Hewlett Packard Enterprise

HPE 3PAR Common Criteria Administrator Guide

HPE 3PAR OS 3.2.2 MU4

Abstract

This manual is for all levels of system and storage administrators. It provides information for operating the HPE 3PAR Storage System in the Common Criteria evaluated configuration. This manual should be read prior to using the HPE 3PAR StoreServ Storage Concepts Guide, HPE 3PAR Command Line Interface Administrator Guide and HPE 3PAR Command Line Interface Reference to administer and maintain the HPE 3PAR Storage System in Common Criteria mode.

Part Number: QL226-99416

Published: October 2017

Edition: 1

Acknowledgments

Contents

1 Introduction

This administrator guide provides information for administering the HPE 3PAR Storage System to operate in the Common Criteria (CC) evaluated configuration mode. The Common Criteria (CC) are internationally well-recognized standards for the evaluation of products incorporating security functionality. When your HPE 3PAR Storage System was installed, it may have been installed to operate using only secure ports to better protect it from malicious activities (this document uses the term “Common Criteria mode” or “CC mode” to refer to a Common Criteria evaluated system that was installed to operate using secure ports only). If this is the case, some of the guidance contained in end user documents, such as the *HPE 3PAR StoreServ Storage Concepts Guide*, *HPE 3PAR Command Line Interface Administrator Guide* and *HPE 3PAR Command Line Interface Reference*, may vary when operating in CC mode or to conform to the CC standard. You should familiarize yourself with the information in this reference to understand the operational impact when running in CC mode.

Audience

This administrator guide is for system and storage administrators who monitor and direct system configurations and resource allocation for HPE 3PAR Storage Systems.

Acronyms

Acronyms are listed in Table 1.

Table 1 Definition of acronyms

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
CA	Certificate Authority
CBC	Cipher Block Chaining
CC	Common Criteria
CHAP	Challenge Handshake Authentication Protocol
CIM	Common Information Model
CLI	Command Line Interface

Acronym	Definition
CTR	Counter Cipher Mode
DAR	Data-at-Rest encryption
EKM	External Key Manager
FC	Fibre Channel
FCoE	FC over Ethernet
FIPS 140-2	Federal Information Processing Standards for cryptography modules
GUI	Graphical User Interface
HPE	Hewlett Packard Enterprise
HPE 3PAR OS	StoreServ Operating System (formerly known as InForm® OS)
HTTP/S	Hypertext Transfer Protocol/Secure
IP	Internet Protocol
iSCSI	Internet SCSI
KMIP	Key Management Interoperability Protocol
LAN	Local Area Network
LDAP	Lightweight Direct Access Protocol
LKM	Local Key Manager
LUN	Logical Unit Number
MC	StoreServ Management Console (previously known as Inform Management Console or IMC)
MP	Multi-Parity
MU	Maintenance Update
NTP	Network Time Protocol
OOTB	Out-of-the-Box script run during initial HPE 3PAR Storage installation
OS	Operating System
P16	Patch 16
PR	Persistent Repository
RFC	Request For Comment
RM-VASA	VMWare-specific component of the Recovery Manager, which provides backup/restore capability with the StoreServ being used as the backend (backup) repository
RSA	Rivest, Shamir, Adelman algorithm for public-key cryptography
SAN	Storage Area Network
SCSI	Small Computer System Interface
SED	Self-Encrypting Drive
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SLP	Service Location Protocol

Acronym	Definition
SNMP	Simple Network Management Protocol
SP	Service Processor, used to perform software upgrades and other service-related functions
SSD	Solid-State Drive
SSH	Secure Shell network protocol
SSL/TLS	Secure Sockets Layer/Transport Layer Security cryptographic protocols
ST	Security Target
StoreServ	HPE 3PAR Storage System is a hardware appliance that offers network- and serial-port accessible administration interfaces to access data storage resources
Syslog	Message logging standard
TCP	Transport Control Protocol
TOE	Target of Evaluation (e.g., HPE 3PAR Storage System)
UDP	User Datagram Protocol
VLUN	Virtual LUN
VPN	Virtual Private Network
VV	Virtual Volume
WWN	WorldWideName

2 Overview

This section provides an overview of Common Criteria.

Common Criteria

The Common Criteria (CC) are internationally well-recognized standards for the evaluation of products incorporating security functionality. Important areas of security functionality are:

- Ensuring that the HPE 3PAR Storage System is accessed by authorized administrators.
- Ensuring that administrator access occurs over a secure interface.
- Ensuring that data is written to storage devices in accordance with the policies established by the system administrator and that data on the storage device is accessible only to hosts that the administrator has specified.
- Ensuring that security relevant transactions are logged and traceable to the administrator or entity performing the activity.
- Ensuring that communication with off-platform entities (e.g., LDAP server) is done in a secure manner.

CC evaluations are performed on a specifically defined product configuration, referred to as the "evaluated configuration." Some pieces of a typical installation for a product may not be included in the evaluated configuration for various reasons. The next section discusses the evaluated configuration. The decision on whether to include an unevaluated feature is left to the end user.

For more information on Common Criteria, see http://www.commoncriteriaportal.org/.

The HPE 3PAR Storage System has previously been certified as Common Criteria compliant on HPE 3PAR OS releases 3.1.1 MU1+P16 and 3.2.1 MU3. See the *HPE Common Criteria Administrator's Reference* for the respective release for more information.

3 Evaluated Configuration

This section provides information on the HPE 3PAR Storage System Common Criteria evaluated configuration.

Hardware and Software

A storage system evaluated for conformance to the CC standard consists of the following:

- HPE 3PAR StoreServ Storage Systems models listed below, each running HPE 3PAR OS (version 3.2.2 MU4):
  - HPE 3PAR StoreServ 7000-Class Storage System models 7200c, 7400c, 7440c and 7450c
  - HPE 3PAR StoreServ 8000-Class Storage System models 8200, 8400, 8440 and 8450
  - HPE 3PAR StoreServ 10000-Class Storage System models 10400 and 10800[1]
  - HPE 3PAR StoreServ 20000-Class Storage System models 20450, 20800, 20840 and 20850
- SSHv2 client to administer the system

WARNING HPE 3PAR hardware and software must be installed by HPE or an HPE 3PAR authorized installer. Failure to do so results in the system not being considered an evaluated configuration.

