HP StoreOnce Backup System Generation 3 Version 3.6.6 Security Target

Version 1.0
February 12, 2014

Prepared for:
Hewlett-Packard

Long Down Avenue
Stoke Gifford
Bristol BS34 8QZ
UK

Prepared By:
Leidos

Common Criteria Testing Laboratory

6841 Benjamin Franklin Drive
Columbia, MD 21046
USA

TABLE OF CONTENTS

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 HP StoreOnce Backup System, Generation 3 Version 3.6.6 provided by Hewlett-Packard.

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

The Security Target contains the following additional sections:

- TOE Description (Section 2)
- Security Problem Definition (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 – HP StoreOnce Backup System, Generation 3 Version 3.6.6 Security Target

ST Version – Version 0.7

ST Date – December 24, 2013

TOE Identification – HP StoreOnce Backup System, Generation 3 Version 3.6.6

Hardware Models

Single Node Appliances	Multi-Node Appliances
HP StoreOnce 2610 iSCSI Backup HP StoreOnce 2620 iSCSI Backup HP StoreOnce 4210 iSCSI Backup HP StoreOnce 4210 FC Backup HP StoreOnce 4220 Backup HP StoreOnce 4420 Backup HP StoreOnce 4430 Backup	HP StoreOnce B6200 Backup System

TOE Developer – Hewlett-Packard

Evaluation Sponsor – Hewlett-Packard

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1 Revision 3, July 2009.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 3, July 2009.
    - Part 3 Conformant
    - Assurance Level: EAL 2 augmented with ALC_FLR.3

1.3 Conventions

The following conventions have been applied in this document:

Security Functional Requirements – Part 2 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 letter placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.

Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).

Selection: allows the specification of one or more elements from a list. Selections are indicated using bold 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 …").

Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.4 Glossary

Acronym	Description
AD	Active Directory
CC	Common Criteria
CHAP	Challenge-Handshake Authentication Protocol
CIFS	Common Internet File System
FC	Fibre Channel
HP	Hewlett-Packard
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
iSCSI	Internet Small Computer System Interface
IQN	iSCSI Qualified Name
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
NAS	Network Attached Storage
NFS	Network File System
NTP	Network Time Protocol
SAN	Storage Area Network
SNMP	Simple Network Management Protocol
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function

VTL	Virtual Tape Library

2 TOE Description

The Target of Evaluation (TOE) is an HP StoreOnce Backup System system with one or more hardware appliances. The TOE models that offer either a single-node or multi-node system and are running Generation 3 Version 3.6.6 software are the target of evaluation. The following appliances allow the TOE to provide varying types of fault-tolerance and are the hardware platform for the TOE.

- HP StoreOnce B6200
- HP StoreOnce 2610 iSCSI Backup
- HP StoreOnce 2620 iSCSI Backup
- HP StoreOnce 4210 iSCSI Backup
- HP StoreOnce 4210 FC Backup
- HP StoreOnce 4220 Backup
- HP StoreOnce 4420 Backup

HP StoreOnce Single-node appliances operate as standalone devices and do not operate as part of a cluster.

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 B6200 appliance is a multi-node appliance. The number of nodes in a model B6200 is determined by the customer. The B6200 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.

2.1 TOE Overview

The HP StoreOnce Backup System is a disk-based storage appliance for backing up host network servers or PCs 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 total number of backup targets offered by an HP StoreOnce Backup System is split between VTL, NAS and StoreOnce Catalyst devices. The number of supported backup targets varies according to model (for single-node appliances) or number of nodes (for clusters). Each node in a cluster is capable of supporting 48 target devices. So as examples, a couplet can support 96 backup targets, while an 8 node (4 couplet) B6200 can support 384 (i.e., 48 x 8) backup targets. These devices may be all VTL, all NAS, or any combination of StoreOnce Catalyst, NAS and VTL devices. The HP StoreOnce Backup 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 HP StoreOnce Backup 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.

A single node appliance or a couplet provides network access using a number of network distinct ports. There are four (4) physical 1GB ports and two (2) physical 10GB ports for Ethernet connections. Another two (2) 10GB network connections are used for the internal network (internal to the cluster only) and not accessible to client-hosts.

Fibre Channel connections (available on some appliances) are only used to present VTL devices that have been configured on the nodes in a couplet.

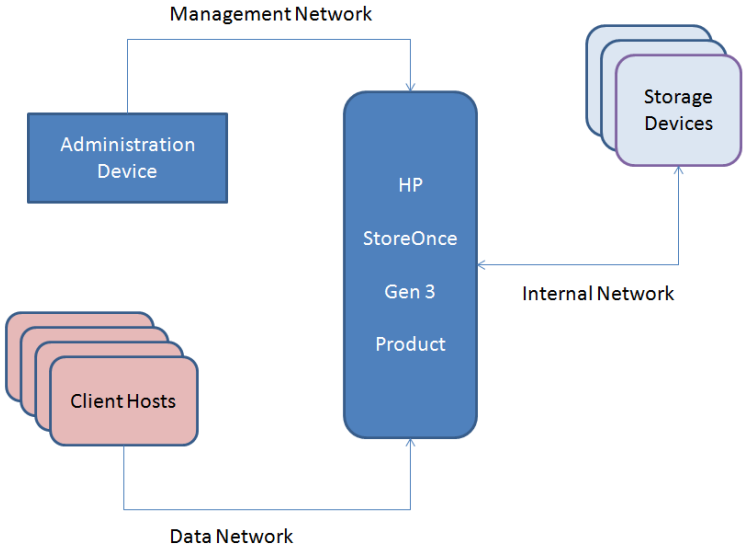

Figure 1 Supported Network Separation

Figure 1 presents a high level depiction of one possible network topology supported by the HP StoreOnce Generation 3 product. Shown in Figure 1 are 3 distinct networks: 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 and storage devices (e.g., a SAN storage device).

Remote administration sessions occurring through the management network are protected using cryptography (SH and HTTPS). Network traffic between the product and NTP or LDAP servers occurs utilizing only protections inherent in the NTP and LDAP protocols. The HP StoreOnce Backup System allows a site to choose to combine the data and management networks. In single-node configurations, the data and management network must be combined. Both single-node and multi-node configurations utilize an Internal network for communication with storage devices. The configuration shown in Figure 1 represents a multi-node configuration.

The HP StoreOnce Backup Systems provides Ethernet network connections for use as a management network (i.e., used for all management traffic). All Ethernet-based networks support only IPv4 networking functionality. IPSec and IPv6 security features are not available, though some protection is supported for administrator network communications (e.g., SSH and HTTPS). The data network can be either Ethernet or Fibre Channel. The internal network will be Ethernet.

The HP StoreOnce Backup Systems include hardware-based RAID 5 or RAID 6 to reduce the risk of user data loss due to disk failure within a couplet.

2.2 TOE Architecture

The HP StoreOnce Backup System product line is available in single-node or multi-node configurations. The Gen 3 architecture of a multi-node configuration is depicted in Figure 2. A single-node configuration would be identical to the architecture of a single node as shown in Figure 2. 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. Single-node configurations support availability of data through the support of RAID levels to protect user and TSF data store within the control of the TOE.

Figure 2 depicts a cluster composed of two couplets. Each couplet includes two nodes. This is an example of a multi-node StoreOnce configuration.

From the perspective of shared configuration data (i.e., TOE Data), there are two significant types of data depicted in Figure 2. The storage of TOE Security Function data is depicted by the box labeled “Fusion Manager Store”. This store of data is accessible to all of the nodes in the cluster. The second type of configuration data is labeled as “Ibrix FS” with N sets of node configuration data. This data is available within a couplet even after one node of that couplet fails.

The multi-node architecture includes distinct physical network ports that are used to isolate node-to-node communications from client-data backup operations. The ability to isolate internal TOE communications (which is not encrypted) to a dedicated network strengthens protection of TSF data. Administrative communication is cryptographically protected using SSHv2 and HTTPS/TLSv1.0. While the administrative communication would occur on the same network as client-data backup operations, they are protected cryptographically. The middle and lower end model single-node configuration, there would be no need for node-to-node communications, so no dedicated network would be employed. In a high end single node product, there is an internal network between the node and the storage devices.

