Hewlett Packard
Enterprise

Security Target

HPE StoreOnce System, Version 3.13

Document Version: 1.2
Date: October 13, 2016

Prepared For:

Hewlett-Packard Enterprise
Long Down Avenue
Stoke Gifford
Bristol BS34 8QZ

UK

***Prepared By*:**

CGI Global IT Security Labs.

1410 Blair Place, 7th floor
Ottawa, ON K1J 9B9, Canada
www.cgi.com/securitylab

Revision History

Ver #	Description of changes	Modified by	Date
0.1	Initial Draft	Matt Mulligan	11/13/2015
0.2	Updates for Lab observations	Matt Mulligan	01/04/2016
0.3	Updates for Lab observations	Matt Mulligan	01/07/2016
0.4	Updates related to SNMP	Matt Mulligan	01/13/2016
0.5	Updates related to SNMP	Matt Mulligan	01/14/2016
0.6	Updates to Sections 1.5.2.2, 4.1 and 4.2	Matt Mulligan	01/28/2016
0.7	Removed references to Public Key authentication	Matt Mulligan	03/21/2016
0.8	Updates added for network separation and CIFS shares	Matt Mulligan	05/19/2016
0.9	Removed claim of iSCSI and added build number	Matt Mulligan	06/06/2016
1.0	Removed "Generation 8" reference to product name. Updated "Guidance Documentation" section	Matt Mulligan	06/30/2016
1.1	Added CAVP certificate numbers for FCS_COP.1	Matt Mulligan	10/13/2016
1.2	Change made to TOE name	Matt Mulligan	10/13/2016

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

This section identifies the Security Target (ST), Target of Evaluation (TOE), document conventions, and terminology. It also provides TOE overview and describes the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE.

1.1 ST Reference

ST Title	Security Target - HPE StoreOnce System, Version 3.13
ST Revision	1.2
ST Publication Date	October 13, 2016
ST Author	CGI Global IT Security Labs – Canada Matthew Mulligan

1.2 Target of Evaluation Reference

TOE Developer	Hewlett Packard Enterprise
TOE Name	HPE StoreOnce System, Version 3.13.3-1612.1
TOE Models	• HPE StoreOnce 6500 (Multi-node)
TOE Type	Data Storage

1.3 Conventions

The Common Criteria allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and selected presentation choices are discussed below to aid the Security Target reader:

- An assignment operation is indicated by [**bold text within brackets**].
- Selections are denoted by [underlined text within brackets].
- Refinement of security requirements is identified using **bold text**. Any text removed is indicated with a strikethrough (Example: ~~TSF~~).
- Iterations are identified by appending a number in parentheses following the component title, for example, FIA_UAU.1 (1) and FIA_UAU.1 (2) refer to two iterations of the FIA_UAU.1 security functional requirement component.

1.4 TOE Overview

The HPE StoreOnce system is a disk-based storage appliance for backing up host network servers to target devices on the appliance. These devices are configured as either Network-Attached Storage (NAS) or Virtual Tape Library (VTL) or StoreOnce Catalyst stores for backup applications.

The Target of Evaluation (TOE) is the HPE StoreOnce 6500 system appliance. The TOE runs on the Version 3.13 software and operates on the Red Hat Linux Operating System. The 6500 model offers a multi-node system that provides varying types of fault-tolerance.

Table 1 - Appliance Model Specifications

	Model 6500
Server platform	DL380p Gen 8
CPU	Intel Xeon E5-2690 v3
No. of server nodes	2 - 8
Raw capacity	120TB – 2240TB
Expansion shelves	N/A
No. of disks available for user data storage	30 x 4TB – 560 x 4TB
Max no. of disks available in head server for user data storage	0
No. of 1GB Ethernet ports	8 per couplet
No. of 10GB Ethernet ports	4 per couplet
No. of Fibre Channel ports	8 per couplet
Max No. of devices (VTLs, NAS shares, StoreOnce Catalyst stores)	96 per couplet
VTL protocol support	Fibre Channel
NAS protocol support	CIFS, NFSv3

Multi-node appliances operate as a cluster. A cluster is composed of from 1 to 4 couplets each couplet having two nodes. A cluster is the scope of administrative control, with the configuration of the cluster defining the behavior of all nodes within the cluster.

The 6500 appliance is a multi-node appliance. The number of nodes in a model 6500 is determined by the customer. The 6500 can be ordered as a single couplet (2 nodes), a 2 couplet (4 node) cluster, a 3 couplet (6 node) cluster or a 4 couplet (8 node) cluster. A customer can buy a cluster of one couplet and then buy additional couplets to expand the cluster up to a maximum of 4 couplets.

The total number of backup targets offered by an HPE StoreOnce system is split between VTL, NAS and StoreOnce Catalyst devices. Each node in a cluster on a HPE StoreOnce 6500 is capable of supporting 48 target devices. So as examples, a couplet can support 96 backup targets, while an 8 node (4 couplet) 6500 can support 384 (i.e., 48 x 8) backup targets. These devices may be all VTL, all NAS, all StoreOnce Catalyst or any combination of StoreOnce Catalyst, NAS and VTL devices. The HPE StoreOnce system supports both Common Internet File System (CIFS) and Network File System (NFS) protocols for connectivity to TOE provided NAS. This allows the TOE to provide backup targets for both Windows and UNIX/Linux hosts.

All devices (i.e., VTL, NAS and StoreOnce Catalyst) automatically include the TOE's data Deduplication functionality. Data Deduplication is a process in which the TOE compares blocks of data being written to a backup device with data blocks previously stored on the device. If duplicate data is found, a pointer is established to the original data, rather than storing the duplicate data. The TOE performs data deduplication at the block level and not at the file level, which reduces the amount of data actually stored on physical disks.

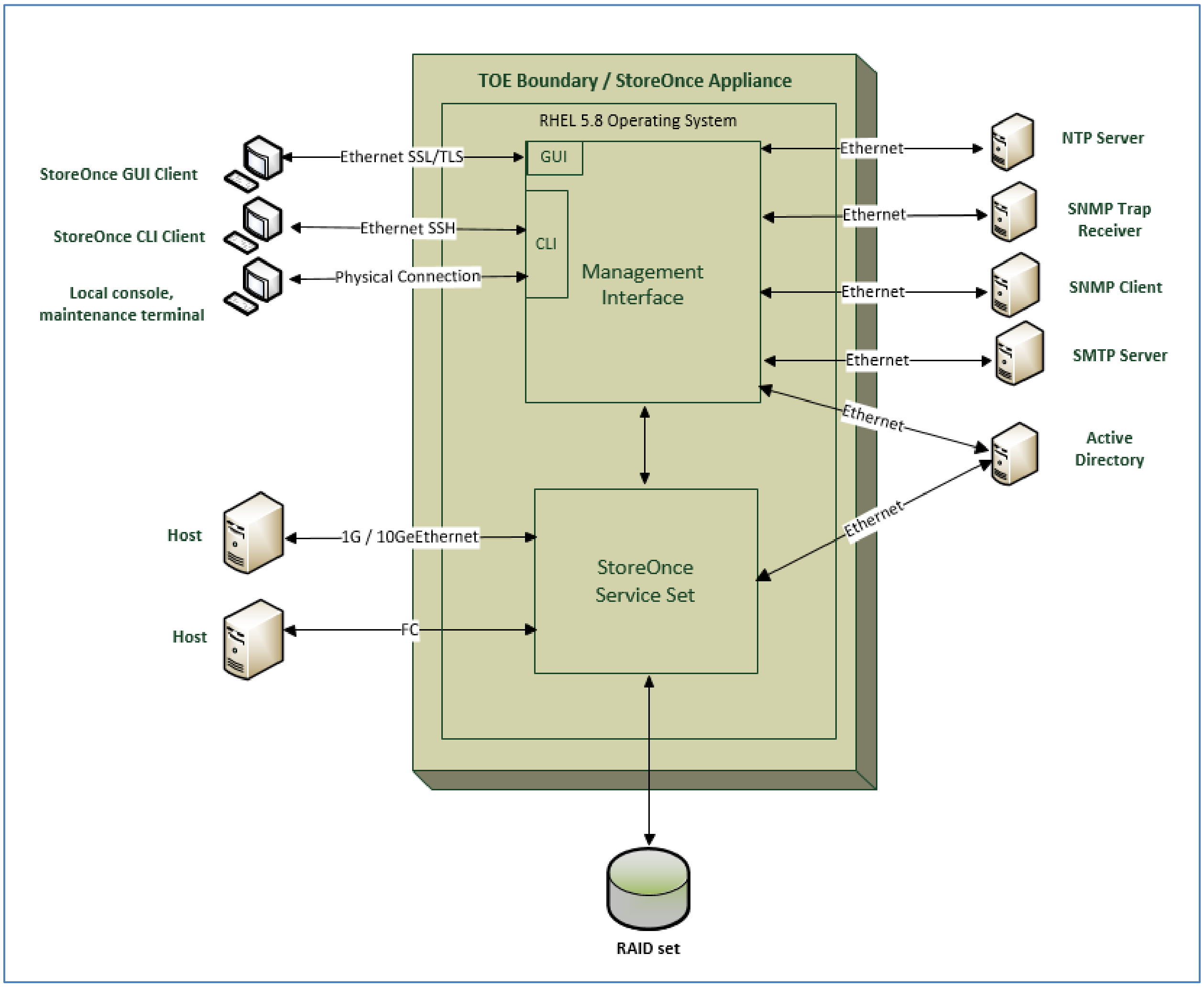
The HPE StoreOnce system products are hardware appliances that offer network accessible administration interfaces in the form of an HTTPS based Graphical User Interface or SSH protected Command Line Interface.

