using the format YYYY/MM/DD HH:MM:SS) in the text field. You can view the newest data and see data points as they are added to the chart dynamically.
Show newest data	Click this option to display only the latest data available. The latest data available depends on the time interval that you specify. For example, if 1h is the specified time interval, then clicking **Show newest data** displays the last 60 minutes of data.

Viewing the disk utilization report

The Disk Utilization report displays information for each AltaVault disk, such as the average percentage utilization, cumulative average queue size, cumulative average wait, and cumulative average service time.

The Disk Utilization report includes the following statistics.

Field	Description
Utilization	The average percentage of the aggregate measurement of access time and transfers per second.
Queue Size	A running average of the number of requests either in service or waiting for service on the AltaVault internal disk subsystem.
Wait Time	A running average of the wait time per I/O operation experienced by the AltaVault internal disk subsystem.
Service Time	A running average service time per I/O operation experienced by the AltaVault internal disk subsystem.

The Disk Utilization report answers the following questions:

- What is the estimated service time for an I/O request on the AltaVault internal disk subsystem?
- What is the availability of AltaVault services to process I/O requests?
- How well are the AltaVault services using the internal disk subsystem?

To view the Disk Utilization report

1. Choose Reports > Disk Utilization.
2. Use the controls in the control panel to customize the report as described in this table.

Control	Description
5m 1h 1d 1w All	Select one of the following report time intervals to filter the display: • 5m - Displays five minutes of data. • 1h - Displays one hour of data. • 1d - Displays one day of data. • 1w - Displays one week of data. • All - Displays all data available for the past 30 days. To type a custom time interval, enter the start time and end time (using the format YYYY/MM/DD HH:MM:SS) in the text field. You can view the newest data and see data points as they are added to the chart dynamically.
Show newest data	Click this option to display only the latest data available. The latest data available depends on the time interval that you specify. For example, if 1h is the specified time interval, then clicking **Show newest data** displays the last 60 minutes of data.

Viewing logs

The AltaVault log reports provide a high-level view of network activity. You can view both user and system logs.

- "Viewing system logs" on page 150
- "Viewing user logs" on page 150

Viewing system logs

You can view system logs in the Maintenance > System Logs page. View System logs to monitor system activity and to troubleshoot problems. The most recent log events are listed first.

To view system logs

1. Choose Maintenance > System Logs.
2. Use the controls to customize the report as described in this table.

Control	Description
Show	Select one of the archived logs or Current Log from the drop-down list.
Lines per page	Specify the number of lines that you want to display in the page.
Jump to	Select one of the following options from the drop-down list: • Page - Specify the number of pages that you want to display. • Time - Specify the time for the log that you want to display.
Filter	Select one of the following filtering options from the drop-down list: • Regular expression - Specify a regular expression on which to filter the log. • Error or higher - Displays error-level logs or higher. • Warning or higher - Displays warning-level logs or higher. • Notice or higher - Displays notice-level logs or higher. • Info or higher - Displays informational-level logs or higher.
Go	Displays the report.

To view a continuous log

1. Choose Maintenance > System Logs.
2. Customize the log as described in "To view system logs" on page 150.
3. Click **Launch Continuous Log** in the upper-right corner of the page.

You can continuously display new lines as the log expands.

Viewing user logs

You can view user logs in the Maintenance > User Logs page. The user log filters messages from the system log to display messages that are of immediate use to the system administrator.

View user logs to monitor system activity and to troubleshoot problems. For example, you can monitor who logged in, who logged out, and who entered particular CLI commands, and you can monitor alarms and errors. The most recent log events are listed first.

To view and customize user logs

1. Choose Maintenance > User Logs.

2. Use the controls to customize the log as described in this table.

Control	Description
Show	Select one of the archived logs or Current Log from the drop-down list.
Lines per Page	Specify the number of lines that you want to display in the page.
Jump to	Select one of the following options from the drop-down list: • Page - Specify the number of pages that you want to display. • Time - Specify the time for the log that you want to display.
Filter	Select one of the following filtering options from the drop-down list: • Regular expression - Specify a regular expression on which to filter the log. • Error or higher - Displays error-level logs or higher. • Warning or higher - Displays warning-level logs or higher. • Notice or higher - Displays notice-level logs or higher. • Info or higher - Displays informational-level logs or higher.
Go	Displays the report.

3. Click the **Launch Continuous Log** in the upper-right corner of the page.

   You can continuously display new lines as the log expands.

To view a continuous log

1. Choose Maintenance > User Logs.
2. Customize the log as described in "To view and customize user logs" on page 150.
3. Click **Launch Continuous Log** in the upper-right corner of the page.

Downloading log files

This section describes how to download user and system log files.

You can download both user and system logs.

- "Downloading user log files" on page 151
- "Downloading system log files" on page 152

Downloading user log files

You can download user logs in the Maintenance > User Logs Download page. Download user logs to monitor system activity and to troubleshoot problems.

To download user logs

1. Choose Maintenance > User Logs Download.
2. Click the name of the log to display the dialog box to display or save the log to disk.

3. Click **Rotate Logs** to archive the current log to a numbered archived log file and then clear the log so that it is empty again.

Downloading system log files

You can download system logs in the Maintenance > System Logs Download page. Download system logs to monitor system activity and to troubleshoot problems.

To download system logs

1. Choose Maintenance > System Logs Download.
2. Click the name of the log to display the dialog box to display or save the log to disk.
3. Click **Rotate Logs** to archive the current log to a numbered archived log file and then clear the log so that it is empty again.

Generating system dumps

You can generate and download system dumps in the Maintenance > System Dumps page. A system dump contains a copy of the kernel data on the system. System dump files can help you diagnose problems in the system.

To generate system dump files

1. Choose Maintenance > System Dumps.
2. Click the name of the system dump file and then click **Download System Dump** to download it.
3. Optionally, under Upload to NetApp Support, type the support case number, click **Upload** to upload the system dump to the NetApp Support site.
4. Under Generate System Dump, select the type of information to include in the report:
   - **Include Statistics** - Select to collect and include CPU, memory, and other statistics in the system dump (this option is enabled by default).
   - **Include All Logs** - Removes the 50 MB limit for compressed log files, to include all logs in the system dump.
5. Click **Generate System Dump**.

Because generating a system dump can take a while, a spinner appears during the system dump creation. When the system dump is complete, it appears in the list of links to download.

To view system dump files

1. Choose Maintenance > System Dumps.
2. Click **Download Link** to view a previously saved system dump.
3. Select the filename to open a file or save the file to disk.

4. To remove an entry, check the box next to the name and click **Remove Selected**.

Viewing process dumps

You can display and download process dumps in the Maintenance > Process Dumps page. A process dump is a saved copy of memory, including the contents of all memory, bytes, hardware registers, and status indicators. It is periodically taken to restore the system in the event of failure. Process dump files can help you diagnose problems in the system.

To view process dump files

1. Choose Maintenance > Process Dumps.
2. Click the filename to open a file or save the file to disk.
3. To remove an entry, select the box next to the name and click **Remove Selected**.

Capturing and uploading TCP dumps

You can create, download, and upload TCP capture files in the Maintenance > TCP Dumps page.

Capture files contain summary information for every Internet packet received or transmitted on the interface to help diagnose problems in the system.

The AltaVault provides an easy way to create and retrieve multiple capture files from the Management Console. You can create capture files from multiple interfaces at the same time, limit the size of the capture file, and schedule a specific date and time to create a capture file. Scheduling and limiting a capture file by time or size allows unattended captures.

The top of the TCP Dumps page displays a list of existing capture files and the bottom of the page displays controls to create a capture file. The bottom of the page also includes the capture files that are currently running, and controls to create a trigger that stops a capture when a specific event occurs. The Running Capture Name list includes captures running at a particular time. It includes captures started manually and also any captures that were scheduled previously and are now running.

To capture TCP trace dumps

1. Choose Maintenance > TCP Dumps.
2. Under TCP Dumps Currently Running, complete the configuration as described in this table.

Control	Description
Add a New TCP Dump	Displays the controls for creating a capture file.

Control	Description
Capture Name	Specify the name of the capture file. Use a unique filename to prevent overwriting an existing capture file. The default filename uses this format: *hostname_interface_timestamp*.cap *hostname* is the hostname of the AltaVault, *interface* is the name of the interface selected for the trace (for example, lan0_0, wan0_0), and *timestamp* is in the YYYY-MM-DD-HH-MM-SS format. If this capture file relates to an open NetApp Support case, specify the capture filename case_*number* where *number* is your NetApp Support case number. For example, case_12345. The .cap file extension is not included with the filename when it appears in the capture queue.
Endpoints	Specify IP addresses and port numbers to capture packets between them: **IPs** - Specify IP addresses of endpoints on *one side*. Separate multiple IP addresses using commas. You can enter IPv6 addresses separated by commas. The default setting is all IP addresses. **Ports** - Specify ports on *one side*. Separate multiple ports using commas. The default setting is all ports. *—and—* **IPs** - Specify IP addresses of endpoints on the *other side*. Separate multiple IP addresses using commas. You can enter IPv6 addresses separated by commas. The default setting is all IP addresses. **Ports** - Specify ports on the *other side*. Separate multiple ports using commas. The default setting is all ports. To capture traffic flowing in only one direction or to enter a custom command, use the CLI **tcpdump** command. For details, see the *NetApp AltaVault Cloud Integrated Storage Command-Line Reference Guide*.
Capture Interfaces	Captures packet traces on the selected interfaces. You can select all interfaces or a base, in-path, or RSP interface. The default setting is none. You must specify a capture interface. If you select several interfaces at a time, the data is automatically placed into separate capture files. When path selection is enabled, NetApp recommends that you collect packet traces on all LAN and WAN interfaces.

Control	Description

Capture Parameters	These parameters let you capture information about dot1q VLAN traffic. You can match traffic based on VLAN-tagged or untagged packets, or both. You can also filter by port number or host IP address and include or exclude ARP packets. Select one of these parameters for capturing VLAN packets:
	• Capture Untagged Traffic Only - Select this option for the following captures:
	– All untagged VLAN traffic.
	– Untagged 7850 traffic and ARP packets.
	– Only untagged ARP packets.
	• Capture VLAN-Tagged Traffic Only - Select this option for the following captures:
	– Only VLAN-tagged traffic.
	– VLAN-tagged packets with host 10.11.0.6 traffic and ARP packets. You must also specify 10.11.0.6 in the IPs field, and specify or arp in the custom flags field on this page.
	– VLAN-tagged ARP packets only. You must also specify and arp in the custom flags field on this page.
	• Capture both VLAN and Untagged Traffic - Select this option for the following captures:
	– All VLAN traffic.
	– Both tagged and untagged 7850 traffic and ARP packets. You must also specify the following in the custom flags field on this page:
	`(port 7850 or arp)` or `(vlan and (port 7850 or arp))`
	– Both tagged and untagged 7850 traffic only. You must also specify 7850 in one of the port fields on this page. No custom flags are required.
	– Both tagged and untagged ARP packets. You must also specify the following options in the custom flags field on this page:
	`(arp)` or `(vlan and arp)`

Capture Duration (Seconds)	Specify a positive integer to set how long the capture runs, in seconds. The default value is 30. Specify 0 or continuous to initiate a continuous trace. For continuous capture, NetApp recommends specifying a maximum capture size and a nonzero rotate file number to limit the size of the TCP dump.
Maximum Capture Size	Specify the maximum capture file size, in megabytes. The default value is 100. After the file reaches the maximum capture size, TCP dump starts writing capture data into the next file, limited by the Number of Files to Rotate field. NetApp recommends a maximum capture file size of 1024 MB (1 GB).
Buffer Size	Optionally, specify the maximum amount of data, in kilobytes, allowed to queue while awaiting processing by the capture file. The default value is 154 KB.
Snap Length	Optionally, specify the snap length value for the capture file, which equals the number of bytes captured for each packet. Having a snap length smaller than the maximum packet size on the network enables you to store more packets, but you might not be able to inspect the full packet content. Specify 0 for a full packet capture (recommended for SMB, MAPI, and SSL captures). The default value is 1518 bytes.
Number of Files to Rotate	Specify how many capture files to keep for each interface before overwriting the oldest file. To stop file rotation, you can specify 0; however, NetApp recommends rotating files, because stopping the rotation can fill the disk partition. This limits the number of files created to the specified number, and begins overwriting files from the beginning, thus creating a rotating buffer. The default value is five files per interface. The maximum value is a 32-bit integer.

Control	Description
Custom Flags	Specify custom flags as additional statements within the filter expression. Custom flags are added to the end of the expression created from the Endpoints fields and the Capture Parameters radio buttons (pertaining to VLANs). If you require an “and” statement between the expression created from other fields and the expression that you are entering in the custom flags field, you must include the “and” statement at the start of the custom flags field. Do not use host, src, or dst statements in the custom flags field. Although it is possible in trivial cases to get these to start without a syntax error, they do not capture GRE-encapsulated packets that some modes of AltaVault communications use, such as WCCP deployments or Interceptor connection-setup traffic. NetApp recommends using bidirectional filters by specifying endpoints. For complete control of your filter expression, use the CLI tcpdump command. For details, see the *NetApp AltaVault Cloud Integrated Storage Command-Line Interface Reference Guide*.
Schedule Dump	Schedules the capture to run at a later date and time. Start Date - Specify a date to initiate the capture, in this format: YYYY/MM/DD. Start Time - Specify a time to initiate the capture, in this format: HH:MM:SS.
Add	Adds the capture request to the capture queue.

Troubleshooting

If your command results in a syntax error with an immediate or scheduled TCP dump, this message appears:

“Error in tcpdump command. See System Log for details.”

Review the system log to see the full tcpdump command attempt. Check the expression for issues such as a missing “and,” as well as contradictory instructions such as looking for VLAN-tagged traffic AND non-tagged traffic.

Custom flag use examples

The examples in this table focus on the custom flag entry but rely on other fields to create a complete filter.

Filter Purpose	Custom Flag
To capture all traffic on VLAN 10 between two specified endpoints: 1.1.1.1 and 2.2.2.2	and vlan 10
To capture any packet with a SYN or an ACK	tcp[tcpflags] & (tcp-syn|tcp-ack) != 0
To capture any packet with a SYN	tcp[tcpflags] & (tcp-syn) != 0 —*or*— tcp[13] & 2 == 2
To capture any SYN to or from host 1.1.1.1	and (tcp[tcpflags] & (tcp-syn) != 0) —*or*— and (tcp[13] & 2 == 2)

Stopping a TCP dump after an event occurs

TCP dumps offer visibility into intermittent network issues, but the amount of traffic they capture can be overwhelming. Also, because rotating logs is common, once a TCP dump logs an event, the AltaVault log rotation can overwrite debugging information specific to the event.

The system makes troubleshooting easier because it provides a trigger that can stop a continuous TCP dump after a specific log event occurs. The result is a smaller file to help pinpoint what makes the event happen.

The stop trigger continuously scans the system logs for a search pattern. When it finds a match, it stops all running captures.

To stop a TCP dump after a specific log event

1. Choose Maintenance > TCP Dumps.

2. Add a new TCP dump and schedule it to run. For more details about adding a TCP Dump, see "To capture TCP trace dumps" on page 153.

3. Scroll down to the TCP Dump Stop Trigger section on the TCP Dumps page.

4. In the Pattern text box, enter a Perl regular expression (regex) to find in a log. The system compares the Perl regex against each new line in the system logs and the trigger stops if it finds a match.

   The simplest regex is a word or a string of characters. For example, if you set the pattern to "Limit," the trigger matches the line "Connection Limit Reached."

   Notes:

   - Perl regular expressions are case-sensitive.
   - Perl treats the space character " \space " like any other character in a regex.
   - Perl reserves some characters, called metacharacters, for use in regex notation. The metacharacters are:

     { } [ ] ( ) ^ $. | * + ? \

     You can match a metacharacter by putting a backslash before it. For example, to search for a backslash in the logs, you must enter two backslashes (\\) as the pattern.
   - The pattern follows Perl regular expression syntax. For details, go to:

     http://perldoc.perl.org/perlre.html
   - You cannot change the pattern while a scan is running. You must stop the scan before changing a pattern.
   - You do not need to wrap the pattern with the metacharacters to match the beginning or end of a line (^ $) or with the wildcard character (*).

5. Specify the amount of time to pause before stopping all running captures when the system finds a match. This gives the system some time to log more data without abruptly cutting off the capture. The default is 30 seconds. Specify 0 for no delay; the capture stops immediately.

   After a trigger has fired, the capture can stop by itself before the delay expires. For example, the capture duration can expire.

6. Click **Start Scan**.

   When the scan stops, the system sends an email to all email addresses on the Configure > Email page appearing under Report Events via Email. The email notifies users that the trigger has fired.

The page indicates “Last Triggered: Never” if a TCP Dump stop trigger has never triggered on the AltaVault. After the delay duration of the stop trigger, the system displays the last triggered time.

Before changing the Perl regular expression or amount of delay, you must first stop the process.

To stop a running scan

- Click **Stop Scan** to halt the background process that monitors the system logs. The system dims this button when the stop trigger is idling.

Stop trigger limitations

These limitations apply to the trigger:

- You cannot create a trigger to stop a specific capture; the trigger affects all running captures.
- If the search pattern contains a typo, the trigger might never find a match.
- Only one instance of a trigger can run at one time.

Viewing a TCP dump

The top of the TCP Dumps page displays a list of existing TCP trace dumps.

To view a capture file

1. Choose Maintenance > TCP Dumps.
2. Under Stored TCP Dumps, select the trace dump name to open the file.
3. Click **Download** to view a previously saved capture file.
4. To remove a capture file, select the check box next to the name and click **Remove Selected**.

