Technical Report

# NetApp AltaVault Cloud-Integrated Storage Appliances

## Security Overview

Christopher Wong, NetApp
November 2017 | TR-4405

## Abstract

This document provides an overview of the NetApp® AltaVault™ cloud-integrated storage appliance security features. AltaVault provides a secure cloud backup solution for enterprise data, and this paper discusses the appliance, data, and transport security mechanisms to keep data protected while managed by AltaVault.

## TABLE OF CONTENTS

## LIST OF FIGURES

# 1 Introduction

This document describes the NetApp AltaVault cloud-integrated storage appliance (AltaVault) security features. AltaVault provides a secure cloud backup solution for enterprise data. Its security goals are:

- **Appliance Security:** AltaVault software is hardened against unauthorized access.
- **Data Security:** User data is secure and private, both on disk and in the cloud.
- **Transport Security:** User data is secure and private when it is transmitted from the appliance to the cloud.
- **Cloud Security:** Data stored in cloud storage is highly controlled to prevent unauthorized access.
- **Security Compliance:** AltaVault offers end-to-end security for data at rest and in flight using FIPS 140-2 level 1-validated encryption.

The information in this document applies to AltaVault software version 4.4 and later.

# 2 Appliance Security

AltaVault provides several features to control access to the management console or to limit the type of changes that authorized users can make. AltaVault also provides logging and auditing features to monitor system activity and configuration changes. For details, refer to chapter 7 of the NetApp AltaVault Cloud Integrated Storage Administration Guide.

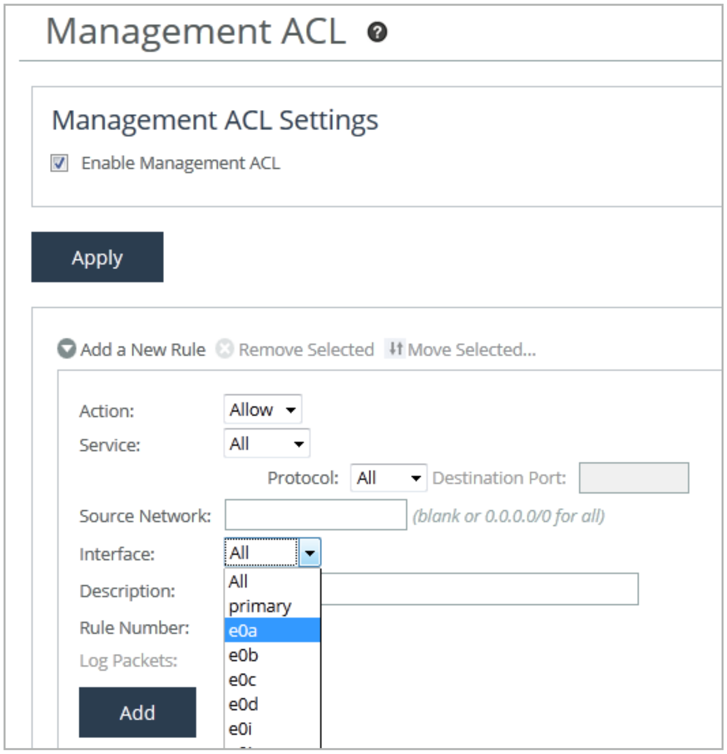
## 2.1 Operating System Security

AltaVault is a storage appliance and is not a general-purpose computing platform. It runs a hardened, minimalist version of Linux with only the necessary libraries and programs. Neither a user nor even an administrator can access the user or root shell on an AltaVault appliance. Root shell access is available only to NetApp Support on a limited and temporary basis for specific maintenance and diagnostic procedures. A multi-factor authentication process initiated by the customer on request of support is required to provide shell access. All activity is logged in support logs that provide an audit log of activity performed. In addition, Auto Support (ASUP) information can be gathered and submitted to proactively capture information about a problem for support, and case generation is automatically performed for critical AltaVault events.

## 2.2 Management ACL

AltaVault provides a Management ACL interface that allows users to easily enable or restrict services to the appliance. This includes specifying the service, such as HTTPS or SNMP access, what protocols such as UDP or TCP it will communicate across, which appliance interfaces will be allowed to interact with those services, and the networks that it will allow connections to occur from. By setting up specific rules, AltaVault can ensure the connections and services that are delivered.

Figure 1) Management ACL.



Management ACL

Management ACL Settings

☑ Enable Management ACL

Action: Allow

Service: All

Protocol: All Destination Port:

Source Network: (blank or 0.0.0.0/0 for all)

Interface: All

Description:

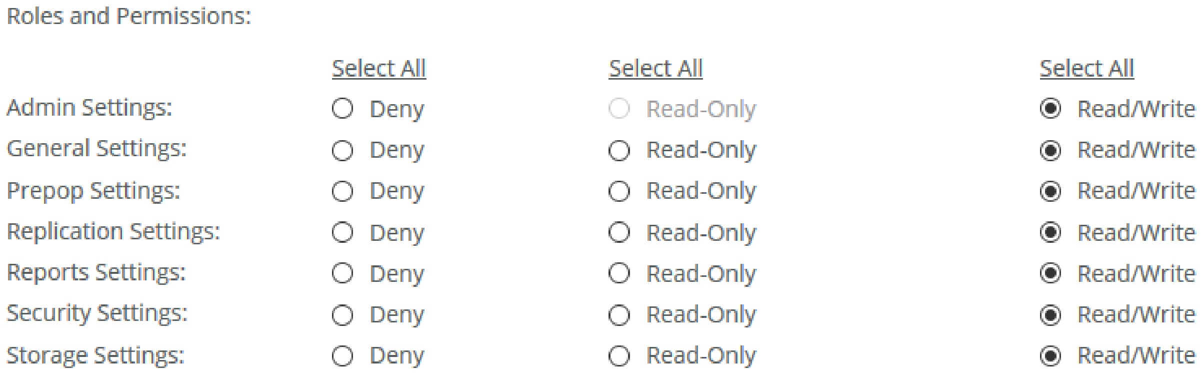
Rule Number:

Log Packets:

## 2.3 Role-Based Management

AltaVault enables multiple users to access the management console, either through HTTPS connections using TLS v1.1 or v1.2, or via SSH v2. The AltaVault role-based management feature enables an administrator to customize which capabilities each user has to configure and/or monitor the appliance. An administrator can assign a set of “roles” to each user. A role represents a group of related configuration properties. For example, the “security” role permits performing security-related functions such as encryption key import and export, management console access, and configuration import and export. You cannot read or change configuration properties unless your role has permissions to configure the feature. You might have only “read-only” access to a role; then you can monitor but you cannot change properties of the feature. In this way, access to the encryption keys can be limited to the minimal necessary subset of operators.

Figure 2) Role-based accounts.



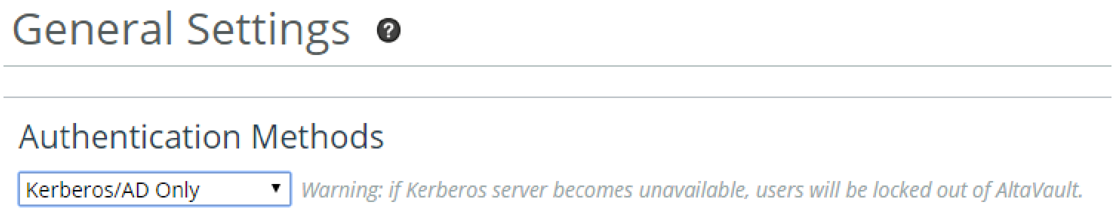
Roles and Permissions:

| | Select All | Select All | Select All |
|---|---|---|---|
| Admin Settings: | ○ Deny | ○ Read-Only | ● Read/Write |
| General Settings: | ○ Deny | ○ Read-Only | ● Read/Write |
| Prepop Settings: | ○ Deny | ○ Read-Only | ● Read/Write |
| Replication Settings: | ○ Deny | ○ Read-Only | ● Read/Write |
| Reports Settings: | ○ Deny | ○ Read-Only | ● Read/Write |
| Security Settings: | ○ Deny | ○ Read-Only | ● Read/Write |
| Storage Settings: | ○ Deny | ○ Read-Only | ● Read/Write |

## 2.4 Windows Active Directory Login Management

Starting with version 4.3, AltaVault supports management login from either the Management Console (UI) or command-line interface (CLI) for domain users using their Active Directory (AD) credentials. This capability eases management of the appliance by allowing users to leverage existing credentials available in Windows AD to login and manage AltaVault appliances, and reduces security complexity and risk by controlling users and passwords at the domain level, rather than at the local appliance level. In addition, AltaVault can be restricted to only allow AD-based authentication, which prevents any possibility of exploiting local user accounts or weak passwords associated with those accounts.

Figure 3) AltaVault authentication methods.



General Settings

Authentication Methods

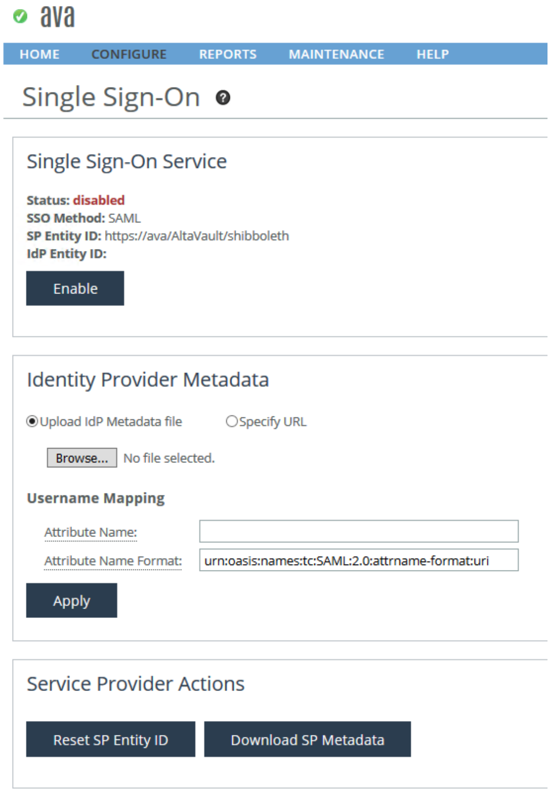
Kerberos/AD Only ▾

*Warning: if Kerberos server becomes unavailable, users will be locked out of AltaVault.*

## 2.5 Single Sign-On

Single Sign-on (SSO) is a feature available with AltaVault version 4.4 and higher that allows users to authenticate users to the AltaVault GUI via a centralized Identity Provider (IdP) host. AltaVault acts as a service provider (SP) requesting identity services from the IdP. SSO uses the Security Assertion Markup Language (SAML) 2.0 standard, which performs the user authentication with the IdP based on a corporate identity store. SSO can incorporate multi-factor authentication (MFA) as well, supporting popular MFA mechanisms such as a RSA token or a pin number.