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 single-node architecture makes use of RAID to provide availability of data stored by a node. In multi-node configurations, 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.

Deduplication (a.k.a., deduping), allows data to be stored only once. When the same data occurs multiple times (as in the backup of data that has not changed) it is handled by reference as opposed to storing multiple copies. Remote copy (i.e., site replication) basically allows all the data to be copied to another cluster and makes use of the same deduping technology.

Remote administrator sessions are encrypted using SSHv2 or HTTPS/TLS. SNMPv2 is also supported. Internal cluster and client-host connections are not encrypted by the TOE.

A cluster can be configured to use NTP to synchronize time with an external server. When so configured, one node in the cluster becomes an NTP server. This NTP server node connects (as a client) to an external NTP server to obtain a time value from that external entity. The NTP server node then acts as a server to each of the other nodes within the cluster which are acting as NTP clients to the one node designated as the NTP server within the cluster.

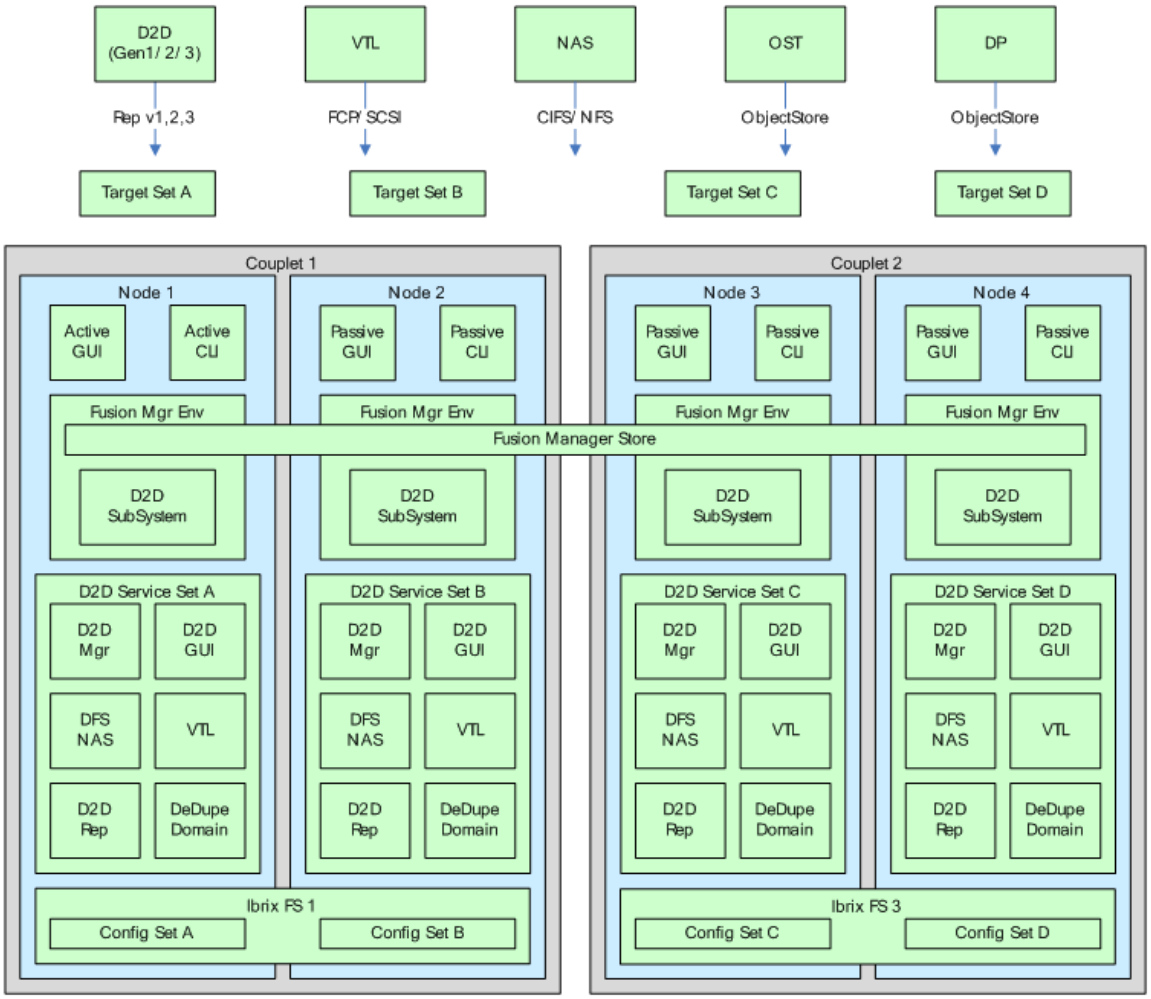

Figure 2 StoreOnce MultiNode Service Architecture

2.2.1 TOE Physical Boundaries

The physical boundary of a HP StoreOnce Backup System is the physical boundary of the hardware of the cluster. Interfaces to this hardware include the following:

- a per-node serial port which provides limited administrative access,
- Fibre Channel ports for Fibre Channel host access to the data network,
- Four (4) Ethernet connections for iSCSI host access to the data network,
- Two (2) Ethernet connections for administrative device access to the management network, and
- two (2) Ethernet connections used for an internal network.

The TOE can be configured to rely on and utilize a number of other components in its operational environment.

- Active Directory servers – The HP StoreOnce Backup System can be configured to utilize Active Directory as an external authentication server.
- Network Time Protocol (NTP) server – The HP StoreOnce Backup System can be configured to act as an NTP client to synchronize the internal clock of the active node with an external source. The product can also be configured to offer NTP server functionality to each individual node in a cluster, to synchronize the clocks within the cluster.

- iSCSI and Fibre Channel client hosts – The HP StoreOnce Backup System attaches to applicable ports which access available storage resources (SANs and VTLs).
- Network Storage Devices – The HP StoreOnce Backup System is typically connected to a storage controller that manages the actual physical storage.

Figure 1 depicts three networks to which the HP StoreOnce Backup System nodes (couplets) may be attached. The TOE nodes, storage devices, and internal network must have physical protections that are consistent with the data being stored and transmitted. This internal network is expected to be dedicated such that communication between the TOE and either another TOE node or a storage device is not modified or disclosed.

The management network is expected to provide connectivity for the TOE, administrative devices, and NTP servers. Active directory servers are accessed from the data network to manage NAS share permissions. Active Directory servers can be deployed with or without cryptographic protections depending on the needs of the operational environment. While physical security of this network is appropriate, TOE remote administrative sessions are protected from disclosure and modification using SSH and HTTPS/TLS,
The data network is used by clients to send data to the TOE for backup purposes. The data network is also expected to provide physical protections that are consistent with the data being stored and transmitted. Network devices on the Ethernet SAN are expected not to intercept, impersonate or otherwise modify communications on the SAN

2.2.2 TOE Logical Boundaries

The HP StoreOnce Backup System includes a number of security features with claims in the security functional requirements of this Security Target (Section 5.2). The HP StoreOnce Backup system also includes features such as deduplication and replication which can be used but for which this Security Target contains no claims (i.e., no security functional requirements). The following sections summarize security functionality of the product.

2.2.2.1 Security Audit

The HP StoreOnce Backup 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.

2.2.2.2 Cryptographic Support

The HP StoreOnce Backup System currently includes cryptographic functions to support SSHv2 and HTTPS (using TLS) protection for communication with remote administrative sessions. Connections to the HP StoreOnce Backup System can be made through SSHv2 to support a Command Line Interface for an administrator. Connections to the HP StoreOnce Backup System utilize HTTPS/TLS to support a graphical user interface for an administrator.

2.2.2.3 User data protection

The HP StoreOnce Backup 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 iSCSI, CIFS or NFS, Ethernet and Fibre Channel.

- iSCSI VTL – The product permits access based upon assigned hosts using its iSCSI Qualified Name (IQN).
- 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.

The TOE implements RAID on physical disks. The single-node architecture makes use of RAID 5 or RAID 6 to provide availability of user data stored by a node. 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.

TSF data stored by a single-node appliance is protected only using the RAID array within the appliance. 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 SNMP or SMTP. Failures of one node within a couplet also generate an alert via SNMP or SMTP[1].