Functionality included in the evaluated configuration

Figure 1 shows the reference configuration for a StoreServ operating in compliance with the Common Criteria evaluated configuration.

[1] HPE 3PAR StoreServ models 10400 and 10800 identify themselves as InServ V400 and InServ V800, respectively.

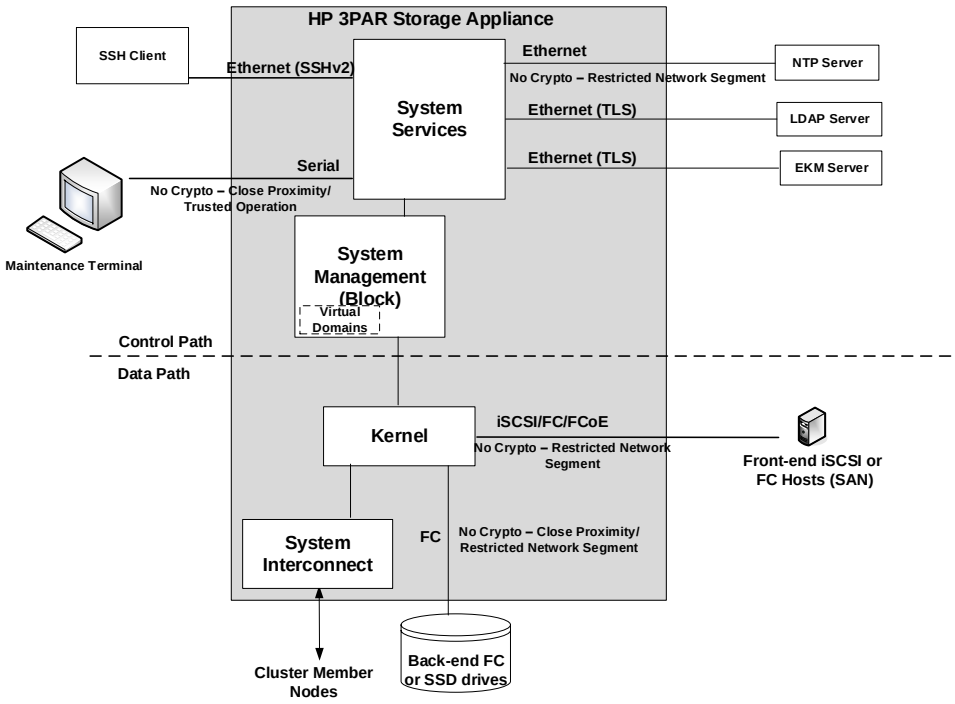

Figure 1 HPE 3PAR StoreServ reference configuration, CC mode

Table 2 briefly describes the security-relevant entities in the evaluated configuration when operating in Common Criteria mode.

Table 2 Functional entities in the CC mode configuration

Function	Item	Description
StoreServ admin	SSH client	An administrator connects to the StoreServ using an SSHv2 client to access the CLI.
NTP	NTP server	The StoreServ is configured to use an NTP server to perform periodic synchronization of the network node's clock. All other nodes sync to the network node.
LDAP	LDAP server	The StoreServ is configured to use Active Directory as an external authentication server operating in a single domain. There is one instance of Active Directory that supports the entire StoreServ cluster.
Protecting communication with an EKM server	EKM server	The StoreServ requires an external key manager (EKM) server, rather than a local key manager (LKM), to manage locking keys. The StoreServ communicates with the EKM server via the FIPS 140-2 compliant Key Management Interoperability Protocol (KMIP). Two types of EKM servers are supported: ■ HP Enterprise Secure Key Manager v4.0 ■ SafeNet KeySecure k450 or k150 version 6.1.2
Virtual Domains		The StoreServ can be configured with Virtual Domains enabled or disabled.

Functionality that is included but not evaluated

The HPE 3PAR OS that operates on the StoreServ consists of multiple features, not all of which are evaluated for Common Criteria operation. Table 3 lists the individual features and disposition with regard to evaluation.

Table 3 HPE 3PAR OS feature disposition in the evaluated configuration

Feature	Description
OS administration tools	Administration tools consist of the following: ■ Remote CLI – Included, not evaluated ■ MC – Included, not evaluated ■ SNMP – Included, not evaluated ■ SMI-S – Included, not evaluated ■ Maintenance terminal – Included, not evaluated
Persistent Ports	Included, not evaluated
Web Services API	Included, not evaluated
Local Key Manager	Included, not evaluated
Rapid Provisioning	Included, not evaluated
Autonomic Groups	Included, not evaluated
Scheduler	Included, not evaluated
Persistent Cache	Included, not evaluated
RAID MP (Multi-Parity)	Included, not evaluated
Full Copy	Included, not evaluated
Access Guard	Included, not evaluated
Thin Copy Reclamation	Included, not evaluated
Adaptive Flash Cache	Included, not evaluated
File Persona	Included, not evaluated
Smart SAN	Included, not evaluated
Remote Copy	Included, not evaluated

The sections that follow provide some additional details of functionality that is not evaluated.

syslog

The HPE 3PAR Storage System can export events (excluding debug events) to an external SYSLOG server, over UDP port 514, using the syslog protocol (RFC 5524). Though the syslog protocol supports TLS, the HPE 3PAR Storage Server does not.

The “debug” version of events in the HPE 3PAR OS are security relevant (user log in/out). Though the events can be viewed using the `showeventlog -debug` CLI command, they are not exported through syslog.

For these reasons, syslog is not evaluated functionality.

Remote Copy

The Remote Copy application involves network communication between HPE 3PAR Storage System peers. This communication uses a protocol that is unencrypted and unauthenticated. Though the application configuration assumes that the connection is a point-to-point VPN including only the two peers, since the protocol is unsecured and the peers do not authenticate each other, Remote Copy is not evaluated functionality.