Figure 4) Single Sign-on.



Single Sign-On

Single Sign-On Service

**Status:** disabled
**SSO Method:** SAML
**SP Entity ID:** https://ava/AltaVault/shibboleth
**IdP Entity ID:**

Enable

Identity Provider Metadata

● Upload IdP Metadata file ○ Specify URL

Browse... No file selected.

**Username Mapping**

Attribute Name:
Attribute Name Format: urn:oasis:names:tc:SAML:2.0:attrname-format:uri

Apply

Service Provider Actions

Reset SP Entity ID Download SP Metadata

## 2.6 SSH Chained Authentication

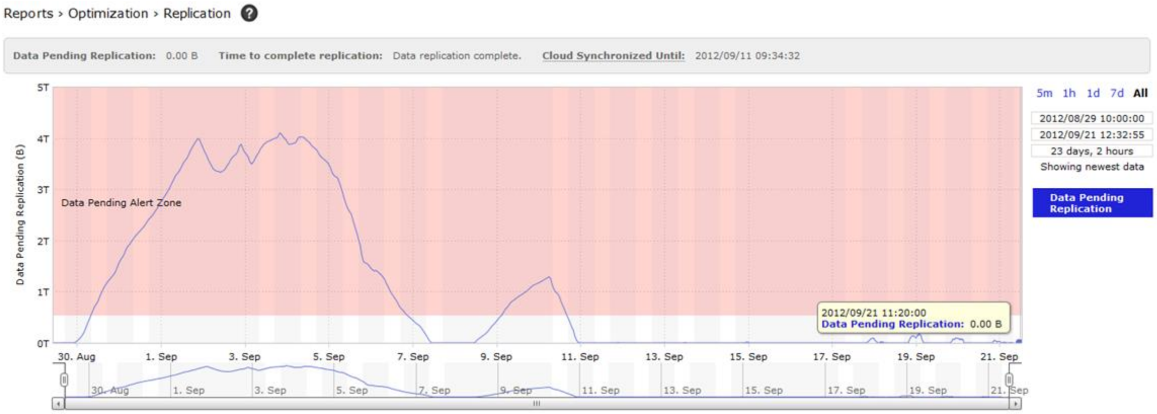
SSH chained authentication is a feature available with AltaVault version 4.4 and higher enabling two-factor authentication for SSH sessions initiated to the AltaVault appliance. SSH chained authentication uses public key and password mechanisms to authenticate users. The public-private keypair can be derived from OpenSSH's key generation tool ssh-keygen. The password can be the AltaVault local account password, or provided using Kerberos/Active Directory, RADIUS, or TACACS depending on the authentication method enabled. This feature compliments Single Sign-on by enforcing more secure authentication mechanisms to access and administer AltaVault.

## 2.7 Logging and Auditing

AltaVault provides two types of logs—system logs and user logs—to facilitate auditing. System logs show all appliance activity and user logs show user-initiated actions. System logs contain all information recorded in the user logs. By default, AltaVault rotates logs daily and retains the last 50 logs. You can configure and change both rotation and retention values. If you need more flexibility, you can set up a remote log server. AltaVault sends all system log activity to the remote log server and also records it in the appliance system logs.

The AltaVault management console provides detailed graphs capturing disk, CPU, and cloud replication statistics. It retains graphs for a maximum of one year.

Figure 5) AltaVault pending cloud activity graph.



Reports › Optimization › Replication

Data Pending Replication: 0.00 B Time to complete replication: Data replication complete. Cloud Synchronized Until: 2012/09/11 09:34:32

2012/08/29 10:00:00
2012/09/21 12:32:55
23 days, 2 hours
Showing newest data

2012/09/21 11:20:00
Data Pending Replication: 0.00 B

## 2.8 AltaVault Services

A number of services run on an AltaVault appliance and can be disabled on an individual basis to reduce the security footprint. These services include:

- **SMB and NFS:** SMB v2 and v3, and NFS v3 and v4, expose network shares or exports on the internal network for data to be read and written. If you use only one of these services, the other can be disabled. Both SMB and NFS also support access control lists to limit the users who can access a network share or export. For example, default guest account access is disabled for SMB access, and specific local or domain account access must be set up when a share is created.
- **OST:** Veritas OpenStorage (OST) API delivers optimized backup integration between NetBackup and storage appliances such as NetApp AltaVault. AltaVault can now leverage the OST framework to provide NetBackup the ability to efficiently stream backups to AltaVault, as well as manage lifecycle policy of copies of backups stored on AltaVault and in the cloud**.**
- **SnapMirror:** The NetApp SnapMirror protocol is used by AltaVault to receive incremental Snapshot™ backups of volumes from ONTAP® Fabric-Attached Storage (FAS) and All-Flash FAS (AFF) systems. This reduces the complexity of protecting data by eliminating the requirement for a traditional backup application to perform data backup, long term archive, and disaster recovery.

- **Web Management Console:** This allows an administrator to change and monitor configuration of an appliance using a web browser. This console can be disabled if only command-line management is needed. The management console can only be accessed by HTTPS by default, but it is possible to enable HTTP access if desired.
- **SSH:** This allows an administrator to change and monitor the configuration of an appliance remotely using the command line. This service can be disabled if you need web-only management.
- **NTP:** This service provides network time support and can be disabled. Correct time is required for proper operation, so if NTP is disabled, manually set the time for the appliance.
- **SNMP:** This service provides remote monitoring functionality and can be disabled.