2.2.2.4 Identification & Authentication

The HP StoreOnce Backup System requires that administrators must login with username and password prior to being able to access functions associated with their defined role. The HP StoreOnce Backup System uses only locally defined accounts to define the "Administrator" and "Operator" accounts.

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

Fibre Channel (FC), iSCSI, and NFS hosts are always identified when they access backup targets, but are not usually authenticated.

Fibre Channel hosts are identified using a Fibre Channel port prior to the TOE granting access to a backup target over a FC network (i.e., part of the "Data network" shown in Figure 1).

An iSCSI host is identified using an iSCSI qualified name (IQN). Since the TOE supports CHAP authentication for iSCSI, a site can choose to use CHAP to authenticate iSCSI hosts. Use of CHAP for authentication is suggested but not required to satisfy the claims in this Security Target.

2.2.2.5 NFS hosts are identified solely using their IP address. Security Management

The HP StoreOnce Backup System is responsible for enabling the management of available storage resources and access by client-hosts. Users 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).

The HP StoreOnce Backup System also supports a read-only SNMPv2 interface to allow network monitoring of a running system.

2.2.2.6 Protection of the TSF

The HP StoreOnce Backup System includes a real-time clock. It also protects especially sensitive security data such as password and cryptographic keys.

2.2.2.7 TOE Access

The HP StoreOnce Backup System can terminate an inactive remote administrative session after an administrator-defined period of inactivity.

2.2.2.8 Trusted Paths/Channels

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

2.3 TOE Documentation

The HP StoreOnce Backup 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[2]:

1) HP StoreOnce Backup System Concepts Guide, September 2011.
2) HP StoreOnce Backup System User Guide, November 2012.

[1] Since single-node appliances are not part of a couplet or cluster, such failures do not generate alarms.
[2] The documents listed here are those available with the version of the product shipping today.

3) HP StoreOnce Backup System Installation and Configuration Guide, December 2012.

3 Security Problem Definition

This section describes the security environment in which the TOE operates. The security environment is defined in terms of assumptions made by the TOE and threats to the TOE.

3.1 Assumptions

The following conditions are assumed to exist in the operational environment.

Assumption	Definition
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.
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.
A.MGMT_NET	It is assumed that a dedicated and protect “Management Network” exists between nodes of the TOE and hosts providing supporting services (e.g., AD and NTP).
A.DATA_NET	Clients on the “Data Network” do not have direct access to the Internal or Management networks that are used for managing, accessing, and supporting the TOE operations.
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.

3.2 Threats

Threat	Definition
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.

4 Security Objectives

This chapter identifies the security objectives of the TOE and its environment. Security objectives identify the responsibilities of the TOE and the support need by the TOE from its environment.

4.1 Security Objectives for the TOE

Objective	Definition
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 Environment

Objective	Definition
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.
OE.HOST_IDENTITY	iSCSI hosts correctly reflect the iSCSI identifier associated with their Host Bus Adapters (HBAs).
OE.MGMT_NET	A dedicated “Management network” provides reliable ad secured communication between the TOE, hosts supporting remote administrative sessions and peer hosts providing supporting services such as Active Directory or NTP.
OE.DATA_NET	Clients on the “Data Network” do not have direct access to the Internal or Management networks that are used for managing, accessing, and supporting the TOE operations.
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.

5 IT Security Requirements

The security requirements for the TOE have been drawn from Parts 2 and 3 of the Common Criteria. The security functional requirements have been selected to correspond to the actual security functions implemented by the TOE while the assurance requirements have been selected to offer a low to moderate degree of assurance that those security functions are properly realized.

5.1 Extended Component Definition

This Security Target includes Security Functional Requirements (SFR) that are not drawn from CC Part 2. These Extended SFRs are identified by having a label '_EXT' after the requirement name for TOE SFRs. The structure of the extended SFRs is modeled after the SFRs included in CC Part 2. The structure is as follows:

A. Class – The extended SFRs included in this ST are part of the identified classes of requirements.

B. Family – The extended SFRs included in this ST are part of several SFR families including the new families defined below.

C. Component – The extended SFRs are not hierarchical to any other components, though they may have identifiers terminating on other than "1". The dependencies for each extended component are identified in the TOE SFR Dependencies section of this ST (Section 8.4, Requirement Dependency Rationale).

5.1.1 Extended Family Definitions

5.1.1.1 FCS_COMM_PROT_EXT

Family Behavior

This family identifies the protocols used to protection remote administrative sessions.

Management: FCS_COMM_PROT_EXT.1

There are no management activities foreseen.

Audit: FCS_COMM_PROT_EXT.1

There are no auditable events foreseen.

5.1.1.1.1 FCS_COMM_PROT_EXT.1 Remote Administrative Session Communication Protection

Hierarchical to: No other components.

Dependencies: None

FCS_COMM_PROT_EXT.1.1 The TSF shall protect remote administrative session communications using [selection: IPsec, SSH] and [selection: TLS/HTTPS, no other protocol].

5.1.1.2 FCS_HTTPS_EXT

Family Behavior

This family identifies the behavior of the TOE when the HTTPS protocol is implemented.

Management: FCS_HTTPS_EXT.1

There are no management activities foreseen.

Audit: FCS_SSH_EXT.1

Basic Level:

- Failure to establish an HTTPS Session
- Establishment/Termination of an HTTPS session

5.1.1.2.1 FCS_HTTPS_EXT.1 – Secure Shell Protocol

Hierarchical to: No other components.

Dependencies: FCS_TLS_EXT.1

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

5.1.1.3 FCS_SSH_EXT

Family Behavior

This family identifies the behavior of the TOE when the Secure Shell (SSH) protocol is implemented.

Management: FCS_SSH_EXT.1

There are no management activities foreseen.

Audit: FCS_SSH_EXT.1

Basic Level:

- Failure to establish an SSH Session
- Establishment/Termination of an SSH session

5.1.1.3.1 FCS_SSH_EXT.1 – Secure Shell Protocol

Hierarchical to: No other components.

Dependencies: FCS_COP.1

FCS_SSH_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, and 4254.

FCS_SSH_EXT.1.2 The TSF shall ensure that the SSH connection be rekeyed after no more than 228 packets have been transmitted using that key.

FCS_SSH_EXT.1.3 The TSF shall ensure that the SSH protocol implements a timeout period for authentication as defined in RFC 4252 of [assignment: timeout period], and provide a limit to the number of failed authentication attempts a client may perform in a single session to [assignment: maximum number of attempts] attempts.

FCS_SSH_EXT.1.4 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.

FCS_SSH_EXT.1.5 The TSF shall ensure that, as described in RFC 4253, packets greater than [assignment: number of bytes] bytes in an SSH transport connection are dropped.

FCS_SSH_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-256, [selection: AEAD_AES_128_GCM, AEAD_AES_256_GCM, no other algorithms].

FCS_SSH_EXT.1.7 The TSF shall ensure that the SSH transport implementation uses SSH_RSA and [selection: PGP-SIGN-RSA, PGP-SIGN-DSS, no other public key algorithms,] as its public key algorithm(s).

FCS_SSH_EXT.1.8 The TSF shall ensure that data integrity algorithms used in SSH transport connection is [selection: hmac-sha1, hmac-sha1-96, hmac-md5, hmac-md5-96].

FCS_SSH_EXT.1.9 The TSF shall ensure that diffie-hellman-group14-sha1 is the only allowed key exchange method used for the SSH protocol.

5.1.1.4 FCS_TLS_EXT

Family Behavior

This family identifies the behavior of the TOE when the Transport Layer Transport Layer Security (TLS) protocol is implemented.

Management: FCS_TLS_EXT.1

There are no management activities foreseen.

Audit: FCS_TLS_EXT.1

Basic Level:

- Failure to establish an TLS Session
- Establishment/Termination of an TLS session

5.1.1.4.1 FCS_TLS_EXT.1 – Transport Layer Security Protocol

Hierarchical to: No other components.

Dependencies: FCS_COP.1

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [selection: TLS 1.0 (RFC 2346), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)] supporting the following ciphersuites:

Mandatory Ciphersuites:
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
Optional Ciphersuites:
[selection:
None
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_ SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
].