Service Processor

Each HPE 3PAR Storage System appliance is shipped with a service processor (SP) that occupies a physical slot. The SP enables remote monitoring and troubleshooting of the appliance by HPE 3PAR. Since it is not part of the normal day-to-day operation, the SP is not evaluated functionality and must be disabled (i.e., not configured) while operating the StoreServ in its evaluated configuration. Section “Service Processor Considerations” on page 27 provides more information on the SP.

Remote CLI and StoreServ MC

For simplicity, these applications are not evaluated as a fully functional CLI client is included on the HPE 3PAR Storage System nodes and is accessible via the SSHv2 interface.

System Event Consumer Interface

The system event consumer interface (em_filter) is a non-encrypted and non-authenticated service on the HPE 3PAR Storage System that allows external clients to receive system-related events. Example users of this interface are the Service Processor and the Recovery Manager (RM) VASA event awareness feature. CC conformance requires that all communications on the management interfaces be secured and authenticated. For these reasons, the system event consumer interface is not evaluated functionality. The impact of this exclusion is that any external component that is dependent on this functionality will not be able to perform this functionality (see “Service Processor Considerations” on page 27).

Physical protection

There are some assumptions made regarding the physical protection given to the HPE 3PAR Storage System CC evaluated configuration in the customer environment:

- It must be physically situated in an access-controlled environment to protect against any unwarranted access or physical connections to system network ports.

- The same physical protection afforded the HPE 3PAR Storage System should be extended to all components that interact with the appliance (e.g., external servers such as NTP and LDAP, remote clients, etc.) to also protect against malicious activity.
- The management network is assumed to be private and have restricted access to only those hosts and administrators that need to configure or monitor the HPE 3PAR Storage System (which includes NTP and LDAP servers, client hosts, etc.).
- The host interface connections (SAN, iSCSI, LAN) are assumed to be private networks and carry no general network traffic. While difficult, access by untrustworthy entities, or hosts, could lead to the spoofing of WWNs or iSCSI names on these network segments. This could result in unintended access to storage resources by those untrustworthy entities. It is therefore assumed that administrators allow only trusted hosts access to these connections and that the hosts themselves are protected from access by untrustworthy entities.
- The node console ports (also known as the maintenance terminal ports) are maintenance only connections and are not to be used by system administrators.

Administrative session management

The HPE 3PAR Storage System supports multiple simultaneous administrative sessions. Though individual administrative sessions are tracked, there is no inherent protection against multiple administrators that attempt to edit system components at the same time. It is expected that administrators are cognizant of ongoing administrative activities. Multiple equally-authorized administrators, with identical domain membership, can interfere with each other if there is no coordination of their activities. Customers can choose to segregate which component(s) can be acted on by which administrator(s).

4 Operating in Common Criteria Mode

This section provides details on HPE 3PAR Storage System evaluated configuration operation in CC mode.

Common Criteria Mode

Common Criteria "mode" operation differs from standard HPE 3PAR Storage System operation in that in this mode only secure (i.e., encrypted) ports can be used. By default, the HPE 3PAR Storage System provides both secure and unsecure ports for performing operational activities. As part of the installation, or upgrade, of a CC compliant system, the installer will take some additional steps to force the disabling, or firewalling, of the unsecured ports on the system. Table 4 summarizes the network ports available and their disposition if the HPE 3PAR Storage System is installed to operate using secure ports only (i.e., the port's availability when operating in CC mode). Further details are provided in the sections following the table.

Table 4 Network Port Mapping

Port	Type	Use	Status in CC mode	Status in non-CC mode
22	TCP	Listens for SSH client connection	Active	Active
123	UDP	NTP client-server communication port	Active	Active
161	UDP	HPE 3PAR SNMP agent – off-platform SNMP manager communication port	Visible but unresponsive (udp-resposne only)	Visible/Active if configured
427	UDP	CIM Service Location Protocol (SLP) discovery port	Visible but unresponsive (udp-resposne only)	Visible/Active if enabled
5001	TCP	TCP diagnostics – factory use only	Visible but closed	Visible but closed
5781	TCP	Port on which the Service Processor listens for HPE 3PAR Storage System events	Not visible (firewalled at installation)	Active

Port	Type	Use	Status in CC mode	Status in non-CC mode
5782	TCP	Unsecured CLI/MC port	Not visible (firewalled at installation)	Active
5783	TCP	Secured (SSL) CLI/MC port	Not visible (firewalled at installation)	Active
5988	TCP	Unsecured (HTTP) CIM server port	Visible but closed	Visible/Active if enabled
5989	TCP	Secured (HTTPS) CIM server port	Visible but closed	Visible/Active if enabled
8008	TCP	Unsecured (HTTP) WSAPI port	Visible but closed	Visible/Active if enabled
8080	TCP	Secured (HTTPS) WSAPI port	Visible but closed	Visible/Active if enabled
9996*	TCP	Unsecured (HTTP) VASA Provider port	Visible but closed	Visible/Active if enabled
9997*	TCP	Secured (HTTPS) VASA Provider port	Visible but closed	Visible/Active if enabled

Ports that are “visible but closed” result in a failure to connect if a connection attempt is made to them. Ports that are “not visible” will not respond if a packet is sent to them (i.e., the packets are thrown away) and the connection attempt will time out. Ports marked “visible but unresponsive” will supply a udp-response packet but no service is supplied on the ports.

All SSH connections on the exposed ports in the evaluated configuration are performed using the cipher suites listed below.

- AES-128-CBC, AES-192-CBC and AES-256-CBC
- AES-128-CTR, AES-192-CTR and AES-256-CTR

See sections “Configuration Steps for CC Operation” on page 26 and “Confirming the System Configuration” on page 29 for more details.

Data Encryption

The following requirements must be met for the HPE 3PAR Storage System to be operating in the evaluated configuration:

- All self-encrypting drives (SEDs) in the system must be FIPS-140-2 compliant.
- The HPE 3PAR Storage System must use an External Key Manager (EKM) server to manage locking keys rather than the onboard Local Key Manager (LKM). The following EKM servers are supported for Common Criteria compliant operation:
  - HP Enterprise Secure Key Manager v4.0
  - SafeNet KeySecure k450 or k150 version 6.1.2

NOTE The EKM server must be installed with FIPS mode enabled. EKM servers typically have FIPS mode initially disabled. Use the EKM server GUI to enable FIPS mode. Refer to the EKM server documentation or contact the EKM server vendor should you require additional information.