# 3 Data Security

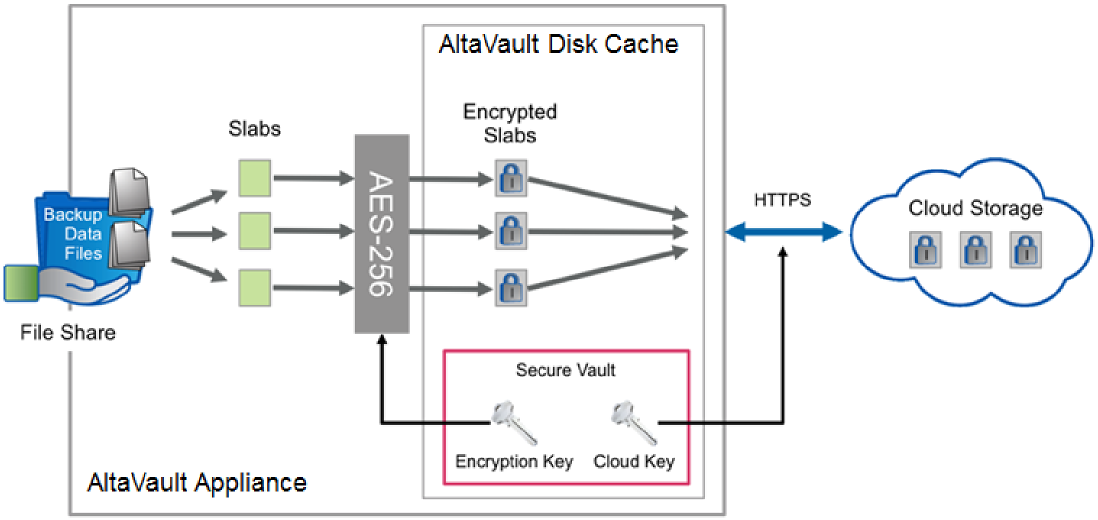
AltaVault provides several features to enable data confidentiality and integrity both on disk and in the cloud. At the heart of security on the appliance is the secure vault, which is an encrypted filesystem on the appliance.

The secure vault securely stores the collection of cryptographic secrets such as the encryption keys, authentication tokens, and certificates used in performing operations. By default, the secure vault is encrypted with a unique key generated when the appliance is installed, and the key is based on the hardware or software serial number combined with a salting value. This default configuration renders the disks—and thus the vault—inaccessible if they're moved to another machine.

Additionally, a customer can supply an optional secure vault password, which must then be entered whenever an appliance boots to complete the unlocking process. The password is incorporated into the process that generates the vault's encryption key. Note that enabling this feature may require changes in operational procedures. If an appliance reboots and an administrator isn't present to supply the password, features that rely on access to the vault's contents will be disabled, such as cloud connectivity and its ability to receive and process incoming data.

The secure vault itself is encrypted with AES-256. The algorithm used to generate the key is the password-based key derivation function 2 (PBKDF2) standard. In the default mode, the inputs into the function include the parameter mentioned earlier. In password mode, the password is also included. Because PBKDF2 produces a derived key after many rounds, brute force attacks are much more difficult. The encrypted secure vault is stored on the file system when the appliance is powered down. When the appliance boots, the contents of the vault are read into memory, decrypted, and mounted (via EncFS, a FUSE-based cryptographic file system) to an in-memory file system object. Since this information is only maintained in memory, when an appliance is rebooted or powered off, the information is no longer available and the in-memory object disappears. Decrypted secure vault contents are never persisted on disk storage. Similar procedures are used across the industry by all compute, storage, and networking devices that must store long-term secrets and also make use of them during normal operation.

Figure 6) AltaVault security diagram and secure vault.



## 3.1 Data Encryption

The AltaVault storage optimization service deduplicates, compresses, encrypts, and replicates user data to the cloud. Symmetric-key encryption protects data stored on disk and in the cloud. AltaVault encrypts all on-disk data using 256–bit AES block cipher in Galois/Counter mode with randomized initialization vectors. AltaVault splits files into variable-byte segments, collects these segments into packages called “slabs,” and encrypts each slab separately using 256–bit AES encryption. It stores only encrypted data on disk and replicates encrypted data to the cloud. There is no unencrypted data on disk or in the cloud. AltaVault also encrypts file metadata (file name, file length, permissions) before storing it in the cloud.

## 3.2 Disk and Cloud Object Structure

The following list summarizes the kinds of data stored both on AltaVault and in the cloud.

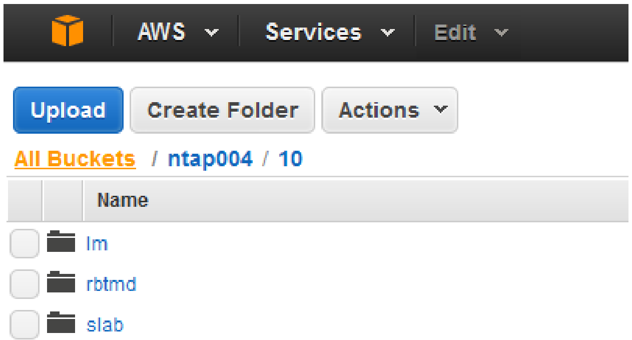
**Stored on AltaVault**

- **Slabs:** These are the 2MB to 4MB segments that make up files stored on an AltaVault appliance. These are encrypted with 256–bit AES encryption.
- **Label maps:** Stored and managed by the AltaVault database.
- **Metadata:** Stored and managed by the AltaVault database.