5.1.1.5 FPT_PTD_EXT

Family Behavior

This family defines the protections required for critical security parameters used by the TOE for authentication or cryptography.

Management: FPT_PTD_EXT.1

There are no management activities foreseen.

Audit: FPT_PTD_EXT.1

There are no auditable events foreseen.

5.1.1.5.1 FPT_PTD_EXT.1 – Protection of TSF Data

Hierarchical to: No other components.

Dependencies: None

FPT_PTD_EXT.1.1 The TSF shall prevent reading of [assignment: critical security parameters].

5.1.1.6 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

Audit: FDP_AVL_EXT.3

Basic Level:

- Failure of a resources subject to an availability policy

5.1.1.6.1 FDP_AVL_EXT.1 – User 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].

5.1.1.6.2 FDP_AVL_EXT.3 – Failure Alerts

Hierarchical to: No other components.

Dependencies: FDP_AVL_EXT.1

FDP_AVL_EXT.3.1 The TSF shall be able to generate an alert when a [assignment: resource] subject to the [assignment: availability policy] fails.

5.1.2 Extended Requirements Rationale:

5.1.2.1 Network Device PP Influenced

The following SFRs are modeled from those found in the NDPP.

- FCS_COMM_PROT_EXT.1: Communications Protection

  This Requirement was modeled from the NDPP where it is defined to specify protocol security. This ST constrained the scope of the requirement to protection of administrative sessions.

- FCS_HTTPS_EXT.1: Explicit HTTPS

  This requirement was copied exactly from the NDPP where it is used as a requirement specific to the HTTPS protocol.

- FCS_SSH_EXT.1: Explicit SSH

  This Requirement was copied exactly from the NDPP where it is used as a requirement specific to the SSH protocol.

- FTA_TSL_EXT.1: Explicit TLS

  This Requirement was copied exactly from the NDPP where it is used as a requirement specific to the TLS protocol.

- FPT_PTD_EXT.1: Protection of TSF Data

  This Requirement was copied from the NDPP where it was stated as two similar requirements: FPT_PTD.1(1) and FPT_PTD.1(2). The naming and numbering of the requirement has been changed to more accurately reflect its nature as an extended requirement. It has also been changed to show assignments which allow the NDPP requirements to be included in this ST without modification.

5.1.2.2 Storage Availability Specific

The following SFRs are 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 secure, 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.

- FDP_AVL_EXT.1: User Data Availability
- FDP_AVL_EXT.2: Availability Alerts (Not used in this ST, but included as part of the family definition).
- FDP_AVL_EXT.3: Failure Alerts

5.2 TOE Security Functional Requirements

The following table describes the SFRs that are candidates to be satisfied by HP StoreOnce Backup System.

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.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
	FCS_COMM_PROT_EXT.1: Communications Protection
	FCS_COP.1(1): Cryptographic Operation (for data encryption/decryption)
	FCS_COP.1(2): Cryptographic Operation (for cryptographic hashing)
	FCS_COP.1(3): Cryptographic Operation (for keyed-hash message authentication)
	FCS_HTTPS_EXT.1: HTTPS Protocol
	FCS_SSH_EXT.1: Secure Shell Protocol
	FCS_TLS_EXT.1: Transport Layer Security Protocol
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)
	FDP_AVL_EXT.3(1): Failure Alerts (User Data)
	FDP_AVL_EXT.3(2): Failure Alerts (TSF Data)
	FDP_AVL_EXT.3(3): Failure Alerts (Couplet)
FIA: Identification and authentication	FIA_ATD.1: User attribute definition
	FIA_UAU.1: Timing of authentication
	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
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security roles
FPT: Protection of	FPT_PTD_EXT.1(1): Protection of TSF Data (authentication data)

the TSF	FPT_PTD_EXT.1(2): Protection of TSF Data (symmetric key data)
	FPT_STM.1: Reliable time stamps
TOE Access	FTA_SSL.3: TSF-initiated Termination
FTP: Trusted path/channels	FTP_TRP.1(1): Trusted Path (Disclosure)
	FTP_TRP.1(2): Trusted Path (Modification)

Table 1 TOE Security Functional Components

5.2.1 Security audit (FAU)

5.2.1.1 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 [

d) The specifically defined auditable events listed in Table 2].

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 2 and the following: severity, component, and cluster name**].

Requirement	Auditable Events	Additional Audit Record Contents
FAU_SAR.1	Reading of information from the audit records.	No additional information.
FCS_COP.1(1) FCS_COP.1(2) FCS_COP.1(3)	Failure on invoking functionality.	No additional information.
FCS_HTTPS_EXT.1	Failure to establish an HTTPS session. Establishment of an HTTPS session.	Reason for failure Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_SSH_EXT.1	Failure to establish an SSH session. Establishment of an SSH session.	Reason for failure Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_TLS_EXT.1	Failure to establish an TLS session. Establishment of an TLS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FDP_ACF.1	Successful requests to perform an operation on an object covered by the SFP.	The identity of the subject performing the operation.
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.
FDP_AVL_EXT.3(1)	Failure of RAID drive protecting user data	No additional information.
FDP_AVL_EXT.3(2)	Failure of RAID drive protecting TSF data	No additional information.
FDP_AVL_EXT.3(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_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: • Audit review events • Managing VTLs • Managing NAS • Managing StoreOnce Catalyst Stores	No additional information.
FTP_TRP.1(1)	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FTP_TRP.1(2)	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.

Table 2 Auditable Events

Application Note: The terms "Component" and "Cluster" refer to individual computers (component) and group of computers working closely together. The "Severity" refers to a value indicating a relative importance of the message to other messages (a.k.a., priority level).

5.2.1.2 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.

5.2.1.3 Audit review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide [**all Administrators**] 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.

5.2.1.4 Selectable audit review (FAU_SAR.3)

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

5.2.1.5 Protected audit trail storage (FAU_STG.1)

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.

5.2.2 Cryptographic Support

5.2.2.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**Random Number Generation**] and specified cryptographic key sizes [**128 to 256 bits**] that meet the following: [**FIPS 140-2**].

5.2.2.2 Communications Protection (FCS_COMM_PROT_EXT.1)

FCS_COMM_PROT_EXT.1.1 The TSF shall protect communications using [**SSH**] and [**HTTPS/TLS**].

5.2.2.3 Cryptographic Operation (for data encryption/decryption) (FCS_COP.1(1))

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

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

5.2.2.4 Cryptographic Operation (for cryptographic hashing) (FCS_COP.1(2))

FCS_COP.1.1(2) The TSF shall perform [**cryptographic hashing services**] in accordance with a specified cryptographic algorithm [**SHA-1, SHA-256,**] and ~~cryptographic key~~ **message digest** sizes [**160, 256 bits**] that meet the following: [**FIPS Pub 180-3, 'Secure Hash Standard'**].

5.2.2.5 Cryptographic Operation (for keyed-hash message authentication) (FCS_COP.1(3))

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

5.2.2.6 HTTPS Protocol (FCS_HTTPS_EXT.1)

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.
FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

5.2.2.7 Secure Shell Protocol (FCS_SSH_EXT.1)

FCS_SSH_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, and 4254.

FCS_SSH_EXT.1.2 The TSF shall ensure that the SSH connection be rekeyed after no more than 2^{28} packets have been transmitted using that key.

FCS_SSH_EXT.1.3 The TSF shall ensure that the SSH protocol implements a timeout period for authentication as defined in RFC 4252 of [**120 seconds**], and provide a limit to the number of failed authentication attempts a client may perform in a single session to [**6**] attempts.

FCS_SSH_EXT.1.4 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.

FCS_SSH_EXT.1.5 The TSF shall ensure that, as described in RFC 4253, packets greater than [**35000**] bytes in an SSH transport connection are dropped.

FCS_SSH_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-256, [**no other algorithms**].

FCS_SSH_EXT.1.7 The TSF shall ensure that the SSH transport implementation uses SSH_RSA and [**no other public key algorithms**] as its public key algorithm(s).

FCS_SSH_EXT.1.8 The TSF shall ensure that data integrity algorithms used in SSH transport connection is [**hmac-sha1, hmac-sha1-96**].

FCS_SSH_EXT.1.9 The TSF shall ensure that diffie-hellman-group14-sha1 is the only allowed key exchange method used for the SSH protocol.