The HPE StoreOnce systems include hardware-based RAID 6 to reduce the risk of user data loss due to disk failure within a couplet.

1.5 TOE Description

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

Figure 1 - HPE StoreOnce



1.5.1 Physical Boundary

The physical boundary of an HPE StoreOnce system is the physical boundary of the hardware. Interfaces to this hardware include Fibre Channel ports for data connections, Ethernet ports for server administration, and a serial port which provides limited administrative access. The RHEL 5.8 Operating System is installed on the TOE and is included within the TOE boundary.

There are three distinct networks supported by a HPE StoreOnce appliance: a management network, a data network and an internal network. The management network would connect the product to any devices associated with managing the product such as an administration workstation, NTP server or LDAP server. The Data Network provides client hosts a communication path with the product. Finally, the internal network is used for communication between nodes of a multi-node system.

For the multi-node appliance, 6500 the management, data and internal networks are separate.

Management Interface:

The web interface is a graphical user interface that is secured by SSL/TLS and accessed from a client management workstation or server. An HPE StoreOnce system user would use the web interface to configure Virtual Tape Libraries, CIFS or NFS shares or StoreOnce Catalyst objects, view performance and storage metrics, view event logs and manage user accounts.

The CLI interface can be accessed either locally from a management console or remotely from a client workstation or server using SSH. The functionality provided by the CLI includes system configuration, and viewing system status.

The Management Interface also provides capabilities of configuring communication with external servers such as LDAP (Active Directory), SNMPv3, SMTP and NTP servers. The Management Interface includes an SNMPv3 Agent that can be configured to communicate with an external SNMPv3 Trap Receiver through a unique path. The agent responds to GET requests from SNMPv3 client (NMS), generates notification messages (traps) for critical events (alerts) and sends traps to remote SNMPv3 Trap Receiver, warning events and informational events and alert state changes. The implementation is SNMPv3-compliant as defined in RFC-3414.

StoreOnce Service Set:

A service set is a collection of various services, such as VTL, NAS, Replication and StoreOnce Catalyst. There is one instance of each service per service set. The auto-configuration process registers and starts a service set by launching a process on the server for each of the services.

Other Components

The TOE can be configured to rely on and utilize a number of other components in its operational environment. All of the following external functionality is outside the scope of the evaluation.

- AD server – The TOE can be configured to use Active Directory as an external authentication server.
- NTP server – The TOE can be configured to use a NTP server to synchronize the internal clock of each individual node.
- SNMPv3 client and (SNMPv3 Trap Receiver) - The TOE can be configured to generate notification messages (traps) for critical events (alerts) and send traps to SNMPv3 Trap Receiver, warning events and informational events and alert state changes. The TOE also runs SNMPv3 agent and processes GET requests sent from SNMPv3 client.
- SMTP server - The HPE StoreOnce system can be configured to send email alerts to specified recipients. These email alerts are generated when certain events occur on the HPE StoreOnce system such as a failed login.
- FC hosts – The TOE attaches to FC hosts, which access available storage resources, either directly through available ports or indirectly through a suitable SAN connected to available ports. Note that when connective via a SAN switch, the FC hosts are still individually identified on the TOE ports with their own respective identifiers.
- Management Workstation – An appropriate client (third party client supporting SSHv2 and/or a modern web browser supporting TLS 1.2) operating on a suitable workstation is required to use the network-accessible administrative interfaces.
- Network Storage Devices – The HPE StoreOnce system is typically connected to a storage controller that manages the actual physical storage.

1.5.1.1 Guidance Documentation

The HPE StoreOnce system offers a series of documents that describe the installation of the product as well as guidance for subsequent use and administration of the applicable security features. These documents include:

- HPE StoreOnce 6500 and B6200 Backup Systems User Guide; HP Part Number: BB897-90963; Published: April 2016; Edition: 14
- HPE StoreOnce Backup system CLI Reference Guide For software version 3.13 and earlier; HP Part Number: BB897-90953; Published: September 2015; Edition: 11
- HPE StoreOnce Systems: Linux and UNIX Configuration Guide; Part Number: BB913-90920; Published: April 2016; Edition: 9
- HPE StoreOnce 6500 Backup Installation Planning and Preparation Guide and Checklists; HP Part Number: BB897-90951; Published: August 2015; Edition: 4

1.5.2 Logical Boundary

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following sections.

1.5.2.1 Security Audit

The HPE StoreOnce system includes its own logging of management events and also user authentication. Administrators can also review the audit data collected by the product. Finally, the product protects audit data, and overwrites the storage space used for audit data once the available storage space becomes full.

1.5.2.2 Cryptographic Support

The HPE StoreOnce system currently includes cryptographic functions to support SSHv2 and HTTPS (using TLS) protection for communication with remote administrative sessions. Cryptographic package in OpenJDK is used to support cryptographic operations for the HTTPS protocol and the libcrypto library in OpenSSL is used to support cryptographic operations for the SSH protocol (OpenSSH, which is used to implement SSH, is dependent on OpenSSL for cryptographic functions). The cryptographic algorithms are CAVP-certified pending.

1.5.2.3 User data protection

The HPE StoreOnce system is designed to offer reliable disk-based backup storage services. Access to TOE resources – Network-Attached Storage (NAS), StoreOnce Catalyst or Virtual Tape Library (VTL) – is provided either through CIFS or NFS, and Fibre Channel.

- CIFS-based NAS – The product permits access based upon a list of users with read-write or read-only permissions. Alternately, the product can use AD user accounts and AD defined access permissions.
- NFS-based NAS – The product permits access based upon a list of hosts defined as permitted for the NFS share.
- Fibre Channel VTL – The product permits Fibre Channel resources to be assigned to specific Fibre Channel ports. Note that the SAN can be zoned to restrict access to specific devices, but that is out of scope of the TOE.

- StoreOnce Catalyst stores: A list of clients is created in the GUI under the StoreOnce Catalyst tab and only these clients can be allowed to create StoreOnce Catalyst stores and access them.
- Client hosts are attached through dedicated storage area networks (SANs) that are generally in close proximity and therefore subject to the same physical protection assumption as the HPE StoreOnce system.

File permissions associated with files under CIFS/NFS shares shall be checked to further control access to files under CIFS/NFS shares.

The TOE implements RAID on physical disks. Multi-node configurations support only RAID 6, however, RAID of physical storage occurs inside a couplet with both nodes accessing the same RAID arrays. There is no RAID or other redundancy between couplets in a cluster.

The multi-node architecture provides mechanisms for high availability support by offering the ability to continue operation in the event of the failure of one node within each couplet as well as by offering support of RAID levels to protect user and TSF data.

TSF data is stored by a multi-node appliance (i.e., a couplet) as a mirrored set in a stripped set (i.e., RAID 1+0).

Any disk failure causes the TOE to generate an alert via SNMPv3 or SMTP. Failures of one node within a couplet also generate an alert via SNMPv3 or SMTP.

1.5.2.4 Identification & Authentication

The HPE StoreOnce system requires that administrators must login with username and password prior to being able to access functions associated with their defined role. The HPE StoreOnce system uses only locally defined accounts to define the “Administrator” and “Operator” accounts.

The HPE StoreOnce system can be configured to use an Active Directory (LDAP) server for user identification and authentication associated with CIFS-based NAS access.

CIFS users, who are configured with User authentication mode, must login with username and password prior to access CIFS shares/files.

SNMPv3 users must login with username and password prior to viewing MIB objects.