The `controlencryption` and `showencryption` CLI commands are used to manage HPE 3PAR Storage System interaction with an EKM server and can be used to show the data encryption status of the system, including the list of EKM servers with which the HPE 3PAR Storage System is configured to operate and the FIPS capability of its drives.

Since the HPE 3PAR Storage System is unaware of CA certificates, should HPE 3PAR Storage System -EKM server interaction require the use of CA certificates, the HPE 3PAR Storage System must import the certificates. The following CLI commands are used for importing CA certificates for use with an EKM server:

- `import ekm-client -ca stdin` imports the certificate of the CA that signed the server certificate that the EKM server presents to the HPE 3PAR Storage System.
- `import ekm-server -ca stdin` imports the certificate of the CA that signed the HPE 3PAR Storage System's client certificate.
- `import ekm-client stdin` imports the certificate from the CA.

When importing a certificate, after executing the `import` command, the administrator pastes the certificate and then hits the enter key twice for the import to complete.

The `createcert -csr ekm-client` CLI command is used to create a Certificate Signing Request (CSR) for use as a client certificate when communicating with the EKM server.

See the *HPE 3PAR Command Line Interface Administrator Guide* for more information on using an EKM server to perform data encryption.

Host Identity and Authentication

There are multiple ways that a volume can be exported (i.e., made accessible) to one or more hosts: Host Sees, Host Set, Port Presents, and Matched Set. Hosts are identified by FC WWN/ iSCSI name and IP address. However, because Port Presents makes VLUNs available to any host that connects through that port (via node:slot:port), its use is not advised to export VLUNs to prevent the possibility of a host gaining access to a volume that it should not.

By default, the HPE 3PAR Storage System does not authenticate hosts. To authenticate the identity of hosts, use iSCSI to interface to the hosts and use the Challenge-Handshake Authentication Protocol (CHAP), or dual-CHAP, for host authentication (CHAP is not supported for the FC interface). CHAP can be configured using the `sethost` CLI command and the `initchap`, `targetchap` CLI subcommands (see the *HPE 3PAR Command Line Interface Reference* for details).

LDAP Server Configuration

The HPE 3PAR Storage Server can be configured to use either a secure or unsecure channel to communicate with an external LDAP server for remote user authentication. To conform to the CC standard, the HPE 3PAR Storage Server should be configured to communicate with the LDAP server using TLS. The *HPE 3PAR Command Line Interface Administrator Guide* provides detailed information on establishing LDAP connections using Simple Binding over SSL (see sections "Active Directory LDAP Configurations with Simple Binding Over SSL" or "OpenLDAP Configuration with Simple Binding Over SSL"). To conform to the CC standard, the following `setauthparam` CLI command specifiers must have the values indicated below:

- `ldap-port` – Set to 636 (secure SSL) or any other site/implementation-defined port that supports encryption (SSL).
- `ldap-ssl` – Set to 1 to use SSL (the default value is 0).
- `ldap-reqcert` – Set to 1 to indicate a valid certificate is required to establish a connection (the default value is 0)
- `ldap-StartTLS` – This is site/implementation-defined and so it should be set for your specific requirements (the default value is "no").

- `allow-ssh-key` – Keep the default value (0) so that an LDAP user is not able to use a public key for SSH authentication when logging into the HPE 3PAR Storage System. Users that are authenticated using a public key for SSH authentication become, effectively, a local user when logged in using the key and a LDAP user when logged in when the key is not available. The key associates them with their LDAP authentication profile at the time the key was installed and therefore no update from the LDAP server will be recognized. See the *HPE 3PAR Command Line Interface Administrator Guide* ("Configuring LDAP Connections") and *HPE 3PAR Command Line Interface Reference* (`setsshkey`, `removesshkey`) for additional details.

Related to the `allow-ssh-key` parameter configuration, it is important that administrators do not create local and remote users having the same user account. Since the HPE 3PAR Storage System checks first if the user has been created locally, it will never look to the LDAP server since the user will have been found to exist locally.

The LDAP/AD server itself should be configured to only use FIPS-approved TLS ciphers.

The `importcert` command is used to import the CA certificate (in prior releases, this was done using the `setauth` command `ldap-ssl-cacert` parameter, which has since been deprecated). The CA certificate is provided using standard input as indicated in the following sample command:

```
importcert cli –f stdin
```

After pressing <enter>, paste the CA certificate content and press <enter> twice. This allows the HPE 3PAR OS LDAP client to validate the certificate sent from the LDAP server.

Local User Password Policy

The Common Criteria mode requires that storage administrators be authenticated via LDAP/AD accounts. In those instances the password policy implemented in the LDAP server is used. It is also desirable to have at least one local user account for emergency use. That account should use a strong password. The HPE 3PAR OS does not implement a strict password policy, but does allow for the control of minimum length of passwords. This value should be set to match the minimum value in the LDAP/AD server. Local passwords can be up to 32 characters in length. A strong password should have the following attributes:

- At least 8 characters in length.
- Should not include names (usernames, your name, your pet's name, company names, etc.).
- Should not include complete words.
- Should not be a reuse of a previous password.
- Should be a mixture of upper and lower case characters, numbers and keyboard punctuation symbols (except the spacebar), and should contain at least one of each category.

SSH Client Usage

The HPE 3PAR OS includes an SSH server that is used to administer the HPE 3PAR Storage System when operating in CC mode. The following are Common Criteria-relevant recommendations for configuring SSH clients and user environments when communicating with the HPE 3PAR Storage System.

- The HPE 3PAR OS supports several key exchange algorithms for securing the channel: diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, diffie-hellman-group-exchange-sha1, and diffie-hellman-group-exchange-sha256. Some clients allow for setting the "preferred" key exchange protocol. If your client allows you to do this, set it to use diffie-hellman-group14-sha1 or diffie-hellman-group-exchange-sha256. Customers are advised to use client key sizes greater than 1024 bits.
- If you use a public key pair for authentication with the SSH server, you should do so only if you are a local user (see "LDAP Server Configuration" on page 17). The public key pair should be a RSA key of 2048 bits or greater. Private keys on the client side must be adequately protected by using a passphrase to encrypt the key or with strict file system protections (or both). Compromise of the private key allows the user to be impersonated.