**Stored in the Cloud**

- **Slabs:** These are the same as slabs stored on local disk and are encrypted.
- **Label maps:** These are the same as the label maps stored by the AltaVault database locally.
- **Metadata files:** These are the same as the metadata files stored on local disk and are encrypted.

Figure 7) Cloud container contents.



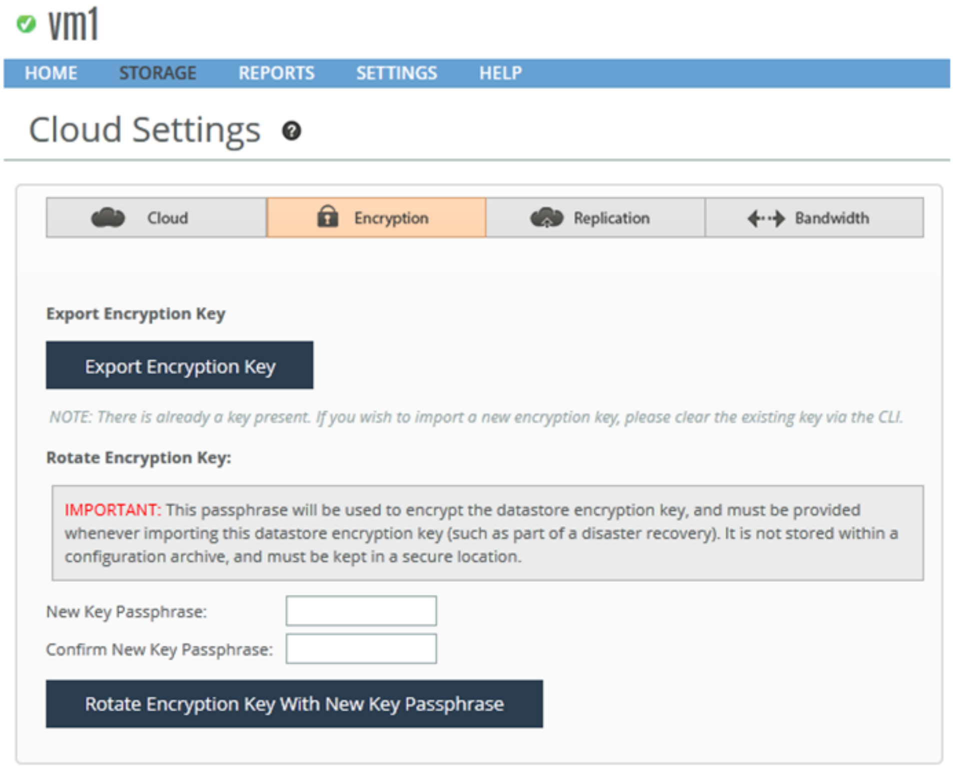
## 3.3 Encryption-Key Protection

The key used to encrypt and decrypt slabs is known as the datastore encryption key. AltaVault stores the datastore encryption key in an encrypted format on the appliance or in exported configuration archives. On the appliance, the datastore encryption key resides in the secure vault.

AltaVault protects the datastore encryption key when you export it from an appliance in configuration archives by exporting the key in a password encrypted form. It encrypts the key using a special key called the user key. To derive the user key, you must enter a key pass-phrase when you generate the datastore encryption key. AltaVault protects the key using your key pass-phrase with the AES Key Wrap algorithm (256-bit AES).

You must enter the same key pass-phrase when you reimport the datastore encryption key on to the appliance, such as during configuration import or disaster recovery. Without the key pass-phrase, AltaVault cannot reconstruct the original datastore encryption key from your configuration archive.

Figure 8) Encryption key.



*NOTE: There is already a key present. If you wish to import a new encryption key, please clear the existing key via the CLI.*

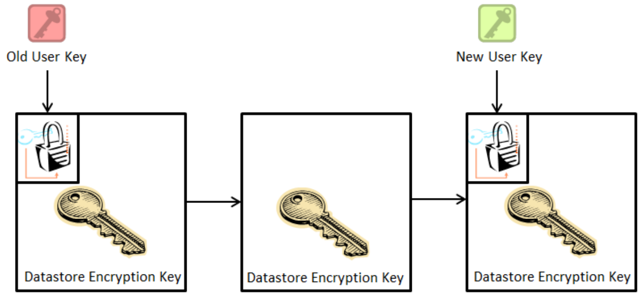
IMPORTANT: This passphrase will be used to encrypt the datastore encryption key, and must be provided whenever importing this datastore encryption key (such as part of a disaster recovery). It is not stored within a configuration archive, and must be kept in a secure location.

## 3.4 Encryption-Key Rotation

Key rotation is the process used to change a potentially compromised encryption key and replace it with a new one. AltaVault does not support rotation of the datastore encryption key because it must download all data from the cloud, re-encrypt it, and re-upload it back to the cloud. This is both an expensive and a time-consuming operation.

Instead, AltaVault supports the rotation of a key pass-phrase, which is the user-provided password used to derive the user key. It re-encrypts the datastore encryption key with the new key pass-phrase. For future exported configuration archives, you must use the new key to import the configuration or perform disaster recovery. Encryption key pass-phrase rotation is typically performed along with cloud credential key rotation to accomplish complete security credential rotation.