1.5.2.5 Security Management

The HPE StoreOnce system is responsible for enabling the management of available storage resources and access by client-hosts. Administrators manage the product with either a graphical user interface or command line interface. Both interfaces enforce the same administrative constraints which limit the operations available to the user. Each user is assigned a role which is currently limited to “administrator” (read and write functionality) or “operator” (read-only functionality).

There is implicitly a third type of user, i.e. NAS users, which access the CIFS shares and files, and NFS shares and files. The TOE provides management of NAS users.

The HPE StoreOnce system can also be configured to generate SNMP trap for network monitoring of a running system. SNMPv3 users can be created through the SSH channel using the CLI interface.

1.5.2.6 Protection of the TSF

The HPE StoreOnce system includes a real-time clock for timestamps when generating audit records.

1.5.2.7 TOE Access

The HPE StoreOnce system can terminate an inactive remote administrative session after an administrator-defined period of inactivity. Users may terminate their sessions at any time.

1.5.2.8 Trusted Paths/Channels

As mentioned above, the HPE StoreOnce system currently provides cryptographic functions that are used to protect administrator sessions. These cryptographic functions include SSHv2 and HTTPS (TLS).

1.5.3 Product Physical/Logical Features and Functions not included in the TOE Evaluation

Features/Functions that are not part of the evaluated configuration of the TOE are:

- StoreOnce Catalyst Clients - Third party applications that have the Catalyst Client plug-in software used to communicate directly with StoreOnce appliances
- Other StoreOnce Appliances: StoreOnce appliances may communicate with other StoreOnce appliances to copy and/or replicate data. The TOE evaluation will not include the connection between multiple StoreOnce appliances.
- Data at Rest Encryption, Data in Flight Encryption, and Secure Erase: They are not evaluated security functions.
- Local/External Key Management: It is not an evaluated security functions.

2 CONFORMANCE CLAIMS

2.1 Common Criteria Conformance Claim

The Security Target is conformant to Common Criteria Version 3.1 Revision 4, September 2012, Part 2 extended and Part 3 conformant. The ST claims conformance to Evaluation Assurance Level 2 augmented with ALC_FLR.2

2.2 Protection Profile Conformance Claim

The Security Target does not make any PP conformance claims.

3 Security Problem Definition

This section defines the security problem which the TOE and its operational environment are supposed to address. Specifically, the security problem makes up the following:

- Any known or assumed threats countered by the TOE or its operational environment.
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

This section identifies assumptions as A.*assumption* and threats as T.*threat*.

3.1 Threats

This section identifies the threats to the assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)

The table below lists threats applicable to the TOE and its operational environment:

Table 2 - Threats

Threat	Description
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms that may go undetected.
T.DATA_AVAILABILITY	User data may become unavailable due to isolated storage resource failures, node failures or due to resource exhaustion.
T.DATA_DISCLOSURE	A connected host might obtain access to user data for which they have no authorization.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TSF data and TSF executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to TSF data or TSF resources. A malicious user, process, or external IT entity may misrepresent itself as the TSF to obtain identification and authentication 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.

3.2 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to operate. The following specific conditions are assumed to exist in an environment where the TOE is employed.

Table 3 - Assumptions

Assumption	Description
A.NO_GENERAL_PURPOSE	It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner. It is assumed that those assigned as Administrators of CIFS shares are trusted, competent and not careless.
A.HOST_IDENTITY	It is assumed that Fibre Channel host identities properly reflect the adapters and hence the hosts to which they are associated such that authentication is not necessary.
A.MGMT_NET	It is assumed that a dedicated and protected “Management Network” exists between nodes of the TOE and hosts providing supporting services (e.g. NTP, SNMPv3, SMTP or AD).
A.DATA_NET	It is assumed that the confidentiality, integrity, and authenticity of the connection between the TOE and the host shall be protected by environment. The NAS clients shall authenticate NAS users (i.e. users who access NFS, and users who access CIFS with AD authentication mode) and managed user accounts properly.
A.INTERNAL_NET	It is assumed that a dedicated and protected “Internal Network” exists that connects nodes of the TOE with network storage devices.
A.ETHERNET	It is assumed that network devices on the Internal Network do not intercept, impersonate or otherwise modify communications on the Internal network.

4 SECURITY OBJECTIVES

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition. This high-level solution is divided into two parts: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are as follows:

Table 4 - TOE Security Objectives

Security Objective	Description
O.AVAILABILITY	The TOE will ensure that data can be stored in a manner that is protected from underlying resource failure and exhaustion.
O.LIMIT_ACCESS	The TOE will ensure that connected hosts can access only data resources for which they are authorized.
O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels for administrators.
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.

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

Table 5 - Operational Environment Security Objectives

Security Objective	Description
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner. Those assigned as Administrators of CIFS shares are trusted, competent and not careless.
OE.HOST_IDENTITY	Fibre Channel hosts correctly reflect the Fibre Channel World Wide Name (WWN) associated with their Host Bus Adapters (HBAs).
OE.MGMT_NET	A protected "Management network" provides reliable and secure

Security Objective	Description
	communication between the TOE and peer hosts providing supporting services such as NTP, SNMPv3, SMTP or Active Directory.
OE.DATA_NET	The confidentiality, integrity, and authenticity of the connection between the TOE and the host shall be protected by environment. The NAS clients shall authenticate NAS users (i.e. users who access NFS, and users who access CIFS with AD authentication mode) and managed user accounts properly.
OE.INTERNAL_NET	A dedicated and protected “Internal Network” exists that connects nodes of the TOE with one another and with network storage devices.
OE.ETHERNET	Hosts on the Internal Network do not intercept communications on the Internal Network, do not modify communications on the Internal Network, and do not impersonate endpoints on the Internal Network.

4.3 Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies if applicable. The following table provides a high level mapping of coverage for each threat, assumption, and policy:

Table 6 - Cross Reference of Threats, Assumptions and Policies

Objectives mapped to Assumptions , Threats and Policies	T.ADMIN_ERROR	T.DATA_DISCLOSURE	T.DATA_AVAILABILITY	T.UNAUTHORIZED_ACCESS	T.UNDETECTED_ACTIONS	A.NO_GENERAL_PURPOSE	A.PHYSICAL	A.TRUSTED_ADMIN	A.HOST_IDENTITY	A.MGMT_NET	A.DATA_NET	A.INTERNAL_NET	A.ETHERNET
O.AVAILABILITY			X										
O.LIMIT_ACCESS		X											
O.PROTECTED_COMMUNICATIONS				X									
O.SYSTEM_MONITORING	X			X	X								
O.TOE_ADMINISTRATION				X									
OE.NO_GENERAL_PURPOSE						X							
OE.PHYSICAL							X						
OE.TRUSTED_ADMIN								X					

Objectives mapped to Assumptions , Threats and Policies	T.ADMIN_ERROR	T.DATA_DISCLOSURE	T.DATA_AVAILABILITY	T.UNAUTHORIZED_ACCESS	T.UNDETECTED_ACTIONS	A.NO_GENERAL_PURPOSE	A.PHYSICAL	A.TRUSTED_ADMIN	A.HOST_IDENTITY	A.MGMT_NET	A.DATA_NET	A.INTERNAL_NET	A.ETHERNET
OE.HOST_IDENTITY									X				
OE.MGMT_NETWORK										X			
OE.DATA_NET											X		
OE.INTERNAL_NET												X	
OE.ETHERNET													X

Table 7 - Detailed Rationale of Threats, Policies and Assumptions

Threats, Policies and Assumptions	Objectives	Security Objective Rationale
T.ADMIN_ERROR An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms that may go undetected.	O.SYSTEM_MONITORING	This threat is countered by ensuring that: • O.SYSTEM_MONITORING: To reduce the potential of an administrative error might be unnoticed or untraceable, the TOE is expected to log security relevant events and store that information locally.
T.DATA_DISCLOSURE A connected host might obtain access to user data for which they have no authorization.	O.LIMIT_ACCESS	This threat is countered by ensuring that: • O.LIMIT_ACCESS: To ensure that connect client hosts cannot access data for which they are not authorized, the TOE is expected to enforce an access policy limiting connected hosts to access only authorized resources.
T.DATA_AVAILABILITY User data may become unavailable due to isolated storage resource failures or due to resource exhaustion.	O.AVAILABILITY	This threat is countered by ensuring that: • O.AVAILABILITY: To reduce the threat of lack of data access due to resource failure or exhaustion, the

Threats, Policies and Assumptions	Objectives	Security Object Rationale
		TOE is expected to ensure that data can be stored in a manner alleviating failure situations and also to allow administrators to configure limits so that user accessible resources are limited and warnings are issued when limits are reached.
T.UNAUTHORIZED_ACCESS A user may gain unauthorized access to the TSF data and TSF executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to TSF data or TSF resources. A malicious user, process, or external IT entity may misrepresent itself as the TSF to obtain identification and authentication data.	O.PROTECTED_COMMUNICATIONS O.SYSTEM_MONITORING O.TOE_ADMINISTRATION	This threat is countered by ensuring that: • 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.
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.	O.SYSTEM_MONITORING	This threat is countered 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 store that information locally.