Logging Security-related Events

The Common Criteria standard defines events to trace the occurrence of various security functions. Table 5 maps the HPE 3PAR Storage System event(s) generated to the auditable events for each Security Functional Requirement (SFR) as set forth in the security targets that govern the HPE 3PAR Storage System Common Criteria conformance. Administrators should pay special attention to monitoring the event log for the occurrence of security-related events. For information on auditing security-relevant events, see "Auditing Security-Relevant Events" on page 30.

(More information on the individual security requirements can be obtained by accessing the HPE 3PAR security target at http://www.niap-ccevs.org/vpl.)

Table 5 Mapping of HPE 3PAR Storage System Events to ST Requirements

Requirement	Auditable Event(s)	Additional Audit Record Content	StoreServ Event
FAU_GEN.1 The TOE can generate audit records for events including starting and stopping the audit function, administrator commands, and all other events identified in this table. Furthermore, each audit record identifies the date/time, event type, outcome of the event, responsible subject/user, as well as the additional event-specific content indicated in this table.	None	None	None
FAU_GEN.2 The TOE identifies the responsible user for each event based on the specific administrator or host (identified by host identifier) that caused the event.	None	None	None
FAU_SAR.1 The TOE provides CLI and MC interfaces to review of its internal audit log.	Reading of information from the audit records	None	The event log will contain a "CLI command executed" event naming 'geteventlog' as the command executed. This is true for both CLI and MC data extraction operations.
FAU_SAR.2 The TOE prohibits users from accessing the internal audit log except for those users that have been granted explicit read access.	Reading of information from the audit records	None	The event log will contain a "CLI command error" event with 'geteventlog' showing "Permission denied" and the command that failed.
FAU_SAR.3 The TOE audit review functions include the ability to search the stored audit logs using regular expressions so that, for example, records resulting from specific user actions can be readily identified.	None	None	None
FAU_STG.1 The TOE doesn't provide the ability to clear the audit log and similarly doesn't provide any functions that allow modification of stored audit records.	None	None	None

Requirement	Auditable Event(s)	Additional Audit Record Content	StoreServ Event
FAU_STG.4 The TOE will automatically overwrite the oldest audit log records with new records as necessary.	Action taken due to the audit storage failure.	None	The storage area is protected by the HPE Storage System's physical storage protections, as the PR resides on an admin VV configured for redundancy. Space on the volume is tightly managed to prevent exhaustion. If the log should fail, em_filter writes an indication to its own private log and continues to record events there until the condition is rectified. The em_filter private log is not accessible to a system administrator. (We have never seen this occur in the field.)
FCS_CKM.1 The TOE shall generate asymmetric cryptographic keys used for key establishment between itself and an external EKM in accordance with *NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for finite field-based key establishment schemes* and specified cryptographic key sizes equivalent to, or greater than 112 bits.	Failure on invoking functionality	None	The OpenSSL FIPS module provides integrity and self-test of functionality when it is initialized. If this fails, no further processing is possible and an event will be written to the eventlog.
FCS_CKM.4 The TOE shall zeroize all plaintext secret and private cryptographic keys and CSPs used for communications with an external EKM when no longer required.	Failure on invoking functionality	None	See FCS_CKM.1.
FCS_COP.1(1) The TOE implements AES with CTR and CBC modes and 128, 192, and 256 bit keys sizes.	Failure on invoking functionality	None	See FCS_CKM.1.
FCS_COP.1(2) The TOE implements the RSA Digital Signature Algorithm with a key size (modulus) including 2048 and greater bits.	Failure on invoking functionality	None	See FCS_CKM.1.
FCS_COP.1(3) The TOE implements SHA-1 cryptographic hashes.	Failure on invoking functionality	None	See FCS_CKM.1.

Requirement	Auditable Event(s)	Additional Audit Record Content	StoreServ Event
FCS_COP.1(4) The TOE implements HMAC-SHA-1 keyed-hash message authentication.	Failure on invoking functionality	None	See FCS_CKM.1.
FDP_ACC.2 The TOE uses Block Access Control policy to control all operations between attached host clients and Virtual Volumes.	None	None	None
FDP_ACF.1 The TOE enforces access control rules to determine whether attached hosts can access (read-only or read-write) configured Virtual Volumes as described in the STs.	All requests to perform an operation on an object covered by the SFP	The identity of the subject performing the operation	All tpdtcl actions that result in modification of objects (create, modify, delete) are logged via the 'CLI Command' type event, where the message includes the name of the command and the result, as well as the user involved and the source of the command.
FDP_AVL_EXT.1 The TOE allows CPGs to be configured in RAID 0, 1, 5, and 6 configurations and both CPGs and VVs are configured with warning and limit levels as described in the STs.	None	None	None
FDP_RIP.1 The TOE ensures that any previous information content of a chunklet is made unavailable upon the allocation of the chunklet to a virtual volume.	None	None	None
FIA_ATD.1 The TOE defines users in terms of user identity (i.e., name), domain, role, password and optionally private key.	None.	None	None
FIA_UAU.1 With the exception of hosts identified by iSCSI identifiers and Fiber Channel WWNs accessing virtual volumes on designated ports, the TOE doesn't offer any services to users until they are successfully authenticated with their user name and password or public key.	All use of the authentication mechanism	Provided user identity, origin of the attempt (e.g., IP address)	All authentications generate events of type: 'Authentication Failure', 'Authentication Error', or 'CLI server process event'. Hosts which appear (e.g., at startup) and disappear (e.g., at shutdown) on their ports display in the audit log as 'Notification' type events with either their FC WWN, or iSCSI name in the message text. The event indicates 'logged in' when a host appears and 'lost' and/or 'logged out' when a host disappears.

