# Hewlett-Packard 3PAR® StoreServ Storage Systems
# Security Target

Version 5.0
12/7/2015

**LIST OF TABLES**

# 1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is Hewlett-Packard 3PAR StoreServ Storage Systems provided by Hewlett-Packard 3PAR. 3PAR StoreServ Storage Systems are physical appliances that primarily serve to host physical disk drives and provide a secure channel to configure the access policy that is enforced between content on the disks and attach storage area network (SAN) hosts. This evaluation includes the 7000c and 10000 (previously known as V-Class) models.

The Security Target contains the following additional sections:

- Product Description (Section 2)
- Security (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 8).

## 1.1 Security Target, TOE and CC Identification

**ST Title –** Hewlett-Packard 3PAR® StoreServ Storage Systems Security Target

**ST Version** – Version 5.0

**ST Date** – 9/25/2015

**TOE Identification** – The TOE consists of the following basic components:

- Hewlett-Packard 3PAR StoreServ Storage Systems (specific models identified below) running HP 3PAR OS (version 3.2.1 MU3)
  - HP 3PAR StoreServ 7000c Storage System models 7200c, 7400c, 7440c and 7450c
  - HP 3PAR StoreServ 10000 Storage System models 10400 and 10800

**TOE Developer** – Hewlett-Packard Company

**Evaluation Sponsor** – Hewlett-Packard Company

**CC Identification** – Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012

## 1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.
  - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.
  - Part 3 Conformant
  - Assurance Level: EAL 2 augmented with ALC_FLR.2

The TOE does not claim conformance to any protection profiles and does not claim conformance to any extended packages.

## 1.3 Commonly Used Terms

Listed below are terms/acronyms used in this document.

| Acronym | Definition |
|---|---|
| AES | Advanced Encryption Standard |
| AK | Authentication Key |
| API | Application Programming Interface |
| ASIC | Application-specific Integrated Circuit |
| CBC | Cipher Block Chaining |
| CC | Common Criteria |
| Chunklet | StoreServ unit of data storage – PDs are divided into chunklets |
| CLI | Command Line Interface |
| CM | Content Management |
| CPG | Common Provisioning Group |
| CTR | Counter Cipher Mode |
| DAR | Data at Rest |
| DES | Data Encryption Standard |
| DSA | Digital Signature Algorithm |
| EKM | External Key Manager |
| FC | Fibre Channel |
| FCoE | Fibre Channel over Ethernet |
| FIPS 140-2 | Federal Information Processing Standards for cryptography modules |
| GNUtls | GNU TLS library |
| GUI | Graphical User Interface |
| HBA | Host Bus Adaptor |
| HMAC | Hashed-based Message Authentication Code |
| HP | Hewlett-Packard |
| HP 3PAR OS | StoreServ Operating System |
| ID | Identifier |
| I/O | Input/Output |
| IP | Internet Protocol |
| iSCSI | Internet SCSI |
| KMIP | Key Management Interoperability Protocol |
| LAN | Local Area Network |
| LD | Logical Disk |
| LDAP | Lightweight Directory Access Protocol |
| LKM | Local Key Manager |

| Acronym | Definition |
|---|---|
| LUN | Logical Unit Number |
| NAS | Network-Accessed Storage |
| MAC | Message Authentication Code |
| MC | StoreServ Management Console |
| NL | Nearline |
| NTP | Network Time Protocol |
| OpenLDAP | Open Source LDAP implementation |
| OpenSSH | Set of computer programs that provide encrypted communications session over a computer network using SSH |
| OS | Operating System |
| PD | Physical Disk |
| RAID | Redundant Array of Independent Disks |
| RSA | Rivest, Shamir, Adelman algorithm for public-key cryptography |
| SAN | Storage Area Network |
| SAR | Security Assurance Requirement |
| SAS | Serial Attached SCSI |
| SCSI | Small Computer System Interface |
| SED | Self-Encrypting Drives |
| SFR | Security Functional Requirement |
| SHA | Secure Hash Algorithm |
| SMI-S | Storage Management Initiative Specification |
| SNMP | Simple Network Management Protocol |
| SP | Service Processor |
| SSD | Solid-state Drive |
| SSH | Secure Shell network protocol |
| SSL/TLS | Secure Sockets Layer/Transport Layer Security cryptographic protocols |
| ST | Security Target |
| StoreServ | HP 3PAR StoreServ Storage System is a hardware appliance that offers network- and serial-port accessible administration interfaces to access data storage resources |
| TCP | Transport Control Protocol |
| TOE | Target of (Security) Evaluation (e.g., the StoreServ) |
| TPVV | Thinly Provisioned VV |
| TSF | TOE Security Function |
| UI | User Interface |
| VLUN | Virtual LUN |
| VV | Virtual Volume |
| WWN | WorldWideName |

# 2. Product Description

The HP 3PAR StoreServ Storage Systems are hardware appliances that offer network- and serial-port accessible administration interfaces. The primary service of a storage system is access to data storage resources (e.g., logical representations of physical disk drives) that are accessible via attached Fiber Channel (FC) or Internet SCSI (iSCSI) storage area networks (SANs). HP provides two families of products to address the storage needs of a mid-range or tier 1 enterprise.

- HP 3PAR StoreServ 7000c Storage System family provides a midrange storage system offering in the HP 3PAR StoreServ product line. Models 7200c and 7400c provide a mid-range value storage solution while models 7450c and 7440c enhance performance by providing an all flash array solution.
- HP 3PAR StoreServ 10000 Storage System family, models 10400 and 10800[1], provides a tier 1 solution for enterprises in which a scaled storage system is desired.

Both families make use of the HP 3PAR ASIC with Thin Built In™ features, which provide an efficient, silicon-based zero-detection mechanism, allowing allocated, but unused, space to be removed without impacting performance. Both families share the same HP 3PAR Operating System and support all the same advanced software, which is available through optional software licenses.

Administrators manage the storage systems using the HP 3PAR CLI client application, which is installed on management client computers and provides a secure tunnel from which to access the available security management functions.

Each appliance consists of a set of distinct devices (**Error! Reference source not found.** and **Table 2**), which vary primarily according to storage capacity, performance, and port type and number.

| | | Model 7200c | Model 7400c | Model 7450c | Model 7440c |
|---|---|---|---|---|---|
| Controller Nodes | | 2 | 2 – 4 | 2 – 4 | 2 – 4 |
| 8 Gb FC Ports | | 4 – 12 | 4 – 24 | 4 – 24 | 4 – 24 |
| 16 Gb FC Host Ports | | 0 – 4 | 0 – 8 | 0 – 8 | 0 – 8 |
| 10 Gb FCoE/iSCSI Ports | | 0 – 4 | 0 – 8 | 0 – 8 | 0 – 8 |
| 1 Gb Ethernet IP Ports | | 0 – 8 | 0 – 16 | 0 – 16 | 0 – 16 |
| 10 Gb Ethernet IP Ports | | 0 – 4 | 0 – 8 | 0 – 8 | 0 – 8 |
| Built-in IP Remote Copy Ports | | 2 | 2 – 4 | 2 – 4 | 2 – 4 |
| GBs cache per node pair / max | | 40/40 | 48/96 | 96/192 | 96/192 |
| GBs flash cache per node pair / max | | 768/768 | 768/1500 | N/A | 1500/3000 |
| Drives/StoreServ | | 8 – 240 | 8 – 576 | 8 – 240 | 8 - 960 |
| Drive Types[2] | SSD FE | yes | yes | yes | yes |
| | SAS FE | yes | yes | no | yes |
| | NL FE | yes | yes | no | yes |
| Max SSD/StoreServ | | 120 | 240 | 240 | 240 |
| Raw Capacity (TB) | | 500 | 1600 | 460 | 2000 |

**Table 1 StoreServ 7000c family, devices**

| | | Model 10400 | Model 10800 |
|---|---|---|---|
| Controller Nodes | | 2 | 2 – 8 |
| 8 Gb FC Ports | | 0 – 96 | 0 – 192 |
| 16 Gb FC Host Ports | | 0 – 48 | 0 – 96 |
| 10 Gb FCoE/iSCSI Ports | | 0 – 48 | 0 – 96 |
| 1 Gb Ethernet IP Ports | | N/A | N/A |
| 10 Gb Ethernet IP Ports | | N/A | N/A |
| Built-in IP Remote Copy Ports | | 2 – 4 | 2 – 8 |
| GBs cache per node pair / max | | 192/384 | 192/768 |
| GBs flash cache per node pair / max | | 2000/4000 | 2000/8000 |
| Drives/StoreServ | | 16 – 960 | 16 – 1920 |
| Drive Types[3] | SAS FE | yes | yes |
| | NL FE | yes | yes |
| Max SSD/StoreServ | | 256 | 512 |
| Raw Capacity (TB) | | 1600 | 3200 |

[1] The StoreServ 10400 and 10800 models identify themselves as InServ V400 and InServ V800, respectively.
[2] Drives must be self-encrypting and FIPS 140-2 compliant.
[3] Drives must be self-encrypting and FIPS 140-2 compliant.

**Table 2 StoreServ 10000 family, devices**

Each appliance primarily consists of drive cages that can accept drive magazines[4] that contain physical disk drives and a backplane that contains slots for controller nodes[5] that provide and manage interfaces available to connect to client hosts and other network entities (e.g., management consoles).

Customers interact with HP sales representatives to determine the feature requirements the appliance must meet and the sales representative uses an HP-internal configuration tool to determine the appliance configuration (software features, drive cages, disk drives, etc.). The customer receives a copy of the configuration to confirm that the appliance meets the requirements.

## 2.1 TOE Overview

The Target of Evaluation (TOE) is two classes of Hewlett-Packard 3PAR® StoreServ Storage Systems. The storage systems in the evaluated configuration include the 7000c family (models 7200c, 7400c, 7450c and 7440c) and the 10000 family (models 10400 and 10800).

The HP 3PAR OS software employed in the TOE is common across the families and models, which share a common architecture that allows them to implement the same security functions and policies. It consists of a set of individual features, some of which are excluded from the evaluated configuration (described in Section 2.1.5). There are also a number of optional features that can be individually licensed for use. Of these features, only one is considered security relevant:

- **HP 3PAR Virtual Domains** limits the privileges of users to only subsets of volumes and hosts in a StoreServ Storage System and ensures that Virtual Volumes (VVs) associated with a specific domain are not exported to hosts outside of that domain. The TOE may operate with Virtual Domains either enabled or disabled.

### 2.1.1 TOE Architecture

The HP 3PAR StoreServ Storage System architecture consists of an array of disk units, managed by pairs of controller nodes (to which the disks are directly connected), clustered via a full-mesh backplane interconnect

The disks are standard Serial Attached SCSI (SAS) disk drives, Nearline (NL) disk drives and/or Solid State Disks (SSD). Controller node pairs manage I/O operations between the installed disks and attached hosts and also facilitate the general operation of the server appliance including security management and logging. While each controller node can operate independently, the available nodes work in pairs to mitigate single node failures and are fully connected with a full-mesh backplane that provides load balancing, cache synchronization and consistency across the cluster. I/O operations can be originated by any node, but is executed by the pair of nodes to which a given physical disk is connected.

Each storage system appliance includes a number of Fiber Channel and Internet SCSI (iSCSI[6]) host ports. These ports can be used to directly connect a number of hosts, connect a number of storage area network (SAN) switches facilitating a very large network of SAN connected hosts, or a combination providing flexibility to support a wide variety of possible deployment environments. Hosts are logically defined and associated with Fiber Channel World Wide Names (WWNs) and/or iSCSI identifiers associated with the Fiber Channel or iSCSI adapters installed in the host. Figure 1 provides a summary of the StoreServ Storage System LAN and SAN connections.[7]

[4] HP 3PAR StoreServ 7000c Storage System family operates with individual drives, rather than magazines, housed in drive enclosures.

[5] Controller nodes can provide an operating environment for optional software features. All controller-hosted software is out of scope for this evaluation.

[6] The iSCSI ports are dedicated Gb Ethernet ports distinct from management Ethernet ports. The ports can be configured to use iSCSI (the default protocol) or the Fibre Channel Protocol (FCP). When configured to use FCP, the port is referred to as Fibre Channel over Ethernet (FCoE) and behaves as a FC port (e.g., host identification is via FCWWNs) except that the transport mechanism is Ethernet. For the remainder of this document, ports will be identified as iSCSI and/or FC, with FCoE being implied.

[7] The figure shows only LAN and SAN connections for the TOE evaluated configuration. Additional connections are provided for functionality that is not evaluated.