Threats, Policies and Assumptions	Objectives	Security Objective Rationale
A.NO_GENERAL_PURPOSE It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.	OE.NO_GENERAL_PURPOSE	This Assumption is satisfied by ensuring that: • OE.NO_GENERAL_PURPOSE: There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
A.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.	OE.PHYSICAL	This Assumption is satisfied by ensuring that: • OE.PHYSICAL: Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
A.TRUSTED_ADMIN TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner. It is assumed that those assigned as Administrators of CIFS shares are trusted, competent and not careless.	OE.TRUSTED_ADMIN	This Assumption is satisfied by ensuring that: • OE.TRUSTED_ADMIN: TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner. Those assigned as Administrators of CIFS shares are trusted, competent and not careless.
A.HOST_IDENTITY It is assumed that Fibre Channel host identities properly reflect the adapters and hence the hosts to which they are associated such that authentication is not necessary.	OE. HOST_IDENTITY	This Assumption is satisfied by ensuring that: • OE. HOST_IDENTITY: Fibre Channel hosts correctly reflect Fibre Channel World Wide Name (WWN) associated with their Host Bus Adapters (HBAs).
A.MGMT_NET It is assumed that a protected “Management Network” exists between nodes of the TOE and hosts providing supporting services (e.g., AD and NTP)	OE.MGMT_NET OE.PHYSICAL	This Assumption is satisfied by ensuring that: • OE.MGMT_NET: A protected “Management network” provides reliable ad secured communication between the TOE and peer hosts providing supporting services such as Active Directory or NTP. • OE.PHYSICAL: Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment for the Management network and all connected devices.
A.DATA_NET	OE.DATA_NET	This Assumption is satisfied by ensuring

Threats, Policies and Assumptions	Objectives	Security Objective Rationale
It is assumed that the confidentiality, integrity, and authenticity of the connection between the TOE and the host shall be protected by environment. The NAS clients shall authenticate NAS users (i.e. users who access NFS, and users who access CIFS with AD authentication mode) and managed user accounts properly.		that: • OE.DATA_NET: The confidentiality, integrity, and authenticity of the connection between the TOE and the host shall be protected by environment. The NAS clients shall authenticate NAS users (i.e. users who access NFS, and users who access CIFS with AD authentication mode) and managed user accounts properly.
A.INTERNAL_NET It is assumed that a dedicated and protected “Internal Network” exists that connects nodes of the TOE with network storage devices.	OE.INTERNAL_NET OE.PHYSICAL	This Assumption is satisfied by ensuring that: • OE.INTERNAL_NET: The “Internal Network” is dedicated to connecting nodes of the TOE to one another and to network storage devices. • OE.PHYSICAL: Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment for the Internal network and all connected devices.
A.ETHERNET It is assumed that network devices on the Internal Network do not intercept, impersonate or otherwise modify communications on the Internal Network.	OE.ETHERNET	This Assumption is satisfied by ensuring that: • OE.ETHERNET: Hosts on the Internal Network honor the Ethernet protocol to not eavesdrop upon or modify network traffic (communications) that are not addressed to the hosts. Further, the hosts on the Internal Network do not impersonate other endpoints on the Internal network.

5 Extended Security Requirement Components Definition

This section defines the extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs) met by the TOE.

5.1 Extended TOE Security Functional Requirement Components

This section specifies the extended SFRs for the TOE.

Extended SFR	Description
FDP_AVL_EXT.1	Data availability

5.1.1 FDP_AVL_EXT

Family Behavior:

This family defines availability features provided by a network storage device. These features can be applied to protection of information on disks or across physically pieces of the TOE. They are intended to describe functionality specific to the TOE's intended purpose as a provider of network storage.

Management: FDP_AVL_EXT.1

There are no management activities foreseen.

Audit: FDP_AVL_EXT.1

Basic Level: Status changes for protected resources

Rational: The SFR is intended to describe functionality specific to the TOE's intended purpose as a provider of network storage. Network storage device providers are responsible for offering mechanisms that ensure the availability of the user data place within the storage device's control. These extended requirements are used to specify the mechanisms offered by a storage area network device to protect and monitor the availability of user data.

5.1.1.1 FDP_AVL_EXT.1 – Data Availability

Hierarchical to:	No other components.
Dependencies:	None
FDP_AVL_EXT.1.1	The TSF shall be able to support a [**assignment: availability policy**] that provides [**assignment: availability metric**] on [**assignment: physical resource**].

5.2 Extended TOE Security Assurance Requirement Components

There are no extended TOE Security Assurance Requirement Components.

6 Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE.

6.1 Security Functional Requirements

The functional security requirements for this Security Target consist of the components from Part 2 of the CC, and those that were explicitly stated, all of which are summarized in the following table:

Table 8 - TOE Security Functional Requirements

Requirement Class	Requirement Name	Description
FAU Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1	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_COP.1	Cryptographic Operation
FDP User data protection	FDP_ACC.2	Complete Access Control
	FDP_ACF.1	Security Attribute Based Access Control
	FDP_AVL_EXT.1(1)	Data availability (User Data)
	FDP_AVL_EXT.1(2)	Data Availability (TSF Data)
	FDP_AVL_EXT.1(3)	Data Availability (Couplet)
FIA Identification and Authentication	FIA_ATD.1	User Attribute Definition
	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(1)	Management of Security Attributes (other than file security properties and file permissions)
	FMT_MSA.1(2)	Management of Security Attributes (file security properties and file permissions)
	FMT_MSA.3(1)	Static Attribute Initialization (other than file security properties and file permissions)
	FMT_MSA.3(2)	Static Attribute Initialization (file security properties and file permissions)

Requirement Class	Requirement Name	Description
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
FPT Protection of TSF	FPT_STM.1	Reliable Time Stamps
FTA TOE Access	FTA_SSL.3	TSF-initiated Termination
	FTA_SSL.4	User-initiated termination
FTP Trusted path/channels	FTP_TRP.1	Trusted Path

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.
Dependencies: FPT_STM.1 Reliable time stamps

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;
c) [**Specifically defined auditable events listed in Table 9**]

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 (if applicable), 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, [**the information detailed in Table 9**].

Table 9 - Auditable Events

COMPONENT	AUDITABLE EVENTS	Additional Audit Record Contents
FCS_COP.1	Failure on invoking functionality.	No additional information.
FDP_AVL_EXT.1(1)	Status changes for RAID protected disks	No additional information.
FDP_AVL_EXT.1(2)	Status changes for RAID protected disks	No additional information
FDP_AVL_EXT.1(3)	Failures of nodes	No additional information
FIA_UAU.1	All use of the authentication mechanisms	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)

COMPONENT	AUDITABLE EVENTS	Additional Audit Record Contents
FIA_UID.2	All use of the user identification mechanism, including the user identity provided.	The user identity provided.
FMT_SMF.1	Use of the management functions: • Managing VTLs • Managing NAS • Managing StoreOnce Catalyst Stores • Managing SNMPv3	No additional information.
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity
FTA_SSL.3	The termination of an interactive session	No additional information
FTA_SSL.4	The termination of an interactive session	No additional information
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

6.1.1.2 FAU_GEN.2 User Identity Association

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

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.

6.1.1.3 FAU_SAR.1 Audit review

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [**all Administrative 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.

6.1.1.4 FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.
Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [**sorting and filtering**] of audit data based on [**date/time, and level**].

6.1.1.5 FAU_STG.1 Protected Audit Trail Storage

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall protect the 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.

