Dell EqualLogic PS Series Storage Array Firmware Version 5.1.1-H2 Security Target

Version:	**2.5**
Status:	**Released**
Last Update:	**2013-01-21**

Trademarks

Dell and the Dell logo are trademarks or registered trademarks of Dell Incorporated in the United States, other countries, or both.

Java is a trademark of Oracle Corporation in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

Legal Notice

This document is provided AS IS with no express or implied warranties. Use the information in this document at your own risk.

This document may be reproduced or distributed in any form without prior permission provided the copyright notice is retained on all copies. Modified versions of this document may be freely distributed provided that they are clearly identified as such, and this copyright is included intact.

Revision History

Revision	Date	Author(s)	Changes to Previous Revision
2.5	2013-01-21	Scott Chapman	EqualLogic ST.

Table of Contents

List of Tables

1 Introduction

1.1 Security Target Identification

Title:	Dell EqualLogic PS Series Storage Array Firmware Version 5.1.1-H2 Security Target
Version:	2.5
Status:	Released
Date:	2013-01-21
Sponsor:	Dell Inc.
Developer:	Dell Inc.
Certification ID:	BSI-DSZ-CC-0688
Keywords:	Dell, EqualLogic, SAN

1.2 TOE Identification

The TOE is Dell EqualLogic PS Series Storage Array Firmware Version 5.1.1-H2.

1.3 TOE Type

The TOE type is Storage Area Network (SAN) firmware.

1.4 TOE Overview

The Dell EqualLogic PS Series Storage Array is a high performance, enterprise-level Storage Area Network (SAN) device. Each device, called an array, contains multiple, hot swappable drives for storing large quantities of data plus one to two controller cards. Multiple arrays can be connected together to function as a single array. One or more logical volumes can be created within a single array or that span across multiple arrays. Client computers connect to the volumes using the Internet Small Computer System Interface (iSCSI) protocol [RFC5048]. A volume can be assigned to one or more iSCSI Clients (through the use of volume access control lists) and used by these clients as filesystems.

Each array supports multiple iSCSI connections for communicating with iSCSI Clients. The arrays support administrative interfaces on the same network as the iSCSI Clients. They also support separate connections for administrative consoles (physically separated from the iSCSI network). Multiple arrays can be logically linked together into a Group. Grouping allows volumes to be spread across multiple arrays and provides performance advantages as well.

The controller cards are the brains of the array and control all functions performed by an array, including:

- all communication between arrays
- all communication between the arrays and client computers (iSCSI and administrative consoles)
- all security enforced by the array
- volume management

The controller cards reside inside each array enclosure.

The TOE is the firmware that resides on the controller card(s) and the supporting guidance documentation.

1.4.1 Required and optional non-TOE hardware and software

The Operational Environment for the TOE consists of the following hardware models:

- PS4000 - E, X, XV
- PS4100 - E, X, XV
- PS6000 - E, X, XV, S
- PS6010 - E, X, XV, S
- PS6100 - E, X, XV, S, ES, XS, XVS
- PS6500 - E, X
- PS6510 - E, X

The letter suffixes in the hardware model numbers have the following definitions:

- E - Serial ATA (SATA) drives or Nearline Serial Attached SCSI (NL SAS) drives
- ES - Combination (hybrid) of E and S
- S - Solid State Drives (SSDs)
- X - 10,000 RPM Serial Attached SCSI (SAS) drives
- XS - Combination (hybrid) of X and S
- XV - 15,000 RPM SAS drives
- XVS - Combination (hybrid) of XV and S

The Operational Environment for the TOE consists of the following *required* software product(s):

- iSCSI initiator software

The Operational Environment for the TOE consists of the following *optional* software product(s):

- Domain Name Service (DNS) server
- Network Time Protocol (NTP) server
- Remote Authentication Dial In User Service (RADIUS) server
- Secure Shell/Secure Copy (SSH/SCP) client
- Web browser

1.4.2 Intended method of use

The iSCSI interface of the TOE allows multiple iSCSI Clients to access volumes controlled by the TOE. The iSCSI interface is intended to be used in a protected network environment where network eavesdropping is not allowed except by network administrative personnel. iSCSI communication with the TOE is not protected from modification or disclosure by the TOE. (Network administrative communication with the TOE via the web browser and via SSH/SCP is protected from modification and disclosure.)

Similarly, the RADIUS server network and the Group network are intended to be used in a protected network environment where network eavesdropping is not allowed except by network administrative personnel. The RADIUS server communication with the TOE and the network communication between Group members are not protected from modification or disclosure by the TOE.

The arrays in which the TOE runs, including all physical connectors on an array, are intended to be accessible by administrative personnel only (e.g., contained in a restricted access room).

1.4.3 Major security features

The major security features of the TOE are:

- Auditing
- User data protection
- Identification and authentication
- Security management
- Reliable time stamps
- Trusted channel

1.5 TOE Description

1.5.1 TOE introduction and logical boundary

The TOE is the firmware that resides on the controller card(s) within the device (a.k.a. array) and the supporting guidance documentation. This firmware controls the device and enforces the security functionality provided by the TOE.

The TOE provides support for multiple logical volumes for storing data. Volumes typically contain filesystems and the filesystems contain user data. Computers mount (connect to) the volumes located on the array across an Ethernet network connection via the iSCSI protocol. To a computer user, the volumes look like normal disk drives. These connections are often long-lived, some lasting as long as several months.