Requirement	Auditable Event(s)	Additional Audit Record Content	StoreServ Event
FIA_UAU.5 The TOE can be configured to automatically utilize an external LDAP server for authentication of users not internally defined.	All use of the authentication mechanism	Origin of the attempt (e.g., IP address)	See FIA_UAU.1. The type of authentication (local, LDAP, keyed) is not included in the log.
FIA_UAU.7 The TOE is designed to not echo passwords when users are logging in.	None	None	None
FIA_UID.2 The TOE doesn't offer any services to users, including client hosts, until they are successfully identified with either user name/password or public-key credentials in the case of administrative users or iSCSI identifier or Fiber Channel WWN in the case of client hosts.	All use of the user identification mechanism	The user identity provided	See FIA_UAU.1.
FMT_MSA.1 The TOE restricts the ability to manage the access settings for Virtual Volumes to users with the super user or that are in the applicable domain with the edit class (aka System Administrators in the domain of the protected object). Note that VVs (in a given domains) can be defined and exported to defined hosts (in the same domain) and/or ports (which are not associated with domains); in turn hosts are associated with specific iSCSI or WWN identifiers. iSCSI and WWN identifiers are properties of hosts that are not configurable or alterable within the TOE.	All modifications of the security attribute values	None	See FDP_ACF.1.

Requirement	Auditable Event(s)	Additional Audit Record Content	StoreServ Event
FMT_MSA.3 The TOE restricts the ability to manage the access settings for Virtual Volumes to users with the super user or that are in the applicable domain with the edit class (aka System Administrators in the domain of the protected object). Note that there aren't actually any defaults beyond the fact that access can only be obtained after access is specifically configured in accordance with the access control rules.	Modifications of the default setting of permissive or restrictive rules All modifications of the security attribute initial values	None	See FDP_ACF.1.
FMT_MTD.1 The TOE restricts the ability to manage security relevant TOE data (i.e., TSF data) to users with any user class (aka System Administrators).	None	None	None
FMT_SMF.1 The TOE provides a full range of functions that can be used to manage the TOE and its security functions including reviewing audit events, managing user accounts, and managing access to Virtual Volumes.	None	None	None
FMT_SMR.2 The TOE implements browse, edit, service, and super user classes. The user classes are collectively referred to as System Administrator in this Security Target.	None	None	None
FPT_APW_EXT.1 The TOE stores passwords in non-plaintext form using SHA-512 hash and ensures that they cannot be read.	None	None	None
FPT_FLS.1 The TOE preserves a secure state when the following types of failures occur: node, power fail, storage availability, and network (e.g., administrative) interface.	Failure of the TSF	TOE component that failed (for example, disk drive or HBA)	None

Requirement	Auditable Event(s)	Additional Audit Record Content	StoreServ Event
FPT_STM.1 The TOE includes its own hardware clock and is capable of being configured to use a network time server for synchronization.	Changes to the time	The old and new values for the time Origin of the attempt (e.g., IP address)	See FDP_ACF.1.Also, adjustment actions taken by NTP are logged as 'Syslog Message' type events with the string 'ntpd' in the text.
FPT_TST_EXT.1 The TOE runs a suite of self-tests during initial start-up to demonstrate it is operating correctly.	None	None	None
FRU_FLT.1 The TOE ensures reading and writing to a virtual volume when individual failures occur (see the security target for the individual failures).	Any failure detected by the TSF All TOE capabilities being discontinued due to a failure	None	
FTA_SSL.4 The TOE allows Administrator-initiated termination of the Administrator's own interactive session.	The termination of an interactive session	None	
FTP_ITC.1 The TOE provides a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.	Initiation of the trusted channel Termination of the trusted channel Failure of the trusted channel functions	None Identification of the initiator and target of failed trusted channels establishment attempt	
FTP_TRP.1 The TOE uses SSH to provide a trusted communication path between itself and remote users that is logically distinct from other communication paths and provides assured identification of its end point and protection of the communicated data from disclosure and detection of modification of the communicated data.	Initiation of the trusted channel Termination of the trusted channel Failures of the trusted path functions	Identification of the claimed user identity	None

Configuration Steps for CC Operation

The following steps should have been taken by HPE 3PAR authorized installers to configure the HPE 3PAR Storage System for CC evaluated configuration operation (to verify that you are actually running in the CC evaluated configuration, see "CC Configuration Validation" on page 29).

WARNING If any of these steps are omitted, the system will not be in the evaluated configuration.

1. Unsecured ports – All unsecured ports must be disabled to operate in the evaluated configuration. The steps to disable unsecured ports differ based on the StoreServ system family type.
   a. For a StoreServ 7xxxx/8xxxx system:
      i. Initiate and complete the SmartStart Storage System Setup Wizard.
      ii. Using an SSHv2 client, disable the unsecured ports using the following command.

      ```
      setnet disableports yes
      ```

      iii. Using an SSHv2 client, disable the port (5783) that the CLI client uses to connect to the HPE 3PAR Storage System using the following command:

      ```
      setnet remotecliports disable
      ```

   b. For a StoreServ 10xxx/20xxx system:
      i. On new installations, the authorized installer uses the "Out-of-the-Box" (OOTB) process to initialize the new system.

      This process allows for the configuration of basic system resources and requirements to be customized to the local site (e.g., IP network configuration, spare disk sizes). The process asks the installer if all unsecured (non-encrypted) ports are to be disabled. The installer must answer "yes" to disable all unsecured ports.

      ii. On system upgrades, using an SSHv2 client, execute the command:

      ```
      setnet disableports yes
      ```

      iii. Disable the port (5783) that the CLI client uses to connect to the HPE 3PAR Storage System using the following command:

      ```
      setnet remotecliports disable
      ```

2. The authorized installer will disassociate the SP from the HPE 3PAR Storage System. (using the **spvar** or **spdood** account) using SPOCC, or spmaint option 3.4, **[remove an InServ]**.
3. Destroy the SP credentials on the HPE 3PAR Storage System using an SSHv2 client and the following command:

   ```
   removespcredential
   ```

4. CIM should not be enabled in the evaluated configuration
    a. On new systems, the authorized installer should not enable CIM while conducting the OOTB process. Additionally, administrators should not issue the `startcim` CLI command.

       To insure that CIM ports are disabled on a new system, the installer must disable CIM ports using the `stopcim -f` CLI command.

    b. On upgraded systems, the system administrator should issue the `stopcim -f` CLI command to disable CIM, if it was in use, and not use the `startcim` command.