To print a capture file

1. Choose Maintenance > TCP Dumps.
2. Under Download Link, select the capture filename to open the file.
3. When the file opens, choose File > Print in your Web browser to open the Print dialog box.

To stop a running a capture

1. Choose Maintenance > TCP Dumps.
2. Select the capture filename in the Running Capture Name list.
3. Click **Stop Selected Captures**.

Uploading a TCP dump

NetApp offers several methods to upload capture files to the support server for sharing with the support team while diagnosing issues.

To upload the capture file to NetApp support

1. In continuous mode, on the TCP Dumps page, select the running capture and click **Stop Selected Captures**.

   For timed captures that are complete, skip to Step 2.

   The capture appears as a download link in the list of Stored TCP Dumps.

2. Select the capture filename.

3. Optionally, specify a case number that corresponds to the capture. NetApp Support recommends using a case number. For example, 194170.

   To specify a URL instead of a case number, you must use the CLI. You can enter the CLI command **file tcpdump upload URL**. When you specify a URL, the capture file goes directly to the URL.

   If the URL points to a directory on the upload server, it must have a trailing backslash (/).

   For example:

   ftp://ftp.netapp.com/incoming/

   (not ftp://ftp.netapp.com/incoming)

   The filename as it exists on the appliance will then match the filename on the upload server.

   For details, see the *NetApp AltaVault Cloud Integrated Storage Command-Line Interface Reference Guide*.

4. Click **Upload**.

Because uploading a capture file can take a while, a progress bar displays the percentage of the total upload completed, the case number (if applicable), and the date and time the upload began. When the capture file finishes uploading, the date, time, and a status of either uploaded (appears in green) or failed (appears in red).

Successful uploads show the status, the case number (if applicable), and the date and time the upload finished.

For uploads that fail, an explanation, the case number (if applicable), and the upload starting date and time appear.

Viewing the appliance monitoring report

The Appliance Monitoring report enables you to view the health status, disk space, and cloud service status of multiple AltaVaults using a monitoring AltaVault.

The Appliance Monitoring report includes the following statistics.

Field	Description
Hostname	Hostname of the monitored appliance.
Appliance Health	Current state of the appliance, which is one of the following options: • Healthy - The AltaVault is active and optimizing storage effectively. You do not need to take any action. • Needs Attention - Accompanies a healthy state to indicate management-related issues that does not affect the ability of the AltaVault to optimize storage. Address the management-related issue in a low-priority order. • Degraded - The appliance is optimizing storage but the system has detected an issue. Address the issue that the system has detected. • Admission Control - The appliance is optimizing storage but has entered the admission control state. Admission control limits the number of connections made to the AltaVault, so that you do not over-consume resources on your system. To clear this state, reduce the number of connections to the AltaVault. • Critical - The AltaVault might or might not be optimizing storage. You must address a critical issue immediately.
Service State	Current state of the storage optimization service.
Expanded Data	Data that is backed up locally by the AltaVault.
Deduplicated Data	Data that has been deduplicated. Deduplication is a method of reducing storage space by eliminating redundant data. It stores only one unique instance of the data. It replaces redundant data with a pointer to the unique data copy.
Deduplication Factor	The average deduplication factor, which is the ratio of the expanded data and total optimized data. The total optimized data includes both deduplication and compression savings.
Cloud Storage Used	The amount of cloud storage used by the appliance.
Cloud Storage Available	The amount of storage available in the cloud.
AltaVault Storage Available	The amount of storage available on the monitored AltaVault.
Bytes Pending Replication	The number of bytes in the local disk that are pending replication to the cloud.

The Appliance Monitoring report provides the following statistics for each monitored appliance: hostname, appliance health, service state, expanded data, deduplicated data, deduplication factor, cloud storage used, cloud storage available, AltaVault storage available, and bytes pending replication.

It also displays a summary of the total expanded data, total deduplicated data, average deduplication factor, total cloud storage used, total cloud storage available, total AltaVault storage available, total bytes pending replication to the cloud for all monitored appliances in the network.

To configure appliance monitoring

1. Choose Reports > Appliance Monitoring.

2. Under Monitored Appliances, complete the configuration as described in this table.

Control	Description
Add Monitored Appliance	Displays controls to add a monitored appliance.
Hostname or IP Address	Specify a valid hostname or IP address for the monitored appliance.
API Access Code	Specify the API access key to access the monitored appliance. To obtain the API access key: • Open a separate browser. • Log in to the appliance that you want to monitor. • Choose Configure > REST API Access. • Generate the API Access key. • Copy it into Notepad. • Log back in to the monitoring AltaVault. • Paste the API access key in this text box.
Add	Click **Add** to add the peer appliance to the list of monitored appliances.
Remove Selected Appliances	Select the check box next to the name and click **Remove Selected Appliances** to delete it from the system.

3. Click **Save** to save your configuration.

Viewing the shelf details

The Shelf Details report enables you to view information about the AltaVault hardware RAID. It is applicable only to AltaVault hardware models; not to AltaVault-v models.

The Shelf Details displays the AltaVault enclosure ID and a visual replica of the hardware disk array that includes the head unit and the expansion shelves.

The shelf serial number can be found on the back of the shelf. The slot number identifies the slot within the shelf.

Hover your mouse over each disk shown on the Shelf Details report to obtain the status of the disk and its serial number.

The top right LED is the power LED. If the disk is online, it is constantly green. If the disk is offline, it is amber.

For details, see the *NetApp AltaVault Cloud Integrated Storage Installation and Service Guide for Physical Appliances.*

The Shelf Details report provides the serial number and status of the AltaVault hardware disk array.

To identify physical location of a drive

- Use the following CLI:

```
CLI > show hwraid disk information
```

To view the shelf details

1. Choose Reports > Shelf Details.

2. Click the serial number of a shelf to obtain alarm information for the RAID.

Viewing the storage RAID group

The Storage RAID groups enables you to view the serial number, status, size, used, model number, and product ID. For AVA400, the maximum number of RAID groups supported is five. For AVA800, the maximum number of RAID groups supported is seven.

For details, see the *NetApp AltaVault Cloud Integrated Storage Installation and Service Guide*.

The Storage RAID groups includes the following statistics.

Field	Description
Serial Number	The serial number of the Storage RAID group.
Status	Current state of the Storage RAID group, which is one of the following options: • Valid - The Storage RAID group is valid and active. • Invalid - The Storage RAID group is not valid. Click the serial number of the alarm information for the Storage RAID group.
Size	The size of the Storage RAID group (terabytes).
Used	Current space occupied by the Storage RAID group.
Model	The Storage RAID group model.
Product ID	The Storage RAID group product ID number.

The Storage RAID Group report provides statistics for each group.

To view the Storage RAID Group report

1. Choose Reports > Storage RAID groups.
2. Click the serial number of a group to obtain information for the RAID.

To view diagnostics using the CLI

- Run the following command to view diagnostics:

```
CLI > # show raidgroups
```

CHAPTER 9 Configuring AltaVault appliances for FIPS-compliant cryptography

This section describes how to configure a AltaVault appliance to use FIPS-compliant cryptography. It includes the following sections:

- "What is FIPS?" on page 163
- "Understanding FIPS on AltaVault" on page 163
- "Basic steps for configuring FIPS compliance" on page 165
- "Configuring AltaVault appliances for FIPS-compliant cryptography" on page 165
- "Disabling FIPS mode" on page 171
- "Viewing reports and logs" on page 172
- "Verifying FIPS mode in system logs" on page 173
- "FIPS CLI" on page 174

You configure and manage FIPS mode through the Command-Line Interface (CLI). This section assumes that you are familiar with the CLI. For detailed information about the CLI, see the *NetApp AltaVault Cloud Integrated Storage Command-Line Reference Guide*.

What is FIPS?

Federal Information Processing Standard (FIPS) is a publicly announced set of validation standards developed by the United States National Institute of Standards and Technology (NIST) for use by government agencies and by government contractors.

FIPS 140-2 details the U.S. and Canadian Government requirements for cryptographic modules. Protection of a cryptographic module within a security system is necessary to maintain the confidentiality and integrity of the information protected by the module.

This standard specifies the security requirements satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified data.

Understanding FIPS on AltaVault

This section describes the NetApp Cryptographic Security Module, as well as the system features that are FIPS compliant and those that are not.

AltaVault offers end-to-end security for data at rest and in flight using FIPS 140-2 level 1-compliant encryption. AltaVault offers end-to-end security for data-at-rest and in-flight with the NetApp Cryptographic Security Module. The module is currently undergoing FIPS 140-2 level 1 validation and is expected to complete the process in 1HCY16.

NetApp cryptographic security module

NetApp Cryptographic Security Module v1.0 defines the cryptographic module that separates the cryptography that is FIPS compliant from the rest of the AltaVault.

The NetApp Cryptographic Security Module is compatible with FIPS 140-2 Level 1 requirements.

The NetApp Cryptographic Security Module appears as the validated cryptographic module on the NIST vendor page instead of a specific AltaVault. The NIST vendor page is available at this URL:

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

---

Note: Throughout this guide, *FIPS-mode* and *FIPS-compliance* refers to use of the NetApp Cryptographic Security Module.

Compliant FIPS cryptography features

The following features use FIPS-compliant cryptography:

- Web interface (Apache Web server)
- Local user passwords and local authentication using SHA256-based or SHA512-based hash
- Image integrity checks for AltaVault OS
- File transfers
- NTP with SHA authentication
- Secure vault
- SNMP except if SNMP user passwords are configured with MD5 or DES protocols
- SSH with approved ciphers
- SSL optimization
- AltaVault storage optimization service
- AltaVault data replication
- Domain-join feature in the AltaVault

Noncompliant FIPS cryptography features

The following features are not FIPS compliant and the system generates a warning if they are enabled or if you attempt to configure them.

The system does not prevent you from using these features, but it does warn you that they are not FIPS compliant. You need to ensure that the system is configured in FIPS mode and uses only FIPS-compliant features to achieve full compliance.

Features Depending on NTLM or Kerberos Domain Authentication

- SMB signing

Features That Use Cryptographic Libraries Outside the NetApp Cryptographic Security Module Boundary

- Kerberos
- SSH with unapproved ciphers

Features with Protocol Specifications That Can Use Noncompliant Hash Algorithms

- Some cloud providers (that you use with the AltaVault) are not fully supported in FIPS mode
  - AT&T Synaptic and EMC Atmos clouds are supported in FIPS mode only in service versions 2.1 and later. Older versions use noncompliant hash algorithms.
  - Not all cloud providers use FIPS 140-2 validated cryptography. It is your responsibility to ensure that the configured cloud provider meets regulatory requirements.
- Local user passwords and local authentication with MD5-based hash
- NTP with MD5 authentication
- RADIUS
- SNMP with users configured with MD5 or DES protocols
- TACACS+

Basic steps for configuring FIPS compliance

To achieve FIPS compliance on a AltaVault, configure the system to run in FIPS operation mode, and adjust the configuration of any features that are not FIPS compliant.

When you operate in FIPS mode, the system automatically uses FIPS-compliant versions where possible, but there are some features with encryption that you need to ensure are compliant.

With FIPS mode enabled, the system monitors configuration changes and provides warnings if you configure a feature to be noncompliant with FIPS. These warning messages appear when you try to change a configuration setting to an unsupported option. You can also view these warnings using the **show fips status** command.

The following table describes the basic steps necessary to configure your AltaVault to use FIPS-validated cryptographic modules.

Steps
1. Ensure passwords for user accounts use FIPS-compliant encryption.
2. Run the show fips status command to view compliance status and make any required configuration changes.
3. Reboot the appliance.

Configuring AltaVault appliances for FIPS-compliant cryptography

This section describes how to configure a AltaVault appliance to use FIPS-compliant cryptography. It includes the following sections:

- “Enabling FIPS mode” on page 166
- “Verifying that your system uses FIPS-compliant encryption” on page 167
- “Working with features to maintain FIPS compliance” on page 167
- “Account passwords” on page 167
- “Cipher requirements” on page 168

- "Key size requirements" on page 168
- "NTP" on page 169
- "RADIUS and TACACS+" on page 169
- "SNMP" on page 170
- "SSH" on page 170
- "Telnet server" on page 171
- "Web proxy" on page 171
- "Viewing user logs" on page 172
- "Viewing system logs" on page 172
- "Downloading user log files" on page 172
- "Downloading system log files" on page 172
- "Verifying that file transfers operate in FIPS mode" on page 173
- "Verifying that NTP operates in FIPS mode" on page 173
- "Verifying that secure vault operates in FIPS mode" on page 173
- "Verifying that SNMP operates in FIPS mode" on page 173
- "Verifying that the web interface operates in FIPS mode" on page 173

Enabling FIPS mode

FIPS mode ensures the system uses only FIPS-compliant encryption algorithms.

Note: Before you can enable FIPS mode, you need to ensure passwords for user accounts use FIPS-compliant encryption. For details, see "Account passwords" on page 167.

Note: Prior to enabling FIPS mode on the AltaVault appliance, remove previously configured local SMB users. FIPS mode does not support local SMB users.

To enable FIPS mode

1. Connect to the CLI.

2. Enter configuration mode, enable FIPS mode, and restart the system.

   At the system prompt, enter the following set of commands:

```
amnesiac > enable
amnesiac # configure terminal
amnesiac (config) # fips enable
You must save the configuration and reload the system to enable FIPS mode.
amnesiac (config) # write memory
amnesiac (config) # reload
Rebooting...
amnesiac (config) #
```

Restarting the system initializes supported features with any FIPS-specific settings and data.

Verifying that your system uses FIPS-compliant encryption

You can verify that your system uses FIPS-compliant encryption by using the show fips status command from the CLI.

To verify that your system is FIPS compliant

1. Connect to the CLI.
2. Enter the following set of commands:

```
amnesiac > enable
amnesiac # configure terminal
amnesiac (config) # show fips status
CMC Autoregistration: Should not be configured in FIPS mode.
Citrix Basic Encryption: Should not be configured in FIPS mode.

FIPS Mode: Enabled
```

The output indicates if FIPS mode is enabled and displays any warnings for features that affect FIPS compliance. If no warnings appear and FIPS mode is enabled, your system is FIPS compliant. If warnings appear, you need to make configuration changes to achieve full compliance.

You cannot review FIPS compliance from the Management Console; however, if you attempt to configure features that affect FIPS compliance through the Management Console when in FIPS mode, the Web interface produces an error message warning you of the conflict.

Working with features to maintain FIPS compliance

It is the responsibility of the system administrator of AltaVault appliance to ensure the system is FIPS compliant. Not all features can be operated in a FIPS-compliant manner and they need to be disabled when in FIPS mode. Some features can be operated in a FIPS-compliant manner by following noted guidance and other features prevent you from entering into FIPS mode.

The system generates a warning message if you configure non-compliant features. You can view the warning messages with the show fips status command.

The following sections describe configurable features that can affect FIPS compliance and describe how to resolve the warnings. The system does not prevent you from using noncompliant features in FIPS mode, but the system does warn you that they are not FIPS compliant. (The exception is account passwords; you cannot enable FIPS mode if all account passwords do not use compliant encryption).

Note: The commands in the following sections are configuration commands. You need to run these from configuration mode in the CLI. For detailed information, see the *NetApp AltaVault Cloud Integrated Storage Command-Line Reference Guide*.

Account passwords

FIPS compliance requires that passwords for user accounts are encrypted using an SHA256-based or SHA512-based hash.

In systems with RCSM, SHA512 is the default hash when creating and updating a user password. However, previous releases used MD5 encryption so when you upgrade to a software release supporting FIPS mode from a release with MD5-based passwords, the MD5 passwords remain in the configuration.

If you attempt to enter FIPS mode on a system with accounts that have MD5 passwords, you see the following error:

```
amnesiac (config) # fips enable
% User admin has a password hashed using a non-FIPS-allowed hash.
The password(s) must be changed before FIPS mode can be enabled.
```

The error message identifies the user accounts that need to be updated; in this example, the admin account. You must update the noncompliant passwords or delete the accounts before you can enable FIPS mode. From the CLI, enter the username password command to change passwords.

Cipher requirements

You need to use the following cipher string when running in FIPS mode: TLSv1.2:kRSA:!eNULL:!aNULL

This requirement impacts SSL optimization, secure peering, and the Web interface security settings.

Note: It is advisable to allow TLS 1.1 or TLS 1.2.

To configure the cipher

- Enter the command web ssl cipher.

  The format of the command is:

  ```
  web ssl cipher TLSv1.2:kRSA:!eNULL:!aNULL
  ```

If you do not configure the required cipher string, the following message appears after enabling FIPS mode or with the show fips status command:

```
Web SSL ciphers must include the elements in TLSv1.2:kRSA:!eNULL:!aNULL and may optionally
delete ciphers.
```

This message also appears if you make any changes to the Web SSL cipher.

Key size requirements

FIPS specifies three techniques for the generation and verification of digital signatures for the protection of data: the Digital Signature Algorithm (DSA), the Elliptic Curve Digital Signature Algorithm (ECDSA), and the Rivest-Shamir-Adelman (RSA) Algorithm.

FIPS includes key size requirements when running in FIPS mode. All imported and generated keys need to be the following sizes:

- RSA-based and DSA-based certificates:
  - 2048 bits
  - 3072 bits
- ECDSA certificates:
  - 224 bits and higher

These requirements apply to SSL optimization, SSL secure peering, and the Web interface.