In iSCSI terminology, the connecting computers are (or contain) iSCSI initiators and the volumes are iSCSI targets. The TOE requires the iSCSI initiators to authenticate to the TOE before making any additional requests. The TOE uses the Challenge Handshake Authentication Protocol (CHAP) [RFC1994] to authenticate iSCSI users. All iSCSI communication is performed in the clear over the network (i.e., the iSCSI communication, including authentication via CHAP, is not protected from disclosure or modification).

The TOE controls access to the volumes through the use of access control lists (ACLs). Each volume has its own ACL.

The TOE also supports the creation of volume snapshots. Snapshots are a point-in-time copy of a volume that exist on the array(s). Each snapshot contains its own ACL used to control access to the snapshot.

Though iSCSI Clients are the typical users of the TOE, the TOE also supports administrative users for managing resources controlled by the TOE. The TOE provides multiple interfaces for administration.

For network-based administrative connections, the TOE provides both a graphical user interface (GUI) over TLS and a command line interface (CLI) via Secure Shell (SSH including Secure Copy (SCP)). The GUI is a Java application (located in the firmware) that is transferred to the administrator's web browser when the browser connects to the TOE. From the GUI interface, an administrator can manage the entire array as well as groups of arrays. The CLI resides in the firmware and provides similar functionality as the GUI. Both the GUI and CLI protect the communication from disclosure and modification. The web browser and SSH/SCP client are part of the Operational Environment, not the TOE.

The TOE supports the following authentication databases:

- local

- RADIUS

A local authentication database is stored on the local storage drives of the array by the TOE. RADIUS is a remote authentication database server and is part of the Operational Environment.

The TOE also supports administration via a serial port/connection located on each array. This connection allows a terminal (or computer with terminal emulator software) to attach directly to the device. From this connection, an administrator has access to the same CLI as described above. (This connection is not protected from disclosure or modification.)

Multiple arrays can be logically linked together (grouped) to act as a single array. This is called a Group. Grouping allows volumes to be spread across multiple arrays.

Within a Group, one array acts as the initial contact point, called the Group leader, for the entire Group. Each Group member must successfully authenticate to the Group leader using the correct Group name and Group membership password in order to join the Group. The TOE performs the Group member identification and authentication.

1.5.2 TOE security features

This section describes the security features of the TOE at a high level.

1.5.2.1 Auditing

The TOE generates audit records for auditing start-up and shutdown events as well as logon and logoff events. It also provides an administrative interface for viewing audit records. The TOE also provides multiple event levels for auditing, specifically: audit, info, warning, error, fatal.

1.5.2.2 User data protection

1.5.2.2.1 Access control

The TOE uses access control lists (ACLs) to protect iSCSI access to individual volumes and snapshots. iSCSI Clients must pass the object's ACL check in order to gain access to data in the object.

1.5.2.2.2 Residual information protection

The TOE zeroizes (write zeros in every byte of) a page of disk space at page allocation time. This prevents unintended access to residual data that may exist on a page from prior usage.

1.5.2.3 Identification and authentication (I&A)

1.5.2.3.1 Client I&A

The TOE supports identification and authentication (I&A) of all client users. Users are required to authenticate when connecting via the iSCSI protocol, the network administrative interface, and the serial connection.

The iSCSI Client interface uses password-based CHAP for authenticating users. The network administrative interfaces prompt for the administrator name and password and pass the responses to the TOE.

The iSCSI accounts can be defined in either the local user account database or in a RADIUS server. In the evaluated configuration, the administrative user accounts must be defined in the local user account database only. For each user, the TOE maintains the following user attributes:

- user name
- user password
- user role

Table 1 shows the authentication databases and the user types supported by each database in the evaluated configuration.

Authentication Databases	Supports iSCSI Client Accounts	Supports Administrative Accounts
Local	✔	✔
RADIUS	✔	

Table 1: Authentication databases and supported user types

The TOE supports the following authentication database configurations:

- Local only
- Local and RADIUS

For iSCSI Client user accounts, if both the local and RADIUS databases are configured, the TOE will accept the user's credentials if there is a credential match in either database.

For iSCSI authentication, the TOE supports mutual authentication in the evaluated configuration. The iSCSI initiator must authenticate to the iSCSI target and the iSCSI target must authenticate to the iSCSI initiator.

1.5.2.3.2 Group I&A

Multiple arrays can be grouped together by a Group Administrator to function as a single array. Each array that joins a Group is known as a Group member. Each Group has an array that acts as the Group leader. As each array joins a Group, it is required to mutually authenticate to the Group leader. The TOE in the Group leader and the TOEs in the other Group members perform the Group identification and authentication (I&A). An array can only be a member of one Group.

Each Group has a single Group name and a single Group membership password defined by the Group Administrator and stored locally by each TOE; hence, RADIUS is not used for Group I&A. As Group members authenticate to the Group leader and detach from the Group leader, the TOE in the Group leader dynamically grows and shrinks its authenticated Group members table to accommodate these changes. The TOE in the Group leader propagates this table to the other Group members so that the other Group member TOEs know which arrays are an active part of the Group in case the Group leader becomes inactive.

Each Group member's IP address is used by the TOE to uniquely identify the Group member in the Group. Each TOE uses CHAP to mutually authenticate to the Group leader using the Group name as the CHAP "User name" and the Group membership password as the CHAP "User password".