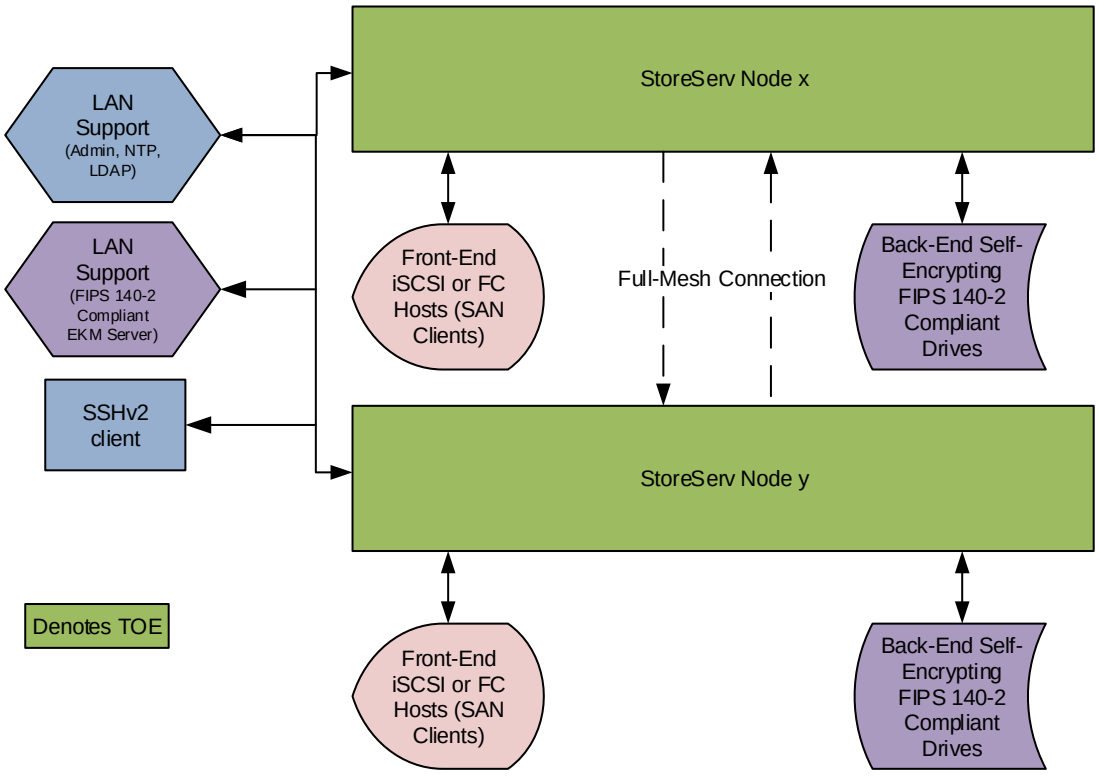


Figure 1 LAN and SAN connections

The TOE architecture separates the control and data sides of each storage system node:

- Client hosts attach to FC and iSCSI ports on the Host Bus Adapters (HBAs) and can perceive only data storage resources that have been configured for host access. Client hosts cannot access or perform any security management of configuration type functions.
- Administrators access storage system nodes via LAN and serial connections from which they can perform security and other management and service operations, but while they can configure available disk resources for access by client hosts they cannot access the content of those disks.

From a client host perspective, the data resources are available in the form of Virtual Volumes (VVs) identified by Virtual Logical Units (VLUNs). Internally, the physical disks are logically divided into pools of 1GB 'chunklets' that are assembled from across available disks into Logical Disks (LDs). Each VV is then built from all or part of a LD or spread across several LDs.

From an administrator perspective, to create a VV an administrator must first create a Common Provisioning Group (CPG). The CPG identifies an initial space allocation, a growth increment, and a RAID level. Additionally, each CPG includes growth warnings and growth limits.

The HP 3PAR StoreServ Storage System uses a Block Access Control Policy to control all operations between attached host clients and VVs. Once hosts and VVs are defined, an administrator can define associations so that hosts can access VVs.

To support the HP 3PAR Data Encryption feature, the HP 3PAR StoreServ Storage System makes use of FIPS 140-2 compliant self-encrypting drives (SEDs) that protect the data on the drives by encrypting it using technology internal to the drives (not performed by the StoreServ itself). All drives in the system must be self-encrypting and FIPS 140-2 compliant. A FIPS 140-2 compliant External Key Manager (EKM) server is used to create and manage the keys used to access the drives to prevent unauthorized access to the drive data. Disk drives and EKM servers are manufactured by other vendors and the TOE assumes FIPS-compliance is as claimed by the manufacturer; The physical drives themselves and the FIPS compliance of these components are outside the scope of this evaluation.

Because at least one domain is always present, the system behaves in a similar manner regardless of whether the HP 3PAR Virtual Domains feature is enabled. With the Virtual Domains feature enabled, up to 1024 domains can be defined. Users can be assigned up to 32 domains (each with its own user role) for which they can configure resources (see Section 6.4). CPGs and hosts are each assigned to a specific domain. There is a least one domain present in the TOE – the "all" domain. When Virtual Domains is not enabled, all users are associated with the "all" domain. When Virtual Domains is enabled, in addition to the "all" domain, users may be associated with additional domains.

### 2.1.2 TOE Administration

The storage system connects to a Local Area Network (LAN) through which administrators can connect and also through which supporting servers (e.g., LDAP, NTP) can be accessed when needed.

An administrator connects to the TOE using SSH via a client with SSHv2 support to access the available CLI functions, providing a secure tunnel that allows the appliance to authorize and authenticate administrators.

### 2.1.3 Physical Boundaries

The physical boundary of an HP 3PAR StoreServ Storage System is the physical boundary of the hardware. Interfaces to this hardware include iSCSI and Fibre Channel ports for data connections and Ethernet ports for server administration. The applicable device classes and models are provided in **Table 1**and **Table 2**.

Administrative interface access is obtained by SSHv2 (for CLI) or TLS (for LDAP) connection.

The TOE is configured to rely on and utilize a number of other components in its operational environment (see Section 6.9 for additional connection details). All of the following external functionality is outside the scope of the evaluation.

- LDAP server – The TOE includes an LDAP client that uses OpenLDAP v2.4.39 to communicate with an authentication server operating on the following platforms:
    - Linux server: OpenLDAP slapd v2.4.39
    - Linux server: RHDS version 9 operating on RHEL version 6.2
    - Windows server: Active Directory on Windows 2003, 2008 and 2012

  TOE-LDAP server communication is secured using TLS.
- Network Time Protocol (NTP) server – The TOE is configured to use a NTP server to synchronize the internal clock of each individual node. Communcation adheres to RFC 5905, Network Time Protocol Version 4: Protocol and Algorithms Specification, June 2010.
- EKM server – The TOE is configured to use an External Key Manager server to create and manage locking keys in support of self-encrypting drives. Two models of EKM server are currently supported:
    - HP Enterprise Secure Key Manager v4.0
    - SafeNet KeySecure k450 or k150 version 6.1.2
- FC and iSCSI client hosts – The TOE attaches to FC or iSCSI hosts, which access available storage resources, either directly through available ports or indirectly through a suitable SAN connected to available ports.
- Management Workstation – An SSHv2 client operating on a suitable workstation is required to use the local (on-node) CLI administrative interface.
- Disk drives – The TOE attaches directly to the disk drives supported by a particular StoreServ family/model (see **Table 1** and **Table 2**). The drives are self-encrypting and FIPS 140-2 compliant.

### 2.1.4 Logical Boundaries

Listed below are the logical boundaries of the HP 3PAR StoreServ Storage Systems. Chapter 6 describes the security functions provided by each boundary.

- Security audit (see Section 6.1)
- Cryptographic support (see Section 6.2)
- User data protection (see Section 6.3)
- Identification and authentication (see Section 6.4)
- Security management (see Section 6.5)
- Protection of the TSF (see Section 6.6)
- Resource utilization (see Section 6.7)
- TOE access (see Section 6.8)
- Trusted path/channels (see Section 6.9)

### 2.1.5 TOE Exclusions

The HP 3PAR OS that operates on the TOE consists of multiple features, not all of which are included in the TOE evaluated configuration. **Table 3** lists the individual features and disposition with regard to evaluation.

| Feature | Evaluated Disposition |
|---|---|
| Persistent Ports – Allows for non-disruptive online software upgrades on StoreServ without relying on multi-pathing software | Included, not evaluated |
| Web Services API – API that customers can use for incorporating the storage infrastructure into their platform for end-to-end automation of their service delivery and management. | Included, not evaluated |
| OS Administration Tools | Administration Tools consist of the following:<br>• Remote CLI – Included, not evaluated<br>• MC – Included, not evaluated<br>• SNMP – Included, not evaluated<br>• SMI-S – 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 |
| LDAP Support | Included |
| Adaptive Flash Cache | Included, not evaluated |
| File Services | Included, not evaluated |
| Remote Copy | Included, not evaluated |

**Table 3 HP 3PAR OS feature disposition in TOE evaluated configuration**

Each HP 3PAR StoreServ 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 HP 3PAR. Since it is not part of the normal day-to-day TOE operation, the SP is not evaluated functionality and must be disabled (i.e., not configured) while operating the TOE in its evaluated configuration.

Each HP 3PAR StoreServ Storage System appliance includes a serial port to which a maintenance terminal can be directly connected to provide access to a subset of CLI functions. The maintenance terminal port is intended only for use by authorized HP 3PAR service personnel only and is not evaluated functionality.

The HP 3PAR OS includes a Local Key Manager (LKM) that is not evaluated functionality.

The EKM server, and back-end SEDs, are assumed to be FIPS-140-2 compliant and are validated by the associated vendors. The discussion of the capabiltities of these components is outside the TOE boundary, and is not evaluated functionality.

## 2.2 TOE Documentation

There are numerous documents that provide information and guidance for the deployment of HP 3PAR StoreServ Storage Severs. The following documents were specifically examined in the context of the evaluation:

- HP 3PAR OS 3.2.1 Concepts Guide
- HP 3PAR OS 3.2.1 CLI Administrator's Manual
- HP 3PAR OS 3.2.1 Command Line Interface Reference
- HP 3PAR OS 3.2.1 Common Criteria Administrator’s Reference

# 3. Security Problem Definition

The Security Problem Definition (composed of organizational policies, threat statements, and assumptions) is specified in this section to specifically identify the threats addressed by storage systems and the assumptions made in so doing.

## 3.1 Threats

| | |
|---|---|
| T.ADMIN_ERROR | An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms. |
| T.DATA_AVAILABILITY | User data may become unavailable due to isolated storage resource failures or due to resource exhaustion. |
| T.TSF_FAILURE | Security mechanisms of the TOE may fail, leading to a compromise of the TSF. |
| T.UNAUTHORIZED_ACCESS_CODE | A user may gain unauthorized access to the TSF executable code. |
| T.UNAUTHORIZED_ACCESS_TSF_DATA | A user may gain unauthorized access to the TSF data.. |
| T.UNAUTHORIZED_ACCESS_USER_DATA | A user may gain unauthorized access to user data. |
| T.UNDETECTED_ACTIONS | Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated. |
| T.USER_DATA_REUSE | User data may be inadvertently sent to a destination not intended by the original sender. |

## 3.2 Assumptions

| | |
|---|---|
| A.HOST_IDENTITY | It is assumed that iSCSI and Fiber Channel host identities properly reflect the adapters and hence the hosts to which they are associated such that authentication is not necessary. Implicit in this assumption is the SAN(s) connecting iSCSI and Fiber Channel must be controlled to mitigate potentially malicious attacks on the SAN(s). |
| A.PHYSICAL_CLIENT_HOSTS | Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment, which includes the client hosts. It is assumed that administrators allow only trusted hosts access to these connections and that the hosts themselves are protected from access by untrustworthy entities. |

| | |
|---|---|
| A.PHYSICAL_MANAGEABILITY | Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment. This also extends to supporting servers (e.g., LDAP, NTP) that are expected to be in close proximity to the TOE. An NTP server is assumed to provide reliable timestamps for use by the TOE. |
| A.TRUSTED_ADMIN | TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner. |

# 4. Security Objectives

The Security Objectives represent the objectives necessary for a storage system TOE to address its corresponding threats as well as operational environment objectives necessary to fulfill the identified assumptions.

## 4.1 Security Objectives for the TOE

| | |
|---|---|
| O.AVAILABILITY | The TOE will ensure that data can be stored in a manner that is protected from underlying resource failure and exhaustion. |
| O.ACESS_CONTROL_DATA | The TOE will ensure that only authorized data path users have access to the user data it stores. |
| O.ACESS_CONTROL_MANAGEABILITY | The TOE will ensure that only authorized users can access configuration, data and resources. |
| O.FAIL_SECURE | The TOE will fail in a secure manner following failure of the power-on self-tests. |
| O.PROTECTED_COMMUNICATIONS | The TOE will provide protected communication channels for administrators. |
| O.RESIDUAL_INFORMATION_CLEARING | The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated. |
| O.SYSTEM_MONITORING | The TOE will provide the capability to generate audit data and provide the means to store and review those data. |
| O.TOE_ADMINISTRATION | The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and restrict logged-in administrators to authorized functions and TSF data. |
| O.TSF_SELF_TEST | The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly. |

## 4.2 Security Objectives for the Environment

| | |
|---|---|
| OE.PHYSICAL_CLIENT_HOSTS | Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment and extends to client hosts. |

| | |
|---|---|
| OE.PHYSICAL_MANAGEABILITY | Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment. This also extends to supporting servers (e.g., LDAP, NTP) that are expected to be in close proximity to the TOE. An external NTP server is assumed to provide reliable timestamps for use by the TOE. |
| OE.TRUSTED_ADMIN | TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner. |

# 5. IT Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs are drawn from the Common Criteria (CC) part 2.

The SARs are drawn from the Common Criteria (CC) part 3.

## 5.1 Conventions

The following conventions have been applied in this chapter:

- Security Functional Requirements – Part 1 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a number in parentheses placed at the end of the component. For example FDP_ACC.1(1) and FDP_ACC.1(2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, (1) and (2).
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …"). Note that 'cases' that are not applicable in a given SFR have simply been removed without any explicit identification.

    Explicitly stated SFRs are identified by having a label 'EXT' after the requirement name for TOE SFRs.