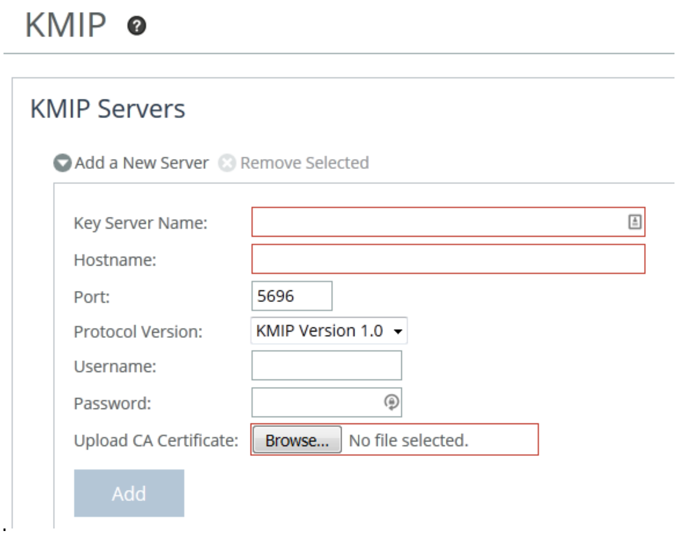
Figure 9) Encryption-key rotation.



## 3.5 Key Management Support

AltaVault supports the use of the Key Management Interoperability Protocol (KMIP) protocol, which allows a Key Management Server (KMS) to manage the cryptographic secrets used by AltaVault. Using a key management server negates the need for the AltaVault secure vault for these cryptographic secrets, since cloud security credentials and encryption keys are managed and delivered through the key management server. 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 that support KMIP. Example KMS implementations supported include SafeNet KeySecure, and Vormetric Data Security Manager. Refer to IMT for all current supported KMS environments.

Figure 10) Key Management Server (KMS) configuration.



| | |
|---|---|
| Key Server Name: | |
| Hostname: | |
| Port: | 5696 |
| Protocol Version: | KMIP Version 1.0 |
| Username: | |
| Password: | |
| Upload CA Certificate: | No file selected. |

.

# 4 Transport Security

AltaVault provides security of data as it flows along the network, ensuring data is not intercepted between the time it receives it, and the time it is stored in the cloud storage target.

## 4.1 Internal Network Security

NetApp assumes that your AltaVault appliance is installed in a trusted network environment behind a network firewall. In the absence of a firewall, AltaVault provides limited IPtables-based firewall support, but this degrades performance and should be used only as a last resort.

AltaVault runs in a trusted environment; therefore, SMB and NFS traffic to and from an AltaVault appliance is not encrypted because this data never reaches the Internet. Both SMB and NFS provide authentication mechanisms to prevent unauthorized users from accessing data within AltaVault shares. AltaVault's SMB authentication mechanism is integrated with the users' Active Directory system. NFS v4 users can choose to use Kerberos authentication, which establishes secure connections based on Kerberos keytab and config files imported onto AltaVault. SMB also provides SMB signing, a way to prevent man-in-the-middle attacks. However, enabling this feature incurs a significant performance penalty and is usually not necessary in an internal network environment.

## 4.2 External Network Security

All communication between an AltaVault appliance and a cloud provider occurs over TLS to provide data confidentiality in transit and prevent man-in-the-middle attacks.

Furthermore, all data that reaches the cloud has already been encrypted (confidentiality is independent of the cloud provider security). Cloud providers never have a copy of any of the encryption keys used by AltaVault. Even if there is a security breach at the cloud provider's organization, this prevents user data from being leaked.