1.5.2.4 Security management

The TOE supports the following authorized user roles:

- Group Administrator

- Pool Administrator
- Volume Administrator
- Read-only Administrator
- iSCSI Client

The Group Administrator role is the most powerful of the roles and is used to manage the arrays including the users assigned to the other roles. The Pool Administrator role is an administrative role used to manage pools of virtual storage space, but the role has less power than the Group Administrator role. The Volume Administrator role is an administrative role used to manage volumes within a pool, but the role has less power than the Pool Administrator role. The Read-only Administrator can monitor administrative information, but cannot modify the information. The iSCSI Client role is the least powerful role and is implicitly assigned to any computer connection that connects to the array through the array's iSCSI network connection(s).

In addition, the TOE provides management interfaces for managing users including user role assignments, managing volume and snapshot ACLs, and managing the time synchronization source.

1.5.2.5 Reliable time stamps

The TOE uses an internal time source to provide reliable time stamps for audit records. Optionally, the TOE can be configured to use the Network Time Protocol (NTP) to synchronize the TOE's internal time source.

1.5.2.6 Trusted channel

The TOE supports the use of web browsers (over TLS) and SSH/SCP as management interfaces. Both of these interfaces provide for protection of the transferred data from disclosure and modification as well as assured identification of both end points.

1.5.3 Security policy data

This section describes the security policy model for the TOE.

1.5.3.1 Subjects and objects

The following subject and object definitions are used in the TOE security policies:

Subjects:

- **Administrator** - Users who have been specifically granted the authority to manage a portion or all of the TOE and whose actions may affect the TOE security policy. The TOE supports the following administrative roles:
  - Group Administrator
  - Pool Administrator
  - Volume Administrator
  - Read-only Administrator
- **Group member** - An array that is a member of a group of arrays that collectively act as a single array.
- **iSCSI Client** - Computers (i.e., users) that communicate to the TOE using the iSCSI protocol.

Objects:

- **Array Page** - A page of disk space.

- **Snapshot** - A point-in-time copy of a volume.
- **Volume** - A set of array pages commonly used to house a single filesystem.

1.5.3.2 TSF data and security attributes

The following TOE Security Functionality (TSF) data and security attributes are maintained by the TOE:

- Audit records
- Time synchronization source setting
- User account data, including the following security attributes:
  - User name
  - User password
  - User role
- Group account data, including the following security attributes:
  - Group name
  - Group membership password
  - Group member's IP address
- Volume and snapshot ACLs

1.5.3.3 User data

The following user data are maintained by the TOE:

- Data contained in a volume or snapshot

1.5.4 Physical boundary

The TOE firmware is contained in the following firmware installation image:

- kit_V5.1.1-H2-R189834_2529064680.tgz (contained in V5-1-1-H2.tar and in V5-1-1-H2.zip)

The TOE includes of the following guidance documents that are independently downloadable from the Dell website:

- EqualLogic PS Series Storage Arrays Common Criteria Configuration Guide
- EqualLogic PS Series Firmware Command Line Reference Version 5.1
- EqualLogic PS Series Group Administration, PS Series Firmware Version 5.1
- EqualLogic PS Series Storage Arrays Release Notes, PS Series Firmware Version 5.1
- EqualLogic Updating PS Series Storage Array Firmware, Firmware Version 5.1
- EqualLogic Master Glossary, PS Series Firmware Version 5.1

The firmware portion of the TOE consists of the following packages:

- EqualLogic Firmware Package
- EqualLogic Group Manager GUI Package
- EqualLogic Group Manager CLI Package

All three packages come bundled as a single installation image and are installed on each array. The firmware package contains the software that controls an array. The GUI package contains the Java-based administrative interface software that is loaded into a web browser and used by

administrative personnel to manage the array. The CLI package contains the administrative command line interface that is used by administrators when they connect to the array using SSH/SCP or the serial port.

1.5.5 Evaluated configuration

The evaluated configuration consists of the firmware and guidance documentation as specified in section 1.5.4 for the hardware models listed in section 1.4.1. It includes the optional use of a RADIUS server as an authentication server, which resides in the Operational Environment. The evaluated configuration also imposes some limitations on the configuration of the product.

The specifications for configuring the TOE in the evaluated configuration are located in the guidance documentation listed in section 1.5.4. The consumer must read, understand, and follow the guidance documentation provided as part of the TOE for the evaluated configuration.

The following restrictions apply to the evaluated configuration:

- The Dell EqualLogic FS Series Network-Attached Storage (NAS) must not be used in the evaluated configuration.
- The Dell PowerEdge blade chassis and server management software must not be used in the evaluated configuration.
- The FTP daemon (ftpd) and the Telnet daemon (telnetd) must be disabled.

1.5.6 Operational Environment

The Operational Environment for the TOE consists of the hardware and software specified in section 1.4.1.

1.5.6.1 Physical

The hardware and networking used by the TOE are part of the Operational Environment. The arrays must be located in rooms restricted to administrative access only. The security of the array depends on the physical security of the arrays.

If Domain Name Service (DNS) servers are used in the Operational Environment, they must be trustworthy. Although the TOE does not depend on DNS servers, the client computers and administrative computers that attach to the TOE may depend on DNS servers to connect to the TOE.

The iSCSI network, Group network, and the RADIUS server network must be located in a non-hostile environment. As mentioned in section 1.4.2, the Operational Environment must provide protection for the network data against modification and disclosure. Protection mechanisms include:

- Providing physical security of the local network
- Providing logical protection of resources through the use of firewalls and/or network isolation
- Providing encrypted VPNs (e.g., IPsec) between enterprise sites
- Providing resources with up-to-date anti-virus tools and applying security updates regularly

2 CC Conformance Claim

This ST is CC Part 2 extended and CC Part 3 conformant, with a claimed Evaluation Assurance Level of EAL2, augmented by ALC_FLR.1.