## 5.2 Extended Requirements

This ST defines the following extended requirements:

- FPT_APW_EXT.1 has been crafted specifically to address protection of manageability path passwords. There are no SFRs in the CC that address protection as it relates to password format. FPT_APW_EXT.1 is defined as follows.

    **FPT_APW_EXT.1.1** The TSF shall store passwords in non-plaintext form using SHA-512 hash; the TSF shall ensure that the stored passwords cannot be read.

    **FPT_APW_EXT.1.2** The TSF shall prevent the reading of plaintext passwords.

- FPT_TST_EXT.1 is an extension of CC SFR FPT_TST.1 that addresses TSF self-test. FPT_TST_EXT.1 is defined as follows.

    **FPT_TST_EXT.1.1** The TSF shall run a suite of self-tests during initial start-up (power on) to demonstrate the correct operation of the TSF.

- FDP_AVL_EXT.1 has been crafted specifically to address availability properties applicable to SAN type TOEs. There are no SFRs in the CC that address the RAID-type reliability or simple warning and limit

levels for the allocation of underlying resources to support those objects exported for use on a SAN. FDP_AVL_EXT.1 is defined as follows.

**FDP_ AVL_EXT.1.1** The TSF shall implement the following RAID Disk Data Format levels [***0, 1, 5, 6, [assignment: other less common levels]***] that comply with the Common RAID Disk Data Format Specification, version 2.0.

**Application Note:** The intent is that a completed requirement would identify the supported RAID level and that the RAID design should conform to the current version of the Common RAID Disk Data Format Specification published by Storage Network Industry Association (SNIA).

**FDP_ AVL_EXT.1.2** The TSF shall be able to generate an alert when a System Administrator configured warning threshold for user data storage is exceeded.

**Application Note:** The intent is that a warning level can be defined when an alert is generated that would potentially enable an administrator to take action to mitigate resource exhaustion.

**FDP_ AVL_EXT.1.3** The TSF shall be able to generate an alert and prevent additional user data storage space allocation when a System Administrator configured limit for user data storage is exceeded.

**Application Note:** The intent is that an allocation limit can be defined and when that limit is reached an alert is generated and no further allocations are allowed.

## 5.3 TOE Security Functional Requirements

The following table describes the SFRs that are satisfied by Hewlett-Packard 3PAR® StoreServ Storage Systems.

| Requirement Class | Requirement Component |
|---|---|
| **FAU: Security audit** | FAU_GEN.1: Audit Data Generation |
| | FAU_GEN.2: User identity association |
| | FAU_SAR.1: Audit Review |
| | FAU_SAR.2: Restricted Audit Review |
| | FAU_SAR.3: Selectable audit review |
| | FAU_STG.1: Protected audit trail storage |
| | FAU_STG.4: Prevention of audit data loss |
| **FCS: Cryptographic support** | FCS_CKM.1: Cryptographic Key Generation (for asymmetric keys) |
| | FCS_CKM.4: Cryptographic Key Zeroization |
| | FCS_COP.1(1): Cryptographic Operation (for data encryption/decryption) |
| | FCS_COP.1(2): Cryptographic Operation (for cryptographic signature) |
| | FCS_COP.1(3): Cryptographic Operation (for cryptographic hashing) |
| | FCS_COP.1(4): Cryptographic Operation (for keyed-hash message authentication) |
| **FDP: User data protection** | FDP_ACC.2: Complete access control |
| | FDP_ACF.1: Security attribute based access control |
| | FDP_AVL_EXT.1: User data availability |
| | FDP_RIP.1: Subset Residual Information Protection |
| **FIA: Identification and authentication** | FIA_ATD.1(1): User attribute definition (for manageability path) |
| | FIA_ATD.1(2): User attribute definition (for data path) |
| | FIA_UAU.1: Timing of authentication |
| | FIA_UAU.5: Multiple authentication mechanisms |
| | FIA_UAU.7: Protected authentication feedback |
| | FIA_UID.2: User identification before any action |
| **FMT: Security management** | FMT_MSA.1: Management of security attributes |
| | FMT_MSA.3: Static attribute initialization |
| | FMT_MTD.1: Management of TSF Data (for general TSF data) |
| | FMT_SMF.1: Specification of Management Functions |
| | FMT_SMR.2: Restrictions on Security Roles |
| **FPT: Protection of the TSF** | FPT_APW_EXT.1: Protection of Administrator Passwords |
| | FPT_FLS.1: Failure with Preservation of Secure State |
| | FPT_STM.1: Reliable Time Stamps |
| | FPT_TST_EXT.1: TSF Testing |
| **FRU: Resource utilization** | FRU_FLT.1: Degraded fault tolerance |
| **FTA: TOE access** | FTA_SSL.4: User-initiated Termination |
| **FTP: Trusted path/channels** | FTP_ITC.1: Inter-TSF trusted channel |
| | FTP_TRP.1: Trusted path |

**Table 4 TOE Security Functional Components**

### 5.3.1 Security audit (FAU)

#### 5.3.1.1 Audit Data Generation (FAU_GEN.1)

**FAU_GEN.1.1** The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the[ ***not specified***] level of audit; and

c) All administrative actions;

d) [***Specifically defined auditable events listed in Table 5***].

**Application Note:** The concept of 'all administrative actions' in this SFR is not intended to include all actions taken by an administrative user, but rather to include only those actions associated with making configuration changes or reviewing potentially sensitive information (e.g., audit records). Otherwise, the concept of an administrator 'browsing' the configuration or non-sensitive TOE data is not necessarily subject to auditing.

**FAU_GEN.1.2** The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [***information specified in column three of Table 5***].

| Requirement | Auditable Events | Additional Audit Record Contents |
|---|---|---|
| FAU_GEN.1 | None | Not applicable |
| FAU_GEN.2 | None | Not applicable |
| FAU_SAR.1 | Reading of information from the audit record | No additional content |
| FAU_SAR.2 | Reading of information from the audit record | No additional content |
| FAU_SAR.3 | None. | Not applicable |
| FAU_STG.1 | None | Not applicable |
| FAU_STG.4 | Action taken due to the audit storage failure. | Not applicable |
| FCS_CKM.1 | Failure on invoking functionality | Not applicable |
| FCS_CKM.4 | Failure on invoking functionality | Not applicable |
| FCS_COP.1(1) | Failure on invoking functionality | No additional content |
| FCS_COP.1(2) | Failure on invoking functionality | No additional content |
| FCS_COP.1(3) | Failure on invoking functionality | No additional content |
| FCS_COP.1(4) | Failure on invoking functionality | No additional content |
| FDP_ACC.2 | None. | Not applicable |
| FDP_ACF.1 | All requests to perform an operation on an object covered by the SFP | Identity of the subject performing the operation |
| FDP_AVL_EXT.1 | None | Not applicable |
| FDP_RIP.1 | None. | Not applicable |
| FIA_ATD.1(1) | None | Not applicable |
| FIA_ATD.1(2) | None | Not applicable |
| FIA_UAU.1 | All use of the authentication mechanism | Provided user identity, origin of the attempt (e.g., IP address) |
| FIA_UAU.5 | All use of the authentication mechanism | Origin of the attempt (e.g., IP address) |
| FIA_UAU.7 | None | Not applicable |
| FIA_UID.2 | All use of the user identification mechanism | The user identity provided |
| FMT_MSA.1 | All modifications of the values of security attributes | No additional content |
| FMT_MSA.3 | Modifications for the default setting of permissive or restrictive rules | No additional content |
| | All modifications for the initial values of security attributes | No additional content |
| FMT_MTD.1 | None | Not applicable |
| FMT_SMF.1 | None | Not applicable |
| FMT_SMR.2 | None | Not applicable |
| FPT_APW_EXT.1 | None | Not applicable |
| FPT_FLS.1 | Failure of the TSF. | TSF component that failed (for example, disk drive or HBA) |

| Requirement | Auditable Events | Additional Audit Record Contents |
|---|---|---|
| FPT_STM.1 | Changes to the time | The old and new values for the time<br>Origin of the attempt (e.g., IP address) |
| FPT_TST_EXT.1 | None | Not applicable |
| FRU_FLT.1 | Any failure detected by the TSF | No additional content |
| | All TOE capabilities being discontinued due to a failure | No additional content |
| FTA_SSL.4 | The termination of an interactive session | No additional information |
| FTP_ITC.1 | Initiation of the trusted channel | No additional information |
| | Termination of the trusted channel | No additional information |
| | Failure of the trusted channel functions | Identification of the initiator and target of failed trusted channels establishment attempt |
| FTP_TRP.1 | Initiation of the trusted channel | Identification of the claimed user identity |
| | Termination of the trusted channel | Identification of the claimed user identity |
| | Failures of the trusted path functions | Identification of the claimed user identity |

**Table 5 Auditable Events**

#### 5.3.1.2 User identity association (FAU_GEN.2)

**FAU_GEN.2.1** For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

#### 5.3.1.3 Audit Review (FAU_SAR.1)

**FAU_SAR.1.1** The TSF shall provide [***authorized users***] with the capability to read [all ***auditable information***] from the audit records.

**FAU_SAR.1.2** The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

#### 5.3.1.4 Restricted audit review (FAU_SAR.2)

**FAU_SAR.2.1** The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

#### 5.3.1.5 Selectable audit review (FAU_SAR.3)

**FAU_SAR.3.1** The TSF shall provide the ability to apply [***filtering***] of audit data based on [**arbitrary data**].

**Application Note:** Users can search the audit log by arbitrary data, which could include date/time, event type, severity and general message information, etc. using regular expression and pattern matching. Audit log filtering is performed using the "**showeventlog –debug**" option and specifying various filtering options based on the information desired. User documentation provides specific details on the filtering mechanisms.

#### 5.3.1.6 Protected audit trail storage (FAU_STG.1)

**FAU_STG.1.1** The TSF shall protect **[33 MB] locally** stored audit records in the audit trail from unauthorized deletion.

**FAU_STG.1.2** The TSF shall be able to [***prevent***] unauthorized modifications to the stored audit records in the audit trail.

**Application Note:** The size of the audit log can be set by the system administrator. The size ranges from 512 KB to 4 MB; the default log size is 3 MB. Since the TOE maintains 11 generations of the audit log, FAU_STG.1.1 states 33 MB (3 MB X 11) of stored audit records are protected.

#### 5.3.1.7 Prevention of audit data loss (FAU_STG.4)

**FAU_STG.4.1** The TSF shall [***overwrite the oldest stored audit records***] and [**no other actions**] if the audit trail is full.

### 5.3.2 Cryptographic support (FCS)

#### 5.3.2.1 Cryptographic Key Generation (FCS_CKM.1)

**FCS_CKM.1.1** The TSF 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**] that meet the following: **[FIPS 140-2 Software Level 1].**

#### 5.3.2.2 Cryptographic Key Zeroization (FCS_CKM.4)

**FCS_CKM.4.1** The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[zeroization**] that meets the following: [**FIPS 140-2 Software Level 1**]**.**

#### 5.3.2.3 Cryptographic Operation (for data encryption/decryption) (FCS_COP.1.1(1))

**FCS_COP.1.1(1)** The TSF shall perform [**encryption and decryption**] in accordance with a specified cryptographic algorithm [***AES operating in CTR and CBC modes***] and cryptographic key sizes [**128 bits, 256 bits, and 192 bits**] that meet the following:

- [**FIPS PUB 197, 'Advanced Encryption Standard (AES)'**
- **NIST SP 800-38A**].

#### 5.3.2.4 Cryptographic Operation (for cryptographic signature) (FCS_COP.1.1(2))

**FCS_COP.1.1(2)** The TSF shall perform [**cryptographic signature services**] in accordance with a specified cryptographic algorithm [**RSA Digital Signature Algorithm (rDSA)] with a key size (modulus)** of **[2048bits or greater**] that meet the following:

- [**FIPS PUB 186-2 or FIPS PUB 186-3, "Digital Signature Standard"**].

#### 5.3.2.5 Cryptographic Operation (for cryptographic hashing) (FCS_COP.1.1(3))

**FCS_COP.1.1(3)** The TSF shall perform [**cryptographic hashing services**] in accordance with a specified cryptographic algorithm [**SHA-1, SHA-256, SHA-512**] and **message digest** sizes [**160, 256, 512**] that meet the following: [**FIPS Pub 180-3, 'Secure Hash Standard**].'

#### 5.3.2.6 Cryptographic Operation (for keyed-hash message authentication) (FCS_COP.1.1(4))

**FCS_COP.1.1(4)** The TSF shall perform [**keyed-hash message authentication**] in accordance with a specified cryptographic algorithm HMAC-[**SHA-1**], **key size** [**160 bits**], and **message digest sizes** [**160**] that meet the following: [**FIPS Pub 198-1, 'The Keyed-Hash Message Authentication Code', and FIPS Pub 180-3, 'Secure Hash Standard**].'

### 5.3.3 User data protection (FDP)

#### 5.3.3.1 Complete access control (FDP_ACC.2)

**FDP_ACC.2.1** The TSF shall enforce the [**Block Access Control policy**] on [

- **subjects: Fiber Channel and iSCSI hosts,**
- **objects: Virtual Volumes]** and

all operations among subjects and objects covered by the SFP.