Web user interface

You need to ensure imported and generated certificates for the Web interface adhere to FIPS size requirements and use only 2048-bit or 3072-bit key sizes.

You manage Web interface certificate keys using the web ssl cert generate key-size * command in the CLI and the Configure > Web Settings page in the Management Console. These methods always generate RSA based self-signed certificates.

In addition to self-signed certificates, you can import certificates using the web ssl cert import-cert * and web ssl cert import-cert-key * commands or the Configure > Web Settings page in the Management Console.

If you specify a key size that is not 2048-bit or 3072-bit with FIPS mode enabled, the system blocks the key generation and warns that the key size is not supported in FIPS mode.

NTP

NTP using either SHA authentication keys or no authentication keys is FIPS compliant. NTP using MD5 keys is not FIPS compliant.

If you configure an MD5 key for NTP using the following command, the system generates a warning message and the system will not be FIPS compliant:

```
amnesiac (config) # ntp authentication key <id> type MD5 secret <secret password>
```

To verify that NTP is running in FIPS mode, examine the system log when NTPD starts (this occurs whenever the NTP configuration is modified) and ensure that the NTPD entry sets FIPS mode:

```
Mar 18 15:49:57 amnesiac pm[4989]: [pm.NOTICE]: Launched ntpd with pid 27617
Mar 18 15:49:57 amnesiac ntpd[27617]: ntpd 4.2.6p4@1.2324-o Thu May 17 21:31:11 UTC 2012 (1)
…
Mar 18 15:49:57 amnesiac ntpd[27617]: FIPS_mode_set(1)
```

For more information about system logs, see “Viewing System Logs” on page 152.

RADIUS and TACACS+

The RADIUS and TACACS+ protocols are not FIPS compliant. These protocols use noncompliant hash algorithms. The system displays a warning message if you configure these features in FIPS mode.

The following commands generate a configuration warning in FIPS mode:

```
aaa accounting per-command default tacacs+
aaa authentication [console-login | login] default [radius | tacacs+]
aaa authorization per-command default tacacs+
```

SNMP

SNMP is FIPS compliant except if SNMP user passwords are configured with noncompliant hash algorithms. If you configure an SNMP user password with MD5 or DES protocols using the following command, the system generates a warning message and the system will not be FIPS compliant:

```
snmp-server user <username> password plain-text <password> [auth-protocol MD5 priv-protocol DES
priv-key plain-text <password>]
```

To verify that SNMP runs in FIPS mode, look for entries similar to the following in the system log when SNMP starts (this occurs whenever the SNMP configuration changes) and ensure that FIPS mode is set:

```
Mar 18 16:05:10 amnesiac pm[4989]: [pm.NOTICE]: Launched snmpd with pid 31709
Mar 18 16:05:10 amnesiac snmpd[31709]: FIPS_mode_set(1)
…
Mar 18 16:05:10 amnesiac snmpd[31709]: NET-SNMP version 5.3.1
```

For more information about system logs, see "Viewing System Logs" on page 152.

SSH

SSH requires the use one of the following ciphers to run in FIPS mode:

- aes128-cbc
- aes192-cbc
- aes256-cbc
- aes128-ctr
- aes192-ctr
- aes256-ctr

Configuring any other ciphers displays a warning message and the system will not be FIPS compliant.

Note: The default ciphers for SSH are aes128-ctr, aes192-ctr, and aes256-ctr. These ciphers are FIPS compliant.

- You can configure SSH ciphers with the following command:

  ```
  amnesiac (config) # ssh server allowed-ciphers aes128-cbc,aes192-cbc,aes256-cbc,aes128-
  ctr,aes192-ctr,aes256-ctr
  amnesiac (config) # write memory
  ```

- To verify your SSH settings, enter the following command:

  ```
  amnesiac (config) # show ssh server allowed-ciphers
  SSH server allowed ciphers:
  ---------------------------
  aes128-cbc
  aes192-cbc
  aes256-cbc
  aes128-ctr
  aes192-ctr
  aes256-ctr
  ```

- To verify that SSH is running in FIPS mode, look for entries similar to the following in the syslog when a user logs in:

  ```
  Mar 18 15:00:30 amnesiac sshd: FIPS_mode_set(1)
  Mar 18 15:00:30 amnesiac sshd[14594]: FIPS mode initialized
  ```

Telnet server

Telnet functionality is not FIPS compliant. Enabling this feature triggers a configuration warning in FIPS mode.

Telnet must be disabled. If Telnet is enabled, an error message appears if you try to enable FIPS mode. If FIPS mode is enabled, the system prevents you from enabling Telnet and provides an error message.

- To disable this feature, use the following commands:

```
amnesiac (config) # no telnet-server enable
amnesiac (config) # no telnet-server permit-admin
amnesiac (config) # write memory
```

- To verify your settings, enter the following command:

```
amnesiac (config) # show telnet-server
Telnet server enabled: no
```

Web proxy

Web proxy functionality for licensing is not FIPS compliant.

- To disable this feature, enter the following commands:

```
amnesiac (config) # no web proxy host <ip-address>
amnesiac (config) # write memory
```

Enabling this feature triggers a configuration warning in FIPS mode.

Disabling FIPS mode

If you no longer want to use FIPS mode, you can turn off this feature.

To disable FIPS mode

1. Connect to the CLI.

2. Enter configuration mode, disable FIPS mode, and restart the system.

   At the system prompt, enter the following set of commands:

```
amnesiac > enable
amnesiac # configure terminal
amnesiac (config) # no fips enable
You must save the configuration and reload the system to disable FIPS mode.
amnesiac (config) # write memory
amnesiac (config) # reload
Rebooting...
amnesiac (config) #
```

When you disable FIPS mode, the system is less restrictive and FIPS compliance configuration warnings no longer appear. Any configuration changes that you made while in FIPS mode (such as disabling certain features or setting specific ciphers) are not modified.

Viewing reports and logs

This section describes how to view common reports and logs. It also describes how to verify FIPS mode activity in the logs. This section includes the following sections:

The NetApp appliance provides access to a wide variety of reports to track usage and activity. You can review reports for features involving networking (including SSL) and diagnostics.

Appliance log reports provide a high-level view of network activity. You can view both user and system logs. The logs are an important tool when you need to monitor activity and ensure that features run in FIPS mode.

Viewing user logs

You can view user logs in the Management Console. The user log filters messages from the system log to display messages that are of immediate use to the system administrator.

View user logs to monitor system activity and to troubleshoot problems; for example, you can monitor who logged in, who logged out, and who entered specific CLI commands, alarms, and errors. The most recent log events appear first.

Viewing system logs

You can view system logs (syslogs) to monitor system activity and to troubleshoot problems. The most recent log events are listed first.

The logs are an important tool when you need to ensure that features run in FIPS mode. For more information, see "Verifying FIPS mode in system logs" on page 173.

Downloading user log files

You can download user logs to monitor system activity and to troubleshoot problems.

The User Logs Download page displays up to 10 archived log files plus the current day log file. By default, the system rotates each file every 24 hours or if the file size reaches one gigabyte uncompressed. You can change this to rotate every week or month. Additionally, you can rotate the files based on file size.

The automatic rotation of system logs deletes your oldest log file, labeled as Archived log #10, pushes the current log to Archived log # 1, and starts a new current-day log file.

Downloading system log files

You can download system logs to monitor system activity and to troubleshoot problems.

The System Logs Download page displays up to 10 archived log files plus the current day log file. By default, the system rotates each file every 24 hours or if the file size reaches one gigabyte uncompressed. You can change this to rotate every week or month. Additionally, you can rotate the files based on file size.

The automatic rotation of system logs deletes your oldest log file, labeled as Archived log #10, pushes the current log to Archived log # 1, and starts a new current-day log file.

Verifying FIPS mode in system logs

You can review the system logs to ensure that features use FIPS mode. Features that run in FIPS mode have entries in the system log that include FIPS_mode_set(1).

The following sections show several examples.

For more information about system logs, see "Viewing system logs" on page 172.

Verifying that file transfers operate in FIPS mode

File transfers, such as configuration fetch, run in FIPS mode and are FIPS compliant. To verify, look for file transfer entries in the syslog when initiating a file download. Ensure these entries have FIPS_mode_set(1).

For example:

```
Mar 18 16:28:34 amnesiac curl: FIPS_mode_set(1)
```

Verifying that NTP operates in FIPS mode

To verify that NTP is running in FIPS mode, examine the system log when NTPD starts (this occurs whenever the NTP configuration is modified) and ensure that the NTPD entry sets FIPS mode:

```
Mar 18 15:49:57 amnesiac pm[4989]: [pm.NOTICE]: Launched ntpd with pid 27617
Mar 18 15:49:57 amnesiac ntpd[27617]: ntpd 4.2.6p4@1.2324-o Thu May 17 21:31:11 UTC 2012 (1)
…
Mar 18 15:49:57 amnesiac ntpd[27617]: FIPS_mode_set(1)
```

Verifying that secure vault operates in FIPS mode

The secure vault contains sensitive information from your AltaVault appliance configuration, including SSL private keys and the data store encryption key. These configuration settings are encrypted on the disk using AES 256-bit encryption.

The secure vault always runs in FIPS mode. To verify, look for the following in the system log at startup:

```
Mar 11 18:28:06 amnesiac encfs: FIPS_mode_set(1)
```

Verifying that SNMP operates in FIPS mode

To verify that SNMP is running in FIPS mode, look for entries similar to the following in the system log when SNMP starts (this occurs whenever the SNMP configuration changes) and ensure that FIPS mode is set:

```
Mar 18 16:05:10 amnesiac pm[4989]: [pm.NOTICE]: Launched snmpd with pid 31709
Mar 18 16:05:10 amnesiac snmpd[31709]: FIPS_mode_set(1)
…
Mar 18 16:05:10 amnesiac snmpd[31709]: NET-SNMP version 5.3.1
```

Verifying that the web interface operates in FIPS mode

The Apache web server for the AltaVault appliance always runs in FIPS mode.

To verify that the web server is in FIPS mode, look for entries similar to the following in the system log:

```
Mar 18 16:22:11 amnesiac httpd: FIPS_mode_set(1)
Mar 18 16:22:11 amnesiac httpd: [Mon Mar 18 16:22:11 2013] [notice] Operating in SSL FIPS mode
```

```
Mar 18 16:22:11 amnesiac httpd: [Mon Mar 18 16:22:11 2013] [notice] Init: Skipping generating
temporary 512 bit RSA private key in FIPS mode
Mar 18 16:22:11 amnesiac httpd: [Mon Mar 18 16:22:11 2013] [notice] Init: Skipping generating
temporary 512 bit DH parameters in FIPS mode
Mar 18 16:22:11 amnesiac httpd: [Mon Mar 18 16:22:11 2013] [notice] Init: Skipping generating
temporary 512 bit RSA private key in FIPS mode
Mar 18 16:22:11 amnesiac httpd: [Mon Mar 18 16:22:11 2013] [notice] Init: Skipping generating
temporary 512 bit DH parameters in FIPS mode
Mar 18 16:22:11 amnesiac httpd: [Mon Mar 18 16:22:11 2013] [notice] Apache/2.2.23 (Unix) mod_ssl/
2.2.23 OpenSSL/1.0.1c-fips configured -- resuming normal operations
```

FIPS CLI

For information about FIPS CLI commands, see the *NetApp AltaVault Cloud Integrated Storage Command-Line Reference Guide*.

CHAPTER 10 Deploying Kerberos-based environments

AltaVault provides an option to join the appliance with a Kerberos-based environment. It includes the following sections:

- "What is Kerberos" on page 175
- "Configuring Kerberos" on page 175

What is Kerberos

Developed at M.I.T., Kerberos is based on symmetric key cryptography and requires a trusted third-party, which is the Key Distribution Center (KDC). Using Kerberos prevents transmission of passwords over the network. Kerberos employs a client/server architecture where a Key Distribution Center knows the keys for all the hosts (realm). When a new host is added, only the KDC and the host must be configured with the host's key (keytab file). A key can be distributed physically or by other secure means.

Configuring Kerberos

You can configure Kerberos from the Configure > NFS page. Kerberos is a protocol that enables a user on a client computer to access files over a network in a manner similar to the way you access local storage.

All Kerberos machines need a keytab file called, /etc/krb5.keytab, to authenticate to the KDC. The keytab file is an encrypted, local, on-disk copy of the host's key. Generate the keytab file to allow AltaVault appliance to authenticate for the NFS services. Provide a valid krb5.keytab file for upload as seen in the left pane.

To set up a Kerberos client on AltaVault appliance, provide a valid krb5.conf configuration file. This file contains Kerberos configuration information, including the locations of KDCs (Key Distribution Centre) and administration servers for the Kerberos realms, default parameters for the current realm and for Kerberos applications, and mappings of host names onto Kerberos realms. Provide a file for upload as seen in the right pane.

Use the two file drop options in the NFS page to drop the krb5.conf and krb5.keytab files on to AltaVault appliance.

To edit an existing configuration

1. Choose Configure > NFS.

2. Expand the export name to complete the configuration as described in this table.

Control	Description
Edit Export	Select this tab to edit the exported NFS share.
Local Path	Change the export file pathname, which starts with a forward slash (/).
Comment	Specify or change the comment about the NFS share.
Export as NFSv4	Select yes or no from the drop-down list to specify the type of NFS export. If you select yes, the export will be configured as NFSv4 export. If you select no, the export will be configured as NFSv3 export.
Kerberos Authentication	Select yes or no from the drop-down list to specify whether or not the export has to be configured with Kerberos authentication. If you select yes, the export will have to be accessed with Kerberos credentials. If you select no, the export will not be configured with Kerberos.
Pinned	Select yes or no from the drop-down list to specify whether or not the data from this share should never be evicted. If you select yes, data written to this share will not be eligible for eviction. If you select no, normal data written to this share is evicted using the default method.
Early Eviction	Select yes or no from the drop-down list to specify whether or not data from this share should be assigned a higher priority for eviction. If you select yes, data written to this share is eligible for eviction earlier than other data. If you select no, data written to this share is evicted using the default method.
Disable Dedupe	Select yes or no from the drop-down list to specify whether or not data written to this share should be checked for duplication. If you select no, then the AltaVault checks if there is duplication of the data written to the share, and deduplicates the data. If you select yes, then the AltaVault does not check if there is duplication of the data written to the share and does not does perform deduplication.
Disable Compression	Select yes or no from the drop-down list to specify whether or not data from this share should be checked for compression. Select yes if your data set is already in a precompressed format. Select no if you data set is not precompressed.
Export Asynchronously	Select the check box to export the NFS share asynchronously. Click the icon i for the following information: Exporting NFS asynchronously forces the server to drop all fsync requests from the client. This is a feature of the NFS protocol. It is required to obtain good performance with NFS clients that issue frequent NFS COMMIT operations, which might degrade the AltaVault performance significantly. Many UNIX clients often execute NFS COMMIT operations when low on memory. To understand the circumstances that cause this behavior and to detect and prevent it, contact your client operating system vendor. The AltaVault automatically synchronizes any file that is idle for a configurable amount of time. The default value is 10 seconds. Although there is a window of time (after the server responds with success for an fsync request and before the data is written to disk), this window is small and performance benefits are large. NetApp recommends exporting NFS asynchronously.
Allow All Clients	Enables all clients connected to the AltaVault system to access the NFS share.

Control	Description
Allow Specified Clients	Enables only the clients that you specify to connect to the AltaVault system to access the NFS share. If you select this option, you must specify the client's IP address and subnet mask in the Client IP/Network text field below it. To enable all clients to access the NFS share, specify 0.0.0.0/0 in the Client IP/Network field.
Mount Commands	Select this tab to display the Linux and UNIX NFS mount commands. You configure the mount commands through the command-line. These commands are for your reference. If the AltaVault is a secondary appliance, the mount commands enable only read permissions and not write permissions.

3. Click **Apply** to apply your changes to the running configuration.

To view mount commands

1. Choose Configure > NFS.
2. Scroll to the bottom and click the share name.

CHAPTER 11 Migrating data from a SteelStore appliance to an AltaVault appliance

This chapter describes how to migrate your data from a physical or virtual SteelStore appliance to a physical AltaVault appliance. The SteelStore appliance is referred to as "source" and the AltaVault appliance is referred to as "target." The physical or virtual SteelStore appliance must be running software version 3.2.3 or higher, and the physical AltaVault appliance must be running version 4.1 or higher.

It includes the following sections:

- "Overview of physical or virtual SteelStore appliance to physical AltaVault appliance" on page 179
- "Data migration connection diagrams" on page 180
- "Data migration process" on page 182
- "Prerequisites" on page 182
- "Performing appliance data migration" on page 184

If you are performing a virtual SteelStore appliance upgrade to a virtual AltaVault appliance, refer to the migration directions in Appendix A of the *NetApp AltaVault Installation and Service Guide for Virtual Appliances*. Do not follow the instructions detailed in this chapter.

Overview of physical or virtual SteelStore appliance to physical AltaVault appliance

SteelStore and AltaVault use a data migration tool to transfer data from a physical or virtual SteelStore appliance to a physical AltaVault appliance. The data is transferred preserving shelf and RAID locality. For example, data from the controller on the source will be migrated to the first RAID group on shelf 1 on the target appliance. Data from the first shelf on the source will be migrated to the second RAID group on shelf 1 on the target appliance, and so on. During data migration both the source and target appliances will be unavailable for backup and recovery.

Data migration connection diagrams

Below are the recommended data migration connectivity diagrams for physical and virtual appliances. The connections you establish will depend on whether you have 1GbE or 10GbE connectivity in your network. Connectivity can include switches, but for best performance it is recommended to use direct connections between appliances using crossover cables.