This ST does not claim conformance to any Protection Profile.

Common Criteria [CC] version 3.1 revision 3 is the basis for this conformance claim.

3 Security Problem Definition

3.1 Threat Environment

This section describes the threat model for the TOE and identifies the individual threats that are assumed to exist in the Operational Environment.

The **IT assets** to be protected comprise the information stored, processed or transmitted by the TOE. The term “information” is used here to refer to all data held within the product.

The TOE counters the general threat of unauthorized access to information, where “access” includes disclosure, modification, and destruction.

The **threat agents** can be categorized as either:

- Unauthorized users of the TOE (i.e., individuals who have not been granted the right to access the system)
- Authorized users of the TOE (i.e., individuals who have been granted the right to access the system)

The threat agents are assumed to originate from a well managed user community in a non-hostile working environment. Therefore, the product protects against threats of security vulnerabilities that might be exploited in the intended environment for the TOE with medium level of expertise and effort. The TOE protects against straightforward or intentional breach of TOE security by attackers possessing a low attack potential.

3.1.1 Threats countered by the TOE

T.Access.Unauthorized

A user (authorized or unauthorized) gains access to TSF data or user data that is stored in the TOE, processed by the TOE, or transmitted via the TOE's network administrative communication channels without proper authorization.

T.Event.NotLogged

Security-relevant activities of unauthorized individuals (such as logon attempts) may go unnoticed.

3.2 Assumptions

3.2.1 Environment of use of the TOE

3.2.1.1 Physical

A.Network.Protected

The Operational Environment protects the iSCSI network traffic, the Group network traffic, and the RADIUS server network traffic from disclosure and modification by non-administrative personnel.

A.Physical.Protected

The Operational Environment protects the hardware providing the runtime environment for the TOE from unauthorized physical access and modification.

3.2.1.2 Personnel

A.Admin.Trained

The administrators of the TOE and of the Operational Environment are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE and Operational Environment in accordance with those policies and procedures.

A.Admin.Trusted

The administrators of the TOE and of the Operational Environment are trustworthy and are not careless, negligent, malicious, or hostile.

A.User.Trained

The TOE users are aware of the security policies and procedures of their organization, and are trained and competent to follow those policies and procedures.

3.2.1.3 Connectivity

A.AdminClient.Trusted

The administrative client software used by the TOE administrators to communicate with the TOE (such as a web browser, SSH client, or SCP client) are trusted to function correctly and to not divulge security information.

A.AuthServers.Protected

The RADIUS server, if used by the TOE, provides protection against unauthorized access to TSF data stored within it.

A.DNS.Trusted

When a Domain Name Service (DNS) is used by the network, the DNS provides trustworthy services.

A.Logical.Protected

The Operational Environment protects the computer resources by running up-to-date anti-virus tools regularly on the computer resources, applying security updates regularly to the computer resources, and using firewalls and/or network isolation to protect the computer resources.

A.NTP.Reliable

When the TOE is configured to use the Network Time Protocol as a time synchronization source, the Network Time Protocol provides a reliable time synchronization source for the TOE.

3.3 Organizational Security Policies

P.Passwords.Complex

Passwords used by the TOE shall meet the following quality metric: the probability that a secret can be obtained by an attacker during the lifetime of the secret is less than 2^-20.

P.SNMP.Unaccessible

Administrative users shall not use the SNMP interface of the TOE and the SNMP interface shall have a sufficiently strong SNMP password to prevent non-administrative users from accessing and using this interface.

P.TOE.Authenticated

For assured identification of the end point, the iSCSI Client shall identify and authenticate the TOE when initiating a request.

4 Security Objectives

4.1 Objectives for the TOE

O.AdmCom.Protected

The TOE shall protect network administrative communication channels from disclosure and modification.

O.Event.Logged

The TOE shall offer a recording mechanism that provides an audit trail of TOE usage. Security-relevant events shall be logged and the logs maintained and protected from unauthorized disclosure or alteration within this audit trail.

O.Event.Viewable

The TOE shall provide a mechanism for authorized administrators to view audit records in a human readable format.

O.Object.Protected

The TOE shall ensure that users are authorized to access the protected objects of the TOE and ensure that users can perform only the actions allowed by the user's User Role in accordance to the security policy of the TOE.

O.Object.Zeroed

The TOE shall remove residual information from deallocated array pages before the array pages are made available.

O.User.Authenticated

The TOE shall require identification and authentication of users before allowing them to use the TOE.

O.User.Managed

The TOE shall provide for the creation, deletion, and management of authorized users and the assigning of administrative roles to administrative users.

4.2 Objectives for the Operational Environment

OE.Admin.Trained

The administrators of the TOE and of the Operational Environment shall be made aware of the security policies and procedures of their organization, shall be trained and competent to follow the manufacturer's guidance and documentation, and shall correctly configure and operate the TOE and Operational Environment in accordance with those policies and procedures.

OE.Admin.Trusted

The administrators of the TOE and of the Operational Environment shall be trustworthy and shall not be careless, negligent, malicious, or hostile.

OE.AdminClient.Trusted

The administrative client software used by the TOE administrators to communicate with the TOE (such as a web browser, SSH client, or SCP client) shall be trusted to function correctly and to not divulge security information.

OE.AuthServers.Protected

The RADIUS server, if used by the TOE, shall provide protection against unauthorized access to TSF data stored within it.

OE.DNS.Trusted

When a Domain Name Service (DNS) is used by the network, the DNS shall be trustworthy.