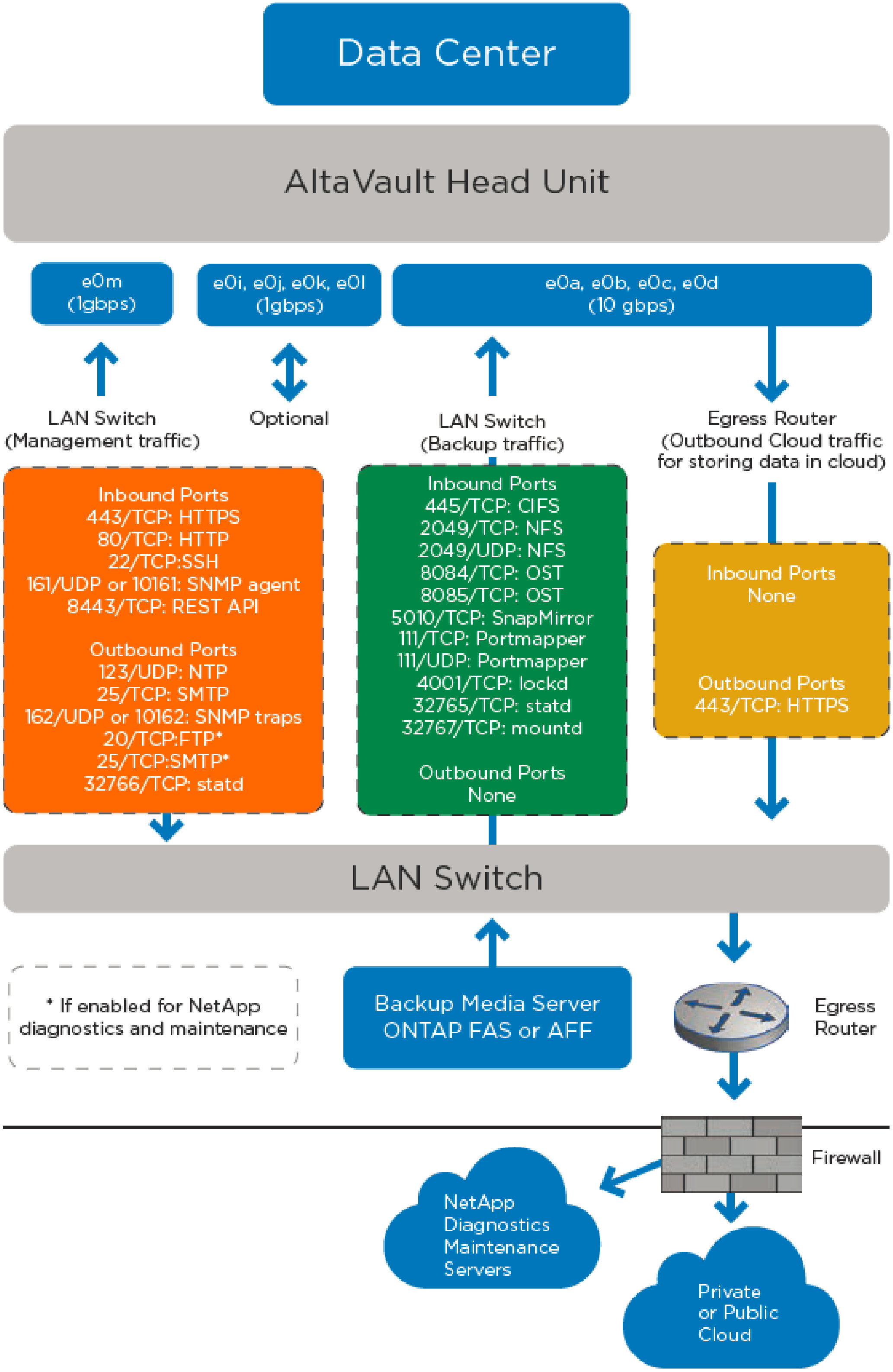
## 4.3 Supported TLS Versions

AltaVault supports TLS v1.1 and v1.2 when communicating with a cloud provider. By default, the appliance and the cloud provider can negotiate the specific version of TLS, such as version 1.1 or 1.2. SSL v3 has been deprecated and is no longer used by AltaVault to perform connections to cloud storage provider targets.

## 4.4 Data Center Topology

The following diagram illustrates how an AltaVault appliance would be connected in a data center. It also lists which ports and services are active on each network interface. The primary management interface (e0m) is used by administrators to communicate with the appliance for appliance management and configuration. Data interfaces are available as either four 1GbE or four 10GbE connections on the appliance. Typical operations will allocate one or more data interfaces to a backup network infrastructure, while one or two data interfaces can be enabled for replicating cloud data from AltaVault to a cloud storage provider. These interfaces will also be used to transmit ASUP (automated support) data back to NetApp to help provide support diagnostics about the appliance and proactively troubleshoot problems, and to open cases automatically in the event of critical AltaVault events.

Figure 11) AltaVault  connectivity.



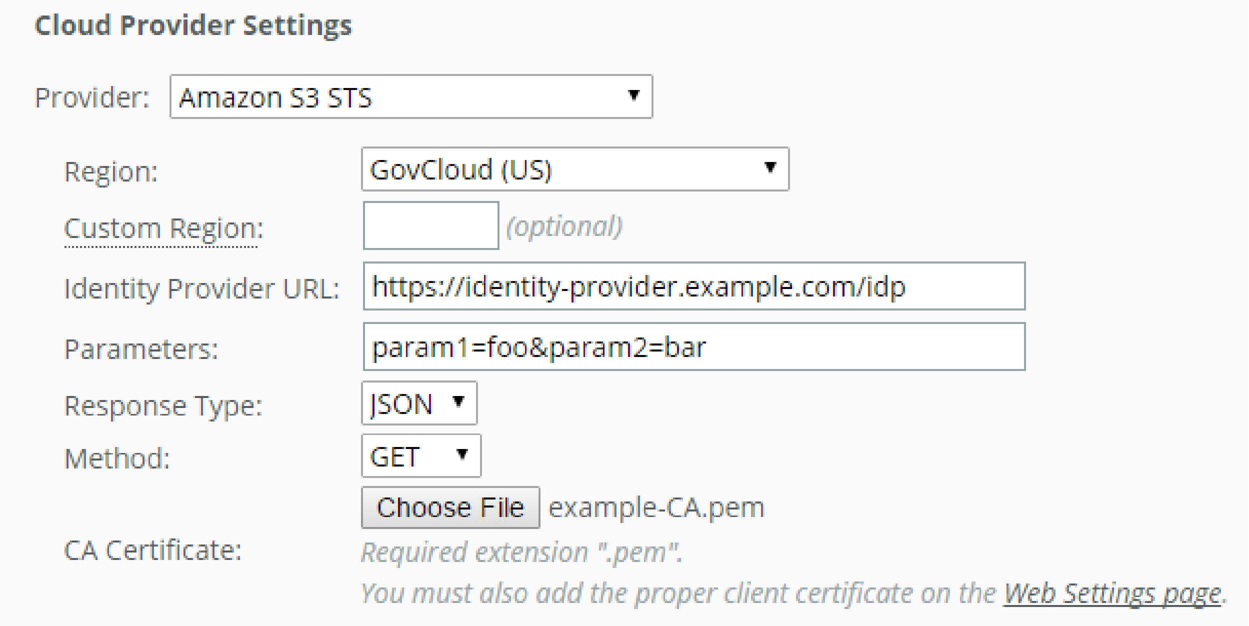
# 5 Cloud Security

Cloud security enhances and controls data access through a variety of mechanisms such as those described below.