5.2.2.8 Transport Layer Security Protocol (FCS_TLS_EXT.1)

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [**TLS 1.0 (RFC 2246)**] supporting the following ciphersuites:
Mandatory Ciphersuites:

TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA

Optional Ciphersuites: [**None**].

5.2.3 User data protection (FDP)

5.2.3.1 Complete access control (FDP_ACC.2)

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

- **subjects: Ethernet and Fibre Chanel hosts,**
- **objects: CIFS-based Network-Attached Storage (NAS), NFS-based NAS, Ethernet-based StoreOnce Catalyst store, Ethernet-based Virtual Tape Libraries (VTL), 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.

5.2.3.2 Security attribute based access control (FDP_ACF.1)

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

- [**Subjects:**
  - **Ethernet hosts: host identifier and user identifier (when configured),**
  - **Fibre Channel hosts: host identifier**
- **Objects:**
  - **CIFS-based NAS: list of permitted users and associated access (read-write or read-only),**
  - **NFS-based NAS: list of permitted Ethernet hosts,**
  - **Ethernet-based VTL: list of permitted Ethernet hosts,**
  - **Fibre Channel-based VTL: assigned Fibre Channel port**.

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) Ethernet-based VTLs can be accessed only if the Ethernet hosts IQN is configured to permit access based on its host identifier;

b) Fibre Channel-based VTLs can be access only if the access attempt comes from its associated Fibre Channel port;

c) CIFS-based NAS can be access only by user specifically permitted to have read-write or read-only access based on its user identifier;

d) NFS-based NAS can be access only by an Ethernet host that has been specifically permitted access based on its host identifier].

FDP_ACF.1.3 The TSF shall explicitly authorise 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**].

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

FDP_AVL_EXT.1.1(1) The TSF shall be able to support a [**User-Data Disk Availability Policy**] that provides the following [**RAID levels 5, 6**] on [**physical disks on a node containing user data**].

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

FDP_AVL_EXT.1.1(2) 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**].

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

FDP_AVL_EXT.1.1(3) 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**].

5.2.3.6 Failure Alerts (User Data) (FDP_AVL_EXT.3(1))

FDP_AVL_EXT.3.1(1) The TSF shall be able to generate an alert when a [**physical disk**] subject to the [**User-Data Disk Availability Policy**] fails.

5.2.3.7 Failure Alerts (TSF Data) (FDP_AVL_EXT.3(2))

FDP_AVL_EXT.3.1(2) The TSF shall be able to generate an alert when a [**physical disk**] subject to the [**TSF-Data Disk Availability Policy**] fails.

5.2.3.8 Failure Alerts (Couplet) (FDP_AVL_EXT.3(3))

FDP_AVL_EXT.3.1(3) The TSF shall be able to generate an alert when a [**single node in a couplet**] subject to the [**Couplet Availability Policy**] fails.

5.2.4 Identification and authentication (FIA)

5.2.4.1 User attribute definition (FIA_ATD.1)

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

5.2.4.2 Timing of authentication (FIA_UAU.1)

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.

5.2.4.3 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 at the local console.

5.2.4.4 User identification before any action (FIA_UID.2)

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.

5.2.5 Security management (FMT)

5.2.5.1 Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1 The TSF shall enforce the [**Access Control policy**] to restrict the ability to [**manage**] **all** the security attributes ~~[assignment: list of security attributes]~~ to [**Administrators**].

5.2.5.2 Static attribute initialization (FMT_MSA.3)

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

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

5.2.5.3 Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to manage the TSF data to the RW Administrators.

5.2.5.4 Specification of Management Functions (FMT_SMF.1)

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

- **Ability to review audit events and**
- **Ability to manage VTL, StoreOnce Catalyst and NAS resources**].

5.2.5.5 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles: [**Administrator and Operator**].
FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.2.6 Protection of the TSF (FPT)

5.2.6.1 Protection of TSF Data (authentication data) (FPT_PTD_EXT.1(1))

FPT_PTD_EXT.1.1(1) The TSF shall prevent reading of [**the plaintext passwords**].

5.2.6.2 Protection of TSF Data (symmetric key data) (FPT_PTD_EXT.1(2))

FPT_PTD_EXT.1.1(2) The TSF shall prevent reading of [**all pre-shared keys, symmetric key, and private keys**].

5.2.6.3 Reliable time stamps (FPT_STM.1)

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

5.2.7 TOE Access (FTA)

5.2.7.1 TSF-initiated Termination (FTA_SSL.3)

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

5.2.8 Trusted path/channels (FTP)

5.2.8.1 Trusted Path (Disclosure) (FTP_TRP.1(1))

FTP_TRP.1.1(1) The TSF shall provide a communication path between itself and [**remote administrators using SSH or HTTPS/TLS**] ~~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**].

FTP_TRP.1.2(1) The TSF shall permit [**remote administrators**]to initiate communication via the trusted path.

FTP_TRP.1.3(1) The TSF shall require the use of the trusted path for [**all remote administrative actions**].

5.2.8.2 Trusted Path (Modification) (FTP_TRP.1(2))

FTP_TRP.1.1(2) The TSF shall provide a communication path between itself and [**remote administrators using SSH or HTTPS/TLS**] ~~users~~ that is logically distinct from other communication paths and provides assured identification of its end points and ~~protection~~ **detection** of the communicated data from [**modification**].

FTP_TRP.1.2(2) The TSF shall permit [**remote administrators**]to initiate communication via the trusted path.

FTP_TRP.1.3(2) The TSF shall require the use of the trusted path for [**all remote administrative actions**].

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 2 augmented with ALC_FLR.3 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

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.3: Systematic flaw remediation
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 3 EAL 2 augmented with ALC_FLR.3 Assurance Components

5.3.1 Development (ADV)

5.3.1.1 Security architecture description (ADV_ARC.1)

ADV_ARC.1.1d The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2d The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3d The developer shall provide a security architecture description of the TSF.

ADV_ARC.1.1c The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2c The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3c The security architecture description shall describe how the TSF initialization process is secure.

ADV_ARC.1.4c The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5c The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

ADV_ARC.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.1.2 Security-enforcing functional specification (ADV_FSP.2)

ADV_FSP.2.1d The developer shall provide a functional specification.

ADV_FSP.2.2d The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.2.1c The functional specification shall completely represent the TSF.

ADV_FSP.2.2c The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.2.3c The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4c For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5c For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

ADV_FSP.2.6c The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.3.1.3 Basic design (ADV_TDS.1)

ADV_TDS.1.1d The developer shall provide the design of the TOE.

ADV_TDS.1.2d The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

ADV_TDS.1.1c The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.1.2c The design shall identify all subsystems of the TSF.

ADV_TDS.1.3c The design shall describe the behaviour of each SFR-supporting or SFR-non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.

ADV_TDS.1.4c The design shall summarise the SFR-enforcing behaviour of the SFR-enforcing subsystems.
ADV_TDS.1.5c The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.
ADV_TDS.1.6c The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.
ADV_TDS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_TDS.1.2e The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

5.3.2 Guidance documents (AGD)

5.3.2.1 Operational user guidance (AGD_OPE.1)

AGD_OPE.1.1d The developer shall provide operational user guidance.
AGD_OPE.1.1c The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
AGD_OPE.1.2c The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.
AGD_OPE.1.3c The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
AGD_OPE.1.4c The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_OPE.1.5c The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AGD_OPE.1.6c The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.
AGD_OPE.1.7c The operational user guidance shall be clear and reasonable.
AGD_OPE.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2 Preparative procedures (AGD_PRE.1)

AGD_PRE.1.1d The developer shall provide the TOE including its preparative procedures.
AGD_PRE.1.1c The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.
AGD_PRE.1.2c The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.
AGD_PRE.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AGD_PRE.1.2e The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.3.3 Life-cycle support (ALC)

5.3.3.1 Use of a CM system (ALC_CMC.2)

ALC_CMC.2.1d The developer shall provide the TOE and a reference for the TOE.
ALC_CMC.2.2d The developer shall provide the CM documentation.
ALC_CMC.2.3d The developer shall use a CM system.
ALC_CMC.2.1c The TOE shall be labelled with its unique reference.
ALC_CMC.2.2c The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.2.3c The CM system shall uniquely identify all configuration items.
ALC_CMC.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.2 Parts of the TOE CM coverage (ALC_CMS.2)