OE.Logical.Protected

The Operational Environment shall protect the computer resources by running up-to-date anti-virus tools regularly on the computer resources, applying security updates regularly to the computer resources, and using firewalls and/or network isolation to protect the computer resources.

OE.Network.Protected

The Operational Environment shall protect the iSCSI network traffic, the Group network traffic, and the RADIUS server network traffic from disclosure and modification by non-administrative personnel.

OE.NTP.Reliable

When the TOE is configured to use the Network Time Protocol as a time synchronization source, the Network Time Protocol shall provide a reliable time synchronization source for the TOE.

OE.Passwords.Complex

The TOE administrators shall ensure that passwords to all TOE accounts meet the following quality metric: the probability that a secret can be obtained by an attacker during the lifetime of the secret is less than 2^-20.

OE.Physical.Protected

The Operational Environment shall protect the hardware providing the runtime environment for the TOE from unauthorized physical access and modification.

OE.SNMP.Unaccessible

Administrative users shall not use the SNMP interface of the TOE and administrative users shall provide a sufficiently strong SNMP password for the SNMP interface to prevent non-administrative users from accessing and using this interface.

OE.TOE.Authenticated

The iSCSI Client shall provide assured identification of the TOE when the iSCSI Client initiates a request to the TOE.

OE.User.Trained

The TOE users shall be aware of the security policies and procedures of their organization and shall be trained and competent to follow those policies and procedures.

4.3 Security Objectives Rationale

4.3.1 Coverage

The following table provides a mapping of TOE objectives to threats and policies, showing that each objective counters or enforces at least one threat or policy, respectively.

Objective	Threats / OSPs
O.AdmCom.Protected	T.Access.Unauthorized
O.Event.Logged	T.Event.NotLogged
O.Event.Viewable	T.Event.NotLogged
O.Object.Protected	T.Access.Unauthorized
O.Object.Zeroed	T.Access.Unauthorized
O.User.Authenticated	T.Access.Unauthorized P.Passwords.Complex P.SNMP.Unaccessible
O.User.Managed	T.Access.Unauthorized

Table 2: Mapping of security objectives to threats and policies

The following table provides a mapping of the objectives for the Operational Environment to assumptions, threats and policies, showing that each objective holds, counters or enforces at least one assumption, threat or policy, respectively.

Objective	Assumptions / Threats / OSPs
OE.Admin.Trained	A.Admin.Trained
OE.Admin.Trusted	A.Admin.Trusted
OE.AdminClient.Trusted	A.AdminClient.Trusted
OE.AuthServers.Protected	A.AuthServers.Protected
OE.DNS.Trusted	A.DNS.Trusted
OE.Logical.Protected	A.Logical.Protected
OE.Network.Protected	A.Network.Protected
OE.NTP.Reliable	A.NTP.Reliable
OE.Passwords.Complex	P.Passwords.Complex

Objective	Assumptions / Threats / OSPs
OE.Physical.Protected	A.Physical.Protected
OE.SNMP.Unaccessible	P.SNMP.Unaccessible
OE.TOE.Authenticated	P.TOE.Authenticated
OE.User.Trained	A.User.Trained

Table 3: Mapping of security objectives for the Operational Environment to assumptions, threats and policies

4.3.2 Sufficiency

The following rationale provides justification that the security objectives are suitable to counter each individual threat and that each security objective tracing back to a threat, when achieved, actually contributes to the removal, diminishing or mitigation of that threat:

Threat	Rationale for security objectives
T.Access.Unauthorized	The threat: ● A user (authorized or unauthorized) gains access to TSF data or user data that is stored in the TOE, processed by the TOE, or transmitted via the TOE's network administrative communication channels without proper authorization. is diminished by: ● O.AdmCom.Protected: The TOE shall protect network administrative communication channels from disclosure and modification. ● O.Object.Protected: The TOE shall ensure that users are authorized to access the protected objects of the TOE and ensure that users can perform only the actions allowed by the user’s User Role in accordance to the security policy of the TOE. ● O.Object.Zeroed: The TOE shall remove residual information from deallocated array pages before the array pages are made available. ● O.User.Authenticated: The TOE shall require identification and authentication of users before allowing them to use the TOE. ● O.User.Managed: The TOE shall provide for the creation, deletion, and management of authorized users and the assigning of administrative roles to administrative users.
T.Event.NotLogged	The threat: ● Security-relevant activities of unauthorized individuals (such as logon attempts) may go unnoticed. is diminished by:

Threat	Rationale for security objectives
	• O.Event.Logged: The TOE shall offer a recording mechanism that provides an audit trail of TOE usage. Security-relevant events shall be logged and the logs maintained and protected from unauthorized disclosure or alteration within this audit trail. • O.Event.Viewable: The TOE shall provide a mechanism for authorized administrators to view audit records in a human readable format.