6.1.1.6 FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss
Dependencies: FAU_STG.1 Protected audit trail storage

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

6.1.2 Cryptographic Support (FCS)

6.1.2.1 FCS_COP.1 Cryptographic Operation

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [**the operations described below**] in accordance with a specified cryptographic algorithm [**algorithms in the modes of operation described below**] and cryptographic key sizes [**key sizes described below**] that meet the following: [**standards described below**]:

Table 10 - Cryptographic Operations

Operation	Algorithm (Mode)	Key Size (in bits)	Standards	CAVP Certificate
SSH				
Encryption and Decryption	AES in CTR and CBC modes	128, 192, 256	FIPS 197, NIST SP 800-38A	4119
	3DES in CBC mode		FIPS 197, NIST SP 800-38E	2249
Keyed-hash message authentication	HMAC-SHA-1 (digest size 160 bits)	160	FIPS 198-1, FIPS 180-3	3388 (SHA), 2690 (HMAC)
SSL (Java)				
Encryption and Decryption	AES in CBC mode	128, 256	FIPS 197, NIST SP 800-38A	3994
Hashing	SHA-1, SHA-256 (digest sizes 160 and 256 bits)		FIPS 180-3	3296
Digital Signatures	RSA	2048	FIPS 186-4	2050

6.1.3 User data protection (FDP)

6.1.3.1 FDP_ACC.2 Complete access control

Hierarchical to: FDP_ACC.1 Subset access control
Dependencies: FDP_ACF.1 Security attribute based access control

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

- **subjects: Fibre Channel hosts, NFS client hosts, StoreOnce Catalyst clients, CIFS/NFS users**
- **objects: CIFS-based Network-Attached Storage (NAS), NFS-based NAS, StoreOnce Catalyst stores, and Fibre Channel-based VTLs]**

and all operations among subjects and objects covered by the SFP.

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.

6.1.3.2 FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

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

- **Subjects:**
  - **NFS client host: identified by NFS client IP address,**
  - **CIFS/NFS user, identified by user identifier,**
  - **Fibre Channel host: identified by given PCI-E slot to which the FC host is connected,**
  - **StoreOnce Catalyst client: identified by Catalyst client ID**
- **Objects:**
  - **CIFS-based NAS: identified by CIFS share names and file names under CIFS shares,**
  - **NFS-based NAS: identified by NFS share names and file names under NFS shares,**
  - **Fibre Channel-based VTL: identified by VTL name,**
  - **StoreOnce Catalyst Store: identified by Catalyst Store name.]**

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

- **Fibre Channel-based VTLs can be access only if the FC host is connected to the PCI-E slot via which the access is permitted;**
- **CIFS-based NAS can be accessed only by user specifically permitted to have read-write or read-only access based on its user identifier;**
- **NFS-based NAS can be accessed only by an NFS client host that has been specifically permitted access based on its IP address; meanwhile, the permission associated with the file being accessed allows such access.**
- **StoreOnce Catalyst Store can be accessed only by the StoreOnce Catalyst Client that has been specifically permitted access based on StoreOnce Client ID].**

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 following additional rules: [**no additional explicit denial rules**].

6.1.3.3 FDP_AVL_EXT.1(1) Data Availability (User Data)

Hierarchical to: No other components
Dependencies: FDP_ACC.1 Subset access control

FDP_AVL_EXT.1.1 The TSF shall be able to support a [**User-Data Disk Availability Policy**] that provides the following [**RAID level 6**] on [**physical disks on a node containing user data**].

6.1.3.4 FDP_AVL_EXT.1(2) Data Availability (TSF Data)

Hierarchical to: No other components
Dependencies: FDP_ACC.1 Subset access control

FDP_AVL_EXT.1.1 The TSF shall be able to support a [**TSF-Data Disk Availability Policy**] that provides the following [**RAID level 1+0**] on [**physical disks on a node containing TSF data**].

6.1.3.5 FDP_AVL_EXT.1(3) Data Availability (Couplet)

Hierarchical to: No other components
Dependencies: FDP_ACC.1 Subset access control

FDP_AVL_EXT.1.1 The TSF shall be able to support a [**Couplet Availability Policy**] that provides [**continued operation of a couplet upon the failure of a single node in that couplet**] on [**each couplet of a multi-node cluster**].

6.1.4 Identification and Authentication (FIA)

6.1.4.1 FIA_ATD.1 User Attribute Definition

Hierarchical to: No other components.
Dependencies: No Dependencies

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**user identity, password and role if appropriate**]

Application Note: Not all roles are explicitly assumed by the user. The user role of SNMPv3 users, which are defined for SNMPv3 agent, and the user role of CIFS/NFS users are implicitly assumed.

6.1.4.2 FIA_UAU.1 Timing of Authentication

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification.

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

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

6.1.4.3 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_UAU.5.1 The TSF shall provide [**local password, LDAP**] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the rules: [**password authentication - if the user is defined there, otherwise the LDAP server will be consulted**].

6.1.4.4 FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

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

6.1.4.5 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification.
Dependencies: No Dependencies.

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

6.1.5 Security Management (FMT)

6.1.5.1 FMT_MSA.1(1) Management of security attributes (other than file security properties and file permissions)

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [**Access Control Policy**] to restrict the ability to [**manage**] the security attributes [**except for file security properties associated with files in CIFS shares or file permissions associated with files in NFS shares]** to [**Admin Role**].

6.1.5.2 FMT_MSA.1(2) Management of security attributes (file security properties and file permissions)

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [**Access Control Policy**] to restrict the ability to [**manage**] the security attributes [**of file security properties associated with files in CIFS shares or file permissions associated with files in NFS shares]** to [**NAS user**].

Application Note: A file or folder within a CIFS share has 'Full Control' permission set for the 'Everyone' Group regardless of the owner. The Owner of the file or folder cannot change this security setting. Therefore special consideration should be given to users assigned rights to the shares.

6.1.5.3 FMT_MSA.3(1) Static attribute initialization (other than file security properties and files permissions)

Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [**Access Control policy**] to provide [restrictive] default values for security attributes [**except for file security properties and file permissions**] that are used to enforce the SFP.

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

6.1.5.4 FMT_MSA.3 (2) Static attribute initialization (file security properties and files permissions)

Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [**Access Control policy**] to provide [restrictive] default values for security attributes [**associated with file security properties for CIFS or file permissions for NFS]** that are used to enforce the SFP.

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

6.1.5.5 FMT_MTD.1 Management of TSF Data

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [manage] the [**TSF data**] to the [**Admin Role**].

6.1.5.6 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.
Dependencies: No Dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [

- **User management:**
  - **Create, modify, delete local users.**
  - **Add, modify, remove external users. (External users are those that are defined in Active Directory).**
  - **Add, modify, remove external groups.**
- **Active Directory settings:**
  - **Join active directory domain**
  - **Leave active directory doman**
- **Audit logging:**
  - **Specify minimum retention period**
  - **Export audit logs**
- **Event logs**
  - **Export events**
  - **Delete events**
- **Email alerts**
  - **Enter SMTP server settings**
  - **Configure email alert recipients**
- **SNMPv3 configuration**

  - o **Configure SNMPv3 trapsink addresses**
  - o **Configure SNMPv3 users**
- **Ability to view SNMPv3 MIB objects**
- **Ability to review audit events and**
- **Ability to manage VTL, StoreOnce Catalyst and NAS resources].**

6.1.5.7 FMT_SMR.1 Security Roles

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles: [**admin, user, SNMPv3 user and NAS user**]

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Application Note: The NAS users only access NAS resources via CIFS or NFS. They cannot carry out TOE administrative tasks via SSH or HTTPS, while users for admin and user roles are administrative users and they may run TOE administrative tasks via SSH and HTTPS. SNMPv3 users can only view MIB objects.

6.1.6 Protection of the TSF (FPT)

6.1.6.1 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.
Dependencies: No Dependencies

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

6.1.7 TOE Access (FTA)

6.1.7.1 FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.
Dependencies: No Dependencies

FTA_SSL.3.1 The TSF shall terminate a **remote** interactive session after an [**administrator-defined interval of session inactivity**].

6.1.7.2 FTA_SSL.4 User-initiated termination

Hierarchical to: No other components.
Dependencies: No Dependencies

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

6.1.8 Trusted path/channels (FTP)

6.1.8.1 FTP_TRP.1 Trusted Path

Hierarchical to: No other components.
Dependencies: No Dependencies

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [**remote] administrators using HTTPS/TLS or SSH** 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 modification].

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

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [**all remote administrative actions**].