**Application Note:** "Subjects" are referred to as "data path users."

**FDP_ACC.2.2** The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

#### 5.3.3.2 Security attribute based access control (FDP_ACF.1)

**FDP_ACF.1.1** The TSF shall enforce the [**Block Storage Access Control Policy**] to objects based on the following:

- [**Subjects:**
  - **Fiber Channel and iSCSI hosts: host identifier (WWN, iSCSI identifier) and port identifier**
- **Objects:**
  - **Virtual Volume: Virtual Logical Unit (VLUN) and associated access (host sees, host set, port presents, or matched set)**].

**FDP_ACF.1.2** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

**a) if a VLUN is configured for 'host sees' access, only hosts with a matching host identifier can access the Virtual Volume as specified in the configuration;**

**b) if a VLUN is configured for 'host set' access, only hosts within the configured host set can access the Virtual Volume as specified in the configuration;**

**c) if a VLUN is configured for 'matched set' access, only hosts accessing the TOE via a port with a matching port identifier and with a matching host identifier can access the Virtual Volume as specified in the configuration**].

**FDP_ACF.1.3** The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**no additional explicit allow rules**].

**FDP_ACF.1.4** The TSF shall explicitly deny access of subjects to objects based on the [**no additional explicit denial rules**].

#### 5.3.3.3 User data availability (FDP_AVL_EXT.1)

**FDP_ AVL_EXT.1.1** The TSF shall implement the following RAID Disk Data Format levels [***0, 1, 5, 6***] that comply with the Common RAID Disk Data Format Specification, version 2.0.

**FDP_ AVL_EXT.1.2** The TSF shall be able to generate an alert when a System Administrator configured warning threshold for user data storage is exceeded.

**FDP_ AVL_EXT.1.3** The TSF shall be able to generate an alert and prevent additional user data storage space allocation when a System Administrator configured limit for user data storage is exceeded.

#### 5.3.3.4 Subset Residual Information Protection (FDP_RIP.1)

**FDP_RIP.1.1** The TSF shall ensure that any previous information content of a resource is made unavailable upon the [***allocation of the resource to***] the following objects [***chunklets, volumes***].

**Application Note:** Volumes consist of chunklets. Chunklets are cleared of any residual information prior to the chunklet being allocated to another data object, which ensures that volume storage is cleared prior to re-use.

### 5.3.4 Identification and authentication (FIA)

#### 5.3.4.1 User attribute definition (manageability path) (FIA_ATD.1)

**FIA_ATD.1.1(1)** The TSF shall maintain the following list of security attributes belonging to individual **manageability path administrative** users: [**user identity, role[super, service, domain user], password, and optionally a public key**].

**Application Note:** If the Virtual Domains feature is disabled, the user will be associated with the "all" domain. Users with roles *super* and *service* transcend domains and have access to all domains that have been established. User's with all other roles are bounded by the permissions defined by those roles and the domains to which the user has been assigned.

#### 5.3.4.2 User attribute definition (data path) (FIA_ATD.1)

**FIA_ATD.1.1(2)** The TSF shall maintain the following list of security attributes belonging to individual **data path** users: [**storage user identity, *[WWN or IP address]]***.

#### 5.3.4.3 Timing of authentication (FIA_UAU.1)

**FIA_UAU.1.1** The TSF shall allow [**host access to virtual volumes in accordance with the Access Control Policy**] on the data path on behalf of the user to be performed before the user is authenticated.

**FIA_UAU.1.2** The TSF shall require each manageability path user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

#### 5.3.4.4 Multiple authentication mechanisms (FIA_UAU.5)

**FIA_UAU.5.1** The TSF shall provide [**public key (if configured), local password, LDAP**] to support **manageability path administrative** user authentication.

**FIA_UAU.5.2** The TSF shall authenticate any user's claimed identity according to the following rule:

- [**Local authentication mechanism – public key authentication when using SSHv2 and the manageability path user has a configured public key, otherwise via password authentication - if the user is defined there, otherwise the LDAP server will be consulted**].

#### 5.3.4.5 Protected Authentication Feedback (FIA_UAU.7)

**FIA_UAU.7.1** The TSF shall provide only [**obscured feedback**] to the user while the authentication is in progress.

#### 5.3.4.6 User identification before any action (FIA_UID.2)

**FIA_UID.2.1** The TSF shall require **each manageability path administrative user and data path user** to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

### 5.3.5 Security management (FMT)

#### 5.3.5.1 Management of security attributes (FMT_MSA.1)

**FMT_MSA.1.1** The TSF shall enforce the [**Block Storage Access Control policy**] to restrict the ability to [***manage***] [**all** the security attributes] to [**System Administrators that have a super or edit *role***].

**Application Note:** The edit role is associated with the "all" domain or the assigned domain when the Virtual Domains feature is enabled.

#### 5.3.5.2 Static attribute initialization (FMT_MSA.3)

**FMT_MSA.3.1** The TSF shall enforce the [**Block Storage Access Control policy**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

**FMT_MSA.3.2** The TSF shall allow the [**System Administrators**] to specify alternative initial values to override the default values when an object ~~or information~~ is created.

**Application Note:** The TOE does not support an explicit notion of default values, rather by implicit default when a new resource (e.g., virtual volume) becomes available no access is possible until it is exported at which time explicit

access rights to a host, set of hosts, port or some combination (e.g., 'host sees', 'host set', 'matched set' as defined in FDP_ACF.1.2) can be granted by System Administrators that have a *super* or *edit* role.

#### 5.3.5.3 Management of TSF Data (for general TSF data) (FMT_MTD.1)

**FMT_MTD.1.1** The TSF shall restrict the ability to [***manage***] the [**TSF data**] to [**Authorized Administrators**].

#### 5.3.5.4 Specification of Management Functions (FMT_SMF.1)

**FMT_SMF.1.1** The TSF shall be capable of performing the following management functions: [
- **Ability to administer the TOE locally and remotely**.]

#### 5.3.5.5 Restrictions on Security Roles (FMT_SMR.2)

**FMT_SMR.2.1** The TSF shall maintain the roles: [**users assigned to user class of browse, edit, super, service, Create, Basic Edit, 3PAR AO, and 3PAR RM**].

**Application Note:** Roles are related to the domain in which the user is defined. Each domain can have a distinct role for that user. When the Virtual Domains feature is disabled, the role is assigned to the "all" domain.

**Application Note:** There are two roles that transcend domains (e.g., live in the "all" domain): super and service.

**FMT_SMR.2.2** The TSF shall be able to associate users with roles.

**FMT_SMR.2.3** The TSF shall ensure that the conditions [
- **Authorized administrator role shall be able to administer the TOE locally;**
- **Authorized administrator role shall be able to administer the TOE remotely;**]

are satisfied.

**Application Note:** Data path users have no security-relevant role other than that defined in FIA_UID.2.

### 5.3.6 Protection of the TSF (FPT)

#### 5.3.6.1 Protection of administrator passwords (FPT_APW_EXT.1)

**FPT_APW_EXT.1.1** The TSF shall store passwords in non-plaintext form using SHA-512 hash; the TSF shall ensure that the stored passwords cannot be read.

**FPT_APW_EXT.1.2** The TSF shall prevent the reading of plaintext passwords.

#### 5.3.6.2 Failure with preservation of secure state (FPT_FLS.1)

**FPT_FLS.1.1** The TSF shall preserve a secure state when the following types of failures occur: [**node, power fail, storage availability, and network (e.g., administrative) interface**].

#### 5.3.6.3 Reliable Time Stamps (FPT_STM.1)

**FPT_STM.1.1** The TSF shall be able to provide reliable time stamps.

#### 5.3.6.4 TSF testing (FPT_TST_EXT.1)

**FPT_TST_EXT.1.1** The TSF shall run a suite of self-tests during initial start-up (on power on) to demonstrate the correct operation of the TSF.

## 5.3.7 Resource utilization (FRU)

### 5.3.7.1 Degraded fault tolerance (FRU_FLT.1)

**FRU_FLT.1.1** The TSF shall ensure the operation of [**reading and writing to a virtual volume**] when the following failures occur:[

- **Failure of a limited number of physical disks in a set of physical disks storing virtual volumes**
- **Failure of a limited number of physical disk sectors in a set of physical disk sectors storing virtual volumes**
- **Failure of a limited number of storage system HBAs in a set of storage system HBAs**
- **Failure of a limited number of TOE instances in a set of TOE instances**
- **Failure of:**
  - **Less than 50% of the nodes in a multi-node StoreServ Storage System cluster**
  - **Network interface**]

**Application Note:** HP 3PAR refers to 'physical disk sectors' as 'chunklets.' A chunklet is the most basic unit of storage for the TOE.

## 5.3.8 TOE access (FTA)

### 5.3.8.1 User-initiated termination (FTA_SSL.4)

**FTA_SSL.4.1** The TSF shall allow user termination of the user's own interactive session.

## 5.3.9 Trusted path/channels (FTP)

### 5.3.9.1 Inter-TSF trusted channel (FTP_ITC.1)

**FTP_ITC.1.1** The TSF shall provide 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**.**

**FTP_ITC.1.2** The TSF shall permit [***the TSF*]** to initiate communication via the trusted channel.

**Application Note**: The communications with the external key management server are supported via a FIPS validated version of OpenSSL which is distinct from the other manageability path communications. See section 6.2.

**FTP_ITC.1.3** The TSF shall initiate communication via the trusted channel for [**authenticating non-local users and external key manager server communications**].

### 5.3.9.2 Trusted Path (FTP_TRP.1)

**FTP_TRP.1.1** The TSF shall use [**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 points and protection of the communicated data from [**disclosure** [***and detection of modification of the communicated data***]].

**FTP_TRP.1.2** The TSF shall permit [***remote users*]** to initiate communication via the trusted path.

**FTP_TRP.1.3** The TSF shall require the use of the trusted path for [***initial user authentication*],** [***and all remote user actions***].

## 5.4 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 2 augmented with ALC_FLR.2 components as specified in Part 3 of the Common Criteria.

| Requirement Class | Requirement Component |
|---|---|
| **ADV: Development** | ADV_ARC.1: Security architecture description |
| | ADV_FSP.2: Security-enforcing functional specification |
| | ADV_TDS.1: Basic design |
| **AGD: Guidance documents** | AGD_OPE.1: Operational user guidance |
| | AGD_PRE.1: Preparative procedures |
| **ALC: Life-cycle support** | ALC_CMC.2: Use of a CM system |
| | ALC_CMS.2: Parts of the TOE CM coverage |
| | ALC_DEL.1: Delivery procedures |
| | ALC_FLR.2: Flaw reporting procedures |
| **ATE: Tests** | ATE_COV.1: Evidence of coverage |
| | ATE_FUN.1: Functional testing |
| | ATE_IND.2: Independent testing - sample |
| **AVA: Vulnerability assessment** | AVA_VAN.2: Vulnerability analysis |

**Table 6 EAL 2 augmented with ALC_FLR.2 Assurance Components**

# 6. TOE Summary Specification

This chapter describes the security functions:

- Security audit
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- Resource utilization
- TOE access
- Trusted path/channels

## 6.1 Security audit

The TOE is designed to be able to generate log records for a wide range of security relevant and other events as they occur. The events that can cause an audit record to be logged include starting and stopping the audit function, any use of an administrator command (including review of audit records, but excluding general 'browsing' which is not considered security relevant when configuration changes are not made and sensitive TSF data is not accessed – see "Browse" in section 6.5) via the CLI interface, as well as all of the events identified in Table 5.

In general, the logged audit records identify the date and time, the nature or type of the triggering event, an indication of whether the event succeeded, failed or had some other outcome, and the identity of the agent (e.g., user or network host) responsible for the event. The logged audit records also include event-specific content that includes at least all of the content required in Table 5.

The TOE includes an internal log implementation that can be used to store and review audit records locally.

Locally stored audit records can be viewed and searched using regular expressions by a user with the *super* or *browse* role via the CLI interface. Users can search the audit log by date/time, event type, severity and general message information using regular expression and pattern matching. Audit log filtering is performed using the "**showeventlog –debug**" option. The *HP 3PAR Command Line Reference* provides information on the filtering options available. The "-debug" option is not generally available (i.e., it is only available to users having the *super* or *service* role) and so its use is described in the *HP 3PAR Common Criteria Admin Reference*.

There are no interfaces/functions that facilitate the clearing or modification of stored records.

Should the available space for audit logs become exhausted, the oldest log file will be overwritten as necessary to accommodate recording new records. The default audit log size is 3 MB and may be changed by the system administrator (the size can range from 512 KB to 4 MB). 11 generations of the audit log are maintained before the oldest records are overwritten to accommodate the newest.

The Security audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1: The TOE can generate audit records for events include starting and stopping the audit function, administrator commands, and all other events identified in **Table 5**. 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 **Table 5**.
- 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.
- FAU_SAR.1: The TOE provides a CLI interface to review its internal audit log.
- FAU_SAR.2: The TOE prohibits users from accessing security relevant events unless they have been granted the *super* or *service* role, in which case the "**showevent –debug**" option can be used to access all events in the internal audit log.

- 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.
- 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. The TOE initially reserves 33 MB for audit log storage.
- FAU_STG.4: The TOE will automatically overwrite the oldest audit log records with new records as necessary if the audit log is full.