Table 4: Sufficiency of objectives countering threats

The following rationale provides justification that the security objectives for the environment are suitable to cover each individual assumption, that each security objective for the environment that traces back to an assumption about the environment of use of the TOE, when achieved, actually contributes to the environment achieving consistency with the assumption, and that if all security objectives for the environment that trace back to an assumption are achieved, the intended usage is supported:

Assumption	Rationale for security objectives
A.Network.Protected	The assumption: • The Operational Environment protects the iSCSI network traffic, the Group network traffic, and the RADIUS server network traffic from disclosure and modification by non-administrative personnel. is satisfied by: • OE.Network.Protected: The Operational Environment shall protect the iSCSI network traffic, the Group network traffic, and the RADIUS server network traffic from disclosure and modification by non-administrative personnel.
A.Physical.Protected	The assumption: • The Operational Environment protects the hardware providing the runtime environment for the TOE from unauthorized physical access and modification. is satisfied by: • OE.Physical.Protected: The Operational Environment shall protect the hardware providing the runtime environment for the TOE from unauthorized physical access and modification.
A.Admin.Trained	The assumption: • The administrators of the TOE and of the Operational Environment are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer’s guidance and documentation, and correctly configure and operate the TOE and Operational Environment in accordance with those policies and procedures. is satisfied by:

Assumption	Rationale for security objectives
	• OE.Admin.Trained: The administrators of the TOE and of the Operational Environment shall be made aware of the security policies and procedures of their organization, shall be trained and competent to follow the manufacturer's guidance and documentation, and shall correctly configure and operate the TOE and Operational Environment in accordance with those policies and procedures.
A.Admin.Trusted	The assumption: • The administrators of the TOE and of the Operational Environment are trustworthy and are not careless, negligent, malicious, or hostile. is satisfied by: • OE.Admin.Trusted: The administrators of the TOE and of the Operational Environment shall be trustworthy and shall not be careless, negligent, malicious, or hostile.
A.User.Trained	The assumption: • The TOE users are aware of the security policies and procedures of their organization, and are trained and competent to follow those policies and procedures. is satisfied by: • OE.User.Trained: The TOE users shall be aware of the security policies and procedures of their organization and shall be trained and competent to follow those policies and procedures.
A.AdminClient.Trusted	The assumption: • The administrative client software used by the TOE administrators to communicate with the TOE (such as a web browser, SSH client, or SCP client) are trusted to function correctly and to not divulge security information. is satisfied by: • OE.AdminClient.Trusted: The administrative client software used by the TOE administrators to communicate with the TOE (such as a web browser, SSH client, or SCP client) shall be trusted to function correctly and to not divulge security information.
A.AuthServers.Protected	The assumption: • The RADIUS server, if used by the TOE, provides protection against unauthorized access to TSF data stored within it. is satisfied by: • OE.AuthServers.Protected: The RADIUS server, if used by the TOE, shall provide protection against unauthorized access to TSF data stored within it.
A.DNS.Trusted	The assumption: • When a Domain Name Service (DNS) is used by the network, the DNS provides trustworthy services.

Assumption	Rationale for security objectives
	is satisfied by: • OE.DNS.Trusted: When a Domain Name Service (DNS) is used by the network, the DNS shall be trustworthy.
A.Logical.Protected	The assumption: • The Operational Environment protects the computer resources by running up-to-date anti-virus tools regularly on the computer resources, applying security updates regularly to the computer resources, and using firewalls and/or network isolation to protect the computer resources. is satisfied by: • OE.Logical.Protected: The Operational Environment shall protect the computer resources by running up-to-date anti-virus tools regularly on the computer resources, applying security updates regularly to the computer resources, and using firewalls and/or network isolation to protect the computer resources.
A.NTP.Reliable	The assumption: • When the TOE is configured to use the Network Time Protocol as a time synchronization source, the Network Time Protocol provides a reliable time synchronization source for the TOE. is satisfied by: • OE.NTP.Reliable: When the TOE is configured to use the Network Time Protocol as a time synchronization source, the Network Time Protocol shall provide a reliable time synchronization source for the TOE.

Table 5: Sufficiency of objectives holding assumptions

The following rationale provides justification that the security objectives are suitable to cover each individual organizational security policy, that each security objective that traces back to an OSP, when achieved, actually contributes to the implementation of the OSP, and that if all security objectives that trace back to an OSP are achieved, the OSP is implemented:

OSP	Rationale for security objectives
P.Passwords.Complex	The OSP: • Passwords used by the TOE shall meet the following quality metric: the probability that a secret can be obtained by an attacker during the lifetime of the secret is less than 2^-20. is satisfied by: • O.User.Authenticated: The TOE shall require identification and authentication of users before allowing them to use the TOE. • OE.Passwords.Complex: The TOE administrators shall ensure that passwords to all TOE accounts meet the following quality metric: the probability that a secret can be obtained by an attacker during the lifetime of the secret is less than 2^-20.

OSP	Rationale for security objectives
P.SNMP.Unaccessible	The OSP: ● Administrative users shall not use the SNMP interface of the TOE and the SNMP interface shall have a sufficiently strong SNMP password to prevent non-administrative users from accessing and using this interface. is satisfied by: ● O.User.Authenticated: The TOE shall require identification and authentication of users before allowing them to use the TOE. ● OE.SNMP.Unaccessible: Administrative users shall not use the SNMP interface of the TOE and administrative users shall provide a sufficiently strong SNMP password for the SNMP interface to prevent non-administrative users from accessing and using this interface.
P.TOE.Authenticated	The OSP: ● For assured identification of the end point, the iSCSI Client shall identify and authenticate the TOE when initiating a request. is satisfied by: ● OE.TOE.Authenticated: The iSCSI Client shall provide assured identification of the TOE when the iSCSI Client initiates a request to the TOE.

Table 6: Sufficiency of objectives enforcing Organizational Security Policies

5 Extended Components Definition

5.1 Class FCS: Cryptographic support

This section describes the functional requirements for the generation of random numbers to be used as secrets for cryptographic purposes or authentication. The IT security functional requirements for a TOE are defined in an additional family (FCS_RNG) of the Class FCS (Cryptographic support).

5.1.1 Generation of random numbers (RNG)

Family behaviour

This family defines quality requirements for the generation of random numbers that are intended to be used for cryptographic purposes.