Figure 11-1. Data migration recommended connectivity diagram for physical appliances

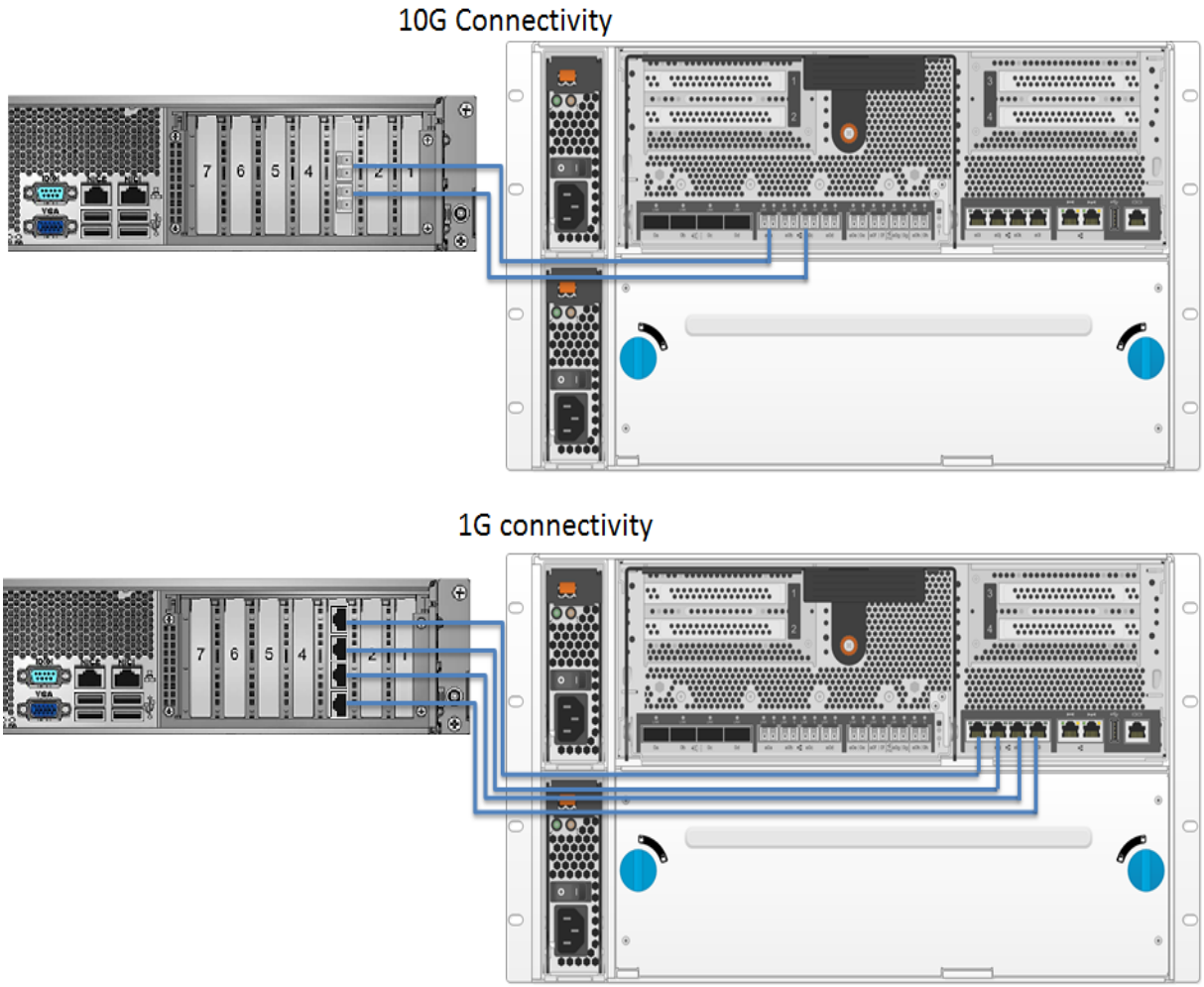
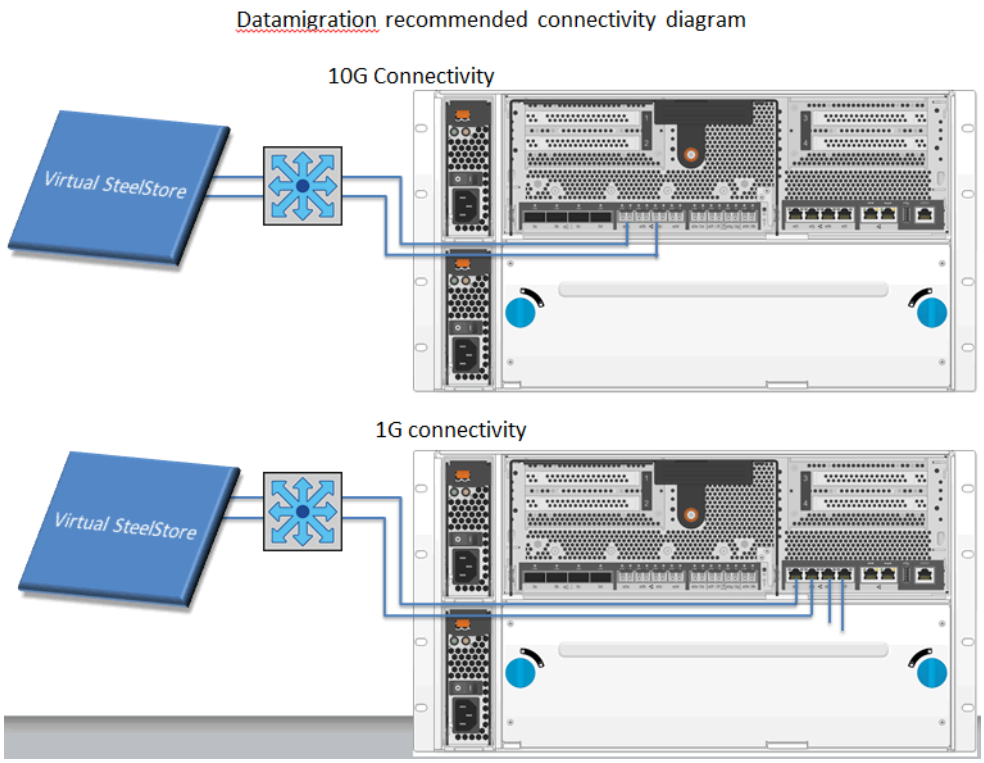


Figure 11-2. Data migration recommended connectivity diagram for virtual appliances



Data migration process

The data migration process is split into four main sections as described in the following table:

Steps	Details
Validate prerequisite steps for source and target appliances	For more information about prerequisite steps, see "Prerequisites" on page 182.
Install the new AltaVault appliance	For information on the procedure, see the *NetApp AltaVault Cloud Integrated Storage Installation Guide for the Physical Appliance*.
Connect the new AltaVault appliance to the original SteelStore appliance	For more information, refer to the suggested network diagram configurations as shown in the "Data migration connection diagrams" on page 180. If further assistance is needed, contact NetApp support.
Run the migration tool to migrate data on to the new AltaVault appliance	For more information on how to migrate, see "Performing appliance data migration" on page 184.
Bring the new AltaVault appliance up	For details, see "Post-data migration procedure" on page 185.
Decommission the SteelStore model	The appliance needs to be decommissioned according to your company's practices regarding decommissioned hardware. If the SteelStore appliance will be reset and used in a new data protection capacity, contact NetApp support for assistance on steps needed to redeploy the appliance.

Note: At any point during the migration process, both the source and the target appliances should not be connected to cloud back-end.

Prerequisites

The following describes the prerequisites required of the source and target appliances prior to performing data migration. It includes the following sections:

- "Prerequisites for the source appliance" on page 182
- "Prerequisites for the target appliance" on page 183

Prerequisites for the source appliance

The following table lists the prerequisites for the source appliance:

Prerequisites for source appliance
The total number of source storage shelves, including the source controller, must be equal to or less than the number of target RAID groups. For example, a SteelStore 3030 with 3 shelves would require an AltaVault appliance with at least 2 shelves, which in turn supports 4 RAID groups. For information on "show shelves" command, see the *NetApp SteelStore Cloud Integrated Storage Command-Line Interface Reference Manual* for 3.2. This does not apply to virtual SteelStore appliances.
The time zone on the source appliance must match that of the target appliance. For more details on identifying the time zone used buy SteelStore, see "Modifying general host settings" on page 67.

Prerequisites for source appliance
The source appliance must be running version 3.2.3 or higher software. To download the required software upgrade, go to https://mysupport.netapp.com. For more information, see the *NetApp SteelStore Cloud Integrated Storage User's Guide 3.2*.
The target appliance must be running version 4.1 or higher software. To download the required software upgrade, go to https://mysupport.netapp.com.

Shut down the storage optimization service. To stop the service using the GUI, go to the Maintenance > Service page. To stop the service using the CLI, open a SSH session to the source appliance and issue the following commands:
`enable`
`configure terminal`
`no service enable`

If an encryption key passphrase was created on the source appliance, make sure to record the value. This passphrase is required for the data migration procedure.
Setup network connectivity to target appliance. Connection via multiple data network interfaces is recommended for faster data transfer and fault tolerance. For more details, see "Data migration connection diagrams" on page 180.
(Optional) If the source appliance has recently recovered from a non-fatal appliance error condition, such as an unexpected reboot, run the File System Check and Verify operations to validate that the data integrity has not been compromised prior to performing data migration. To perform these operations, go to the Reports > Diagnostics > SteelStore File System Check and Reports > Diagnostics > Verify pages. **Note:** File System Check and Verify operations can take several days to run, depending on the amount of storage that must be scanned.

Prerequisites for the target appliance

The following table lists the prerequisites for the target appliance:

Prerequisites for target appliance
The total number of source storage shelves, including the source controller, must be equal to or less than the number of target RAID groups. For example, a SteelStore 3030 with 3 shelves would require an AltaVault appliance with at least 2 shelves, which in turn supports 4 RAID groups. For information on "show raidgroups" command, see the *NetApp AltaVault Cloud Integrated Storage Command-Line Interface Reference Guide*.
The time zone on the source appliance must match that of the target appliance. For details on modifying host settings, see the *NetApp AltaVault Cloud Integrated Storage User's Guide* or the *NetApp SteelStore Cloud Integrated Storage User's Guide.*
The target appliance must be running version 4.1 or higher software. To download the required software upgrade, go to https://mysupport.netapp.com. For more information, review the *NetApp AltaVault Cloud Integrated Storage User's Guide.*
The source appliance must be running version 3.2.3 or higher software. To download the required software upgrade, go to https://mysupport.netapp.com.

Shut down the storage optimization service. To stop the service using the GUI, go to the Reports > Optimization Service page. To stop the service using the CLI, open a SSH session to the source appliance and issue the following commands:
`enable`
`configure terminal`
`no service enable`

Prerequisites for target appliance
The target appliance must be minimally configured with a management IP address, and IP addresses for any data interfaces that the appliance will use to receive data during the data migration process. For details on configuring the management and data interfaces, see "Modifying management interfaces" on page 69 and "Modifying data interfaces" on page 71.

The target datastore must be empty. Use the following CLI commands to format the local datastore:
`enable`
`config t`
`no service enable`
`datastore format local`

Performing appliance data migration

Use the following procedures to perform physical appliance data migration:

- "To perform physical appliance data migration"

To perform physical appliance data migration

1. On the target appliance, start data migration using the following CLI commands. After executing these commands, you will be prompted to enter the encryption key passphrase used to setup the encryption key on the source appliance. This passphrase will be used to import the encryption key on the target appliance. If no passphrase was created, press Enter to continue.

```
<target appliance> > enable
<target appliance> # configure terminal
<target appliance (config)> # datamigration receive
```

2. Once the target appliance is ready, data migration can be initiated on the source appliance. Data migration can transmit both the metadata and the data, or just the metadata. If only metadata is migrated, all data must have been previously replicated to cloud storage by the source appliance. Migrating data and metadata requires additional time, but allows AltaVault to have immediate access to data in cache for quick restore. If the data migration is stopped or interrupted and started again, then migration will continue from where it was interrupted.

   (a). To transfer the data and metadata, use the following CLI commands on the source appliance to start data migration:

```
<source appliance> > enable
<source appliance> # configure terminal
<source appliance (config)> # datamigration send dest-ip <ipaddress1,ipaddress2...>
```

   (b). To exclude data and only send metadata, which includes the hash store, labelmaps, etc. to the target appliance, use the following CLI command.

```
<source appliance (config)> # datamigration send dest-ip <ipaddress1,ipaddress2...>
metadata-only
```

   With metadata-only option, the data pinned on the source appliance will not be transfered to the target appliance. Newly ingested data on the target appliance into pinned shares, as that on the source appliance, will continue to be pinned.

When data migration is performed with metadata-only option, the migration process completes faster than migrating both the data and metadata. The new backup and/or archival data written to the target appliance can dedupe against the data written to the source appliance. However, metadata-only option is not optimized for data restore on the target appliance. Since there are no local cached data on the target appliance it can incur cost to fetch data from cloud storage target. One or more destination interface IP addresses can be provided as part of the data migration command. If more than one destination interface IP address can be provided in comma-separated form as part of the data migration across these interfaces

---

Note: Special consideration must be given when migrating data with AWS Glacier cloud storage target. The default configuration for AWS Glacier cloud storage target is to disable cloud-based deduplication. The datastore cache contains dedupe hashes of only those data segments that are cached locally. A metadata-only transfer of an appliance that is configured to use AWS Glacier cloud back-end might cause data ingested into the new appliance to dedupe against data segments found only in cloud.

---

3. Once data migration is initiated on the source appliance, the tool will validate the state with the receiver on the target appliance. This step depends on the amount of data on the source appliance. It can take up to 5 minutes per shelf on the source appliance.To display the status of data migration, use the following CLI command:

   ```
   <source appliance (config)> # show datamigration status
   ```

4. To stop data migration tool on the source appliance, use the following command:

   ```
   <source appliance (config)> # datamigration send stop
   ```

5. To stop data migration on the target appliance, use the following command:

   ```
   <target appliance (config)> # datamigration receive stop
   ```

6. To reset and restart data migration from the beginning, issue the following CLI commands on both on the source and target appliances. Then repeat step 1 and step 2 to initiate a new data migration.

   ```
   <target appliance (config)> # datamigration receive reset
   <source appliance (config)> # datamigration send reset
   ```

Note: Data pinned on the source appliance will continue to be pinned on the target appliance.

Post-data migration procedure

Once data migration is complete, you need to complete the setup of the target appliance for production use.

To set up the target appliance for production

1. Disconnect the target appliance if it is directly connected to the source appliance, and connect it to the network infrastructure that it will be used in.

2. If required, reconfigure the data interfaces on the target appliance for the new network.

3. Issue the following CLI commands on the target appliance to complete data migration and return the appliance to production use:

   ```
   <target appliance (config)> # megastore guid reset
   <target appliance (config)> # service restart
   ```

APPENDIX A AltaVault appliance MIB

This section provides a reference to the AltaVault Management Information Base (MIB) and SNMP traps. These tools enable you to easily manage and integrate the AltaVault into existing network management systems.

This appendix includes the following sections:

- "Accessing AltaVault appliance MIB" on page 187
- "SNMP traps" on page 187

Accessing AltaVault appliance MIB

AltaVault MIB monitors device status and peers, and provides network statistics for seamless integration into network management systems such as Hewlett-Packard OpenView Network Node Manager, PRTG, and other SNMP browser tools.

For details about configuring and using these network monitoring tools, consult their companies' Web sites.

The following guidelines describe how to download and access the AltaVault MIB using common MIB browsing utilities:

- You can download the AltaVault MIB (NTAP-MIB.txt or AVA-MIB.txt) from the Management Console and load it into any MIB browser utility.
- Some utilities might expect a file type other than a text file. If this occurs, change the file type to the one expected.
- Some utilities assume that the root is mib-2 by default. If the utility sees a new node, such as enterprises, it might look under mib-2.enterprises. If this occurs, use .iso.org.dod.internet.private.enterprises.rbt as the root.
- Some command-line browsers might not load all MIB files by default. If this occurs, find the appropriate command option to load the NTAP-MIB.txt file. For example, for NET-SNMP browsers, snmpwalk -m all.

SNMP traps

Every AltaVault supports SNMP traps and email alerts for conditions that require attention or intervention. An alarm fires for most, but not every, event and the related trap is sent. For most events, when the condition clears, the system clears the alarm and also sends out a clear trap. The clear traps are useful in determining when an event has been resolved.

This section describes the SNMP traps. It does not list the corresponding clear traps.

AltaVault includes support for SNMP v3. This SNMP version not only provides more security and detailed MIB information, but also allows thresholds and alerts on MIBs.

You can view the AltaVault health at the top of each Management Console page, by entering the CLI show info command, and through SNMP (health, systemHealth).

The AltaVault tracks key hardware and software metrics and alerts you of any potential problems so that you can quickly discover and diagnose issues. Appliance health falls into one of the following states:

- Healthy - The AltaVault is functioning and optimizing storage.
- Needs Attention - The AltaVault is optimizing storage, but there are management-related issues. This state accompanies the Healthy state.
- Degraded - The AltaVault is optimizing storage but the system has detected an issue.
- Critical - The AltaVault might not be optimizing storage; you need to address a critical issue.

This table summarizes the SNMP traps sent out from the system to configured trap receivers and their effect on AltaVault health state.