## 6.2 Cryptographic support

The TOE provides cryptographic support for communications on the manageability path using unmodified versions of libcrypto (OpenSSL) and libgcrypt(GNUtls). The libraries have been shown to operate in a FIPS approved manner as used by the TOE when subjected to the Cryptographic Algorithm Verification Program (CAVP) as shown in the table below.

| Function | Standard | Certificate |
|---|---|---|
| Encryption/Decryption | | |
| • AES CTR and CBC (128-256 bits) | FIPS PUB 197<br>NIST SP 800-38A | Cert # 3631 (libcrypto) and Cert #3633 (libgcrypt) |
| Cryptographic signature services | | |
| • RSA Digital Signature Algorithm (rDSA) (modulus 1024 and 2048) | FIPS PUB 186-2 | Cert # 1872 (libcrypto) and Cert # 1874 (libgcrypt) |
| Cryptographic hashing | | |
| • SHA-1 and SHA-256 (digest sizes 160, 256) | FIPS Pub 180-3 | Cert #3049 (libcrypto) and Cert # 3051 (libgcrypt) |
| Keyed-hash message authentication | | |
| • HMAC-SHA-1 (digest size 160 bits) | FIPS Pub 198-1<br>FIPS Pub 180-3 | Cert # 2382 (libcrypto) and Cert # 2384 (libgcrypt) |

**Table 7 Cryptographic Functions**

Additionally, to support self-encrypting drives, the TOE uses an additional version of OpenSSL to communicate with the required EKM server. This version of OpenSSL is FIPS capable, and built and used in a vendor affirmed manner using CMVP cert #1747.

Random numbers used to create cryptographic keys for communications are generated internally to libcrypto and libgcrypt. Random number generation in both cases is done in accordance with ANSI X9.31.

The Cryptographic support function is designed to satisfy the following security functional requirements:

- FCS_CKM.1: The TOE uses random number generation to create keys between 128 and 256 bits in length for communications with an EKM server only.
- FCS_CKM.4: The TOE performs immediate (i.e., when no longer needed) and complete (i.e., the entire key or parameter) zeroization of plaintext cryptographic keys and security parameters used for communication with an external EKM server only.
- FCS_COP.1.1(1): The TOE implements AES with CTR and CBC modes and 128, 192, and 256 bit keys sizes.
- FCS_COP.1.1(2): The TOE implements the RSA Digital Signature Algorithm with a key size (modulus) including 2048 and greater.

- FCS_COP.1.1(3): The TOE implements SHA-1, and SHA-512 hashes cryptographic hashes.
- FCS_COP.1.1(4): The TOE implements HMAC-SHA-1 keyed-hash message authentication.

## 6.3 User data protection

From a client host perspective, the data resources are available in the form of Virtual Volumes (VVs) identified by Virtual Logical Units (VLUNs). Internally, the physical disks are installed in either magazines that are installed into cages (StoreServ 10000) or individually in drive enclosures (StoreServ 7000c) of individual nodes and are logically divided into pools of 1GB 'chunklets' that are assembled from across available disks into Logical Disks (LDs). Each VV is then built from all or part of a LD or spread across several LDs. Chunklets can be allocated from different cages, magazines, and physical disks to form RAID 0, RAID 10 (mirroring + striping), RAID 50 (RAID 5 + striping), and RAID Multi-parity (aka RAID 6) configurations to form LDs in order to achieve the required levels of availability and fault tolerance.

From an administrator point of view, in order to create a VV an administrator must first create a Common Provisioning Group (CPG). The CPG identifies an initial space allocation, a growth increment, and a RAID level. Additionally, each CPG includes growth warnings and growth limits. When the size of VVs associated with the CPG reaches the growth warning, an alert is generated so that an administrator can take action to avoid subsequent failure related to CPG exhaustion. When the size of VVs associated with the CPG reaches the growth limit, additional alerts will be generated and write operations that require additional space will fail.

The TOE uses a Block Access Control Policy to control operations between host clients and Virtual Volumes. Once hosts and VVs are defined, an administrator can define associations so that hosts can access VVs. Access to a VV can be limited to a given host, a group of hosts (i.e., a host set), a given port (i.e., a Host Bus Adapter – HBA – through which hosts connect to the storage system), or a specific host-port combination. When hosts or host sets are identified, it doesn't matter which port the access comes from. When just a port is specified, then any host connected to that port can access the applicable VV. Note that multiple hosts could be connected to a single port when, for example, a SAN switch is connected to the port. However, when a host-port combination is specified then the VV can be accessed only via the identified host and via the identified port. Note that VV access applies to an entire VV and can be configured to be read-only or read-write.

Hosts are defined within the TOE and are associated with host identifiers – World Wide Names (WWNs) in the case of Fiber Channel hosts and iSCSI identifiers for iSCSI hosts. To assist administrators in defining hosts, the TOE can report host identifiers that have been encountered but are not associated with a current host definition and also there is a host-based application – the Host Explorer Agent – that reports information to the TOE corresponding a given actual host and the identifiers associated with its Host Bus Adapters (HBAs).

Hosts can be grouped into host sets associated with a given VLUN. Additionally, hosts access the TOE through specific Fiber Channel or iSCSI ports.

Users with the *super* or *edit* role can define access to Virtual Volumes identified by VLUN in the following ways:

- **Host Sees**: The TOE makes the Virtual Volume visible via its VLUN to specifically identified hosts. The port used by the host is irrelevant.
- **Host Set**: The TOE makes the Virtual Volume visible via its VLUN to all members of an identified host set. Any hosts added to the host set would automatically obtain access to the associated Virtual Volume. Similarly, a removed host loses access. The port used by the host is irrelevant.
- **Matched Set**: The TOE makes the Virtual Volume visible via its VLUN to a particular host on a particular port.

In each case, when a Virtual Volume is visible to a host, it will be accessible though in some cases the access is further restricted to read-only access (e.g., when a read-only snapshot is exported). Also, Virtual Volumes that are not 'visible' to hosts cannot be accessed in any way. Hence, other than attempting to violate a read-only restriction, a given host cannot attempt to access an unauthorized Virtual Volume – there are simply no mechanics for that. However, a given host can query the available Virtual Volumes and the result will be consistent with these access rules.

As mentioned previously, physical disks are divided into chunklets which form the basis of LDs, CPGs, and ultimately VVs. Internally, if a chunklet is returned to the available chunklet pool it is zeroed by the TOE. When a chunklet is allocated for a new use – either when a fully provisioned VV is created or a thinly-provisioned VV requires more space – that newly allocated space is also zeroed prior to any read or write operation. The TOE also makes use of data caches and implements a strict write-before-read policy for access to the cache and the TOE is designed to ensure that cache requests correspond to their represented media before allowing read access to the data therein. When a disk is marked as failed the TOE attempts to write zeroes to all the chunklets. Obviously, that might not be 100% effective. HP offers customers the option of disposing of failed media, as opposed to returning it to mitigate data disclosure concerns.

When CPGs are created by a user with the super or edit role, that user can identify whether the CPG should utilize a RAID 0, 1, 5, or 6 fault tolerance configuration as well as whether fault tolerance (i.e., parity) should be on the granularity of a disk drive, drive magazine, drive cage, or controller node. Additionally, the user must define warning and limit levels for the CPG. As the CPG resources are allocated to one or more VVs, if the configured warning level is reached an alert is generated in the form of a log indicating that the level has been reached and perhaps some remedial action should be taken. Furthermore, if CPG resources are allocated to its limit level an alert will be generated and no more resources can be allocated and applicable write operations will fail.

In addition, when a Thinly Provisioned VV (TPVV) is created by a user with the super or edit role, warning and limit levels must also be configured for the TPVV. As with CPGs, when the resources allocated to the TPVV reach the warning level, an alert is issued and when resources allocated to the TPVV reach the limit level an alert is issued and write operations will fail since no further resources will be allocated to the TPVV.

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_ACC.2: The TOE controls all operations between attached host clients and Virtual Volumes.
- 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 above.
- 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 above.
- FDP_RIP.1: The TOE is designed to ensure that residual information will be cleared prior to any potential access when underlying resources are reallocated between Virtual Volumes.

## 6.4 Identification and authentication

The TOE includes an internal data base where manageability path administrative users (administrative users) can be defined with a user name, domain, class, and password. Additionally, administrative users can provide a public-key-based authentication credential to the TOE, which will be stored and used to support public-key based authentication. The TOE can also be configured to utilize the services of an external LDAP server (i.e., Active Directory) to authenticate administrative users and determine their assigned class.

All interactive user interfaces (SSHv2 client) require administrative users to log in with a user name and valid password (or optionally public-key-based authentication credentials when using SSHv2) prior to successfully being connected to the TOE and enabling access to security management functions. If the administrative user is defined in the internal user database, that information will be used. If the administrative user is not defined internally, the configured LDAP server will be consulted. In each case, the administrative user authentication will either succeed or not. Administrative users not defined internally will not be able to successfully log in. Note that passwords are not echoed or otherwise displayed when logging into any of the available interactive user interfaces. In the case of public-key authentication, applicable credentials are not exposed to users.

Administrative user passwords consist of any combination of printable ASCII characters, Passwords may be between 6 and 32 characters in length, with the minimum length established for the entire system by a system administrator having a *super* user role (user guidance indicates that the recommended minimum password length be no less than 15 characters). Passwords can only be created by system administrators with the *super* user role or the user_create right.

In the case of locally defined administrative users, they have an assigned user role. In the case of LDAP-defined administrative users, the LDAP server is consulted to query the administrative user's groups. The TOE maintains a mapping between LDAP groups and administrative user roles and domains. Once the administrative user's groups are queried, the TOE mapping is consulted to determine the user's domains and roles. If the user doesn't belong to a mapped group, the login attempt will fail.

Once an administrative user is successfully logged in, their user domains and roles will be used to limit the set of functions the user can successfully exercise. If the Virtual Domains feature license is in use, a user can be assigned to up to 32 domains (of the 1024 that can be defined in the TOE) by virtue of associated groups. CPGs and hosts are each assigned to a specific domain. Each domain assignment includes its own user role assignment; otherwise all users are assigned to a single domain (the 'all' domain effectively means they are unassigned and management is limited to users that are not restricted to a specific domain). VVs, LDs, and VLUNs are also implicitly associated with the domain of their associated CPG. When dealing with CPGs (and derived resources – VVs, LDs, and VLUNs) and hosts assigned to a domain, only administrative users assigned to that specific domain or the 'all' domain or unrestricted administrative users can manage those hosts and CPG-derived data resources (such as creating or exporting VVs). Furthermore, VVs in a given domain can be exported only to hosts in the same domain regardless of user role or domain. If the Virtual Domains feature is enabled, a user could have the *browse* role for one domain and the *edit* role for another. However, the *service* and *super* roles transcend domains (these users cannot be assigned to a domain; they are always associated with the "all" domain).

Client host users are identified using iSCSI identifiers and Fiber Channel World Wide Names (WWNs). The iSCSI and Fibre Channel WWNs are well defined in their respective standards. In general the client host identifiers are not authenticated by the TOE as it is assumed that servers' identities properly reflect the adapters and hence the servers to which they are associated such that authentication is not necessary. However, the TOE administrator needs to ensure the assumed authenticity of host identifiers in their operational environment. This likely would require physical protection of the applicable storage area networks as well as some suitable knowledge about (they are appropriately evaluated) or control over the respective hosts. Note that while not specifically claimed or otherwise addressed, it should be understood that the TOE can be configured to require iSCSI hosts to use Challenge-Handshake Authentication protocol (CHAP) authentication, but that is not claimed herein since it is not a default behavior and there is no subsequent use of cryptographic functions, for example, that would serve to protect the integrity of traffic to and from authenticated hosts limiting any assurance that may have been gained.

The Identification and authentication function is designed to satisfy the following security functional requirements:

- FIA_ATD.1: The TOE defines individual manageability path users in terms of user identity (i.e., name), domain, class and password.
- 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.
- FIA_UAU.5: Local (internally defined) administrative users are authenticated using a password or public-key credentials. The TOE can be configured to automatically utilize an external LDAP server for authentication of administrative users not internally defined. iSCSI and FC hosts (e.g., data path users) accessing virtual volumes for performing read/write operations are not authenticated.
- FIA_UAU.7: The TOE is designed to not echo passwords when users are logging in.
- FIA_UID.2: The TOE doesn't offer any services to users, including client hosts, until they are successfully identified by 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.

## 6.5 Security management

The TOE supports four standard user roles that can be assigned to individual manageability path users. Users assigned the *super* role can perform any functions (e.g., all security functions of the TOE including managing audit events, user accounts, and access control). While other users have more limited access they each can perform security-relevant security management functions nonetheless. If the Virtual Domains feature is active, users are assigned to domains and each domain assignment is associated with a role; otherwise all users are assigned to the "all" domain. However, the *super* and *service* roles transcend domains, so if a user is assigned one of these user roles their domain assignments are irrelevant in regard to functions associated with those roles. Similarly, the 'all' domain is effectively a superset of all domains, providing access based on the user role (i.e., *browse* or *edit*) to all system resources.

The standard roles can generally perform the following operations (the ability to perform domain management is only possible if the Virtual Domains feature is enabled):

- **Super**: Allows access to all system functions. This role can review and otherwise manage the audit events in the local audit log, manage (define user accounts with specific domains and user classes) user accounts, manage domain definitions, define hosts (by associating specific WWNs or iSCSI identifiers with them), manage LDAP group association with user classes and domains, and manage (i.e., define and specify the exported VLUN attributes) access to Virtual Volumes.

  *This role is not limited by domain, so a user assigned this role can perform the associated functions on all TOE resources, though there are restrictions as described below*

- **Service**: Allows access to limited system functions to service the storage server; allows limited access to user information and user group resources. Note that this role doesn't provide the ability to perform any of the identified security management functions.