Component levelling

FCS_RNG.1 Generation of random numbers, requires that the random number generator implements defined security capabilities and that the random numbers meet a defined quality metric.

Management: FCS_RNG.1

There are no management activities foreseen.

Audit: FCS_RNG.1

There are no audit events foreseen.

5.1.1.1 FCS_RNG.1 - Random number generation

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1 **The TSF shall provide a deterministic random number generator that implements:**

- **DRG.2.1: If initialized with a random seed [selection: *using PTRNG of class PTG.2 as random source, using PTRNG of class PTG.3 as random source, using NPTRNG of class NTG.1 as random source, [assignment: other requirements for seeding]*], the internal state of the RNG shall [selection: *have [assignment: amount of entropy], have [assignment: work factor], require [assignment: guess work]*].**
- **DRG.2.2: The RNG provides forward secrecy.**
- **DRG.2.3: The RNG provides backward secrecy.**

FCS_RNG.1.2 **The TSF shall provide random numbers that meet:**

- **DRG.2.4: The RNG initialized with a random seed [assignment: *requirements for seeding*] generates output for which [assignment: *number of strings*] strings of bit length 128 are mutually different with probability [assignment: *probability*].**

- **DRG.2.5: Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A [assignment: *additional test suites*].**

6 Security Requirements

6.1 TOE Security Functional Requirements

The following table shows the Security functional requirements for the TOE, and the operations performed on the components according to CC part 2: iteration (Iter.), refinement (Ref.), assignment (Ass.) and selection (Sel.).

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
FAU - Security audit	FAU_GEN.1 Audit data generation		CC Part 2	No	No	Yes	Yes
	FAU_GEN.2 User identity association		CC Part 2	No	No	No	No
	FAU_SAR.1 Audit review		CC Part 2	No	No	Yes	No
FCS - Cryptographic support	FCS_CKM.1 Cryptographic key generation		CC Part 2	No	No	Yes	No
	FCS_CKM.2 Cryptographic key distribution		CC Part 2	No	Yes	Yes	No
	FCS_COP.1-hmac Cryptographic operation	FCS_COP.1	CC Part 2	Yes	No	Yes	No
	FCS_COP.1-sym Cryptographic operation	FCS_COP.1	CC Part 2	Yes	No	Yes	No
	FCS_RNG.1 Random number generation		ECD	No	No	Yes	Yes
FDP - User data protection	FDP_ACC.1 Subset access control		CC Part 2	No	No	Yes	No
	FDP_ACF.1 Security attribute based access control		CC Part 2	No	No	Yes	No
	FDP_RIP.1 Subset residual information protection		CC Part 2	No	No	Yes	Yes
FIA - Identification and authentication	FIA_ATD.1 User attribute definition		CC Part 2	No	No	Yes	No
	FIA_UAU.2 User authentication before any action		CC Part 2	No	No	No	No
	FIA_UID.2 User identification before any action		CC Part 2	No	No	No	No
	FIA_USB.1 User-subject binding		CC Part 2	No	No	Yes	No
FMT - Security management	FMT_MOF.1 Management of security functions behaviour		CC Part 2	No	No	Yes	Yes
	FMT_MSA.1 Management of security attributes		CC Part 2	No	No	Yes	Yes

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
	FMT_MSA.3 Static attribute initialisation		CC Part 2	No	Yes	Yes	Yes
	FMT_MTD.1 Management of TSF data		CC Part 2	No	No	Yes	Yes
	FMT_SMF.1 Specification of management functions		CC Part 2	No	No	Yes	No
	FMT_SMR.1 Security roles		CC Part 2	No	No	Yes	No
FPT - Protection of the TSF	FPT_STM.1 Reliable time stamps		CC Part 2	No	No	No	No
FTP - Trusted path/channels	FTP_ITC.1 Inter-TSF trusted channel		CC Part 2	No	Yes	Yes	Yes

Table 7: Security functional requirements for the TOE

6.1.1 Security audit (FAU)

6.1.1.1 Audit data generation (FAU_GEN.1)

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

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

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

c) [

- **iSCSI logon/logoff success and failure**
- **administrator logon/logoff success and failure**

].

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**event level (audit, info, warning, error, fatal)**].

6.1.1.2 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.

6.1.1.3 Audit review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide [

- **Group Administrators**
- **Pool Administrators**
- **Volume Administrators**
- **Read-only Administrators**

] with the capability to read [

- **event date**
- **event time**
- **event description (including event type and event outcome)**
- **event level**
- **subject identity (if applicable)**

] from the audit records.

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

6.1.2 Cryptographic support (FCS)

6.1.2.1 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 [

- **SSH-2 symmetric key and secret key generation**
- **TLSv1.0 symmetric key and secret key generation**

] and specified cryptographic key sizes [

- **SSH-2:**
  - **128, 192, and 256 bits for AES keys**
  - **168 bits for TDEA keys**
  - **160 bits for HMAC SHA-1 secrets**
  - **96 bits for HMAC SHA-1-96 secrets**
- **TLSv1.0:**
  - **128 and 256 bits for AES keys**
  - **168 bits for TDEA keys**
  - **160 bits for HMAC SHA-1 secrets**

] that meet the following: [

- **SSH-2:**
  - **[RFC4251] (SSH-2 symmetric key generation and secret key generation)**
  - **[RFC4253] (SSH-2 HMAC support)**
- **TLSv1.0:**
  - **[RFC2246] (TLSv1.0 symmetric key and secret key generation)**

- **[RFC3268] (TLSv1.0 AES support)**

].