ALC_CMS.2.1d The developer shall provide a configuration list for the TOE.
ALC_CMS.2.1c The configuration list shall include the following: The TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.
ALC_CMS.2.2c The configuration list shall uniquely identify the configuration items.
ALC_CMS.2.3c For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.
ALC_CMS.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.3 Delivery procedures (ALC_DEL.1)

ALC_DEL.1.1d The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.
ALC_DEL.1.2d The developer shall use the delivery procedures.
ALC_DEL.1.1c The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.
ALC_DEL.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.4 Systematic flaw remediation (ALC_FLR.3)

ALC_FLR.3.1d The developer shall document and provide flaw remediation procedures addressed to TOE developers.
ALC_FLR.3.2d The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.
ALC_FLR.3.3d The developer shall provide flaw remediation guidance addressed to TOE users.
ALC_FLR.3.1c The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
ALC_FLR.3.2c The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.
ALC_FLR.3.3c The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
ALC_FLR.3.4c The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.
ALC_FLR.3.5c The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.
ALC_FLR.3.6c The flaw remediation procedures shall include a procedure requiring timely response and the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw.
ALC_FLR.3.7c The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.
ALC_FLR.3.8c The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.
ALC_FLR.3.9c The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.
ALC_FLR.3.10c The flaw remediation guidance shall describe a means by which TOE users may register with the developer, to be eligible to receive security flaw reports and corrections.
ALC_FLR.3.11c The flaw remediation guidance shall identify the specific points of contact for all reports and enquiries about security issues involving the TOE.
ALC_FLR.3.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Tests (ATE)

5.3.4.1 Evidence of coverage (ATE_COV.1)

ATE_COV.1.1d The developer shall provide evidence of the test coverage.
ATE_COV.1.1c The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.
ATE_COV.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.2 Functional testing (ATE_FUN.1)

ATE_FUN.1.1d The developer shall test the TSF and document the results.
ATE_FUN.1.2d The developer shall provide test documentation.
ATE_FUN.1.1c The test documentation shall consist of test plans, expected test results and actual test results.
ATE_FUN.1.2c The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.3c The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.4c The actual test results shall be consistent with the expected test results.
ATE_FUN.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.3 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1d The developer shall provide the TOE for testing.
ATE_IND.2.1c The TOE shall be suitable for testing.
ATE_IND.2.2c The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
ATE_IND.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2e The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.
ATE_IND.2.3e The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.3.5 Vulnerability assessment (AVA)

5.3.5.1 Vulnerability analysis (AVA_VAN.2)

AVA_VAN.2.1d The developer shall provide the TOE for testing.
AVA_VAN.2.1c The TOE shall be suitable for testing.
AVA_VAN.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VAN.2.2e The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
AVA_VAN.2.3e The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.
AVA_VAN.2.4e The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6 TOE Summary Specification

This chapter describes the following security functions:

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

6.1 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.

In a single node appliance, the disks containing the configuration and event log data are setup as either RAID 5 (for lower end models) or RAID 6 (for higher end models). For multi-node appliances, 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
- Opening the Event Log for review
- 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 and failed 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
- Successful connections to VTLs and NAS
- Changes to the system clock and NTP settings

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), 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 6.4 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: The TOE generates audit records with contents as described above. These records a stored in an Event Log.
- FAU_GEN.2: The TOE associates an administrator identity or network client identity with all auditable events which are caused by an administrator or network entity.
- FAU_SAR.1: The audit records can be read by administrators through the GUI and CLI.
- FAU_SAR.3: The GUI offers sorting and filtering of records based upon the fields identified above.
- FAU_STG.1: The TOE stores audit records internally and provides access to that data only to authenticated administrators. The TOE does not offer GUI or CLI interfaces which allow for the modification of audit data.
- FAU_STG.4: The TOE stores audit data in a round-robin fashion where the oldest records are overwritten as necessary.

6.2 Cryptographic support

The TOE uses cryptography only in the context of protection of the communications surrounding remote administrator sessions. A remote administrative session can occur using either a GUI or CLI. Administrators use an SSHv3 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 generates random numbers in a manner that is consistent with FIPS 140-2 for use in the generation of cryptographic keys, using the functions provided by the industry standard OpenSSL packages using the RAND() function, with bit sizes from 128 bits to 256 bits.

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 (cipher-block chaining) mode. 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 Pub 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 TLSv1.0.

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 TLSv1.0.

The TOE implements SSHv3 as specified by RFCs 4251, 4252, 4253 and 4254. The TOE SSH implementation will force a rekey operation when the 228 packets of data have been transmitted using a key. The TOE SSH implementation includes a timeout period for authentication of 120 seconds and provides a limit of 6 failed

authentication attempts a client may perform in a single session attempt. The TOE SSH implementation supports public key-based and password based authentication. The TOE SSH implementation uses AES-CBC-128, and AES-CBC-256 algorithms for encryption and decryption of transmitted data. The TOE SSH implementation also uses SSH_RSA as its public key algorithm. For data integrity, the TOE SSH implementation uses hmac-sha-1 and hmac-sha1-96. The TOE SSH implementation supports only the DH Group 14 key exchange.

The TOE implements HTTPS as specified by RFC 2818. The TOE does not support HTTP connections for administration. The TOE implements TLS version 1.0 as specified by RFC 2246 using the following ciphersuites.

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA

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

- FCS_CKM.1: The TOE generates random numbers in a manner that is consistent with FIPS 140-2 for use in the generation of cryptographic keys with bit sizes from 128 bits to 256 bits.
- FCS_COMM_PROT_EXT.1: The TOE uses TLS and SSH to provide protection of the communications surrounding the remote administrative sessions from disclosure and from modification.
- FCS_COP.1(1): The TOE implements AES for encryption and decryption of data as described above to meet FIPS PUB 197 and NISP SP 800-38A with the required bit sizes and mode.
- FCS_COP.1(2): The TOE implements SHA-1 and SHA-256 for hashing services as described above to meet FIPS Pub 180-3 with the required message digest sizes.
- FCS_COP.1(3): The TOE implements HMAC-SHA-1 for keyed-hash authentication as described above to meet FIPS Pub 198-1 and FIPS Pub 180-3 with the required key sizes.
- FCS_HTTPS_EXT.1: The TOE implements HTTPS as described in the text above. The TOE uses TLS version 1.0 as cryptographic protection for HTTPS.
- FCS_SSH_EXT.1: The TOE implements SSHv3 as described in the text above supporting all required algorithms, hashes and key exchanges.
- FCS_TLS_EXT.1: The TOE implements TLS Version 1.0 as described in the text above providing all required ciphersuites.

6.3 User data protection

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

Thus, the TOE makes NAS and VTL storage accessible via iSCSI, NFS, CIFS, and Fibre Channel connections and protocols. The TOE provides NAS 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 and VTL resources.

- **Ethernet-based (i.e., iSCSI) VTLs** are configured to specify access by specific IQNs.

  The TOE enforces the following access requirements upon client host operations on TOE provided storage. For Ethernet-based client hosts accessing VTLs, the Ethernet host specified in the IQN must be configured in access. This is done by configuring the VTL to include the host identifier of the client host (e.g., IP address or Domain Name). An IQN is a text string composed of the following four (4) fields each concatenated by periods (“.”).

  - The literal “iqn”;

- A date that the naming authority took ownership of the domain (in te form YYYY-MM);
- A reversed domain name for the authority; and
- An string defined by the naming authority specifying the name of the storage target.

An example of an IQN would be, iqn.2011-09.com.hp.somehost:storage:tape1.sys1.hp.com. In this example, the iSCSI host would be "somehost.hp.com" and the storage device would be "tape1.sys1.hp.com".

- **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.

The TOE implements RAID on physical disks. RAID combines several physical disks into a larger logical disk. This larger logical disk can be configured to improve both read and write performance and data reliability for the storage node. The TOE supports RAID 5, RAID 6 and RAID 1+0.