## 5.1 Support for Amazon Security Token Service

AltaVault version 4.0.1 and later provides integration with Amazon Security Token Service (STS), which enables a more secure authentication method to Amazon services than the typical method of providing a permanent set of cloud credentials to a user. When configured with Amazon STS, AltaVault authenticates and obtains temporary cloud credentials from an on-premise trusted identity provider (also known as an identity broker) who performs initial authentication with Amazon STS on behalf of AltaVault. Cloud credentials in this configuration are designed to expire after one hour, limiting the potential for misuse. AltaVault renews credentials automatically when the previous credentials expire. In addition, the security team can control the authentication process since they maintain the identity provider that AltaVault must authenticate through.

**Figure 12) AltaVault STS settings page.**



Cloud Provider Settings

Provider: Amazon S3 STS

Region: GovCloud (US)

Custom Region: (optional)

Identity Provider URL: https://identity-provider.example.com/idp

Parameters: param1=foo&param2=bar

Response Type: JSON

Method: GET

CA Certificate: Choose File example-CA.pem

*Required extension ".pem".*

*You must also add the proper client certificate on the Web Settings page.*

## 5.2 Integration with AWS Identity and Access Management

Amazon Identity and Access Management (IAM) further ensures that only eligible users are allowed to consume cloud resources, even if users have access to cloud security credentials. IAM specifically grants or denies privileges to specific Amazon services, including S3 and Glacier object storage. AltaVault accordingly requires that IAM be configured properly so that it is allowed to perform operations to and from each service. This can be entered into Amazon either through the Amazon policy wizard or via a scripting engine. A list of the specific permission requirements and a recommended script for IAM are documented in Appendix B of the NetApp AltaVault Cloud Integrated Storage Administration Guide.

# 6 Security Compliance

This section describes accreditations and NetApp's internal development process as they relate to security.

## 6.1 FIPS 140-2 Level 1

AltaVault offers end-to-end security for data-at-rest and in-flight with the NetApp Cryptographic Security Module (NCSM). This module provides cryptographic algorithms for all functions on AltaVault that require cryptography. This includes, but is not limited to:

- Encryption and decryption of user data through the storage optimization service
- SSL/TLS connections to and from the cloud
- Password hashes of user accounts on the AltaVault management console
- SMBv3 shares

You can enable AltaVault to run in FIPS-enabled mode, in which the security module verifies that all cryptographic operations use only ciphers allowed by the FIPS 140-2 standard. AltaVault uses FIPS 140-2 level 1 validated encryption. AltaVault does not provide a guarantee that the configured cloud provider uses FIPS 140-2–validated cryptography. It is your responsibility to verify that the cloud provider meets regulatory requirements. For details, refer the NetApp AltaVault Cloud Integrated Storage Administration Guide.

## 6.2 Vulnerability Scanning

NetApp runs vulnerability scans against AltaVault appliances to catch software vulnerabilities and patch them in a timely manner. It uses tools such as Nessus to perform these scans. Weekly automated scans enable software vulnerabilities to be found during development and testing.

Because of the imprecise manner in which vulnerability scanning tools find potential vulnerabilities, it is possible for them to report false positives. NetApp recommends that you run your own security audits on your AltaVault installations and inquire about possible vulnerabilities. In many cases, they might be false positives, or workarounds or patches might be available.

## 6.3 NetApp Internal Security

The software development process at NetApp is aimed at creating reliable and secure software. All code changes go through internal code reviews. Bugs and vulnerabilities are tracked through internal bug-tracking software and security vulnerabilities are specially marked for expedited resolution. All code is stored on internal servers that are inaccessible to non-NetApp personnel.

For information regarding NetApp product security and vulnerability response policies, refer to the following links:

- http://www.netapp.com/security
- http://www.netapp.com/us/legal/vulnerability-handling-response-policy.aspx
- https://kb.netapp.com/support/index?page=content&channel=SECURITY_ADVISORY

# Where to Find Additional Information

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

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

- AltaVault Resources page http://mysupport.netapp.com/altavault/resources

## Version History

| Version | Date | Document Version History |
|---|---|---|
| Version 1.0 | February 2015 | Initial version |
| Version 2.0 | May 2015 | Covers AltaVault 4.0 release changes and updates |
| Version 2.1 | August 2015 | Covers AltaVault 4.0.1 release changes and updates |
| Version 2.2 | November 2015 | Covers AltaVault 4.1 release changes and updates |
| Version 2.3 | April 2016 | Covers AltaVault 4.2 release changes and updates |
| Version 2.4 | August 2016 | Covers AltaVault 4.2.1 release changes and updates |
| Version 2.5 | January 2017 | Covers AltaVault 4.3 release changes and updates |
| Version 2.6 | April 2017 | Covers AltaVault 4.3.1 release changes and updates |
| Version 2.7 | November 2017 | Covers AltaVault 4.4 release changes and updates |

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

### Copyright Information

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

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

### Trademark Information

TR-4405-1117