Trap and OID	AltaVault Appliance State	Text	Description
procCrash (1.3.6.1.4.1.17163.1.102.4.0.1)		A procCrash trap signifies that a process managed by PM has crashed and left a core file. The variable sent with the notification indicates which process crashed.	A process has crashed and subsequently been restarted by the system. The trap contains the name of the process that crashed. A system snapshot associated with this crash has been created on the appliance and is accessible via the CLI or the Management Console. NetApp Support might need this information to determine the cause of the crash. No other action is required on the appliance because the crashed process is automatically restarted.
procExit (1.3.6.1.4.1.17163.1.102.4.0.2)		A procExit trap signifies that a process managed by PM has exited unexpectedly, but not left a core file. The variable sent with the notification indicates which process exited.	A process has unexpectedly exited and been restarted by the system. The trap contains the name of the process. The process might have exited automatically or due to other process failures on the appliance. Review the release notes for known issues related to this process exit. If none exist, Contact NetApp Support to determine the cause of this event. No other action is required on the appliance because the crashed process is automatically restarted.
configChange ((1.3.6.1.4.1.17163.1.102.4.0.3)		A change has been made to the system's configuration.	A configuration change has been detected. View the log files around the time of this trap to determine what changes were made and whether they were authorized.
cpuUtil (1.3.6.1.4.1.17163.1.102.4.0.4)	Degraded	The average CPU utilization in the past minute has gone above the acceptable threshold.	Average CPU utilization has exceeded an acceptable threshold. If CPU utilization spikes are frequent, it might be because the system is undersized. Sustained CPU load can be symptomatic of more serious issues. Consult the CPU Utilization report to gauge how long the system has been loaded and also monitor the amount of traffic currently going through the appliance. A one-time spike in CPU is normal but NetApp recommends reporting extended high CPU utilization to NetApp Support. No other action is necessary because the alarm clears automatically.
pagingActivity (1.3.6.1.4.1.17163.1.102.4.0.5)	Degraded	The system has been paging excessively (thrashing).	The system is running low on memory and has begun swapping memory pages to disk. This event can be triggered during a software upgrade while the storage optimization service is still running, but there can be other causes. If this event triggers at any other time, generate a debug sysdump report and send it to NetApp Support. No other action is required because the alarm clears automatically.

Trap and OID	AltaVault Appliance State	Text	Description
linkError (1.3.6.1.4.1.17163.1.102.4.0.6)	Degraded	An interface on the appliance has lost its link.	The system has lost one of its Ethernet links due to a network event. Check the physical connectivity between the AltaVault and its neighbor device. Investigate this alarm as soon as possible. Depending on what link is down, the system might no longer be optimizing and a network outage could occur. This is often caused by surrounding devices, like routers or switches transitioning their interfaces. This alarm also accompanies service or system restarts on the AltaVault.
powerSupplyError (1.3.6.1.4.1.17163.1.102.4.0.7)	Degraded	A power supply on the appliance has failed (not supported on all models).	A redundant power supply on the appliance has failed and needs to be replaced. Contact NetApp Support for an RMA replacement soon.
fanError (1.3.6.1.4.1.17163.1.102.4.0.8)	Degraded	A fan has failed on this appliance (not supported on all models).	A fan is failing or has failed and needs to be replaced. Contact NetApp Support for an RMA replacement soon.
memoryError (1.3.6.1.4.1.17163.1.102.4.0.9)	Degraded	A memory error has been detected on the appliance (not supported on all models).	A memory error has been detected. A system memory stick might be failing. Try reseating the memory first. If the problem persists, contact NetApp Support for an RMA replacement soon.
ipmi (1.3.6.1.4.1.17163.1.102.4.0.10)	Degraded	An IPMI event has been detected on the appliance. Check the details in the alarm report on the Web UI (not supported on all models).	An Intelligent Platform Management Interface (IPMI) event has been detected. Check the Alarm Status page for more detail. You can also view the IPMI events on the AltaVault by entering the CLI command: `show hardware error-log all`
localFSFull (1.3.6.1.4.1.17163.1.102.4.0.11)		The appliance local file system is full.	The AltaVault local file system is full. Check the Eviction report and contact NetApp Support.
temperatureCritical (1.3.6.1.4.1.17163.1.102.4.0.12)	Critical	The system temperature has reached a critical stage.	This trap/alarm triggers a critical state on the appliance. This alarm occurs when the appliance temperature reaches 90 degrees Celsius. The temperature value is not user configurable. Reduce the appliance temperature.
temperatureWarning (1.3.6.1.4.1.17163.1.102.4.0.13)	Degraded	The system temperature has exceeded the threshold.	The appliance temperature is a configurable notification. By default, this notification is set to trigger when the appliance reached 70 degrees Celsius. Raise the alarm trigger temperature if it is normal for the AltaVault to get that hot, or reduce the temperature of the AltaVault.
scheduledJobError (1.3.6.1.4.1.17163.1.102.4.0.14)		A scheduled job has failed during execution.	A scheduled job on the system (for example, a software upgrade) has failed. To determine which job failed, use the CLI or the Management Console.

Trap and OID	AltaVault Appliance State	Text	Description
confModeEnter (1.3.6.1.4.1.17163.1.102.4.0.15)		A user has entered configuration mode.	A user on the system has entered a configuration mode from either the CLI or the Management Console. A login to the Management Console by user admin sends this trap as well. This message is for notification purposes only; no other action is necessary.
confModeExit (1.3.6.1.4.1.17163.1.102.4.0.16)		A user has exited configuration mode.	A user on the system has exited configuration mode from either the CLI or the Management Console. A logout of the Management Console by user admin sends this trap as well. This message is for notification purposes only; no other action is necessary.
secureVaultLocked (1.3.6.1.4.1.17163.1.102.4.0.17)	Needs Attention	The secure vault is locked. The secure data cannot be used.	The secure vault is locked. The datastore cannot be encrypted. Check the Alarm Status page for more details. The alarm clears when the secure vault is unlocked.
dirtyCloud (1.3.6.1.4.1.17163.1.102.4.0.19)		The cloud bucket is not empty even though the local datastore is.	There is data in the cloud although the AltaVault datastore is empty. Enable replication and recovery to ensure that the cloud storage is synchronized with the datastore.
license (1.3.6.1.4.1.17163.1.102.4.0.21)		The WWBASE license is missing, expired, or invalid.	A license on AltaVault has been removed, has expired, or is invalid. The alarm clears when a valid license is added or updated.
lowSpace (1.3.6.1.4.1.17163.1.102.4.0.22)		The backup service is running out of space.	The AltaVault storage optimization service is running out of space. Delete extra files and ensure that there is more space.
overCapacity (1.3.6.1.4.1.17163.1.102.4.0.24)		The cloud bucket has reached its licensed capacity.	AltaVault capacity license manages the capacity of the storage within the cloud that the system can address. The cloud storage has reached the licensed capacity limit. You must increase your capacity license or decrease your data storage.
replicationError (1.3.6.1.4.1.17163.1.102.4.0.25)		Replication encountered a non-fatal error.	There was an error in the replication process. The system automatically retries the replication process. Contact your cloud service provider or NetApp Support.
replicationPause (1.3.6.1.4.1.17163.1.102.4.0.26)		Replication was paused.	Replication was paused because you scheduled it to pause at the current time.
serviceError (1.3.6.1.4.1.17163.1.102.4.0.27)	Degraded	The backup service could not initialize properly.	The storage optimization service has encountered a condition that might degrade its performance. See the system log for more information. No other action is necessary.
portalUnreachable (1.3.6.1.4.1.17163.1.102.4.0.28)		The NetApp Cloud Portal is unreachable.	The AltaVault cannot access the NetApp Cloud Portal.

Trap and OID	AltaVault Appliance State	Text	Description
rplctdBytesPending (1.3.6.1.4.1.17163.1.102.4.0.29)		Too many bytes pending to be replicated.	The number of bytes pending replication to the cloud has exceeded the “Bytes pending replication” alert limit. This might be due to a slow replication link or because the appliance is undersized. Increase the amount of replication bandwidth available to the AltaVault or temporarily stop backup operations so that replication can normalize.
cloudDispError (1.3.6.1.4.1.17163.1.102.4.0.30)		The appliance might be connecting to another appliance’s cloud bucket.	This indicates that the cloud bucket that the AltaVault is trying to connect to might be in use by another AltaVault. This prevents corruption of the files in the cloud.
dataEviction (1.3.6.1.4.1.17163.1.102.4.0.31)		The appliance had to evict recent data to prevent running out of space in the datastore.	This indicates that the system has detected an issue with datastore eviction. The alarm triggers when the appliance starts evicting data from the local disk cache and the age of the evicted data is relatively young. An AltaVault has disk space much smaller than the total addressable space on the cloud, and if disk space runs low, the appliance starts evicting data from disk that has not been used recently. This keeps only fresh and frequently accessed data in cache. The AltaVault keeps statistics about how old the evicted data is (this is the average evicted age). Usually, only old data is evicted. This behavior is generally not a problem and does not trigger an alarm. However, the appliance might be experiencing such a huge workload that more and more recent data needs to be evicted from the appliance to make space for incoming data. This causes the average evicted age to decrease, and when it goes below a certain threshold, the average evicted age alarm triggers. This alarm is an anomalous event, signaling that the appliance is handling a much larger workload than expected. This alarm is useful in detecting whether the appliance is undersized relative to your normal workload. If the alarm is constantly triggered, then you should consider moving your data to a AltaVault model with a larger disk cache.

Trap and OID	AltaVault Appliance State	Text	Description
approachingCapacity (1.3.6.1.4.1.17163.1.102.4.0.32)		The cloud bucket is approaching its licensed capacity.	This indicates that the amount of storage that the AltaVault used in the cloud bucket is approaching the licensed cloud capacity amount. Consider the following options: • Upgrade the AltaVault to a version that can accommodate more space. • Add more AltaVaults (each of which will account for subsets of your entire data) in your network. • Delete data from the AltaVault and reclaim used space.
blockstoreFull (1.3.6.1.4.1.17163.1.102.4.0.34)		The System reserved space is full.	The amount of reserved space on the AltaVault is full. Contact NetApp Support.
shelfError (1.3.6.1.4.1.17163.1.102.4.0.35)		One or more shelves have errors.	One or more expansion shelves attached to the AltaVault have errors. Contact NetApp Support.
lowMemory (1.3.6.1.4.1.17163.1.102.4.0.36)		The system doesn't have enough memory to start service.	Memory usage on the AltaVault is high. The storage optimization system performance might decrease if the amount of memory available to the AltaVault remains low.
restoresNotThrottled (1.3.6.1.4.1.17163.1.102.4.0.37)		The appliance has exceeded its free restore limit or restore throttling has been disabled.	The restore throttling alarm is applicable only when the cloud storage used is AWS Glacier. AWS Glacier documentation specifies a monthly limit up to which no restore costs are charged for retrieving data from Glacier. Once this limit is crossed, data retrieval costs can be substantial. For details, see AWS Glacier documentation. By default, the AltaVault has a restore throttle for data retrieved from Glacier. This throttle keeps retrievals below the no-cost limit. The default value of this restore throttle is 5%. Therefore, you can use the AltaVault to restore 5% of total cloud usage in a month. The throttle is enforced on an hourly basis. Hourly data retrieval is limited to (5% of the total cloud use)/(hours per month). You can increase the 5% restore throttle limit up to 100% or completely disable it by setting the limit to 0. You might incur data retrieval charges when you make this change.
hwraidDiskIndivError (1.3.6.1.4.1.17163.1.102.4.0.38)		The appliance has detected an error with one or more disks.	One or more disks had has detected an error.

Trap and OID	AltaVault Appliance State	Text	Description
shelfPowerSupply (1.3.6.1.4.1.17163.1.102.4.0.39)		One or more shelves have a power supply error.	One or more shelves have a power supply error.
hwraidBbuError (1.3.6.1.4.1.17163.1.102.4.0.40)		The Storage Optimization Service is disabled because the RAID is degraded and the battery backup unit is not sufficiently charged.	The Storage Optimization Service is disabled because the RAID is degraded and the battery backup unit is not sufficiently charged.
bbuIndivError (1.3.6.1.4.1.17163.1.102.4.0.41)		One or more battery backup units have errors.	One or more battery backup units have errors.
hwraidIntegrityCheckError (1.3.6.1.4.1.17163.1.102.4.0.42)		RAID integrity check alarm triggered due to unclean shutdown.	RAID integrity check alarm triggered due to unclean shutdown.
evalModeExpiry (1.3.6.1.4.1.17163.1.102.4.0.43)		Evaluation mode for this virtual appliance is expiring soon.	Evaluation mode for this virtual appliance is expiring soon.
metadataSpaceFull (1.3.6.1.4.1.17163.1.102.4.0.44)		The space reserved for metadata is full.	The space reserved for metadata is full.
inodesThresholdReached (1.3.6.1.4.1.17163.1.102.4.0.45)		The maximum inodes limit has been reached.	The maximum inodes limit has been reached.
dataIntegrityError (1.3.6.1.4.1.17163.1.102.4.0.46)		Data integrity check has reported an inconsistency.	The data integrity check has reported an inconsistency.
replicationInconsistent (1.3.6.1.4.1.17163.1.102.4.0.47)		Replication is experiencing high number of retries.	The replication is experiencing high number of retries.
inconsistentCloudData (1.3.6.1.4.1.17163.1.102.4.0.48)		Possible cloud data corruption or inconsistency.	A possible cloud data corruption or inconsistency has been detected.
softwareUpdateAvailable (1.3.6.1.4.1.17163.1.102.4.0.49)		Software updated available.	A software update is available.
firmwareUpgrade (1.3.6.1.4.1.17163.1.102.4.0.50)		Firmware upgrade available.	A firmware upgrade is available.
controllerPowerSupplyError (1.3.6.1.4.1.17163.1.102.4.0.51)		A power supply on the controller has failed.	A power supply on the controller has failed.
controllerFanError (1.3.6.1.4.1.17163.1.102.4.0.52)		A fan has failed on the controller.	A fan has failed on the controller.

Trap and OID	AltaVault Appliance State	Text	Description
cpuUtilClear (1.3.6.1.4.1.17163.1.102.4.0.10004)		The average CPU utilization has fallen back within the acceptable threshold.	Average CPU utilization exceeded an acceptable threshold, but has now fallen back to an acceptable threshold. If CPU utilization spikes are frequent, it might be because the system is undersized. Sustained CPU load can be symptomatic of more serious issues. Consult the CPU Utilization report to gauge how long the system has been loaded and also monitor the amount of traffic currently going through the appliance. A one-time spike in CPU is normal but NetApp recommends reporting extended high CPU utilization to NetApp Support. No other action is necessary because the alarm clears automatically.
pagingActivityClear (1.3.6.1.4.1.17163.1.102.4.0.10005)	Degraded	The system has stopped paging excessively (thrashing).	The system that was running low on memory and was swapping memory pages to disk has stopped paging excessively, and the alarm clears.
linkErrorClear (1.3.6.1.4.1.17163.1.102.4.0.10006)		An interface on the appliance has regained its link.	The system has regained the Ethernet link it lost due to a network event and clears the alarm.
powerSupplyErrorClear (1.3.6.1.4.1.17163.1.102.4.0.10007)		All power supplies are now functioning normally.	A redundant power supply had failed on the appliance, but this is now corrected and all power supplies are functioning properly.
fanErrorClear (1.3.6.1.4.1.17163.1.102.4.0.10008)		All system fans are now functioning normally.	A fan on the appliance had failed, but now all fans are functioning normally.
memoryErrorClear (1.3.6.1.4.1.17163.1.102.4.0.10009)		A memory error has been rectified on the appliance.	There was an alarm due to a memory error on the appliance, but this is now cleared because the memory error has been corrected.
ipmiClear (1.3.6.1.4.1.17163.1.102.4.0.10010)		An IPMI event has been rectified on the appliance.	An Intelligent Platform Management Interface (IPMI) event was detected, but it is now corrected.
localFSFullClear (1.3.6.1.4.1.17163.1.102.4.0.10011)		The appliance local file system usage is below threshold.	The appliance local file system usage exceeded the permitted threshold, but the usage is now below the threshold.
temperatureNonCritical (1.3.6.1.4.1.17163.1.102.4.0.10012)		The system temperature is no longer in a critical stage.	The alarm that occurred when the appliance temperature reached 90 degrees Celsius is now cleared.
temperatureNormal (1.3.6.1.4.1.17163.1.102.4.0.10013)		The system temperature is back within the threshold.	The temperature of the appliance exceeded the threshold (default value of 70 degrees Celsius), but is now back within the threshold.
secureValutUnlocked (1.3.6.1.4.1.17163.1.102.4.0.10017)		Secure vault is unlocked. The secure data store can be used now.	The secure vault, which was locked, is now unlocked and you can use the secure datastore.
dirtyCloudClear (1.3.6.1.4.1.17163.1.102.4.0.10019)		The cloud consistency issue has been resolved.	Both the cloud bucket and the datastore are synchronized.