6.2 Dependency Rationale

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

Table 11 – Dependency Rationale

SFR	DEPENDENCY	Satisfaction of dependency
FAU_GEN.1	FPT_STM.1	Satisfied
FAU_GEN.2	FAU_GEN.1 and FIA_UID.1	Satisfied
FAU_SAR.1	FAU_GEN.1	Satisfied
FAU_SAR.3	FAU_SAR.1	Satisfied
FAU_STG.1	FAU_GEN.1	Satisfied
FAU_STG.4	FAU_STG.1	Satisfied
FCS_COP.1	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1), FCS_CKM.4	Satisfied: Although FCS_CKM.1 and FCS_CKM.4 are missing, Canadian Scheme Instruction #4 allows it.
FDP_ACC.2	FDP_ACF.1	Satisfied
FDP_ACF.1	FDP_ACC.1 and FMT_MSA.3	Satisfied
FDP_AVL_EXT.1(1)	None	None
FDP_AVL_EXT.1(2)	None	None
FDP_AVL_EXT.1(3)	None	None
FIA_ATD.1	None	None
FIA_UAU.1	FIA_UID.1	Satisfied
FIA_UAU.5	None	None

SFR	DEPENDENCY	Satisfaction of dependency
FIA_UAU.7	FIA_UAU.1	Satisfied
FIA_UID.2	None	None
FMT_MSA.1(1)	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	Satisfied
FMT_MSA.1(2)	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	Satisfied
FMT_MSA.3(1)	FMT_MSA.1 and FMT_SMR.1	Satisfied
FMT_MSA.3(2)	FMT_MSA.1 and FMT_SMR.1	Satisfied
FMT_MTD.1	FMT_SMR.1 and FMT_SMF.1	Satisfied
FMT_SMF.1	None	None
FMT_SMR.1	FIA_UID.1	Satisfied
FPT_STM.1	None	None
FTA_SSL.3	None	None
FTA_SSL.4	None	None
FTP_TRP.1	None	None

6.3 Security Functional Requirements Rationale

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives.

6.3.1 Security Functional Requirements Mapping

The following table provides a high level mapping of coverage for each security objective:

Table 12 – Mapping of SFR's to Objectives

SFR Mapped to Objectives	O.AVAILABILITY	O.LIMIT_ACCESS	O.PROTECTED_COMMUNICATIONS	O.SYSTEM_MONITORING	O.TOE_ADMINISTRATION
FAU_GEN.1				X	
FAU_GEN.2				X	

SFR Mapped to Objectives	O.AVAILABILITY	O.LIMIT_ACCESS	O.PROTECTED_COMMUNICATIONS	O.SYSTEM_MONITORING	O.TOE_ADMINISTRATION
FAU_SAR.1				X	
FAU_SAR.3				X	
FAU_STG.1				X	
FAU_STG.4				X	
FCS_COP.1			X		
FDP_ACC.2		X			
FDP_ACF.1		X			
FDP_AVL_EXT.1(1)	X				
FDP_AVL_EXT.1(2)	X				
FDP_AVL_EXT.1(3)	X				
FIA_ATD.1					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.1					X
FPT_STM.1				X	
FTA_SSL.3					X
FTA_SSL.4					X
FTP_TRP.1			X		

6.3.2 Security Functional Requirements Rationale

The following table provides detailed evidence of coverage for each security objective:

Table 13 - Security Functional Requirements Rationale

Security Objective	SFR	Rationale

O.AVAILABILITY	FDP_AVL_EXT.1(1)
	FDP_AVL_EXT.1(2)
	FDP_AVL_EXT.1(3)
		This TOE Security Objective is satisfied by ensuring that:
		• FDP_AVL_EXT.1(1): The TOE provides RAID functionality for physical disk drives used to store user data, thus allowing the TOE to continue operation following disk failures.
		• FDP_AVL_EXT.1(2): The TOE provides RAID functionality for physical disk drives used to store TSF data, thus allowing the TOE to continue operation following disk failures.
		• FDP_AVL_EXT.1(3): The TOE mechanisms to detect and continue operations when a single node within a cluster fails.

O.LIMIT_ACCESS	FDP_ACC.2 FDP_ACF.1	• FDP_ACC.2: The TOE is required to implement an access policy controlling all operations between attached hosts and virtual storage 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 storage.
O.PROTECTED_COMMUNICATIONS	FCS_COP.1 FTP_TRP.1	• FCS_COP.1: The TOE is required to implement FIPS-conformant ○ AES in support of cryptographic protocols. ○ RSA cryptographic digital signatures. ○ SHA-1 and SHA-256 in support of cryptographic protocols. ○ HMAC SHA-1 in support of cryptographic protocols. • FTP_TRP.1: The TOE is required to protect communication between itself and its administrators from disclosure and modification.
O.SYSTEM_MONITORING	FAU_GEN.1 FAU_GEN.2 FAU_SAR.1 FAU_SAR.3 FAU_STG.1 FAU_STG.4 FPT_STM.1	• 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.3: The TOE is required to provide functions to sort audit records to make their review more effective.

Security Objective	SFR	Rationale
		• 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.
O.TOE_ADMINISTRATION	FIA_ATD.1 FIA_UAU.1 FIA_UAU.5 FIA_UAU.7 FIA_UID.2 FMT_MSA.1 FMT_MSA.3 FMT_MTD.1 FMT_SMF.1 FMT_SMR.1 FTA_SSL.3 FTA_SSL.4	• 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. • FMT_MSA.1: The TOE is required to limit the ability to manage the security attributes except for file permissions to authorized administrators. The TOE allows the CIFS/NFS users to manage file permissions. • FMT_MSA.3: The TOE is required to implement default secure values (other than file permissions) and limit the management of default values (other than file permissions) to authorized administrators. The TOE allows the CIFS/NFS users to set restrictive defaults values for file permissions. • 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.1: The TOE is required to implement a minimum of the admin and user roles and can implement additional roles where necessary. There is implicitly additional types/roles of users:

Security Objective	SFR	Rationale
		NAS users which access CIFS/NFS shares and files and SNMPv3 users that can view networking information. NAS users can be configured by admin role. SNMPv3 users can be configured through the CLI by admin role. • FTA_SSL.3: The TOE is required to terminate a remote interactive session after an administrator-defined interval of session inactivity. • FTA_SSL.4: The TOE is required to allow user-initiated termination of the user's own interactive session.

6.4 Security Assurance Requirements

This section defines the Security Assurance Requirements (SARs) for the TOE. The assurance requirements are taken from EAL 2 components as specified in Part 3 of the CC and are augmented with ALC_FLR.2 requirements. The assurance components are summarized in the following table:

Table 14 – Security Assurance Requirements

CLASS	FAMILY	DESCRIPTION
ASE: Security Target	ASE_INT.1	ST Introduction
	ASE_CCL.1	Conformance Claims
	ASE_SPD.1	Security Problem Definition
	ASE_OBJ.2	Security Objectives
	ASE_ECD.1	Extended Components Definition
	ASE_REQ.2	Derived security requirements
	ASE_TSS.1	TOE Summary Specification
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: Lifecycle 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

CLASS	FAMILY	DESCRIPTION
	ATE_IND.2	Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

6.5 Security Assurance Requirements Rationale

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. No operations are applied to the assurance components.

EAL 2 augmented with ALC_FLR.2 was chosen to provide a low to moderate level of assurance that is consistent with standard commercial practices. The chosen assurance level is appropriate given the threats defined for the operational environment.

7 TOE SUMMARY SPECIFICATION

This section presents information to detail how the TOE meets the security functional requirements described in previous sections of this ST. The following security functions will be described:

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

7.1 Security Audit

The TOE includes a logging mechanism that gathers and displays information about events occurring within the TOE. The TOE generates audit records (i.e., messages) and places them into an Event Log. Messages written into the Event Log describe activity pertaining to the operation of the user data handling mechanisms and security features.

The configuration and event log data is stored on the RAID1+0 partition of each node in the cluster.

The following is a list of the events that cause audit records to these two sources.

- System Startup
- System Shutdown or Reboot
- Failed cryptographic operations during generation of random numbers for key generation
- TOE failure to encrypt or decrypt data
- TOE failure to generate a hash
- TOE failure to generate a keyed-has message authentication code
- Successful SSH session establishment
- SSH Session termination
- Successful and failed TLS session establishment
- TLS Session termination
- Changes to the RAID status for physical storage resources
- Failures of nodes within a couplet
- Creating and deleting VTLs, StoreOnce Catalyst stores and NAS shares
- Changing configuration data for VTLs, StoreOnce Catalyst stores and NAS shares
- All login activities

The information within an Event Log audit record includes the following:

- Date and time of the event,
- Severity Level,
- Message

The message indicates relevant information about the event such as outcome, subjects (e.g. client host identifier, user identifier) and physical node/disk/device causing the event.

The TOE stores audit records internally and provides access to that data only to the “Administrator” account and to the “Operator” account (see section 7.4 for information about these accounts). These accounts have the ability to view Event Log data through the graphical user interface (GUI). Using the GUI, these accounts can sort displayed data based on time and severity level. These accounts can also establish filters for the audit records displayed in the GUI using severity level and event ID.

The TOE does not offer GUI or CLI interfaces which allow for the modification of audit data. The entire Event Log can be completely cleared, or events from the previous N (i.e., Administrator specified number) days can be erased, but individual records cannot be changed.