RAID 5	provides data redundancy by distributing data blocks across all disks in a RAID set. Redundant information is stored as parity distributed across the disks.
RAID6	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 single-node architecture makes use of RAID 5 or RAID 6 to provide availability of user data stored by a node. Multi-node configurations also support RAID 5 or 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.

TSF data stored by a single-node appliance is protected only using the RAID array within the appliance. 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).

The TOE supports SNMPv2 for use with outgoing alert messages. The TOE sends SNMP messages to the IP address that is configured as its destination for SNMP messages (i.e., an SNMPTRAP). Any disk failure causes the TOE to generate an alert via SNMP or SMTP. Failures of one node within a couplet also generate an alert via SNMP or SMTP.

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: The TOE implements an access control policy between client hosts and storage devices that can be either NAS or a VTL as described above.
- FDP_AVL_EXT.1(1): The TOE implements RAID 5 and RAID 6 for physical storage devices holding user data within a node as described above.
- FDP_AVL_EXT.1(2): The TOE implements RAID 1+0 for physical storage devices holding TSF data within a node as described above.
- FDP_AVL_EXT.1(3): The TOE provides redundancy of TSF functionality and TSF data in a couplet. This allows the TOE to continue to provide security functions when one node within a couplet fails.
- FDP_AVL_EXT.3(1) and FDP_AVL_EXT.3(2): The TOE generates alarms in the form of SNMP alerts or SMTP messages whenever a physical disk that is part of a RAID volume with user data or TSF data fails.
- FDP_AVL_EXT.3(3):The TOE generates alarms in the form of SNMP alerts or SMTP messages whenever a node that is part of a couplet is down or not reachable by the backup node in the couplet.

6.4 Identification and authentication

The TOE supports three different user communities: administrative accounts, client hosts and CIFS users.

Client hosts are identified by a network identifier (e.g., IP address, DNS hostname, IQN) and optionally authenticated using CHAP. For client hosts authenticated using CHAP, the TOE maintains the client host identifier and a shared secret. The TOE can use CHAP to authenticate iSCSI hosts that are accessing VTLs. The TOE does not authenticate Fibre Channel (FC) hosts when supporting their requests for data.

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 or a public key 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). Thus, the "root" account is not used during

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 TOE also supports SNMPv2 for reporting only. That is, SNMP is used for outgoing messages only. The TOE sends SNMP messages to the IP address that is configured as its destination for SNMP messages. The TOE configuration also includes a "community string" that is included with outgoing SNMP messages.

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.

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.
- Public Key – A cryptographic key used, in place of a password, to authenticate the user during SSH login attempts.

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 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. 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 TOE also identifies Fibre Channel (FC), iSCSI, and NFS hosts when they attempt to access a backup target. Fibre Channel hosts are identified using a Fibre Channel port. While, NFS hosts are identified solely using their IP address.

An iSCSI host is identified using an iSCSI qualified name (IQN – See section 6.3 for an explaination of the IQN structure).

An example of an IQN would be, iqn.2011-09.com.hp.somehost:storage:tape1.sys1.hp.com. In this example, the iSCSI host would be "**somehost.hp.com**" and the storage device would be "**tape1.sys1.hp.com**".

The TOE supports CHAP authentication for iSCSI. Thus, a site can choose to use CHAP to authenticate iSCSI hosts. Use of CHAP for authentication is suggested but not required to satisfy the claims in this Security Target.

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

- FIA_ATD.1: The TOE maintains information about locally defined users as described above.
- FIA_UAU.7: The TOE does not echo passwords during a login at the local console.
- FIA_UAU.1, FIA_UID.2: The TOE does not provide any function to administrators until they have been successfully identified and authenticated. The TOE does allow FC and iSCSI hosts to access volumes only after they have been identified. The TOE also allows NFS hosts to access NFS shares only after identifying the host by its IP addess.

6.5 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 HP StoreOnce Backup 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 an iSCSI host) at which time explicit access rights (i.e., read-write, read-only, or none) to a host are also defined.

The HP StoreOnce Backup System products offer a full range of management functions. The list below identifies a subset that is related to other security features claimed in this document.

Through the GUI and CLI the TOE offers the ability to perform the following actions.

- Review audit events that are stored locally;
- Create, delete and modify VTLs;
- Create, delete and modify NAS shares;
- Create, delete and modify Catalyst stores
- Assign FC and iSCSI hosts permission to VTLs; and
- Configure RAID settings for physical storage devices.

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

- FMT_MSA.1: The TOE ensures that only the "Administrator" can configure TSF data related to the configuration and access permissions of a volume.
- FMT_MSA.3: The TOE ensures that only the "Administrator" can assign a server permission to a volume and that unless granted permission, the server cannot access a volume.
- FMT_MTD.1: The TOE ensures that only the "Administrator" can configure TSF data.
- FMT_SMF.1: The TOE provides management functions identified in the text above to support an administrator's ability to securely install, configure and operate the system as described in the above section.
- FMT_SMR.1: The TOE recognizes "Administrator" and "operator" accounts as distinct roles for controlling the capabilities of administrative personnel.

6.6 Protection of the TSF

The TOE stores password and private symmetric keys in internal files in a hashed form. The TOE does not provide interfaces to allow for the viewing of passwords by administrators. Also, the TOE does not offer an interface to query symmetric keys.

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_PTD_EXT.1(1): The TOE does not offer an interface to query existing passwords and stores passwords internally in a hashed form.
- FPT_PTD_EXT.1(2): The TOE does not offer an interface to query symmetric or private keys. The products currently does not support the use of pre-shared keys.
- FPT_STM.1: Each node of a cluster maintains its own hardware clock that is used to provide timestamps for use in audit records. The NTP protocol is use to synchronize the clocks in the nodes of a cluster. NTP can also be used (in a single-node or a cluster) to obtain time from an external NTP server on the management network.

6.7 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.

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

- FTA_SSL.3: The TOE implements an inactivity timeout that expires an administrative session after a period of time configured by an administrator.

6.8 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 TLSv1.0.

TLSv1.0 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 TLSv1.0 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). Under TLS, the TOE does not currently support the use of pre-shared keys.

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

- FTP_TRP.1(1): As described in section6.4, administrators connect to the TOE using either SSH to use the CLI or HTTPS/TLS to use the GUI.
- FTP_TRP.1(2): As described in section 6.4, administrators connect to the TOE using either SSH to use the CLI or HTTPS/TLS to use the GUI.

7 Protection Profile Claims

There are no Protection Profile claims in this Security Target.

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.

8.1.1 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_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			X		X	
OE.TRUSTED_ADMIN									X					
OE.HOST_IDENTITY										X				
OE.MGMT_NETWORK											X			
OE.DATA_NET												X		
OE.INTERNAL_NET													X	
OE.ETHERNET														X

8.1.1.1 T.AVAILABILITY

A user may not be held accountable for their actions.

This Threat is countered by ensuring that:

O.AUDIT_GENERATION: The TOE will provide the capability to create, view and protect records of security relevant events associated with users.

8.1.1.2 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 of an administrative error might be unnoticed or untraceable, the TOE is expected to log security relevant events and export those logs to an external log server.

8.1.1.3 T.DATA_DISCLOSURE

A connected host might obtain access to user data for which they have no authorization.

This threat is satisfied 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.

8.1.1.4 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 and also to allow administrators to configure limits so that user accessible resources are limited and warnings are issued when limits are reached.

8.1.1.5 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.

This threat is satisfied 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 and export those logs to an external log server.
- 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.

8.1.1.6 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.

8.1.1.7 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.

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.

8.1.1.8 A.PHYSICAL

Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

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.

8.1.1.9 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 are trusted to follow and apply all administrator guidance in a trusted manner.

8.1.1.10 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.*

This assumption is satisfied by ensuring that:

- OE. HOST_IDENTITY: iSCSI and Fiber Channel hosts correctly reflect the iSCSI identifier (IQN) or Fiber Channel World Wide Name (WWN) associated with their Host Bus Adapters (HBAs).

8.1.1.11 A.MGMT_NET

It is assumed that a dedicated "Management Network" exists between nodes of the TOE and hosts providing supporting services (e.g., AD and NTP)

This assumption is satisfied by ensuring that:

- OE.MGMT_NET: A dedicated "Management network" provides reliable ad secured communication between the TOE, hosts supporting remote administrative sessions 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.