Trap and OID	AltaVault Appliance State	Text	Description
licenseClear (1.3.6.1.4.1.17163.1.102.4.0.10021)		The appliance is now properly licensed.	A license on the AltaVault was removed, had expired, or was invalid, but, the license has been installed correctly again.
lowSpaceClear (1.3.6.1.4.1.17163.1.102.4.0.10022)		The appliance now has enough space for datastore.	The appliance did not have enough space for datastore earlier. Now, it has enough space and the alarm is cleared.
overCapacityClear (1.3.6.1.4.1.17163.1.102.4.0.10024)		The cloud bucket is no longer over its licensed capacity.	The cloud storage meets the storage limit allocated by its capacity license.
replicationErrorClear (1.3.6.1.4.1.17163.1.102.4.0.10025)		Replication error has been cleared.	There was an error in the replication process, but this is now cleared.
replicationPauseClear (1.3.6.1.4.1.17163.1.102.4.0.10026)		Replication was resumed.	Replication had paused, but it has resumed.
serviceErrorClear (1.3.6.1.4.1.17163.1.102.4.0.10027)		The backup service initialized properly.	There was an error in the storage optimization service, but this is now corrected.
portalUnreachableClear (1.3.6.1.4.1.17163.1.102.4.0.10028)		The NetApp Cloud Portal is now reachable.	The AltaVault could not access the NetApp Cloud Portal, but this is now corrected.
rplctdBytesPendingClear (1.3.6.1.4.1.17163.1.102.4.0.10029)		Number of bytes pending replication is within normal range now.	The number of bytes pending replication had exceeded the bytes pending alert limit, but this is now corrected.
cloudDispErrorClear (1.3.6.1.4.1.17163.1.102.4.0.10030)		The appliance is now connecting to its own cloud bucket.	The cloud bucket that the AltaVault was connecting to was in use by another AltaVault. This issue is now corrected and the AltaVault is connected to its own cloud bucket.
dataEvictionClear (1.3.6.1.4.1.17163.1.102.4.0.10031)		The appliance is no longer evicting data.	The datastore eviction issue is now corrected.
blockstoreFullClear (1.3.6.1.4.1.17163.1.102.4.0.10033)		The System reserved space is now enough.	The amount of reserved space on the AltaVault is now sufficient for the storage optimization service to run efficiently.
shelfErrorClear (1.3.6.1.4.1.17163.1.102.4.0.10034)		All shelves are working properly.	There was an error in one of the expansion shelves attached to the AltaVault, but this is now corrected.
lowMemoryClear ((1.3.6.1.4.1.17163.1.102.4.0.10035)		The system has enough memory.	The amount of memory available to the AltaVault is now sufficient.
restoresNotThrottledClear (1.3.6.1.4.1.17163.1.102.4.0.10036)		Restore throttling is now in effect.	The restore throttling alarm is applicable only when the cloud storage used is AWS Glacier. The restore operations were not throttled due to an error, but this is now corrected.
hwraidDiskIndivClear (1.3.6.1.4.1.17163.1.102.4.0.10037)		All disks are functioning properly.	All the disks are functioning properly.
shelfPowerSupplyClear (1.3.6.1.4.1.17163.1.102.4.0.10038)		All shelves have proper power supply.	All the shelves have proper power supply.

Trap and OID	AltaVault Appliance State	Text	Description
hwraidBbuErrorClear (1.3.6.1.4.1.17163.1.102.4.0.10039)		The storage optimization service is no longer disabled.	The storage optimization service is no longer disabled.
bbuIndivClear (1.3.6.1.4.1.17163.1.102.4.0.10040)		All battery backup units are functioning properly.	All the battery backup units are functioning properly.
hwraidIntegrityCheckClear (1.3.6.1.4.1.17163.1.102.4.0.10041)		RAID integrity check alarm cleared.	The RAID integrity check alarm cleared.
evalModeExpiryClear (1.3.6.1.4.1.17163.1.102.4.0.10042)		The virtual appliance is no longer running in evaluation mode.	The virtual appliance is no longer running in evaluation mode.
metadataSpaceFullClear (1.3.6.1.4.1.17163.1.102.4.0.10043)		The metadata reserved space is now enough.	The metadata reserved space is sufficient.
inodesThresholdReachedClear (1.3.6.1.4.1.17163.1.102.4.0.10044)		The number of inodes is now below the maximum limit.	The number of inodes is now below the maximum limit.
dataIntegrityErrorClear (1.3.6.1.4.1.17163.1.102.4.0.10045)		The data integrity check alarm cleared.	The data integrity check alarm has cleared.
replicationInconsistentClear (1.3.6.1.4.1.17163.1.102.4.0.10046)		The replication is no longer experiencing retries now.	The replication is no longer experiencing retries.
inconsistentCloudDataClear (1.3.6.1.4.1.17163.1.102.4.0.10047)		Restored cloud data consistency.	The cloud data consistency has been restored.
softwareUpdateAvailableClear (1.3.6.1.4.1.17163.1.102.4.0.10048)		Software update available alarm cleared.	The software update alarm has been cleared.
firmwareUpgradeClear (1.3.6.1.4.1.17163.1.102.4.0.10049)		Firmware upgrade alarm cleared.	The firmware upgrade alarm is cleared.
controllerPowerSupplyErrorClear (1.3.6.1.4.1.17163.1.102.4.0.10050)		All power supplies are now functioning normally.	All the power supplies are functioning.
controllerFanErrorClear (1.3.6.1.4.1.17163.1.102.4.0.10051)		All controller fans are now functioning normally.	All the controller fans are functioning.

APPENDIX B Amazon AWS IAM and S3 bucket policies

Amazon AWS provides the ability to specify Identity and Access Management (IAM) policies and bucket policies to control permissions related to AWS users and S3 cloud buckets. In general, IAM users and buckets should be configured with the minimum permissions required for normal operation. For more details about Amazon's best practices, see
http://docs.aws.amazon.com/IAM/latest/UserGuide/IAMBestPractices.html.

For more information on Amazon AWS, see the *NetApp AltaVault Cloud Integrated Storage Installation and Service Guide for Cloud Appliances*.

This appendix includes the following sections:

- "Typical AltaVault setup" on page 199
- "IAM policies for AltaVault" on page 199
- "Bucket policies for AltaVault" on page 201

Typical AltaVault setup

A typical AltaVault setup includes the following AWS configuration:

- One IAM user created exclusively for AltaVault. Access keys are generated for the user and entered into the AltaVault cloud configuration. AltaVault never requires access keys for the root AWS account. It is recommended that access keys are not generated for the root account.
- An IAM group is created with the AltaVault user. A policy is set on the group that allows only the permissions used by AltaVault.
- If a bucket policy is required, then a bucket is created for use by AltaVault, with a policy that allows only the AltaVault user to access it. It is not necessary to create the bucket prior to AltaVault using it if bucket policies are not required.

IAM policies for AltaVault

IAM policies allow access to the Amazon S3 account and its associated cloud buckets via different users with restricted permissions, in contrast to the root account which has unrestricted access to the account and cloud buckets. It is recommended that programmatic access (including access via appliances such as AltaVault) to Amazon AWS and S3 are done via IAM users with the appropriate permissions rather than via the root AWS account.

AltaVault requires the following IAM user permissions:

- On all buckets:
  - ListAllMyBuckets (not required for normal operation, but some features may not work)
- On the configured cloud bucket:
  - CreateBucket (not required if the bucket has been created beforehand)
  - GetBucketLocation
  - ListBucket
  - ListBucketMultipartUploads
  - GetLifecycleConfiguration
  - PutLifecycleConfiguration
- On objects inside the configured cloud bucket:
  - AbortMultipartUpload
  - DeleteObject
  - GetObject
  - ListMultipartUploadParts
  - PutObject
  - RestoreObject

Sample of IAM policy

Below is a sample of the IAM policy implementing the above permissions:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1394143726000",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets"
      ],
      "Resource": [
        "arn:aws:s3:::*"
      ]
    },
    {
      "Sid": "Stmt1394143742000",
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource": [
        "arn:aws:s3:::bucket_name"
      ]
    },
```

```
    {
      "Sid": "Stmt1394143790000",
      "Effect": "Allow",
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:ListMultipartUploadParts",
        "s3:GetObject",
        "s3:PutObject",
        "s3:RestoreObject"
      ],
      "Resource": [
        "arn:aws:s3:::bucket_name/*"
      ]
    }
  ]
}
```

Bucket policies for AltaVault

Amazon S3 bucket policies can be configured to allow only specific users (including users outside the AWS account) to access an S3 cloud bucket, and can be used in conjunction with IAM user policies. AltaVault requires that the cloud bucket (configured in the AltaVault management console under Configure > Cloud Settings) allows access by the IAM user configured for AltaVault. No access by any other user is required.

AltaVault requires a set of permissions in the bucket policy similar to the set of permissions for an IAM policy, with the exception of s3:ListAllMyBuckets and s3:CreateBucket, which are not relevant at the bucket level.

Sample of bucket policy

Below is a sample of the bucket policy:

```
{
  "Id": "Policy1394662102999",
  "Statement": [
    {
      "Sid": "Stmt1394661890920",
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetLifecycleConfiguration",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutLifecycleConfiguration"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::bucket_name",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/user_name"
        ]
      }
    },
    {
      "Sid": "Stmt1394661925663",
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:ListMultipartUploadParts",
        "s3:GetObject",
```