The TOE stores audit records (Event Logs) in a round-robin fashion where the oldest records are overwritten as necessary. An administrator configures the amount of space that the TOE can allocate for the Event Log. The logs expand until all of the space has been allocated. Subsequent write operations to the logs overwrite the oldest records as necessary. Thus, the audit space allocated to each type of log or file becomes full and remains perpetually full. The amount of space available for audit records is limited by the amount of space the administrator chooses to dedicate to log records.

The Security audit function is designed to satisfy the following security functional requirements: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.3, FAU_STG.1, FAU_STG.4

7.2 Cryptographic Support

The TOE uses cryptography for protection of the communications surrounding remote administrator sessions. A remote administrative session can occur using either a GUI or CLI. Administrators use an SSHv2 session to connect to the TOE to establish a CLI session. Administrators connect to the TOE using the GUI through a TLS session. All protocols involved in support of the administrative GUI are tunneled through TLS.

TLS and SSH are used to provide protection of the communications surrounding the remote administrative sessions from disclosure and from modification.

The TOE provides cryptographic support for communications on the manageability path using unmodified versions of OpenJDK for the HTTPS protocol and OpenSSH for the SSH protocol. 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).

The TOE implements the AES algorithm as defined by FIPS PUB 197 and consistent with NISP SP 800-38A. The TOE uses AES for encryption and decryption of data as part of the support for the SSH and TLS protocols. The TOE can use AES in CBC or CTR modes. The TOE supports the use of 128-bit, 192-bit and 256-bit AES keys.

The TOE also provides cryptographic hashing services using the SHA-1 and SHA-256 algorithms as defined by FIPS 180-3 ‘Secure Hash Standard’. The TOE supports message digest sizes of 160-bits and 256 bits for this hashing service. These cryptographic hashing services are used by the TOE implementation of SSHv2 and TLS.

The TOE provides keyed-hash authentication using HMAC-SHA-1 with a keys size of 160-bits. The TOE implementation of HMAC-SHA-1 is built to meet FIPS Pub 198-1 and FIPS Pub 180-3. These crypto keyed-hash authentication services are used by the TOE implementation of SSHv2 and TLS.

The TOE implements HTTPS as specified by RFC 2818. The TOE does not support HTTP connections for administration. The TOE implements TLS versions using the following cipher suites:

Table 15 - Cypher Suites

Protocols	Ciphers
TLSv1.0	TLS_RSA_WITH_AES_128_CBC_SHA
	TLS_RSA_WITH_AES_256_CBC_SHA
TLSv1.1	TLS_RSA_WITH_AES_128_CBC_SHA
	TLS_RSA_WITH_AES_256_CBC_SHA
TLSv1.2	TLS_RSA_WITH_AES_128_CBC_SHA
	TLS_RSA_WITH_AES_128_CBC_SHA256
	TLS_RSA_WITH_AES_256_CBC_SHA
	TLS_RSA_WITH_AES_256_CBC_SHA256

The Cryptographic support function is designed to satisfy the following security functional requirements: FCS_COP.1

7.3 User data protection

The TOE implements NAS, StoreOnce Catalyst and VTLs as storage locations. The TOE makes storage locations available to client hosts on Ethernet (i.e. Ethernet hosts) and Fibre Channel (i.e. Fibre Channel hosts). These storage locations can be a Virtual Tape Library (VTL), Catalyst Store or Network Attached Storage (NAS). The VTLs can be accessed either through Fibre Channel protocol. The NAS can be accessed as either CIFS-based storage devices or NFS-based storage devices.

Thus, the TOE makes NAS, Catalyst Stores and VTL storage accessible via NFS, CIFS, and Fibre Channel connections and protocols. The TOE provides NAS, Catalyst Stores and VTL storage access only to network devices and users specifically configured to have access. The TOE implements an access policy whereby client-hosts can access configured NAS, Catalyst Stores and VTL resources.

- **Fibre Channel-based VTLs** are configured to specify access by a specific Fibre Channel port.

  For client hosts on a Fibre channel network that are accessing VTLs, the VTL must be configured to include the Fibre Channel port used by the client host.

- **NFS-based NAS** are configured to specify access by a specific list of hosts.

  A NAS configured for NFS access can be accessed only by an Ethernet client host. The host identifier (i.e., IP Address or DNS name) must be included in the TOE's configuration of the NFS share in order for access to be permitted. Each client host can have “Read/Write Access”, “Read-Only Access” or “No Access” to the NFS share.

- **CIFS-based NAS** are configured to specify access by specific users who are assigned read-write or read-only access.

  A NAS configured for CIFS-based access can be accessed by specific users. The following are the three (3) types of access configuration for CIFS shares:

  - **None**: no access control, the share is accessible to anyone;

  - **User**: Users are created on the TOE. Each user that is created has its own user ID and password. Access by a user to each CIFS share can be controlled, the access modes being “Access” & “No Access”
  - **Active Directory**: The TOE is registered with the AD server as a device within the domain, just like another server in the domain. The TOE does not create users in the Active Directory nor assign permission (read-write, read only or no access) to access the CIFS share. Users and permissions are assigned directly with the AD server, not through the TOE.
- **StoreOnce Catalyst stores:** A list of clients is created in the GUI under the StoreOnce Catalyst tab and only these clients can be allowed to create StoreOnce Catalyst stores and access them.

Access to files under CIFS/NFS shares is further controlled based on file permissions.

Client hosts are attached through dedicated storage area networks (SANs) that are generally in close proximity and therefore subject to the same physical protection assumption as the HPE StoreOnce system. Client hosts should be placed on a restricted network segment. While difficult, access by untrustworthy entities, or hosts, could lead to the spoofing on these network segments. This could result in unintended access to backup targets by those untrustworthy entities. It is therefore assumed that administrators allow only trusted hosts access to these connections and that the hosts themselves are protected from access by untrustworthy entities.

The TOE implements RAID on physical disks. The TOE supports RAID 6 and RAID 1+0.

- **RAID 6**: may be thought of as RAID5 with dual parity. The dual parity of RAID6 provides fault tolerance from two drive failures in each of two RAID sets. Each array continues to operate with up to two failed drives. RAID6 significantly reduces the risk of data loss if a second hard disk drive fails while the RAID array is rebuilding.
- **RAID 1+0**: provides mirrored sets in a striped set (minimum four drives; even number of drives). RAID 1+0 provides fault tolerance and improved performance but increases complexity.

The HPE StoreOnce Series system uses RAID 6 storage devices. RAID 6 provides protection against double disk failures and failures while a single disk is rebuilding. This means that one disk can fail within each pool or 6–disk array and the system will continue to function correctly. Once the failed disk is replaced, the RAID rebuilds automatically.

Server nodes: two disks in each node mirror each other. If one fails, the system will continue to function correctly. The failed disk should be replaced as soon as possible. The presence of a replacement disk invokes the Smart Array Automatic Data Recovery (ADR) feature to rebuild the replaced drive.

Disk enclosures: the HPE StoreOnce 6500 system has two disk enclosures with base storage of 11 disks for user data + 4 hot spare disks. Up to five Capacity Expansion kits may be added to the disks in each disk enclosure to increase the backup data capacity, also RAID 6. These disks are configured in RAID 6 pools, such that two disks per pool can be lost without loss of backup data.

TSF data is stored by a multi-node appliance (i.e., a couplet) as a mirrored set in a stripped set (i.e., RAID 1+0).

StoreOnce implements RAID 1+0 for root filesystem storage, therefore the disk drives are mirrored.

The multi-node architecture supports up to four couplets of nodes in a cluster. Each cluster portrays a single management interface and one data interface per node. When a node in a couplet fails, the lost physical data interface is virtualized by the other node. Virtualization can occur for either an Ethernet or Fibre Channel interface. When both nodes of a couplet fail, the data within that couplet is unavailable to users. Each time the active management node fails, reboots or is put in to a maintenance mode for repairs, a negotiation occurs between all remaining nodes in the cluster to elect a new active management node.

The TOE clears resources when they are initially introduced (e.g., a new disk volume). When a VTL resource is assigned, the resource is treated as a tape and an End-of-Tape mark is written by the TOE to the beginning of the resource. The TOE does not allow reading past this End-of-Tape mark. Storage is assigned to a VTL resource only as needed (the entire tape is NOT preallocated). When a NAS resource is assigned no storage is associated with the resource until a write operation is performed.

The TOE performs data deduplication at the block level on all backup resources. Data deduplication is a process in which the TOE compares blocks of data being written to a backup device with data blocks previously stored on the device. If duplicate data is found, a pointer is established to the original data, rather than storing the duplicate data.