8.1.1.12 A.DATA_NET

Clients on the "Data Network" do not have direct access to the Internal or Management networks that are used for managing, accessing, and supporting the TOE operations.

This assumption is satisfied by ensuring that:

- OE.DATA_NET: The protected Management and Internal networks are not directly connected to the Data Network, thus ensuring that clients on the Data Network do not have direct access to the Management nor Internal Network.

8.1.1.13 A.INTERNAL_NET

It is assumed that a dedicated and protected "Internal Network" exists that connects nodes of the TOE with network storage devices.

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.

8.1.1.14 A.ETHERNET

It is assumed that network devices on the Internal Network do not intercept, impersonate or otherwise modify communications on the Internal Network.

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.

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note Table 4 indicates the requirements that effectively satisfy the individual objectives.

8.2.1 Security Functional Requirements Rationale

All of the 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.LIMIT_ACCESS	O.PROTECTED_COMMUNICATIONS		O.SYSTEM_MONITORING	O.TOE_ADMINISTRATION
FAU_GEN.1					X	
FAU_GEN.2					X	
FAU_SAR.1					X	
FAU_SAR.3					X	
FAU_STG.1					X	
FAU_STG.4					X	
FCS_CKM.1			X			
FCS_COMM_PROT_EXT.1			X			
FCS_COP.1(1)			X			
FCS_COP.1(2)			X			
FCS_COP.1(3)			X			
FCS_HTTPS_EXT.1			X			

	O.AVAILABILITY	O.LIMIT_ACCESS	O.PROTECTED_COMMUNICATIONS		O.SYSTEM_MONITORING	O.TOE_ADMINISTRATION
FCS_SSH_EXT.1			X			
FCS_TLS_EXT.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					
FDP_AVL_EXT.3(1)	X					
FDP_AVL_EXT.3(2)	X					
FDP_AVL_EXT.3(3)	X					
FIA_ATD.1						X
FIA_UAU.1						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_PTD_EXT.1(1)						X
FPT_PTD_EXT.1(2)						X
FPT_STM.1			X			
FTA_SSL.3					X	
FTP_TRP.1(1)			X			
FTP_TRP.1(2)			X			

Table 4 Objective to Requirement Correspondence

1.1.1.1 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(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.

- FDP_AVL_EXT.3(1) and FDP_AVL_EXT.3(2): The TOE provides alerts to administrators to indicate the failure of physical disks that are being used with RAID to store user and TSF data.
- FDP_AVL_EXT.3(3): The TOE provides alerts to administrators to indicate the failure of a single node within a couplet.

1.1.1.2 O.LIMIT_ACCESS

The TOE will ensure that connected hosts can access only data resources for which they are authorized.

This TOE Security Objective is satisfied by ensuring that:

- 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.

1.1.1.3 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.
- FCS_COMM_PROT_EXT.1: The TOE is required to implement SSH or IPSEC and optionally TLS to protect its network communication channels.
- FCS_COP.1(1): The TOE is required to implement FIPS-conformant AES in support of cryptographic protocols.
- FCS_COP.1(2): The TOE is required to implement FIPS-conformant SHA-1 and SHA-256 in support of cryptographic protocols.
- FCS_COP.1(3): The TOE is required to implement FIPS-conformant HMAC SHA-1 in support of cryptographic protocols.
- FCS_SSH_EXT.1: The TOE is required to implement SSH properly to protect applicable network communication channels.
- FCS_TLS_EXT.1: The TOE is required to implement TLS properly to protect applicable network communication channels.
- FPT_PTD_EXT.1(2): The TOE is required to prevent even administrators from readily accessing sensitive user and TSF data such as cryptographic keys.
- FTP_TRP.1(1): The TOE is required to protect communication between itself and its administrators from disclosure and modification.
- FTP_TRP.1(2): The TOE is required to protect communication between itself and its administrators from disclosure and modification.

1.1.1.4 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.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.

1.1.1.5 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.
- 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.1: The TOE is required to implement a minimum of a System Administrator role and can implement additional roles where necessary.
- FPT_PTD_EXT.1(1): The TOE is required to prevent even administrators from readily accessing sensitive user and TSF data such as passwords.

8.3 Security Assurance Requirements Rationale

The security assurance requirements for the TOE are the EAL 2 augmented with ALC_FLR.3 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

EAL 2 augmented with ALC_FLR.3 was selected as the assurance level because the TOE is a commercial product whose users require a low to moderate degree of independently assured security. ALC_FLR.3 was selected to exceed EAL2 assurance objectives in order to ensure that identified flaws are addressed. The TOE is targeted at a relatively benign environment with good physical access security and competent administrators. Within such environments it is assumed that attackers will have little attack potential. As such, EAL 2 augmented with ALC_FLR.3 is appropriate to provide the assurance necessary to counter the limited potential for attack.

8.4 Requirement Dependency Rationale

The following table demonstrates the dependencies among the claimed security requirements. It shows that all dependencies are satisfied. Therefore the requirements work together to accomplish the overall objectives defined for the TOE.

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.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_CKM.2 or FCS_COP.1) and FCS_CKM.4	FCS_COP.1(1)
FCS_COMM_PROT_EXT.1	none	none
FCS_COP.1(1)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1)	FCS_CKM.1
FCS_COP.1(2)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1)	FCS_CKM.1
FCS_COP.1(3)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1)	FCS_CKM.1
FCS_HTTPS_EXT.1	FCS_TLS_EXT.1	FCS_TLS_EXT.1
FCS_SSH_EXT.1	FCS_COP.1	FCS_COP.1(1)
FCS_TLS_EXT.1	FCS_COP.1	FCS_COP.1(1)
FDP_ACC.2	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 and FMT_MSA.3	FDP_ACC.2 and FMT_MSA.3
FDP_AVL_EXT.1(1)	none	none
FDP_AVL_EXT.1(2)	none	none
FDP_AVL_EXT.1(3)	none	none
FDP_AVL_EXT.3(1)	FDP_AVL_EXT.1	FDP_AVL_EXT.1(1)
FDP_AVL_EXT.3(2)	FDP_AVL_EXT.1	FDP_AVL_EXT.1(2)
FDP_AVL_EXT.3(3)	FDP_AVL_EXT.1	FDP_AVL_EXT.1(3)
FIA_ATD.1	none	none
FIA_UAU.1	FIA_UID.1	FIA_UID.2
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1
FIA_UID.2	none	none
FMT_MSA.1	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1 and FMT_SMF.1 and FDP_ACC.2
FMT_MSA.3	FMT_MSA.1 and FMT_SMR.1	FMT_MSA.1 and FMT_SMR.1
FMT_MTD.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_SMF.1	none	none
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_PTD_EXT.1(1)	none	none
FPT_PTD_EXT.1(2)	none	none
FPT_STM.1	none	none
FTA_SSL.3	none	none
FTP_TRP.1(1)	none	none
FTP_TRP.1(2)	none	none
ADV_ARC.1	ADV_FSP.1, 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.1	ALC_CMS.2
ALC_CMS.2	none	none
ALC_DEL.1	none	none
ALC_FLR.3	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

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 5 Security Functions vs. Requirements Mapping** 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**	**TOE Access**	**Trusted path/channels**
FAU_GEN.1	X							
FAU_GEN.2	X							
FAU_SAR.1	X							
FAU_SAR.3	X							
FAU_STG.1	X							
FAU_STG.4	X							
FCS_CKM.1		X						
FCS_COMM_PROT_EXT.1		X						
FCS_COP.1(1)		X						
FCS_COP.1(2)		X						
FCS_COP.1(3)		X						
FCS_HTTPS_EXT.1		X						
FCS_SSH_EXT.1		X						
FCS_TLS_EXT.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					
FDP_AVL_EXT.3(1)			X					
FDP_AVL_EXT.3(2)			X					
FDP_AVL_EXT.3(3)			X					
FIA_ATD.1				X				
FIA_UAU.1				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_PTD_EXT.1(1)						X		
FPT_PTD_EXT.1(2)						X		
FPT_STM.1						X		
FTA_SSL.3							X	
FTP_TRP.1(1)								X
FTP_TRP.1(2)								X

Table 5 Security Functions vs. Requirements Mapping