```
        "s3:PutObject",
        "s3:RestoreObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::bucket_name/*",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/user_name"
        ]
      }
    }
  ]
}
```

APPENDIX C Root certificates

You cannot import a root certificate onto the AltaVault appliance. If you are configuring a cloud that does not use one of the installed root certificates, you can select Enable Cloud CA Certificate on the Configure > Cloud Settings page and upload a certificate to the AltaVault.

Below is a list of the root certificates issuers that are installed on the AltaVault appliance.

Issuer: C=AT, O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH, OU=A-Trust-nQual-03, CN=A-Trust-nQual-03

Issuer: CN=ACCVRAIZ1, OU=PKIACCV, O=ACCV, C=ES

Issuer: CN=ACEDICOM Root, OU=PKI, O=EDICOM, C=ES

Issuer: C=CO, O=Sociedad Cameral de Certificaci\xC3\xB3n Digital - Certic\xC3\xA1mara S.A., CN=AC Ra\xC3\xADz Certic\xC3\xA1mara S.A.

Issuer: C=IT, L=Milan, O=Actalis S.p.A./03358520967, CN=Actalis Authentication Root CA

Issuer: C=SE, O=AddTrust AB, OU=AddTrust External TTP Network, CN=AddTrust External CA Root

Issuer: C=SE, O=AddTrust AB, OU=AddTrust TTP Network, CN=AddTrust Class 1 CA Root

Issuer: C=SE, O=AddTrust AB, OU=AddTrust TTP Network, CN=AddTrust Public CA Root

Issuer: C=SE, O=AddTrust AB, OU=AddTrust TTP Network, CN=AddTrust Qualified CA Root

Issuer: C=US, O=AffirmTrust, CN=AffirmTrust Commercial

Issuer: C=US, O=AffirmTrust, CN=AffirmTrust Networking

Issuer: C=US, O=AffirmTrust, CN=AffirmTrust Premium

Issuer: C=US, O=AffirmTrust, CN=AffirmTrust Premium ECC

Issuer: C=US, O=America Online Inc., CN=America Online Root Certification Authority 1

Issuer: C=US, O=America Online Inc., CN=America Online Root Certification Authority 2

Issuer: C=JP, O=Japanese Government, OU=ApplicationCA

Issuer: CN=Atos TrustedRoot 2011, O=Atos, C=DE

Issuer: C=ES, CN=Autoridad de Certificacion Firmaprofesional CIF A62634068

Issuer: C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root

Issuer: C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=http://www.usertrust.com, CN=UTN-USERFirst-Hardware

Issuer: C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=http://www.usertrust.com, CN=UTN-USERFirst-Hardware

Issuer: C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=http://www.usertrust.com, CN=UTN-USERFirst-Hardware

Issuer: C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=http://www.usertrust.com, CN=UTN-USERFirst-Hardware

Issuer: C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=http://www.usertrust.com, CN=UTN-USERFirst-Hardware

Issuer: C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=http://www.usertrust.com, CN=UTN-USERFirst-Hardware

Issuer: C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=http://www.usertrust.com, CN=UTN-USERFirst-Hardware

Issuer: C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=http://www.usertrust.com, CN=UTN-USERFirst-Hardware

Issuer: C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=http://www.usertrust.com, CN=UTN-USERFirst-Hardware

Issuer: C=NO, O=Buypass AS-983163327, CN=Buypass Class 2 CA 1

Issuer: C=NO, O=Buypass AS-983163327, CN=Buypass Class 2 Root CA

Issuer: C=NO, O=Buypass AS-983163327, CN=Buypass Class 3 CA 1

Issuer: C=NO, O=Buypass AS-983163327, CN=Buypass Class 3 Root CA

Issuer: C=SK, L=Bratislava, O=Disig a.s., CN=CA Disig

Issuer: C=SK, L=Bratislava, O=Disig a.s., CN=CA Disig Root R1

Issuer: C=SK, L=Bratislava, O=Disig a.s., CN=CA Disig Root R2

Issuer: C=CN, O=CNNIC, CN=CNNIC ROOT

Issuer: C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO Certification Authority

Issuer: C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Certification Authority

Issuer: C=EU, O=AC Camerfirma SA CIF A82743287, OU=http://www.chambersign.org, CN=Chambers of Commerce Root

Issuer: C=EU, O=AC Camerfirma SA CIF A82743287, OU=http://www.chambersign.org, CN=Global Chambersign Root

Issuer: C=FR, O=Dhimyotis, CN=Certigna

Issuer: C=FR, O=Certinomis, OU=0002 433998903, CN=Certinomis - Autorit\xC3\xA9 Racine

Issuer: C=FR, O=Certplus, CN=Class 2 Primary CA

Issuer: C=PL, O=Unizeto Sp. z o.o., CN=Certum CA

Issuer: C=PL, O=Unizeto Technologies S.A., OU=Certum Certification Authority, CN=Certum Trusted Network CA

Issuer: C=EU, L=Madrid (see current address at www.camerfirma.com/address)/serialNumber=A82743287, O=AC Camerfirma S.A., CN=Chambers of Commerce Root - 2008

Issuer: C=CN, O=China Internet Network Information Center, CN=China Internet Network Information Center EV Certificates Root

Issuer: CN=ComSign CA, O=ComSign, C=IL

Issuer: CN=ComSign Secured CA, O=ComSign, C=IL

Issuer: C=GB, ST=Greater Manchester, L=Salford, O=Comodo CA Limited, CN=AAA Certificate Services

Issuer: C=GB, ST=Greater Manchester, L=Salford, O=Comodo CA Limited, CN=Secure Certificate Services

Issuer: C=GB, ST=Greater Manchester, L=Salford, O=Comodo CA Limited, CN=Trusted Certificate Services

Issuer: O=Cybertrust, Inc, CN=Cybertrust Global Root

Issuer: C=DE, O=D-Trust GmbH, CN=D-TRUST Root Class 3 CA 2 2009

Issuer: C=DE, O=D-Trust GmbH, CN=D-TRUST Root Class 3 CA 2 EV 2009

Issuer: C=US, O=Digital Signature Trust, OU=DST ACES, CN=DST ACES CA X6

Issuer: O=Digital Signature Trust Co., CN=DST Root CA X3

Issuer: C=DE, O=Deutsche Telekom AG, OU=T-TeleSec Trust Center, CN=Deutsche Telekom Root CA 2

Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Assured ID Root CA

Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA

Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert High Assurance EV Root CA

Issuer: C=US, O=Digital Signature Trust Co., OU=DSTCA E1

Issuer: C=US, O=Digital Signature Trust Co., OU=DSTCA E2

Issuer: C=TR, O=Elektronik Bilgi Guvenligi A.S., CN=e-Guven Kok Elektronik Sertifika Hizmet Saglayicisi

Issuer: C=TR, L=Ankara, O=E-Tu\xC4\x9Fra EBG Bili\xC5\x9Fim Teknolojileri ve Hizmetleri A.\xC5\x9E., OU=E-Tugra Sertifikasyon Merkezi, CN=E-Tugra Certification Authority

Issuer: CN=EBG Elektronik Sertifika Hizmet Sa\xC4\x9Flay\xC4\xB1c\xC4\xB1s\xC4\xB1, O=EBG Bili\xC5\x9Fim Teknolojileri ve Hizmetleri A.\xC5\x9E., C=TR

Issuer: C=ES, O=Agencia Catalana de Certificacio (NIF Q-0801176-I), OU=Serveis Publics de Certificacio, OU=Vegeu https://www.catcert.net/verarrel (c)03, OU=Jerarquia Entitats de Certificacio Catalanes, CN=EC-ACC

Issuer: C=EE, O=AS Sertifitseerimiskeskus, CN=EE Certification Centre Root CA/emailAddress=pki@sk.ee

Issuer: O=Entrust.net, OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.), OU=(c) 1999 Entrust.net Limited, CN=Entrust.net Certification Authority (2048)

Issuer: C=US, O=Entrust.net, OU=www.entrust.net/CPS incorp. by ref. (limits liab.), OU=(c) 1999 Entrust.net Limited, CN=Entrust.net Secure Server Certification Authority

Issuer: C=US, O=Entrust, Inc., OU=www.entrust.net/CPS is incorporated by reference, OU=(c) 2006 Entrust, Inc., CN=Entrust Root Certification Authority

Issuer: C=US, O=Equifax, OU=Equifax Secure Certificate Authority

Issuer: C=US, O=Equifax Secure Inc., CN=Equifax Secure Global eBusiness CA-1

Issuer: C=US, O=Equifax Secure Inc., CN=Equifax Secure eBusiness CA-1

Issuer: C=NL, O=DigiNotar, CN=DigiNotar Cyber CA/emailAddress=info@diginotar.nl

Issuer: C=NL, O=DigiNotar, CN=DigiNotar Cyber CA

Issuer: C=NL, O=DigiNotar, CN=DigiNotar Root CA/emailAddress=info@diginotar.nl

Issuer: C=NL, O=DigiNotar, CN=DigiNotar Services 1024 CA/emailAddress=info@diginotar.nl

Issuer: C=NL, O=DigiNotar B.V., CN=DigiNotar PKIoverheid CA Overheid en Bedrijven

Issuer: C=NL, O=DigiNotar B.V., CN=DigiNotar PKIoverheid CA Organisatie - G2

Issuer: C=US, O=GTE Corporation, OU=GTE CyberTrust Solutions, Inc., CN=GTE CyberTrust Global Root

Issuer: O=Entrust.net, OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.), OU=(c) 1999 Entrust.net Limited, CN=Entrust.net Certification Authority (2048)

Issuer: C=US, O=GTE Corporation, OU=GTE CyberTrust Solutions, Inc., CN=GTE CyberTrust Global Root

Issuer: C=US, O=GeoTrust Inc., CN=GeoTrust Global CA

Issuer: C=US, O=GeoTrust Inc., CN=GeoTrust Global CA 2

Issuer: C=US, O=GeoTrust Inc., CN=GeoTrust Primary Certification Authority

Issuer: C=US, O=GeoTrust Inc., OU=(c) 2007 GeoTrust Inc. - For authorized use only, CN=GeoTrust Primary Certification Authority - G2

Issuer: C=US, O=GeoTrust Inc., OU=(c) 2008 GeoTrust Inc. - For authorized use only, CN=GeoTrust Primary Certification Authority - G3

Issuer: C=US, O=GeoTrust Inc., CN=GeoTrust Universal CA

Issuer: C=US, O=GeoTrust Inc., CN=GeoTrust Universal CA 2

Issuer: C=BE, O=GlobalSign nv-sa, OU=Root CA, CN=GlobalSign Root CA

Issuer: OU=GlobalSign Root CA - R2, O=GlobalSign, CN=GlobalSign

Issuer: OU=GlobalSign Root CA - R3, O=GlobalSign, CN=GlobalSign

Issuer: C=EU, L=Madrid (see current address at www.camerfirma.com/address)/serialNumber=A82743287, O=AC Camerfirma S.A., CN=Global Chambersign Root - 2008

Issuer: C=US, O=The Go Daddy Group, Inc., OU=Go Daddy Class 2 Certification Authority

Issuer: C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc., CN=Go Daddy Root Certificate Authority - G2

Issuer: C=GR, O=Hellenic Academic and Research Institutions Cert. Authority, CN=Hellenic Academic and Research Institutions RootCA 2011

Issuer: C=HK, O=Hongkong Post, CN=Hongkong Post Root CA 1

Issuer: C=FR, ST=France, L=Paris, O=PM/SGDN, OU=DCSSI, CN=IGC/A/ emailAddress=igca@sgdn.pm.gouv.fr

Issuer: C=ES, O=IZENPE S.A., CN=Izenpe.com

Issuer: emailAddress=pki@sk.ee, C=EE, O=AS Sertifitseerimiskeskus, CN=Juur-SK

Issuer: C=US, O=Equifax Secure Inc., CN=Equifax Secure Global eBusiness CA-1

Issuer: C=HU, L=Budapest, O=Microsec Ltd., OU=e-Szigno CA, CN=Microsec e-Szigno Root CA

Issuer: C=HU, L=Budapest, O=Microsec Ltd., CN=Microsec e-Szigno Root CA 2009/emailAddress=info@e-szigno.hu

Issuer: C=HU, L=Budapest, O=NetLock Kft., OU=Tan\xC3\xBAs\xC3\xADtv\xC3\xA1nykiad\xC3\xB3k (Certification Services), CN=NetLock Arany (Class Gold) F\xC5\x91tan\xC3\xBAs\xC3\xADtv\xC3\xA1ny

Issuer: C=HU, L=Budapest, O=NetLock Halozatbiztonsagi Kft., OU=Tanusitvanykiadok, CN=NetLock Uzleti (Class B) Tanusitvanykiado

Issuer: C=HU, L=Budapest, O=NetLock Halozatbiztonsagi Kft., OU=Tanusitvanykiadok, CN=NetLock Expressz (Class C) Tanusitvanykiado

Issuer: C=HU, ST=Hungary, L=Budapest, O=NetLock Halozatbiztonsagi Kft., OU=Tanusitvanykiadok, CN=NetLock Kozjegyzoi (Class A) Tanusitvanykiado

Issuer: C=HU, L=Budapest, O=NetLock Halozatbiztonsagi Kft., OU=Tanusitvanykiadok, CN=NetLock Minositett Kozjegyzoi (Class QA) Tanusitvanykiado/emailAddress=info@netlock.hu

Issuer: C=US, O=Network Solutions L.L.C., CN=Network Solutions Certificate Authority

Issuer: C=CH, O=WISeKey, OU=Copyright (c) 2005, OU=OISTE Foundation Endorsed, CN=OISTE WISeKey Global Root GA CA

Issuer: CN=Autoridad de Certificacion Raiz del Estado Venezolano, C=VE, L=Caracas, ST=Distrito Capital, O=Sistema Nacional de Certificacion Electronica, OU=Superintendencia de Servicios de Certificacion Electronica/emailAddress=acraiz@suscerte.gob.ve

Issuer: C=BM, O=QuoVadis Limited, OU=Root Certification Authority, CN=QuoVadis Root Certification Authority

Issuer: C=BM, O=QuoVadis Limited, CN=QuoVadis Root CA 2

Issuer: C=BM, O=QuoVadis Limited, CN=QuoVadis Root CA 3

Issuer: L=ValiCert Validation Network, O=ValiCert, Inc., OU=ValiCert Class 3 Policy Validation Authority, CN=http://www.valicert.com//emailAddress=info@valicert.com

Issuer: O=RSA Security Inc, OU=RSA Security 2048 V3

Issuer: C=ES, O=Generalitat Valenciana, OU=PKIGVA, CN=Root CA Generalitat Valenciana

Issuer: C=DE, ST=Baden-Wuerttemberg (BW), L=Stuttgart, O=Deutscher Sparkassen Verlag GmbH, CN=S-TRUST Authentication and Encryption Root CA 2005:PN

Issuer: CN=SG TRUST SERVICES RACINE, OU=0002 43525289500022, O=SG TRUST SERVICES, C=FR

Issuer: C=JP, O=Japan Certification Services, Inc., CN=SecureSign RootCA11

Issuer: C=US, O=SecureTrust Corporation, CN=SecureTrust CA

Issuer: C=US, O=SecureTrust Corporation, CN=Secure Global CA

Issuer: C=JP, O=SECOM Trust Systems CO.,LTD., OU=Security Communication EV RootCA1

Issuer: C=JP, O=SECOM Trust Systems CO.,LTD., OU=Security Communication RootCA2

Issuer: C=JP, O=SECOM Trust.net, OU=Security Communication RootCA1

Issuer: C=FI, O=Sonera, CN=Sonera Class1 CA

Issuer: C=FI, O=Sonera, CN=Sonera Class2 CA

Issuer: C=NL, O=Staat der Nederlanden, CN=Staat der Nederlanden Root CA

Issuer: C=NL, O=Staat der Nederlanden, CN=Staat der Nederlanden Root CA - G2

Issuer: C=US, O=Starfield Technologies, Inc., OU=Starfield Class 2 Certification Authority

Issuer: C=US, ST=Arizona, L=Scottsdale, O=Starfield Technologies, Inc., CN=Starfield Root Certificate Authority - G2

Issuer: C=US, ST=Arizona, L=Scottsdale, O=Starfield Technologies, Inc., CN=Starfield Services Root Certificate Authority - G2

Issuer: C=IL, O=StartCom Ltd., OU=Secure Digital Certificate Signing, CN=StartCom Certification Authority

Issuer: C=IL, O=StartCom Ltd., OU=Secure Digital Certificate Signing, CN=StartCom Certification Authority

Issuer: C=IL, O=StartCom Ltd., CN=StartCom Certification Authority G2

Issuer: C=CH, O=SwissSign AG, CN=SwissSign Gold CA - G2

Issuer: C=CH, O=SwissSign AG, CN=SwissSign Platinum CA - G2

Issuer: C=CH, O=SwissSign AG, CN=SwissSign Silver CA - G2

Issuer: C=ch, O=Swisscom, OU=Digital Certificate Services, CN=Swisscom Root CA 1

Issuer: C=ch, O=Swisscom, OU=Digital Certificate Services, CN=Swisscom Root CA 2

Issuer: C=ch, O=Swisscom, OU=Digital Certificate Services, CN=Swisscom Root EV CA 2

Issuer: C=DE, O=T-Systems Enterprise Services GmbH, OU=T-Systems Trust Center, CN=T-TeleSec GlobalRoot Class 2

Issuer: C=DE, O=T-Systems Enterprise Services GmbH, OU=T-Systems Trust Center, CN=T-TeleSec GlobalRoot Class 3

Issuer: C=DE, O=TC TrustCenter GmbH, OU=TC TrustCenter Class 2 CA, CN=TC TrustCenter Class 2 CA II

Issuer: C=DE, O=TC TrustCenter GmbH, OU=TC TrustCenter Class 3 CA, CN=TC TrustCenter Class 3 CA II

Issuer: C=DE, O=TC TrustCenter GmbH, OU=TC TrustCenter Universal CA, CN=TC TrustCenter Universal CA I

Issuer: C=DK, O=TDC Internet, OU=TDC Internet Root CA

Issuer: CN=T\xC3\x9CRKTRUST Elektronik Sertifika Hizmet Sa\xC4\x9Flay\xC4\xB1c\xC4\xB1s\xC4\xB1, C=TR, L=ANKARA, O=(c) 2005 T\xC3\x9CRKTRUST Bilgi \xC4\xB0leti\xC5\x9Fim ve Bili\xC5\x9Fim G\xC3\xBCvenli\xC4\x9Fi Hizmetleri A.\xC5\x9E.

Issuer: CN=T\xC3\x9CRKTRUST Elektronik Sertifika Hizmet Sa\xC4\x9Flay\xC4\xB1c\xC4\xB1s\xC4\xB1, C=TR, L=Ankara, O=T\xC3\x9CRKTRUST Bilgi \xC4\xB0leti\xC5\x9Fim ve Bili\xC5\x9Fim G\xC3\xBCvenli\xC4\x9Fi Hizmetleri A.\xC5\x9E. (c) Aral\xC4\xB1k 2007

Issuer: CN=T\xC3\x9CRKTRUST Elektronik Sertifika Hizmet Sa\xC4\x9Flay\xC4\xB1c\xC4\xB1s\xC4\xB1, C=TR, L=Ankara, O=T\xC3\x9CRKTRUST Bilgi \xC4\xB0leti\xC5\x9Fim ve Bili\xC5\x9Fim G\xC3\xBCvenli\xC4\x9Fi Hizmetleri A.\xC5\x9E. (c) Kas\xC4\xB1m 2005

Issuer: C=TW, O=TAIWAN-CA, OU=Root CA, CN=TWCA Global Root CA

Issuer: C=TW, O=TAIWAN-CA, OU=Root CA, CN=TWCA Root Certification Authority

Issuer: C=TW, O=Government Root Certification Authority

Issuer: O=TeliaSonera, CN=TeliaSonera Root CA v1

Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc, OU=Certification Services Division, CN=Thawte Premium Server CA/emailAddress=premium-server@thawte.com

Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc, OU=Certification Services Division, CN=Thawte Server CA/emailAddress=server-certs@thawte.com

Issuer: C=GB, O=Trustis Limited, OU=Trustis FPS Root CA

Issuer: C=TR, L=Gebze - Kocaeli, O=T\xC3\xBCrkiye Bilimsel ve Teknolojik Ara\xC5\x9Ft\xC4\xB1rma Kurumu - T\xC3\x9CB\xC4\xB0TAK, OU=Ulusal Elektronik ve Kriptoloji Ara\xC5\x9Ft\xC4\xB1rma Enstit\xC3\xBCs\xC3\xBC - UEKAE, OU=Kamu Sertifikasyon Merkezi, CN=T\xC3\x9CB\xC4\xB0TAK UEKAE K\xC3\xB6k Sertifika Hizmet Sa\xC4\x9Flay\xC4\xB1c\xC4\xB1s\xC4\xB1 - S\xC3\xBCr\xC3\xBCm 3

Issuer: C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=http://www.usertrust.com, CN=UTN - DATACorp SGC

Issuer: C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=http://www.usertrust.com, CN=UTN-USERFirst-Client Authentication and Email

Issuer: C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=http://www.usertrust.com, CN=UTN-USERFirst-Hardware

Issuer: C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=http://www.usertrust.com, CN=UTN-USERFirst-Object

Issuer: L=ValiCert Validation Network, O=ValiCert, Inc., OU=ValiCert Class 1 Policy Validation Authority, CN=http://www.valicert.com//emailAddress=info@valicert.com

Issuer: L=ValiCert Validation Network, O=ValiCert, Inc., OU=ValiCert Class 2 Policy Validation Authority, CN=http://www.valicert.com//emailAddress=info@valicert.com

Issuer: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2007 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 3 Public Primary Certification Authority - G4

Issuer: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2006 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 3 Public Primary Certification Authority - G5

Issuer: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2008 VeriSign, Inc. - For authorized use only, CN=VeriSign Universal Root Certification Authority

Issuer: C=US, O=VeriSign, Inc., OU=Class 1 Public Primary Certification Authority

Issuer: C=US, O=VeriSign, Inc., OU=Class 1 Public Primary Certification Authority - G2, OU=(c) 1998 VeriSign, Inc. - For authorized use only, OU=VeriSign Trust Network

Issuer: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 1999 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 1 Public Primary Certification Authority - G3

Issuer: C=US, O=VeriSign, Inc., OU=Class 2 Public Primary Certification Authority - G2, OU=(c) 1998 VeriSign, Inc. - For authorized use only, OU=VeriSign Trust Network

Issuer: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 1999 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 2 Public Primary Certification Authority - G3

Issuer: C=US, O=VeriSign, Inc., OU=Class 3 Public Primary Certification Authority

Issuer: C=US, O=VeriSign, Inc., OU=Class 3 Public Primary Certification Authority

Issuer: C=US, O=VeriSign, Inc., OU=Class 3 Public Primary Certification Authority - G2, OU=(c) 1998 VeriSign, Inc. - For authorized use only, OU=VeriSign Trust Network

Issuer: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 1999 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 3 Public Primary Certification Authority - G3

Issuer: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 1999 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 4 Public Primary Certification Authority - G3

Issuer: C=US, O=VISA, OU=Visa International Service Association, CN=Visa eCommerce Root

Issuer: C=US, O=Wells Fargo WellsSecure, OU=Wells Fargo Bank NA, CN=WellsSecure Public Root Certificate Authority

Issuer: C=US, OU=www.xrampsecurity.com, O=XRamp Security Services Inc, CN=XRamp Global Certification Authority

Issuer: C=RO, O=certSIGN, OU=certSIGN ROOT CA

Issuer: C=TW, O=Chunghwa Telecom Co., Ltd., OU=ePKI Root Certification Authority

Issuer: C=US, O=thawte, Inc., OU=Certification Services Division, OU=(c) 2006 thawte, Inc. - For authorized use only, CN=thawte Primary Root CA

Issuer: C=US, O=thawte, Inc., OU=(c) 2007 thawte, Inc. - For authorized use only, CN=thawte Primary Root CA - G2

Issuer: C=US, O=thawte, Inc., OU=Certification Services Division, OU=(c) 2008 thawte, Inc. - For authorized use only, CN=thawte Primary Root CA - G3

APPENDIX D Installing and configuring NetApp AltaVault OST Plug-in

The NetApp AltaVault OST Plug-in can be installed and configured either using Windows or Linux environment.

This section includes:

- "Installing and configuring AltaVault OST Plug-in on Windows" on page 211
- "Installing and configuring AltaVault OST Plug-in on Linux" on page 212
- "Next steps for AltaVault OST Plug-in" on page 213
- "Upgrading AltaVault OST Plug-in" on page 214

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate the exact product and feature versions described in this document are supported for your specific environment.

Installing and configuring AltaVault OST Plug-in on Windows

Before you begin the installation process, verify that you have the following:

- NetApp AltaVault 4.2 or higher
- Veritas NetBackup version 7.6 or 7.7
- Latest updates for Windows installed on the NetBackup Media Server
- Microsoft Visual C++ 2015 Redistributable (x64) package: https://www.microsoft.com/en-us/download/details.aspx?id=48145
- Write permission to create the folder C:\ntapav, which contains AVA OST Plug-in configuration and log files

To install the OST plug-in for Windows

1. Download the plug in from the NetApp Support Site downloads section.
2. Copy the ost_installer.msi file onto the Windows NetBackup media server.
3. Shut down the NetBackup services on the media server host.
4. Double-click on the ost_installer.msi file.
5. In the NetApp AltaVault Plug-in for NetBackup Setup window, check the box to accept the license agreement.
6. Click Install.
7. Click Finish.

8. Start up the NetBackup services on the media server host.

9. To verify that the AltaVault OST Plug-in is installed properly, enter the following:

```
C:\Program Files\Veritas\NetBackup\bin\admincmd> .\bpstsinfo.exe -pi -sp NetAppAltaVault
Plugin Info:
   Plugin Name: libstspiAltaVaultDisk.dll
   Prefix: NetAppAltaVault
   Label: NetApp AltaVault Plugin
   Build Version: 11
   Build Version Minor: 1
   Operating Version: 11
   Vendor Version: v1.1 /27-Jun-16
```

The plug-in should now be installed.

To configure the AltaVault OST Plug-in for SSL on Windows

SSL is optional on Windows. It is not enabled by default. To enable SSL, perform the following steps on AltaVault:

1. Select Configure > OST >Global OST Settings.

2. Check the box to enable SSL.

3. Choose Maintenance > Service and restart the optimization service.

4. From the NetApp AltaVault appliance GUI, choose Configure > Web Settings.

5. Under the Web Certificate section, select the PEM tab and copy the certificate.

6. On the Windows NetBackup media server where you installed AltaVault OST Plug-in, navigate to the \ntapav folder on your C:\ drive.

7. Create a text file called "cert.pem." Open the file in a text editor and paste the certificate contents from Step 5.

Installing and configuring AltaVault OST Plug-in on Linux

Before you begin the installation process, verify that you have the following:

- NetApp AltaVault 4.2 or higher
- Veritas NetBackup 7.6 or 7.7
- Write permission to create the directory /usr/ntapav, which contains AVA OST Plug-in configuration and log files.

To install the AltaVault OST Plug-in for Linux

1. Download the plug in from the NetApp Support Site downloads section.

2. Unzip the archive file to a temporary directory on the NetBackup media server:

   ```
   >tar zxvf AltaVaultOSTPlugin-1.1.tar.gz
   ```

   The file name may be different depending on the version downloaded from the support site.

3. Shut down the NetBackup services on the media server host.

4. Go to the NetAppOSTInstaller subdirectory and run the script NetAppOSTInstaller.sh to copy the libraries:

```
>./NetAppOSTInstaller.sh
```

5. Start up the NetBackup services on the media server host.

The plug-in should now be installed.

6. To verify that the AltaVault OST Plug-in is installed properly, enter the following:

```
# /usr/openv/netbackup/bin/admincmd/bpstsinfo -pi -sp NetAppAltaVault
Plugin Info:
    Plugin Name: libstspiNetAppAltaVaultMT.so
    Prefix: NetAppAltaVault
    Label: NetApp AltaVault Plugin
    Build Version: 11
    Build Version Minor: 1
    Operating Version: 11
    Vendor Version: v1.1 /27-Jun-16
```

The plug-in should now be installed.

To configure AltaVault OST Plug-in for SSL on Linux

SSL is optional on Linux. It is not enabled by default. To enable SSL, perform the following steps on AltaVault:

1. Select Configure > OST >Global OST Settings.
2. Check the box to enable SSL.
3. Choose Maintenance > Service and restart the optimization service.
4. Choose Configure > Web Settings.
5. Under Web Certificates section, select the PEM tab and copy the certificate.
6. Navigate to /usr/ntapav.
7. Create a file called "cert.pem", and paste the certificate.

Next steps for AltaVault OST Plug-in

A complete AltaVault OST installation requires you to configure OST settings on both the NetBackup media server and NetApp AltaVault.

To configure AltaVault OST follow the instructions in Chapter 3, “Configuring storage settings.”

To configure NetBackup media servers for AltaVault OST, go to the *NetApp AltaVault Cloud Integrated Storage Deployment Guide*.

You can use the AltaVault command line interface (CLI) to enable, disable, or show information for the OST plug-in. Make sure you are in configure terminal mode before issuing the OST command. See the *NetApp AltaVault Cloud Integrated Storage Command-Line Reference Guide*.

Upgrading AltaVault OST Plug-in

Note: The AltaVault OST Plug-in requires compatibility with the AltaVault version running in your environment. Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate compatible versions.

If you have previously installed the AltaVault OST Plug-in and require an upgrade for compatibility with AltaVault as indicated in the IMT, refer to the following procedures.

To upgrade the AltaVault OST Plug-in for Windows

To upgrade AltaVault OST Plug-in for Windows, follow the steps below.

1. Uninstall the existing AltaVault OST Plug-in from the Windows server:

   a. Go to Control Panel.

   b. Double-click on Programs and Features.

   c. Select NetApp AltaVault Plugin for NetBackup.

   d. Right click on the selection, and click Uninstall.

2. Install the AltaVault OST Plug-in as described in the procedure "To install the OST plug-in for Windows" on page 211.

3. Configure the plug-in for SSL as described in the procedure "To configure the AltaVault OST Plug-in for SSL on Windows" on page 212.

To upgrade the AltaVault OST Plug-in for Linux

To upgrade AltaVault OST Plug-in for Linux, follow the steps below.

1. Install the AltaVault OST Plug-in as described in the procedure "To install the AltaVault OST Plug-in for Linux" on page 212.

2. Configure the plug-in for SSL as described in the procedure "To configure AltaVault OST Plug-in for SSL on Linux" on page 213.

Copyright Information

Copyright © 1994-2016 NetApp, Inc. All rights reserved. Printed in the U.S.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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

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

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

Trademark Information

NetApp, the NetApp logo, Go Further, Faster, AltaVault, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCenter, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, and WAFL and other names are trademarks or registered trademarks of NetApp, Inc., in the United States, and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. A current list of NetApp trademarks is available on the web.

http://www.netapp.com/us/legal/netapptmlist.aspx.

How to Send Your Comments

You can help us to improve the quality of our documentation by sending us your feedback.

Your feedback is important in helping us to provide the most accurate and high-quality information. If you have suggestions for improving this document, send us your comments by email to *doccomments@netapp.com*. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

Index

Numerics
802.3ad 73

A
Access Control List 123
access control lists (ACL) 81
Access Key 19, 23, 26, 40, 42, 44, 45
access policy 98
  adding 100
Account Name 109
Accounts
  capability-based 107
  privileges 107
  role-based 107
ACL (access control list) 81
Action 125
Add 56, 70, 71, 72, 73, 109, 112, 114, 125
Add a New Group 99
Add a New Log Server 103
Add a New NTP Authentication Key 94
Add a New NTP Server 93
Add a New Route 70, 71, 72
Add a New Rule 125
Add a New Security Name 99
Add a New TCP Dump 153
Add a New Trap Receiver 95
Add a New User 97
Add a Radius Server 112
Add a TACACS+ Server 113
Add an Export 57, 58
Add Share 54
Add SMB Share 53
Add SMB User 55
Admin 107
Administrator password 107
Admission Control 87, 140
Alarm
  admission control 140
  cloud bucket consistency 140
  cloud bucket disparity 140
  cloud bucket over capacity 140
  CPU utilization 140
  data integrity error 140
  datastore eviction 140
  licensing 141
  link state 142
  memory paging 142
  process dump staging directory inaccessible 142
  secure vault 143
  software update available 143
  system disk full 91, 144
Alarm status
  link duplex error 141
  link I/O error 142
Alarm Status report
  definition of 140
  viewing 144
Alarm thresholds, setting 86
Alert 102, 103, 104
Allow All Clients 58, 59, 176
Allow Everyone Access 54
Allow Session Timeouts When Viewing Auto-Refreshing Pages 115
Allow Specified Clients 58, 59, 177
AltaVault
  benefits 10
AltaVault appliance
  configuration steps 14
  deployments 9
Amazon Glacier, 19
Amazon S3 23
Announcement, setting on home page 85
Appliance Information 12
Appliance monitoring report, viewing 159
Appliance monitoring, configuring 117, 122
Apply Changes 77
Authentication 95, 97
Authentication methods 106
  Local 105
Authentication Port 112, 113
Authentication Protocol 95, 97
Authentication Type 112, 113
authentication type
  standard 20
  STS 21
Authentication, setting general security 84, 105
Authorization Policy 106
Autodiscover rules, overview of 125
Autolicense critical event 89

B
Back-End Throughput Optimization report 134
Bandwidth Limit, setting 51

C
Cancel This Job 77
Capability-based accounts 107
Cascading menus
  displaying 13
Change Active Configuration 84
Change Password 114
CHAP 112
CIFS users, adding 60
cli 104
Cloud and Disk Storage Allocation 12
Cloud Bucket Consistency 87, 140
Cloud Bucket Disparity 87, 140
Cloud Bucket Over Capacity 87, 140
Cloud Information 12
Cloud Storage Reclamation 12
Comment 54, 58, 77, 176
Common Name 116
Community 96
Community String 99
Configuration files, managing 83
Configuration, saving 13
Configuring AltaVault appliance, steps 14
Confirm Global Key 113
Confirm Server Key 112, 113
Continuous log, viewing 151
CPU utilization 87, 140
CPU Utilization report
  definition of 144
  viewing 144
Created 77
Critical 102, 103, 104
Current Configuration 84
Current Password 114

D
Data Integrity Error 140
Data interface routing, configuring 71, 72
Data interfaces, modifying 71
Datastore Eviction 87, 140
Datastore Low Space 87, 140
Deduplicated Data 131
Deduplication 12
Deduplication factor 131
Default User 106
Deny in-path rules, overview of 125
Description 125
Destination 71, 72
Destination IPv4 Address 70
Destination Port 95, 125
Disable Compression 54, 58, 59, 176
Disable Dedup 54, 57, 59, 176
Disk Full 88, 141
Disk Statistics report
  definition of 147, 148
  viewing 147, 148
Disk Utilization report
  definition of 148
  viewing 149
DNS settings, specifying 68
Dynamic DNS 17, 70

E
Early Eviction 54, 57, 59, 176
Edit Export 58, 176
Email notification, setting 101
Emergency 102, 103, 104
Enable Account 109
Enable Data Interface 71, 72
Enable Scheduling 139
Enable SNMP Traps 95
Enable/Disable Job 77
Enabled 112, 113
Error 102, 103, 104
Event and failure notification, setting 101
Eviction Optimization report
  definition of 135
  viewing 135
Execute Now 77
Executes On 77
Expanded Data 131
Export Asynchronously 58, 59, 176
Export, adding 57, 58, 176

F
Fan Error 88, 141
Filter logs 151
Fingerprint 116
FIPS-mode
  verifying your system is compliant 167
Flash Error 88
From Local File 81
From URL 81
Front-End Throughput Optimization
    report 132
FTP proxy access 67

G
Gateway 71, 72
Gateway IPv4 Address 70
Global Key 112, 113

H
hald 104
Home page announcement, setting 85
Home page, overview of 12
Host settings, modifying 67
Hostname 93, 113
Hostname, changing 67
Hosts 67

I
Import 84
Import a New Configuration 84
Import Shared Data Only 84
Info 102, 103, 104
Install 81
Interface 69, 125
  management 69
  primary 69
Interface Statistics report
  definition of 146
  viewing 147
Interval 77
IP Address 93, 113
IP Configuration 72
IP/Hostname 84
IPMI 88, 141
IPv4 address
  obtaining automatically 17, 70

specifying manually 17, 70
IPv4 Subnet Mask 70
Issued By 116
Issued To 116

J
Jobs
scheduling 76
viewing details 76

K
Key 97, 116
Key ID 93, 94
Known issues 14

L
Last Run 77
Licensing 89, 141
Lines Per Log Page 102
Link Duplex 89
Link duplex alarm status 141
Link I/O error alarm status 142
Link I/O Errors 89
Link state 89, 142
Local logging 91
Local logging, setting 102
Local Only 106
Local Path 58
Local path 58, 176
Log Packets 125
Log server, adding or removing 103
Logs
downloading 151
filtering 103
rotating 102
system logs, downloading 152
system logs, viewing 150
user logs, downloading 151
user logs, viewing 150
viewing 149, 172
viewing continuous 150
Low Memory 89

M
Main routing table 69
Management ACL 123
Management console
connecting to 11
navigating 12
overview of 9
Management interfaces, modifying 69
Manually specifying
primary interface IPv4 address 17, 70
Max Pinnable Limit 89
Maximum No. of Log Files 102
MD5 95, 97
MD5 key identifier 94
Media Independent Interface 73
Member Interfaces (comma-separated) 72, 73
Memory Error 88
Memory Paging 89, 142
Memory Paging report
definition of 145
viewing 146
Message of the day 85
mgmtd 104
Minimum Severity 102, 103
Mode 73
Modifying
data interfaces 71
host settings 67
management interfaces 69
Monitor 107
Monitor password 107
monitored appliance 122
monitoring appliance 122
Monitoring interval 73
MOTD, setting 85
MOTD. See Message of the day.
Mount Commands 59, 177
Move Selected 125
MTU 70
MTU value, setting 70, 71, 72

N
Name 57, 67, 77
Network File System 57
New Config Name 84
New host, adding 68
New Password 114
New Password Confirm 114
NFS, adding an export 57, 58, 176
NFS. See Network File System.
Notice 102, 103, 104

O
Object Identifiers, viewing through SNMP 100
Offline File System Check
definition of 63
Offline File System Check report
viewing 63
Online documentation 14
Online File System Check 64
OpenStorage Technology (OST) 60
Optimization Service 12
OST 60
Override the Global Default Key 112, 113
Overview, of the Management Console 9

P
Pages and reports, printing 13
PAP 112
Password 114
password policy 111
Path 54
Perl regular expression 157
Pin Export 57
Pin Share 54
Pinned Data 53
pinned data 60
Pinned Data Information 57
pm 104
Power Supply 88
Prepopulation 62
Prepopulation viewing 62
Primary Interface 69
Primary interface 69
setting 70
specifying IPv4 address 17, 70

Private cloud, customizing 28
Process Dump Creation Error 90
Process Dump Staging Directory
Inaccessible 142
Process dumps, displaying and
downloading 153
Process dumps, viewing 153
Protocol 125
Proxies 67
Proxy
addresses for Web access 67
setting an IP for Web/FTP 68

Q
Queue
capture file 154
specifying the trace dump size 155

R
RADIUS authentication method, setting 105
RAID 88
RAID battery information 12
Read Only 54
Read-Only Community String 95
Reboot 82
Receiver 95
Receiver Type 95
Remote Admin Password 84
Remote Config Name 84
Remote First 106
Remote Only 106
Remote User 95
Remove Selected 54, 55, 56, 58, 70, 71, 72, 84,
112, 114, 125
Remove Selected Jobs 77
Remove Selected Users 109
Replicated Data 12
Replication 50
definition 12, 49
scheduling 50
Replication Error 91, 144
Replication Optimization report
definition of 136
viewing 136, 138
Replication Paused 91, 144
Reports
Alarm Status 140
Appliance Monitoring 159
Back-End Throughput Optimization 134
CPU Utilization 144
Disk Statistics 147, 148
Disk Utilization 148
Eviction Optimization 135
Front-End Throughput Optimization 132
Interface Statistics 146
Memory Paging 145
Offline File System Check 63
Replication Optimization 136
Scheduled Reports 138
Storage Optimization 131
TCP trace dump 153
Verify 65
Restore Throttling 90, 143
Restrict inbound IP access to SteelStore
gateway 123
Retries 112, 113
Role-based
user permissions 107
Rotate Based On 102
Rule Number 125

S
Save Current Configuration 84
Scanning system logs 157
sched 104
Schedule Reports 138
Schedule Upgrade for Later 81
Scheduled Reports
purpose 138, 139
Scheduled reports
configuring 139
Scheduling, replication 50
Secret (Text) 94
Secret Key 25, 26, 29, 32, 44, 45
Secure access by inbound IP address 123
Secure Access Policies 98
Secure Groups 98
Secure groups, setting 99
Secure Vault 90, 143
unlocking and changing the password 114
Secure Vault Locked 143
Secure Views 98
setting 100
Security Models 98
Security Models and Name Pairs 99
Security Name 99
Security Names 98
Security, general 84, 105
Server IP 103
Server Key 112, 113
Service 125
Services, starting, stopping, restarting 75
Set a Global Default Key 113
SHA 95, 97
Share Name 53
Share pinning 53, 57
share pinning 60
Shared Secret 30, 43
Shelf Details report, viewing 161
Shelf Error 90
Shut down 82
SMB users, adding 52, 53, 55, 61
SMTP Port 101
SMTP Server 101
SNMP
access policies 100
access policy security 96, 101
access policy, adding 100
ACLs 94
adding groups 99
adding or removing trap receivers 95
adding views 100
configuring v3 96
features 98
including specific OIDs in a view 100
MIB, accessing 187
secure groups, setting 99
secure views, setting 100
setting trap receivers 94
supported versions 94

testing a trap 96
traps, summary of sent 189
Software Update Available 143
Software, upgrading 80
Source IP Address and Mask Bits 99
Source Network 125
SSL
peering list 115
standard authentication type 20
Storage Optimization 12
Storage optimization report, viewing 131
Storage Optimization Service 91, 143
Storage Optimization Service Down 91, 143
Storage Optimization Service Error 91, 143
Storage Optimization Service Replication 91
STS authentication type 21
Sub Tenant ID 24, 30, 34
Subnet Mask 71, 72
Synchronizing, AltaVault appliance to NTP server 93
System Contact 95
System Disk Full 91, 144
System dump, viewing 152
System Location 95
System logs, downloading 152
System logs, viewing 150
System Status 12
System, logging out of 14

T
TACACS+ authentication method, setting 105
TCP dump 153
TCP trace dump 153
Temperature 91
Tenant ID 27, 37, 38
Throughput Optimization report
viewing 132, 133, 134
Time zone 92
Timeout 112, 113
Transmit Load Balance 73
Transmit/Receive Load Balance 73
Trap receivers, adding or removing 95
Traps 94
Traps, summary of SNMP traps sent 189

U
UID 30, 34, 43
Unlock Secure Vault 114
User logs
downloading 151, 172
viewing 150, 172
User Name 55
User permissions 107

V
Validity 116
Vault, unlocking and changing the password 114
Verify report
definition of 65
viewing 65
Version 93
View-Based Access Control Mechanism 94
Virtual Interface 72
Virtual Interface Name 73
VLAN 73
VLAN Interface 72

W
Warning 102, 103, 104
wdt 104
Web Inactivity Timeout 115
webasd 104
Wizard
running 16