When data is deleted by the TOE (e.g. a VTL cartridge is overwritten or erased), any unique blocks are marked for removal, any non-unique blocks are de-referenced and their reference count decremented. The process of removing blocks of data is not an inline operation because this would significantly impact performance. This process, termed “housekeeping”, runs on the appliance as a background operation, it runs on a per VTL cartridge and NAS file or StoreOnce Catalyst object basis and will run as soon as the VTL cartridge is unloaded and returned to its storage slot or a NAS file or StoreOnce Catalyst object has completed writing and has been closed by the appliance.

The User data protection function is designed to satisfy the following security functional requirements: FDP_ACC.2, FDP_ACF.1, FDP_AVL_EXT.1(1), FDP_AVL_EXT.1(2), FDP_AVL_EXT.1(3)

7.4 Identification and Authentication

The TOE supports different user communities: administrative accounts and CIFS users.

For administrative accounts, the TOE recognizes two accounts as being permitted to perform administrative operations (i.e., the administrative accounts) and a restricted “root” account. The two administrative accounts are the “Administrator” and the "Operator" accounts. A site (i.e., a customer installing the product) is expected to assign the two administrative accounts in a manner suitable for the customer’s needs. Each account has associated with it a password for authentication. The TOE verifies this authentication information before the TOE allows the user to perform any actions. The TOE also recognizes a “root” account that can login only at the local console. This account is not used for normal administrative activity, but instead is provided only for special maintenance operations (e.g., resetting password of the “administrator” account). The "root" account is not shared with end users.

The GUI and local CLI connections require the use of a password as the authentication information. A remote administrative session using SSH to connect to a CLI session can authenticate using either cryptographically with a public/private key pair exchange or using a password. Regardless the authentication information the TOE does not provide any CLI or GUI services until the authentication information has been verified for the account.

The “Administrator” account is a read-write account that has the ability to handle configuration and has predominantly full control over the CLI and GUI commands. The TOE also supports the "operator" account, which is read-only and provides a more limited CLI and GUI functionality. Both the "Administrator" and "Operator" accounts typically do not have access to any of the user data.

For locally defined administrative accounts, the information that the TOE stores about each user is maintained in an internal shadow password file. The TOE does not offer general purpose shells to administrative users, but rather starts the CLI following successful login. The TOE maintains the following information about each locally defined administrative account.

- UID – A TOE internal user identifier that uniquely designates the user account within the system.
- Username – An identifier allowing a person to identify themselves to the TOE.
- Password – A hashed value known only to the TOE and the user.

Administrators must login either through the GUI or CLI prior to having the ability to perform any TOE management operations. The login process occurs slightly differently at the GUI than the CLI. The following occurs during a password-based login at either at the local console or through an SSH session:

- the TOE prompts the user for username,
- the user provides a username,
- the TOE prompts for a password,
- the user provides a password, and
- the TOE validates that the username and password provided by the user are a valid pair.

During logon at the GUI, the following occurs:

- the TOE offers a logon window requesting a username and password,
- the user provides both a username and password to the TOE, and
- the TOE validates that the username and password provided by the user are a valid pair.

In these cases, no management operations are provided to a user prior to their providing a valid username and password pair. Also, when a user is providing a password at a local console, an SSH or GUI Session, the TOE does not echo that password to the screen.

During a public-key based authentication using SSH, the user's private key is used by the SSH client to cryptographically authenticate to the TOE's SSH server. If the TOE and SSH client can successfully negotiate and establish an SSH session using the public/private key of the user, then the user's identity is authenticated and the TOE starts a CLI session using the authenticated SSH tunnel.

The TOE supports access controls based upon a user's identity during client host operations upon Common Internet File System (CIFS) storage objects. A NAS configured as a CIFS share can be accessed by users that are defined either locally within the TOE or remotely using an external Active Directory (AD) server. However, these users do not have access to any TOE management tasks. The AD authentication can be supported over a remote, secure connection using TLS. The Active Directory server is provided by the environment.

For authentication of a user accessing a CIFS share, the TOE collects a user ID & Password from the user. If the share is configured to use local authentication, the TOE verifies the user ID & password. If the share is configured to use Active Directory authentication, the TOE passes the ID & Password to the AD server for verification. The TOE then permits or denies permission to the CIFS-share based upon the permissions configured for that user.

The Management Interface includes an SNMP v3 Agent. SNMPv3 users must successfully authenticate to the SNMPv3 agent in the TOE prior to viewing MIB objects. The SNMPv3 users can be created through the SSH channel using the CLI interface.

The Identification and authentication function is designed to satisfy the following security functional requirements: FIA_ATD.1, FIA_UAU.1, FIA_UAU.5, FIA_UAU.7, FIA_UID.2

7.5 Security Management

The TOE restricts the management of storage resources to the administrative accounts: “Administrator” and “Operator”. The “Operator” account can query, but cannot change any settings. The TOE restricts management of storage resources to the “Administrator” account which has read/write access.

The nodes within a cluster cooperate to provide backup storage services to client hosts. In multi-node systems, the TOE replicates configuration data across all nodes in the cluster. This keeps configuration data available to operational nodes despite the failure of one node in each couplet. Single-node appliances operate as standalone systems and thus do not replicate configuration data.

The HPE StoreOnce system products do not support an explicit notion of default values, rather by implicit default when a new resource becomes available no access is possible until it is specifically configured (i.e., to be accessible by a FC host) at which time explicit access rights (i.e., read-write, read-only, or none) to a host are also defined.

The HPE StoreOnce system products offer a full range of management functions. Through the GUI and CLI the TOE offers the ability to perform the following actions.

- User management:
  - Create, modify, delete local users.
  - Add, modify, remove external users. (External users are those that are defined in Active Directory).
  - Add, modify, remove external groups.
- Active Directory settings:
  - Join active directory domain
  - Leave active directory doman
- Audit logging:
  - Specify minimum retention period
  - Export audit logs
- Event logs
  - Export events
  - Delete events
- Email alerts
  - Enter SMTP server settings
  - Configure email alert recipients
- SNMPv3 configuration
  - Configure SNMPv3 users
  - Configure SNMPv3 trapsink addresses
- Ability to view SNMPv3 MIB objects
- Ability to review audit events and
- Ability to manage VTL, StoreOnce Catalyst and NAS resources.

The Security management function is designed to satisfy the following security functional requirements: FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1

7.6 Protection of the TSF

The TOE uses an internal hardware clock within each node as the source for timestamps when generating audit records. Each node of a cluster operates as an NTP client obtaining its time from the Active Manager which is running an NTP server available only to other nodes. The Active Manager can be configured to synchronize time (i.e., be an NTP client) to other connected hosts using NTP. The Active Manager can also obtain time using NTP from an external NTP server on the Management network.

The Protection of the TSF function is designed to satisfy the following security functional requirements: FPT_STM.1

7.7 TOE Access

The TOE allows only one (1) active session for each account. The TOE monitors for inactivity at the GUI and CLI interfaces. By default, after a period of 20 minutes of user inactivity the session will time out and return to the Login screen.

Administrators can log out of their individual sessions, thereby terminating the session.

The TOE Access function is designed to satisfy the following security functional requirements: FTA_SSL.3, FTA_SSL.4

7.8 Trusted path/channels

A remote administrative session can occur using either a graphical user interface (GUI) or command-line interface (CLI). Administrators use an SSHv2 session to connect to the TOE to establish a CLI session. An administrative GUI is provided through the HTTPS protocol using TLS.

TLS and SSHv2 are used to provide protection of the communications surrounding the remote administrative sessions from disclosure and from modification. This functionality is provided by default by the industry standard OpenSSL and OpenSSH packages that installed on the TOE. Protection from disclosure and modification is inherent with the TLS and SSH protocols.

Using public-key cryptography with the TLS and SSHv2 protocols, the TOE identifies itself to clients. Under SSH, the TOE’s public key must be known to the client prior to the communications (this must be done out-of-band).

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

The Trusted path/channels function is designed to satisfy the following security functional requirements: FTP_TRP.1

8 ACRONYMS

Table 16 – Acronym

Acronym	Definition
AD	Active Directory
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CC	Common Criteria
CEM	Common Evaluation Methodology
CIFS	Common Internet File System
FC	Fibre Channel
FIPS	Federal Information Processing Standard
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MIB	Management Interface Base
NAS	Network Attached Storage
NFS	Network File System
NTP	Network Time Protocol
PP	Protection Profile
SAN	Storage Area Network
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TLS	Transport Layer Security
TSF	TOE Security Functionality
VTL	Virtual Tape Library