  *This role is not limited by domain, so a user in this class can perform the associated functions on all TOE resources.*

- **Edit**: Allows access to most system functions, such as defining hosts, creating and editing Virtual Volumes (including selecting availability options and assigning domains), and managing access to Virtual Volumes. The edit role allows access to all identified security management functions, but does not offer access to some non-security related service functions.

  *This role is limited by domain, so a user assigned this role can perform the associated functions only on TOE resources in the same domain. In other words, a user with the edit role can only create VVs using CPGs in the same domain and can export VVs to hosts in the same domain. Users in the 'all' domain are not limited in terms of resources they can manage, except as explained below.*

- **Browse**: Allows read-only accessibility, including review of the audit events and alerts.

*This role is limited by domain, so a user assigned this role can perform the associated functions only on TOE resources in the same domain (where applicable). In other words, a user assigned the edit role can only browse, for example, CPGs, VVS, hosts, and users in the same domain. Users in the 'all' domain are not limited in this regard.*

In addition to the standard user roles are four extended roles (listed below). There is no functional difference between standard and extended roles except they involve different sets of allowable functions and as such should generally be considered subsets of the Super role, above, and also are assigned to the 'all' domain and cannot be restricted in that regard. The extended roles define a set of rights optimized for CLI users with specialized or restricted tasks. In general, the minimum set of rights should be assigned to each user.

- **Create:** Rights are limited to creating objects. For example, virtual volumes, CPGs, hosts, and schedules.
- **Basic Edit:** Rights are similar to the Edit role. For example, creating and editing virtual volumes and other objects. The rights to remove objects are more restricted for the Basic Edit role than the Edit role. On the other hand, this role can create domains, configure authentication parameters, and create users.
- **3PAR AO:** Rights are limited to internal use by HP for Adaptive Optimization operations.
- **3PAR RM:** Rights are limited to internal use by HP for Recovery Manager operations.

When configuring and exporting storage resources, administrative users cannot normally export resources from one domain to hosts of another domain, regardless of their user class. The exception is that a Super user can create domain sets and assign hosts and individual domains to those domain sets such that ultimately volumes exported to hosts within a domain set can be accessible by other hosts in the domain set. This can facilitate cross-domain access to the volume exported in this manner.

The security functions of the TOE are managed by authorized users using CLI functions available via SSHv2 sessions.

The Security management function is designed to satisfy the following security functional requirements:

- FMT_MSA.1: The TOE restricts the ability to manage the access settings for Virtual Volumes to users assigned the super role or that are in the applicable domain (the "all" or the assigned domain when the Virtual Domains feature is enabled) with the edit role (aka System Administrators in the domain of the protected object). Note that VVs (in a given domain) 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.
- FMT_MSA.3: The TOE restricts the ability to manage the access settings for Virtual Volumes to users assigned the super role or that are in the applicable domain (the "all" or the assigned domain when the Virtual Domains feature is enabled) with the edit role (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.
- FMT_MTD.1: The TOE restricts the ability to manage security relevant TOE data (i.e., TSF data) to users assigned any user role (aka System Administrators).
- 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.
- FMT_SMR.2: The TOE implements browse, edit, service, and super user roles. The user roles are collectively referred to as System Administrator in this Security Target. There is no distinction made in the functionality available to local or remote users; any defined user with an assigned role can access the TOE remotely or locally and perform the same functions.

## 6.6 Protection of the TSF

The TOE is a series of hardware appliance Controller Nodes, each of which includes a hardware-based real-time clock. The TOE's embedded OS manages the clock and exposes administrator clock-related functions. The TOE is configured to use a network time server in order to automatically synchronize the time of its internal clock.

Each TOE appliance is a stand-alone physical device that does not host or execute untrusted applications. The TOE appliance is designed with separate physical connections so that administrative and supporting service network communications are physically isolated from client host communications. Each of the physical interfaces is associated with a well-defined set of standards-based services that have been carefully designed to comply with the applicable standards and to implement and enforce the security and other access policies of the TOE without offering any functions that might serve to bypass or allow any of those policies to be subverted in any way.

The redundant architecture of the TOE results in no changes to security policies due to degradation in the state of the TOE. For example, if a node or disk becomes inoperable, the redundant capabilities of the system at the component level result in adherence to the same security policies as if no degradation existed.

Once the TOE is properly installed and configured, it runs through a common initialization process after starting from a cold state or restarting from an operating state. Host ports are in a suspended state until all volumes are started. The SSH daemon starts just prior to the first volume (admin volume)starting. Until these processes start, it is not possible to access hosts or storage devices or alter system configuration information in any way. If the TOE encounters a problem during initialization, it logs an alert and continues its processing (if it can). Alerts can be viewed using the "showalert" CLI command and additional information on the messages displayed when viewing an alert, such as troubleshooting information, can be found by logging into the HP Guided Troubleshooting website.

The TOE clients are applications designed to provide administrative interfaces. They are carefully designed to provide functions to administrators correctly, but necessarily must be used in conjunction with hosts that will protect them from potential tampering. While the administrative interface is function-rich, the TOE is designed specifically to provide access only to SHA-512 hashed (and not plain text) local passwords and also, while cryptographic keys can be entered, the TOE does not disclose any keys stored in the TOE.

The TOE is designed to preserve a secure state should it experience individual or subsystem component failures. Individual component failures are typically handled at the component level and the redundant nature of the architecture typically protects data and system integrity (in the case of storage and network interface failures). Subsystem component failures (node, power failure) are more complex because they can often extend across different nodes and result in the suspension of I/O until the failure is mitigated. In extreme cases, the TOE makes use of a process referred to as the "lock step recovery process," which is a series of ordered steps to recover from a failure and prevent data loss due to transactions that are in progress but not yet completed. This process is initiated for the following failures:

- Node failure: Because there is a data integrity issue when transacting with a failed node, all I/O is suspended. I/O is resumed later after the failure has been addressed.
- Power failure: Local node transactions are written to local disk. A local node first writes its own transactions to disk and then writes the dirty pages of other nodes' transactions that it has (it has these transactions because the node is serving as the backup node to another node).

Secure state preservation for storage availability occurs based on how storage is allocated across TOE hardware:

- Cage availability: The default TOE availability type is cage availability, which means each node in a node pair is served by a different cage. A node pair writing to different cages provides data redundancy should one of the cages become inoperable.
- Magazine availability: Each cage typically contains 10 magazines, each containing four drives. Magazine availability means that none of the disks supporting a data set belong to the same magazine.
- Chunklet availability: The TOE always ensures that chunklets do not originate from the same physical drive in a RAID set to prevent the data in a RAID set from being inaccessible should a single drive become inoperable.

A TOE will, in the case of a failed drive, cryptographically erase the drive prior to its removal from the system. Administrators can also dismiss unused drives and manually issue the command to cryptographically erase them.

For the network manageability interface, the interface exists on multiple nodes in a StoreServ cluster but is only active on one. If the TOE determines that the interface is no longer functional, it switches the IP address to another node, making it the active network manageability interface.

The TOE provides the capability for system administrators to query its current version of firmware/software using the CLI **showversion** command.

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_APW_EXT.1: The TOE protects administrator passwords by encrypting them and not providing any mechanism that would allow them to be read in plain text.
- FPT_FLS.1: The TSF shall preserve a secure state when the following types of failures occur: node, power fail, storage availability, network (administrative) interface.
- FPT_STM.1: The TOE includes its own hardware clock and is capable of being configured to use a network time server for synchronization.
- FPT_TST_EXT.1: The TOE startup process does not offer host or storage device accessibility until the TOE has validated that it has started correctly and is operating properly.

## 6.7 Resource utilization

Software that operates on each StoreServ System cluster node is responsible for ensuring that the member nodes can communicate with each other and have the same view of all other nodes in the cluster (e.g., same view of cluster membership).

An important aspect of the StoreServ cluster platform is its ability to handle different types of failures without losing data. Component failures (e.g., disk failure, link failure) are relatively self-contained and are primarily handled by a single subsystem component. More complex failures are those that require interdependent high-availability failure handling across subsystem components and cluster members (e.g., node and power failures). The full-mesh architecture of the StoreServ platform protects the data integrity of the system in the event of a subsystem component failure.

As indicated in FRU_FLT.1, the TSF ensures there is no degradation in security function when reading and writing a virtual volume if the following conditions occur:

- Failure of a limited number of physical disks in a set of physical disks storing virtual volumes.
- Failure of a limited number of physical disk sectors in a set of physical disk sectors storing virtual volumes.
- Failure of a limited number of storage system HBAs in a set of storage system HBAs.
- Failure of a limited number of TOE instances in a set of TOE instances.
- Failure of less than 50% of the nodes in a multi-node StoreServ Storage System cluster.
- Failure of the network (e.g., administrative) interface.

Failure due to the lack of availability of disk storage (physical disks and physical disk sectors) is mitigated as described in the previous section (cage, magazine and chunklet availability).

The previous section also discusses node failure handling as well as the network interface.

The Resource utilization function is designed to satisfy the following security functional requirement:

- FRU_FLT.1: The TOE operates in a fault tolerant manner, with no impact to its security policies, when it experiences a degraded mode of operation.

## 6.8 TOE access

Administrative interfaces are unavailable until the HP 3PAR StoreServ Storage system has transitioned from a cold state (powered off) to a completely operational state. Until it has reached an operational state such that it can accept connection to an administrative interface, it is not possible to tamper with it in any way.

TOE drive data is inaccessible until the StoreServ has reached an operational state. Drives cannot be accessed until each drive is unlocked with a key the StoreServ obtains from a FIPS 140-2 compliant EKM server.

In all cases, an administrator is required to provide an appropriate username and password or credentials (when using public-key based authentication with SSH) that are verified before a connection is established. Once logged on, an administrator's assigned privilege level (e.g., "role") limits access to the available management functions.

Administrators can log out of their individual sessions, thereby terminating the session. If an administrator does not log out of a sessions, CLI sessions are terminated after a period of inactivity, requiring the user to login to establish a new session. The period of inactivity is configurable by an administrator with the *super* or *service* role using the CLI **setsys** command (the default period of inactivity is one hour).

Hosts (i.e., data path users) must identify themselves before they can access TOE data.

From a purely physical protection perspective, it is assumed that due to the function that the StoreServ provides (e.g., critical data storage) and its cost, customers provide the necessary physical environment to ensure that it cannot be physically damaged. In addition to simply providing this protection to the appliance itself, it should be extended to all components that interact with the appliance.

The TOE access function is designed to satisfy the following security functional requirements:

- FTA_SSL.4: The TOE allows an administrative user to terminate its own interactive session.

## 6.9 Trusted path/channels

In the cases of SSHv2, the TOE provides a secure command line interface (CLI) for interactive administrator sessions. An administrator with an appropriate SSHv2 client can establish secure remote connections with the TOE. However, to successfully establish such an interactive session, the administrator must be able to provide acceptable user credentials (e.g., user id and password), after which they will be able to issue commands within their assigned authorizations.

Additionally, the TOE can be configured to protect communication with a configured LDAP server using TLSv1.

The TOE communicates with the EKM server using the KMIP protocol over TLS connections through a FIPS validated OpenSSL library that exists on the StoreServ.

Communication with NTP and client hosts is not subject to cryptographic protection. Client hosts are attached via dedicated Storage Area Networks that are generally in close proximity and hence subject to the same physical protection assumption as the TOE. NTP communication does not natively support encryption options so it is expected that either that is not a concern in a given operational environment or alternately the servers will be placed in close proximity to the TOE like client hosts.

The StoreServ architecture results in all cluster node communication occurring through the backplane. For this reason, there are no external interfaces used for data transported between clustered StoreServ nodes.

The Trusted path/channels function is designed to satisfy the following security functional requirements:

- FTP_ITC.1: The TSF uses [*SSH, TLS*] to provide a trusted communication path between itself and authorized IT entities supporting the following capabilities: [*authentication server, external key management server]* that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of

modification of the channel data. The TSF initiates all communication with the authorized IT entities via the trusted channel. None of the authorized entities initiate communication with the TSF.

- FTP_TRP.1: The TOE provides SSH based on its embedded OpenSSL/OpenSSH libraries, to support secure remote administration. The administrator can initiate the remote session, the remote session is secured (disclosure and modification) using cryptographic operations, and all remote security management functions require the use of one of these secure channels.

# 7. Protection Profile Claims

This ST does not conform to any Protection Profile.

# 8. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives
- Security Functional Requirements
- Security Assurance Requirements
- Requirement Dependencies
- TOE Summary Specification

## 8.1 Security Objectives Rationale

This section shows that all secure usage assumptions, organizational security policies, and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption, organizational security policy, or threat.