       If CIM was not in use, it is not necessary to issue the `stopcim -f` CLI command to disable CIM as is required when installing a new system (step a.).
5. SNMP should not be used in the evaluated configuration.
    a. On new systems, administrators should not use the `addsnmpmgr` and `createsnmpuser` CLI commands.
    b. On upgraded systems, administrators should disable SNMP using the following CLI commands: `removesnmpmgr`, `removesnmpuser` (for each user created), `removesnmppw -r`, `removesnmppw -rw`, and `removesnmppw -w`.
6. Remote Copy should not be used in the evaluated configuration.
    a. On new systems, administrators should not issue the `startrcopy` CLI command.
    b. On upgraded systems, administrators should stop the remote copy feature using the `stoprcopy` CLI command and not issue the `startrcopy` command.
7. Default users on the system should be replaced with site-specific users, with the exception of the **3parsvc** user (see "Service Processor Considerations" in the following section). On the SP, the **spvar, 3parcust,** and **cpmaint** users should have their passwords changed.

   The default cli user **3paradm** is a super level user defined on the StoreServ for the purpose of performing initial configuration. Once new customer super users have been created, **3paradm** should be removed, or its password changed to a local value.
8. The '**audit-role**' user should not be present in day to day operations in common criteria mode. Use the **showuser** command to list all users, and if an **audit** user is present, use the **removeuser** command to remove that user.

Service Processor Considerations

The Service Processor (SP) is used only as a maintenance tool in the evaluated configuration. The remote access capabilities of the system are rarely allowed in sites where Common Criteria mode operation is desired and the event monitoring capabilities are disabled in the evaluated configuration (see "**Error! Reference source not found.**" on page 12). The SP was therefore excluded from the evaluated configuration.

The SP is still used by maintenance personnel, as a maintenance tool only, to guide maintenance activities and perform software upgrades to the HPE 3PAR Storage System. The following discussion is intended as a guide to how it can be securely used in an environment with HPE 3PAR Storage System(s) in the evaluated configuration.

For maintenance activities, the following steps can be taken in cooperation with a HPE 3PAR authorized maintainer to associate the SP with a particular HPE 3PAR Storage System. Following initial configuration, the administrator can disable the association of the SP to the HPE 3PAR Storage System using steps 5-7 below.

1. Using an SSHv2 client, enable the port (5783) that the CLI client uses to connect to the HPE 3PAR Storage System using the following command:

   ```
   setnet remotecliports enable
   ```

2. The authorized service provider can boot the SP and log in as local user **spvar** using a password assigned by the administrator (authorized maintainers will use **spvar**; HPE employees will use **spdood**, which has a password known only to HPE support personnel).

3. The authorized service provider uses the SPOCC or spmaint interface to associate the HPE 3PAR Storage System to the SP (spmaint menu option 3.2 **[add new inserv]**) and supplies the IP address of the HPE 3PAR Storage System.

   The process will ask for a customer admin username and password (typed by the customer), which will be used to perform the attach operation. This username must be that of a 'super' level CLI user.

   This causes the SP to exchange a public key with the HPE 3PAR Storage System, change the password of **3parsvc** to a random value, and create accounts **3parservice**, **3parbrowse** and **3paredit** (all with random passwords).

4. The maintenance activity is then performed as required.

5. On completion, the authorized service provider removes the SP – HPE 3PAR Storage System association using SPOCC or spmaint interface (spmaint menu option 3.4 **[remove an inserv]**).

   This changes the SP-related credentials on the HPE 3PAR Storage System to random values and destroys any SP-related keys.

6. The system administrator can change the **spvar** password on the SP if desired.

7. The SP can then be powered off if desired.

8. Using an SSHv2 client, disable the port (5783) that the CLI client uses to connect to the HPE 3PAR Storage System using the following command:

   ```
   setnet remotecliports disable
   ```

9. Using an SSHv2 client, remove the SP related credentials from the HPE 3PAR Storage System via the following command:

   ```
   removespcredential
   ```

5 Confirming the System Configuration

Administrators can use the information in this section to verify that the HPE 3PAR Storage System that was ordered has the correct system components and was installed and configured as intended.

See the *HPE 3PAR Command Line Interface Reference* for individual CLI command details.

Hardware

To determine that the installed hardware matches that which was ordered for a system, the administrator can use the `showinventory` CLI command. This lists all installed hardware components, with serial number and model number if available. This information can then be compared to the ordered configuration, based on sales invoices, to be certain that the hardware is correct. Also, following a maintenance procedure that replaces parts, the command can be used to produce a list to compare against a previous list to provide a check on the parts replaced and the location of those parts.

Software

To determine if the system software ordered matches what is installed and running, the administrator can use the `showversion` CLI command. This lists the version levels of all major components of the HPE 3PAR OS. To see an exhaustive list, use the `showversion -a` CLI command. After performing software maintenance activities, these commands can be used and compared against prior output to validate what components were changed.

Licensed Features

To determine what licensed features have been installed on the system, use the `showlicense` CLI command.

CC Configuration Validation

Use the steps below to determine if the system is running in the Common Criteria evaluated configuration.

1. Using a port scanner from a machine on the management network, scan the HPE 3PAR Storage System for open ports.

The only open ports should indicate that they support encrypted connections. This is useful following a maintenance activity that may have changed networking configuration on the HPE 3PAR Storage System. The `netcconf` command, used by service personnel on the console, can cause unsecured port blocking to be turned off if not executed correctly. For example, using the popular scanner "nmap":

```
nmap  –sT -sU –vv –p1-65535 <ip address of HPE 3PAR Storage System>
```

a. If you find unsecured, open ports in the scan following a maintenance procedure, use `setnet disableports yes` and `setnet remotecliports disable` to correct it.