### 8.1.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of organizational policies and usage assumptions by the security objectives.

| | T.ADMIN_ERROR | T.DATA_AVAILABILITY | T.TSF_FAILURE | T.UNAUTHORIZED_ACCESS_TSF_DATA | T.UNAUTHORIZED_ACCESS_CODE | T.UNAUTHORIZED_ACCESS_USER_DATA | T.UNDETECTED_ACTIONS | T.USER_DATA_REUSE | A.PHYSICAL_MANAGEABILITY | A.PHYSICAL_CLIENT_HOSTS | A.TRUSTED_ADMIN | A.HOST_IDENTITY |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **O.AVAILABILITY** | | X | | | | | | | | | | |
| **O.ACCESS_CONTROL_DATA** | | | | | | X | | | | | | |
| **O.ACCESS_CONTROL_MANAGEABILITY** | | | | X | X | | | | | | | |
| **O.FAIL_SECURE** | | | X | | | | | | | | | |
| **O.PROTECTED_COMMUNICATIONS** | | | | X | X | X | | | | | | |
| **O.RESIDUAL_INFORMATION_CLEARING** | | | | | | | | X | | | | |
| **O.SYSTEM_MONITORING** | X | | | X | X | X | X | | | | | |
| **O.TOE_ADMINISTRATION** | | | | X | X | | | | | | | |
| **O.TSF_SELF_TEST** | | | X | | | | | | | | | |
| **OE.PHYSICAL_CLIENT_HOSTS** | | | | | | X | | | | X | | |
| **OE.PHYSICAL_MANAGEABILITY** | | | | X | X | | | | X | | | X |
| **OE.TRUSTED_ADMIN** | | | | | | | | | | | X | |

**Table 8 Environment to Objective Correspondence**

#### 8.1.1.1 T.ADMIN_ERROR

*An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms that may go undetected.*

This Threat is satisfied by ensuring that:

- O.SYSTEM_MONITORING: To reduce the potential that an administrative error might be unnoticed or untraceable, the TOE is expected to log security relevant events.

#### 8.1.1.2 T.DATA_AVAILABILITY

*User data may become unavailable due to isolated storage resource failures or due to resource exhaustion.*

This Threat is satisfied by ensuring that:

- O.AVAILABILITY: To reduce the threat of lack of data access due to resource failure or exhaustion, the TOE is expected to ensure that data can be stored in a manner alleviating failure situations.

#### 8.1.1.3 T.TSF_FAILURE

*Security mechanisms of the TOE may fail, leading to a compromise of the TSF.*

This Threat is satisfied by ensuring that:

- O.FAIL_SECURE: The TOE shall fail in a secure manner following failure of the power-on self-tests.
- O.TSF_SELF_TEST: The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.

#### 8.1.1.4 T.UNAUTHORIZED_ACCESS_TSF_DATA

*A user may gain unauthorized access to the TSF data.*

This Threat is satisfied by ensuring that:

- O.ACESS_CONTROL_MANAGEABILITY: To reduce the potential of unauthorized users gaining access to the TOE, the TOE will ensure that only authorized users have access to its data, resources and executable code.
- O.PROTECTED_COMMUNICATIONS: To reduce the potential that an attacker might gain unauthorized access to the TOE or its data via data transmitted across a network, the TOE is expected to protect its administrator communication channels from disclosure, modification, and also to ensure the identity of the TSF.
- O.SYSTEM_MONITORING: To reduce the potential of unauthorized access attempts that might go unnoticed, the TOE is expected to log security relevant events.
- O.TOE_ADMINISTRATION: To reduce the potential of unauthorized access to TOE security functions and data, the TOE is expected to be designed to ensure that only presumably authorized administrators can log in and access security management functions. Note that the TOE is expected to restrict access to security functions and TSF data so that only authorized administrators can access it and in some cases TSF data is not accessible at all.
- OE.PHYSICAL_MANAGEABILITY: Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment. This also extends to supporting servers (e.g., LDAP, NTP) that are expected to be in close proximity to the TOE.

#### 8.1.1.5 T.UNAUTHORIZED_ACCESS_CODE

*A user may gain unauthorized access to the TSF executable code.*

This Threat is satisfied by ensuring that:

- O.ACESS_CONTROL_MANAGEABILITY: To reduce the potential of unauthorized users gaining access to the TOE executable code, the TOE will ensure that only authorized users have access to the TOE.

- O.PROTECTED_COMMUNICATIONS: To reduce the potential that an attacker might gain unauthorized access to the TOE or its data via data transmitted across a network, the TOE is expected to protect its administrator communication channels from disclosure, modification, and also to ensure the identity of the TSF.
- O.SYSTEM_MONITORING: To reduce the potential of unauthorized access attempts that might go unnoticed, the TOE is expected to log security relevant events.
- O.TOE_ADMINISTRATION: To reduce the potential of unauthorized access to TOE security functions and data, the TOE is expected to be designed to ensure that only presumably authorized administrators can log in and access security management functions. Note that the TOE is expected to restrict access to security functions and TSF data so that only authorized administrators can access it and in some cases TSF data is not accessible at all.
- OE.PHYSICAL_MANAGEABILITY: Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment. This also extends to supporting servers (e.g., LDAP, NTP) that are expected to be in close proximity to the TOE.

#### 8.1.1.6 T.UNAUTHORIZED_ACCESS_USER_DATA

*A user may gain unauthorized access to the user data*.

This Threat is satisfied by ensuring that:

- O.ACESS_CONTROL_DATA: To reduce the potential of unauthorized users gaining access to the TOE user data, the TOE will ensure that only authorized users have access to the TOE.
- O.PROTECTED_COMMUNICATIONS: To reduce the potential that an attacker might gain unauthorized access to the TOE or its data via data transmitted across a network, the TOE is expected to protect its administrator communication channels from disclosure, modification, and also to ensure the identity of the TSF.
- O.SYSTEM_MONITORING: To reduce the potential of unauthorized access attempts that might go unnoticed, the TOE is expected to log security relevant events.
- OE.PHYSICAL_CLIENT_HOSTS: Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment. This also extends to client hosts that are expected to be in close proximity to the TOE.

#### 8.1.1.7 T.UNDETECTED_ACTIONS

*Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.*

This Threat is satisfied by ensuring that:

- O.SYSTEM_MONITORING: To reduce the potential of security relevant actions occurring without notice, the TOE is expected to log security relevant events and export those logs to an external log server.

#### 8.1.1.8 T.USER_DATA_REUSE

*User data may be inadvertently sent to a destination not intended by the original sender.*

This Threat is satisfied by ensuring that:

- O.RESIDUAL_INFORMATION_CLEARING: To reduce the potential of data being erroneously sent to an unintended recipient, the TOE is expected to ensure that residual data is appropriately managed.

#### 8.1.1.9 A.PHYSICAL_MANAGEABILITY

*Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment. This also extends to supporting servers (e.g., LDAP, NTP) that are expected to be in close proximity to the TOE. An external NTP server is assumed to provide reliable timestamps for use by the TOE.*

This Assumption is satisfied by ensuring that:

- OE.PHYSICAL_MANAGEABILITY: Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment. This also extends to supporting servers (e.g., LDAP, NTP) that are expected to be in close proximity to the TOE. An external NTP server is assumed to provide reliable timestamps for use by the TOE.

#### 8.1.1.10 A.PHYSICAL_CLIENT_HOSTS

*Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment. This also extends to client hosts that are expected to be in close proximity to the TOE.*

This Assumption is satisfied by ensuring that:

- OE.PHYSICAL_CLIENT_HOSTS: Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment. This also extends to client hosts that are expected to be in close proximity to the TOE.

#### 8.1.1.11 A.TRUSTED_ADMIN

*TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.*

This Assumption is satisfied by ensuring that:

- OE.TRUSTED_ADMIN: TOE Administrators will be carefully selected to ensure they are trusted and trained to follow and apply all administrator guidance in a trusted manner.

#### 8.1.1.12 A.HOST_IDENTITY

*It is assumed that iSCSI and Fiber Channel host identities properly reflect the adapters and hence the hosts to which they are associated such that authentication is not necessary. Implicit in this assumption is the SAN(s) connecting iSCSI and Fiber Channel must be controlled to mitigate potentially malicious attacks on the SAN(s).*

This Assumption is satisfied by ensuring that:

- OE.PHYSICAL: iSCSI and Fiber Channel hosts are in close proximity to the TOE and therefore controlled to mitigate potentially malicious attacks on the SAN(s).

## 8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note that **Table 9** indicates the requirements that effectively satisfy the individual objectives.

### 8.2.1 Security Functional Requirements Rationale

All Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

| | O.AVAILABILITY | O.ACCESS_CONTROL_DATA | O.ACCESS_CONTROL_MANAGEABILITY | O.FAIL_SECURE | O.PROTECTED_COMMUNICATIONS | O.RESIDUAL_INFORMATION_CLEARING | O.SYSTEM_MONITORING | O.TOE_ADMINISTRATION | O.TSF_SEFL_TEST |
|---|---|---|---|---|---|---|---|---|---|
| **FAU_GEN.1** | | | | | | | X | | |
| **FAU_GEN.2** | | | | | | | X | | |
| **FAU_SAR.1** | | | | | | | X | | |
| **FAU_SAR.2** | | | | | | | X | | |
| **FAU_SAR.3** | | | | | | | X | | |
| **FAU_STG.1** | | | | | | | X | | |
| **FAU_STG.4** | | | | | | | X | | |
| **FCS_CKM.1** | | | | | X | | | | |
| **FCS_CKM.4** | | | | | X | | | | |
| **FCS_COP.1(1)** | | | | | X | | | | |
| **FCS_COP.1(2)** | | | | | X | | | | |
| **FCS_COP.1(3)** | | | | | X | | | | |
| **FCS_COP.1(4)** | | | | | X | | | | |
| **FDP_ACC.2** | | X | | | | | | | |
| **FDP_ACF.1** | | X | | | | | | | |
| **FDP_AVL_EXT.1** | X | X | | | | | | | |
| **FDP_RIP.1** | | X | | | | X | | | |
| **FIA_ATD.1.1 (1)** | | | X | | | | | X | |
| **FIA_ATD.1.1 (2)** | | X | | | | | | X | |
| **FIA_UAU.1.1** | | X | | | | | | X | |
| **FIA_UAU.1.2** | | | X | | | | | X | |
| **FIA_UAU.5.1** | | | X | | | | | X | |
| **FIA_UAU.5.2** | | | X | | | | | X | |
| **FIA_UAU.7** | | | | | | | | X | |
| **FIA_UID.2.1** | | X | X | | | | | X | |

| | O.AVAILABILITY | O.ACCESS_CONTROL_DATA | O.ACCESS_CONTROL_MANAGEABILITY | O.FAIL_SECURE | O.PROTECTED_COMMUNICATIONS | O.RESIDUAL_INFORMATION_CLEARING | O.SYSTEM_MONITORING | O.TOE_ADMINISTRATION | O.TSF_SEFL_TEST |
|---|---|---|---|---|---|---|---|---|---|
| **FMT_MSA.1** | | | | | | | | X | |
| **FMT_MSA.3** | | | | | | | | X | |
| **FMT_MTD.1** | | | | | | | | X | |
| **FMT_SMF.1** | | | | | | | | X | |
| **FMT_SMR.2** | | | | | | | | X | |
| **FPT_APW_EXT.1** | | | | | | | | X | |
| **FPT_FLS.1** | | | | X | | | | | |
| **FPT_STM.1** | | | | | | | X | | |
| **FPT_TST_EXT.1** | | | | X | | | | | X |
| **FRU_FLT.1** | | | | X | | | | | |
| **FTP_ITC.1** | | | | | X | | | | |
| **FTP_TRP.1** | | | | | X | | | | |

**Table 9 Objective to Requirement Correspondence**

#### 8.2.1.1 O.AVAILABILITY

*The TOE will ensure that data can be stored in a manner that is protected from underlying resource failure and exhaustion.*

This TOE Security Objective is satisfied by ensuring that:

- FDP_AVL_EXT.1: The TOE is required to implement selected RAID levels to defend against resource failures and also to implement warning and limit levels so that administrators can define maximum resource allocation and also when to receive alerts about impending resource exhaustion.

#### 8.2.1.2 O.ACCESS_CONTROL_DATA

*The TOE will ensure that only authorized data path users have access to the user data that it stores.*

This TOE Security Objective is satisfied by ensuring that:

- FIA_ATD.1.1(2): The TOE is required to maintain the following list of security attributes belonging to individual data path users: [storage user identity, [WWN or IP address]].
- FIA_UAU.1.1: The TOE is required to allow host access to virtual volumes in accordance with the Access Control Policy on the data path on behalf of the user to be performed before the user is authenticated.
- FIA_UID.2.1: The TOE is required to successfully identify each data path user before allowing any other TSF-mediated actions on behalf of that user.
- FDP_ACC.2: The TOE is required to implement an access policy controlling all operations between attached hosts and virtual volumes managed by the TOE.
- FDP_ACF.1: The TOE is required to implement an effective set of rules to enforce the access control policy between hosts and virtual volumes.

- FDP_RIP.1: The TOE is required to clear all information when allocating virtual volumes for subsequent activities.
- FDP_AVL_EXT.1: The TOE is required to implement selected RAID levels to defend against resource failures and also to implement warning and limit levels so that administrators can define maximum resource allocation and also when to receive alerts about impending resource exhaustion.

#### 8.2.1.3 O.ACCESS_CONTROL_MANAGEABILITY

*The TOE will ensure that only authorized users can access configuration, data and resources.*

This TOE Security Objective is satisfied by ensuring that:

- FIA_ATD.1.1(1): The TOE is required to maintain the following list of security attributes belonging to individual manageability path administrative users: [user identity, role[super, service, domain user], password, and optionally a public key].
- FIA_UAU.1.2: The TOE is required to successfully authenticate each manageability path user before allowing any other TSF-mediated actions on behalf of that user.
- FIA_UAU.5.1: The TOE is required to provide [public key (if configured), local password, LDAP] to support manageability path administrative user authentication.
- FIA_UAU.5.2: The TOE is required to authenticate a user's claimed identity according to the following rule: Local authentication mechanism – public key authentication when using SSHv2 and the manageability path user has a configured public key; otherwise via password authentication – if the user is defined there, otherwise the LDAP server will be consulted.
- FIA_UID.2.1: The TOE is require to successfully identify each manageability path administrative user before allowing any other TSF-mediated actions on behalf of that user.