2. Verify that CIM is not running using the `showcim` CLI command.
   a. Use the `stopcim` CLI command if CIM is running and you want to turn it off.
3. Verify that SNMP is not in use by using the `showsnmpmgr`, `showsnmppw`, and `showsnmpuser` CLI commands.
   a. Use `removesnmpmgr`, `removesnmpuser` for each SNMP user, `removesnmppw –r`, `removesnmppw –rw`, and `removesnmppw –w` if you want to disable it.
4. Validate that the Remote Copy feature is not running using the `showrcopy` CLI command.
   a. Use the `stoprcopy` CLI command if you want to disable it.
5. Use the `showencryption` CLI command to confirm that all disk drives are self-encrypting and FIPS compliant.
6. Validate that the default user passwords have been changed and that unused accounts have been deleted (except **3parsvc**).
   a. Use the `removeuser` CLI command to remove the desired users and the `setpassword –u <username>` CLI command to change the password on those you want to change.
7. Use the showuser CLI command to display all local user accounts on the system. If there is a user with 'audit' role defined it should be removed.
   a. Use the removeuser CLI command to remove any audit role user.

Auditing Security-Relevant Events

Administrators with super level authority can see a complete picture of security-relevant activity (including login/logout activity and failed login attempts) by using the `showeventlog` CLI command with the `–debug` operand. The `showeventlog –debug`

command can be used with filters to limit the output. For example, to find the activity of the user "user_one" for the past 25 minutes, use the command shown below.

```
showeventlog –debug –min 25 –msg "user_one"
```

NOTE The `–debug` operand of `showeventlog` is not defined in the *HPE 3PAR Command Line Interface Reference* and it is limited to super and service level users. It should, generally, be used with a filter of some kind, since it can produce enormous amounts of output.

To prevent the loss of security-relevant events due to event log roll-over, customers should consider archiving the output of the `showeventlog –debug` command every 24 hours. The command below defines the exact period to archive to avoid missing events and unnecessary duplication of events.

```
showeventlog –debug –startt "yyyy-MM-dd hh:mm:ss" –endt "yyyy-MM-
dd hh:mm:ss"
```

6 Documentation Errata

This section identifies Common Criteria-related errors in the HPE 3PAR Storage System customer documents.

Concepts Guide

Data Encryption (p. 61)

The note at the end of the section indicates that the data encryption solution is not FIPS 140-2 compliant. While this is correct if the LKM is used to manage authentication keys, it is incorrect for the Common Criteria evaluated configuration, which requires an EKM server and FIPS 140-2 compliant SEDs and is therefore FIPS 140-2 compliant.

CLI Administrator Guide

Active Directory LDAP Configuration with Simple Binding Over SSL (p. 27)

The procedure incorrectly uses the `setauthparam ldap-ssl-cacert` command to import the CA certificate. This command has been deprecated as of release 3.2.2. Use the `importcert` command to import the CA certificate (see “LDAP Server Configuration” on page 17).

CLI User Name Restrictions Using SSH (p. 57)

The user name restrictions have nothing to do with SSH. These are user names that already exist on the system and therefore cannot be created using the `createuser` CLI command. It is not possible to log onto the HPE 3PAR Storage System through the CLI using these user names. Additionally, the list of reserved names is incorrect and should read: root, daemon, bin, console, nobody, sshd, telnetd, sys, sync, man, statd, ntp, messagebus, libuuid, games, lp, mail, news, uucp, proxy, www-data, backup, list, irc, gnats, dnsmasq, and libvirt-qemu.

Supported Configurations, HPE 3PAR StoreServ Storage (p. 115)

Incorrectly indicates which HPE 3PAR StoreServ Storage systems support data encryption. Families/model 7xxxc, 8xxx, 10xxx and 20xxx support data encryption.

Appendix A (p. 151) and Appendix B (p. 162)

The tables do not include all rights supported by the HPE 3PAR Storage System (missing are the pd_tune and sys_tune rights).

7 Support and Other Resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  http://www.hpe.com/assistance

- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  http://www.hpe.com/support/hpesc

Information to Collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing Updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates, go to either of the following:
  - Hewlett Packard Enterprise Support Center Get connected with updates page:

    www.com/hpesupport/e-updates

  - Software Depot website:

    www.com/hpesupport/e-updates

- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center More Information on Access to Support Materials page:

  http://www.hpe.com/support/AccessToSupportMaterials

IMPORTANT! Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

Websites

Website	Link
Hewlett Packard Enterprise Information Library	www.hpe.com/info/enterprise/docs
Hewlett Packard Enterprise Support Center	www.hpe.com/support/hpesc
Contact Hewlett Packard Enterprise Worldwide	www.hpe.com/assistance
Subscription Service/Support Alerts	www.hpe.com/support/e-updates
Software Depot	www.hpe.com/support/softwaredepot
Customer Self Repair	www.hpe.com/support/selfrepair
Insight Remote Support	www.hpe.com/info/insightremotesupport/docs
Serviceguard Solutions for HP-UX	www.hpe.com/info/hpux-serviceguard-docs
Single Point of Connectivity Knowledge (SPOCK) Storage compatibility matrix	www.hpe.com/storage/spock
Storage white papers and analyst reports	www.hpe.com/storage/whitepapers

HPE 3PAR documentation

For information about:	See:
Supported hardware and software platforms	The Single Point of Connectivity Knowledge for HPE Storage Products (SPOCK) website: SPOCK (http://www.hpe.com/storage/spock)
Locating 3PAR documents	The Hewlett Packard Enterprise Storage Information Library: Storage Information Library (http://www.hpe.com/go/storage/docs) By default, **HPE 3PAR Storage** is selected under **Products and Solutions**

For information about:	See:
Customer Self Repair procedures (media)	The Hewlett Packard Enterprise Customer Self Repair Services Media Library: Customer Self Repair Services Media Library (http://www.hpe.com/support/csr) Under **Product category**, select **Storage**. Under **Product family**, select **3PAR StoreServ Storage** for 3PAR StoreServ 7000, 8000, 10000, and 20000 Storage systems.
All Hewlett Packard Enterprise products	Hewlett Packard Enterprise Support Center: Hewlett Packard Enterprise Support Center (http://www.hpe.com/info/3PAR-SmartSAN-UG)

Customer Self Repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

www.hpe.com/support/selfrepair

Remote Support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

For more information and device support details, go to the following website:

www.hpe.com/info/insightremotesupport/docs

Documentation Feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front

cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.