#### 8.2.1.4 O.FAIL_SECURE

*The TOE will ensure that it fails in a secure manner following failure of the power-on self-tests.*

This TOE Security Objective is satisfied by ensuring that:

- FPT_FLS.1: The TOE shall preserve a secure state when the following types of failures occur: node, power fail, storage availability, network (e.g., administrative) interface.
- FPT_TST_EXT.1: The TOE is required to run a suite of self-tests during initial start-up (on power on) to demonstrate that it operates correctly.
- FRU_FLT.1: The TOE is required to continue operating in a secure state despite the occurrence of the following: failure of a limited number of physical disks in a set of physical disks storing virtual volumes, failure of a limited number of physical disk sectors in a set of physical disk sectors storing virtual volumes, failure of a limited number of storage system HBAs in a set of storage system HBAs, failure of a limited number of TOE instances in a set of TOE instances, failure of less than 50% of the nodes in a multi-node StoreServ Storage system, and failure of the network (administrative) interface..

#### 8.2.1.5 O.PROTECTED_COMMUNICATIONS

*The TOE will provide protected communication channels for administrators.*

This TOE Security Objective is satisfied by ensuring that:

- FCS_CKM.1: The TOE is required to be able to generate encryption keys to support other cryptographic operations related to ephemeral keys for communication with an external EKM.
- FCS_CKM.4: The TOE is required to zeroize keys when no longer need to prevent subsequent disclosure for those keys used for communication with an external EKM.
- FCS_COP.1.1(1): The TOE is required to implement FIPS-conformant AES in support of cryptographic protocols.
- FCS_COP.1.1(2): The TOE is required to implement FIPS-conformant RSA cryptographic digital signatures.

- FCS_COP.1.1(3): The TOE is required to implement FIPS-conformant SHA-1 and SHA-256 in support of cryptographic protocols.
- FCS_COP.1.1(4): The TOE is required to implement FIPS-conformant HMAC SHA-1 in support of cryptographic protocols.
- FTP_ITC.1: The TOE is required to provide a trusted communication path between itself and authorized IT entities that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.
- FTP_TRP.1: The TOE is required to protect communication between itself and its administrators from disclosure and modification.

#### 8.2.1.6 O.RESIDUAL_INFORMATION_CLEARING

*The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.*

This TOE Security Objective is satisfied by ensuring that:

- FDP_RIP.1: The TOE is required to clear all information when allocating storage resources for subsequent activities.

#### 8.2.1.7 O.SYSTEM_MONITORING

*The TOE will provide the capability to generate audit data and provide the means to store and review those data.*

This TOE Security Objective is satisfied by ensuring that:

- FAU_GEN.1: The TOE is required to be able to generate audit events for security relevant activities on the TOE.
- FAU_GEN.2: The TOE is required to associate audit events to users to ensure proper accountability.
- FAU_SAR.1: The TOE is required to provide the means for a user to review recorded audit records.
- FAU_SAR.2: The TOE is required to provide the means to restrict a user from reviewing recorded audit records.
- FAU_SAR.3: The TOE is required to provide functions to sort audit records to make their review more effective.
- FAU_STG.1: The TOE is required to protect stored audit records so they cannot be inappropriately modified.
- FAU_STG.4: The TOE is required to have well-defined behavior when the available audit storage space becomes exhausted so that appropriate procedures can be in place to mitigate that possibility.
- FPT_STM.1: The TOE is required to generate reliable time stamps to be used in its audit records for proper accounting.

#### 8.2.1.8 O.TOE_ADMINISTRATION

*The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and restrict logged-in administrators to authorized functions and TSF data.*

This TOE Security Objective is satisfied by ensuring that:

- FIA_ATD.1: The TOE is required to facilitate the definition of users with appropriate user attributes.
- FIA_UAU.1: The TOE is required to ensure that users must be authenticated in order to access functions, other than those specifically intended to be accessed without authentication (i.e., user data resources available to client hosts).
- FIA_UAU.5: The TOE is required to implement a local authentication mechanism and can support additional authentication mechanisms.
- FIA_UAU.7: The TOE is required to not echo passwords when being entered to mitigate the chance of an accidental password disclosure.
- FIA_UID.2: The TOE is required to ensure that users must be identified in order to access functions of the TOE. The TOE does not offer services to administrative users until they are successfully identified and authenticated by user name and password or public-key credentials. With respect to data path users, the TOE allows iSCSI and FC hosts access to virtual volumes in accordance with the Block Storage Access Control Policy after the hosts have been identified but without requiring authentication.
- FMT_MSA.1: The TOE is required limit the ability to manage the access control functions to authorized administrators.
- FMT_MSA.3: The TOE is required to implement default secure values and limit the management of default values to authorized administrators.
- FMT_MTD.1: The TOE is required to restrict access to security relevant data to administrators.
- FMT_SMF.1: The TOE is required to provide a minimum set of security functions to ensure the TOE security features can be properly managed.
- FMT_SMR.2: The TOE is required to implement a minimum of a System Administrator role and can implement additional roles where necessary and that a System Administrator can manage the TOE.
- FPT_APW_EXT.1 The TOE is required to store passwords in non-plaintext format and shall prevent the reading of plaintext passwords.

#### 8.2.1.9 O.SELF_TEST

*The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.*

This TOE Security Objective is satisfied by ensuring that:

- FPT_TST_EXT.1: The TOE is required to run a suite of self-tests during initial start-up (on power on) to demonstrate that it operates correctly.

## 8.3 Security Assurance Requirements Rationale

The Security Assurance Requirements (SARs) correspond to EAL2 augmented with ALC_FLR.2.

## 8.4 Requirement Dependency Rationale

As can be seen in the following table, all of the SFR and SAR dependencies are satisfied in this ST.

| ST Requirement | CC Dependencies | ST Dependencies |
|---|---|---|
| **FAU_GEN.1** | FPT_STM.1 | FPT_STM.1 |
| **FAU_GEN.2** | FAU_GEN.1 and FIA_UID.1 | FAU_GEN.1 and FIA_UID.2 |
| **FAU_SAR.1** | FAU_GEN.1 | FAU_GEN.1 |
| **FAU_SAR.2** | FAU_SAR.1 | FAU_SAR.1 |
| **FAU_SAR.3** | FAU_SAR.1 | FAU_SAR.1 |
| **FAU_STG.1** | FAU_GEN.1 | FAU_GEN.1 |
| **FAU_STG.4** | FAU_STG.1 | FAU_STG.1 |
| **FCS_CKM.1** | FCS_COP.1 and FCS_CKM.4 | FCS_COP.1(*) and FCS_CKM.4 |
| **FCS_CKM.4** | (FTP_ITC.1 or FCS_CKM.1) | FCS_CKM.1 |
| **FCS_COP.1(1)** | (FTP_ITC.1 or FCS_CKM.1) and FCS_CKM.4 | FCS_CKM.1 and FCS_CKM.4 |
| **FCS_COP.1(2)** | (FTP_ITC.1 or FCS_CKM.1) and FCS_CKM.4 | FCS_CKM.1 and FCS_CKM.4 |
| **FCS_COP.1(3)** | (FTP_ITC.1 or FCS_CKM.1) and FCS_CKM.4 | FCS_CKM.1 and FCS_CKM.4 |
| **FCS_COP.1(4)** | (FTP_ITC.1or FCS_CKM.1) and FCS_CKM.4 | FCS_CKM.1 and FCS_CKM.4 |
| **FDP_ACC.2** | FDP_ACF.1 | FDP_ACF.1 |
| **FDP_ACF.1** | FDP_ACC.2 and FMT_MSA.3 | FDP_ACC.2 and FMT_MSA.3 |
| **FDP_AVL_EXT.1** | None | none |
| **FDP_RIP.1** | none | none |
| **FIA_ATD.1** | none | none |
| **FIA_UAU.1** | FIA_UID.2 | FIA_UID.2 |
| **FIA_UAU.5** | none | none |
| **FIA_UAU.7** | FIA_UAU.1 | FIA_UAU.1 |
| **FIA_UID.2** | none | none |
| **FMT_MSA.1** | (FDP_ACC.2 or FDP_IFC.1) and FMT_SMR.1 and FMT_SMF.1 | FDP_ACC.2 and FMT_SMR.1 and FMT_SMF.1 |
| **FMT_MSA.3** | FMT_MSA.1 and FMT_SMR.1 | FMT_MSA.1 and FMT_SMR.2 |
| **FMT_MTD.1** | FMT_SMR.1 and FMT_SMF.1 | FMT_SMR.2 and FMT_SMF.1 |
| **FMT_SMF.1** | none | none |
| **FMT_SMR.2** | FIA_UID.2 | FIA_UID.2 |
| **FPT_APW_EXT.1** | None | none |
| **FPT_FLS.1** | None | none |
| **FPT_STM.1** | none | none |

| ST Requirement | CC Dependencies | ST Dependencies |
|---|---|---|
| **FPT_TST_EXT.1** | None | none |
| **FRU_FLT.1** | FPT_FLS.1 | FPT_FLS.1 |
| **FTA_SSL.4** | none | none |
| **FTP_ITC.1** | none | none |
| **FTP_TRP.1** | none | none |
| **ADV_ARC.1** | ADV_FSP.1 and ADV_TDS.1 | ADV_FSP.2 and ADV_TDS.1 |
| **ADV_FSP.2** | ADV_TDS.1 | ADV_TDS.1 |
| **ADV_TDS.1** | ADV_FSP.2 | ADV_FSP.2 |
| **AGD_OPE.1** | ADV_FSP.1 | ADV_FSP.2 |
| **AGD_PRE.1** | none | none |
| **ALC_CMC.2** | ALC_CMS.2 | ALC_CMS.2 |
| **ALC_CMS.2** | none | none |
| **ALC_DEL.1** | none | none |
| **ALC_FLR.2** | none | none |
| **ATE_COV.1** | ADV_FSP.2 and ATE_FUN.1 | ADV_FSP.2 and ATE_FUN.1 |
| **ATE_FUN.1** | ATE_COV.1 | ATE_COV.1 |
| **ATE_IND.2** | ADV_FSP.2 and AGD_OPE.1 and AGD_PRE.1 and ATE_COV.1 and ATE_FUN.1 | ADV_FSP.2 and AGD_OPE.1 and AGD_PRE.1 and ATE_COV.1 and ATE_FUN.1 |
| **AVA_VAN.2** | ADV_ARC.1 and ADV_FSP.2 and ADV_TDS.1 and AGD_OPE.1 and AGD_PRE.1 | ADV_ARC.1 and ADV_FSP.2 and ADV_TDS.1 and AGD_OPE.1 and AGD_PRE.1 |

**Table 10 Requirement Dependencies**

## 8.5 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. **Table 11** demonstrates the relationship between security requirements and security functions.

| | Security audit | Cryptographic support | User data protection | Identification and authentication | Security management | Protection of the TSF | Resource utilization | TOE access | Trusted path/channels |
|---|---|---|---|---|---|---|---|---|---|
| **FAU_GEN.1** | X | | | | | | | | |
| **FAU_GEN.2** | X | | | | | | | | |
| **FAU_SAR.1** | X | | | | | | | | |
| **FAU_SAR.2** | X | | | | | | | | |
| **FAU_SAR.3** | X | | | | | | | | |
| **FAU_STG.1** | X | | | | | | | | |
| **FAU_STG.4** | X | | | | | | | | |
| **FCS_CKM.1** | | X | | | | | | | |
| **FCS_CKM.4** | | X | | | | | | | |
| **FCS_COP.1(1)** | | X | | | | | | | |
| **FCS_COP.1(2)** | | X | | | | | | | |
| **FCS_COP.1(3)** | | X | | | | | | | |
| **FCS_COP.1(4)** | | X | | | | | | | |
| **FDP_ACC.2** | | | X | | | | | | |
| **FDP_ACF.1** | | | X | | | | | | |
| **FDP_AVL_EXT.1** | | | X | | | | | | |
| **FDP_RIP.1** | | | X | | | | | | |
| **FIA_ATD.1(1)** | | | | X | | | | | |
| **FIA_ATD.1(2)** | | | | X | | | | | |
| **FIA_UAU.1** | | | | X | | | | | |
| **FIA_UAU.5** | | | | X | | | | | |
| **FIA_UAU.7** | | | | X | | | | | |
| **FIA_UID.2** | | | | X | | | | | |
| **FMT_MSA.1** | | | | | X | | | | |
| **FMT_MSA.3** | | | | | X | | | | |
| **FMT_MTD.1** | | | | | X | | | | |
| **FMT_SMF.1** | | | | | X | | | | |
| **FMT_SMR.2** | | | | | X | | | | |
| **FPT_APW_EXT.1** | | | | | | X | | | |
| **FPT_FLS.1** | | | | | | X | | | |
| **FPT_STM.1** | | | | | | X | | | |
| **FPT_TST_EXT.1** | | | | | | X | | | |
| **FRU_FLT.1** | | | | | | | X | | |
| **FTA_SSL.4** | | | | | | | | X | |
| **FTP_ITC.1** | | | | | | | | | X |
| **FTP_TRP.1** | | | | | | | | | X |

**Table 11 Security Functions vs. Requirements Mapping**