6.1.2.2 Cryptographic key distribution (FCS_CKM.2)

FCS_CKM.2.1 The TSF shall distribute *symmetric* cryptographic keys in accordance with a specified cryptographic key distribution method [

- **SSH-2:**
  - **diffie-hellman-group1-sha1**
  - **diffie-hellman-group14-sha1**
  - **diffie-hellman-group-exchange-sha1**
  - **diffie-hellman-group-exchange-sha256**
- **TLSv1.0:**
  - **Anonymous Diffie-Hellman (ADH)**

] that meets the following: [

- **SSH-2:**
  - **[RFC4253] (SSH-2 key exchange algorithms)**
  - **[RFC4419] (SSH-2 additional key exchange algorithms)**
- **TLSv1.0:**
  - **[RFC2246] (TLSv1.0 key exchange algorithms)**

].

6.1.2.3 Cryptographic operation (FCS_COP.1-hmac)

FCS_COP.1.1 The TSF shall perform [**data authentication**] in accordance with a specified cryptographic algorithm [

- **SSH-2:**
  - **HMAC-SHA-1**
  - **HMAC SHA-1-96**
- **TLSv1.0:**
  - **HMAC-SHA-1**

] and cryptographic key sizes [

- **160 bits (HMAC SHA-1)**
- **96 bits (HMAC SHA-1-96)**

] that meet the following: [

- **SSH-2:**
  - **[RFC4251] (SSH-2 general HMAC support)**
  - **[RFC4253] (SSH-2 detailed HMAC support)**
- **TLSv1.0:**
  - **[RFC2246] (TLSv1.0)**

].

6.1.2.4 Cryptographic operation (FCS_COP.1-sym)

FCS_COP.1.1 The TSF shall perform [**symmetric encryption and decryption**] in accordance with a specified cryptographic algorithm [

- **SSH-2:**
  - **AES (CBC mode and CTR mode)**
  - **TDEA with three independent keys (CBC mode)**
- **TLSv1.0:**
  - **AES (CBC mode)**
  - **TDEA with three independent keys (CBC mode)**

] and cryptographic key sizes [

- **SSH-2:**
  - **128, 192, and 256 bits (AES)**
  - **168 bits (TDEA)**
- **TLSv1.0:**
  - **128 and 256 bits (AES)**
  - **168 bits (TDEA)**

] that meet the following: [

- **SSH-2:**
  - **[RFC4253] (SSH-2 using TDEA with CBC mode and AES with CBC mode)**
  - **[RFC4344] (SSH-2 using AES with CTR mode)**
- **TLSv1.0:**
  - **[RFC3268] (TLSv1.0 using AES with CBC mode)**
  - **[RFC2246] (TLSv1.0 using TDEA with CBC mode)**

].

6.1.2.5 Random number generation (FCS_RNG.1)

FCS_RNG.1.1 The TSF shall provide a deterministic random number generator that implements:

- DRG.2.1: If initialized with a random seed [**using vendor specific RNG as random source**], the internal state of the RNG shall [**have a minimum entropy of 40 bits**].
- DRG.2.2: The RNG provides forward secrecy.
- DRG.2.3: The RNG provides backward secrecy.

Application Note: *The vendor specific RNG uses timing information from external input signals such as input-randomness, interrupt-randomness, and disk-randomness as entropy sources.*

FCS_RNG.1.2 The TSF shall provide random numbers that meet:

- DRG.2.4: The RNG initialized with a random seed [**holding 80 bits of entropy**] generates output for which [**at least 2^{14}**] strings of bit length 128 are mutually different with probability [**of greater than $1-2^{-8}$**].

- DRG.2.5: Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A.

Application Note: *The TOE contains one vendor specific RNG which is used for both TLS and SSH-2 key generation.*

6.1.3 User data protection (FDP)

6.1.3.1 Subset access control (FDP_ACC.1)

Volume/Snapshot SFP		
Type	**Short name**	**Definition**
Subjects	S_iSCSI_Client	Computers that communicate to the TOE using the iSCSI protocol. This does not include array Group member communication.
Objects	O_Snapshot	A point-in-time copy of a volume.
	O_Volume	A set of array pages commonly used to house a single filesystem.
Operations	Read	Read the contents within the object.
	Write	Modify (including creating and deleting) the contents within the object.
Security Attributes of Subjects	AS_ChapName	The subject’s CHAP user name.
	AS_InitiatorName	The subject’s iSCSI initiator name.
	AS_IpAddress	The subject’s IP address.
Security Attributes of Objects	AO_SnapshotAcl	The snapshot's ACL.
	AO_VolumeAcl	The volume's ACL.
Rules	R_Empty	All subjects are denied access to an object when no ACL entries exist in that object’s ACL.
	R_Entries	A subject can read and write the contents within an object when the subject’s security attributes match all specified subject security attributes (CHAP user name and/or IP address and/or iSCSI initiator name) of one or more ACL entries in that object’s ACL.

Table 8: Volume/Snapshot SFP

FDP_ACC.1.1 The TSF shall enforce the [**Volume/Snapshot SFP**] on [**subjects, objects, and operations as defined by the Volume/Snapshot SFP**].

6.1.3.2 Security attribute based access control (FDP_ACF.1)

FDP_ACF.1.1 The TSF shall enforce the [**Volume/Snapshot SFP**] to objects based on the following: [**subjects and objects as defined by the Volume/Snapshot SFP, and for each, the security attributes as defined by the Volume/Snapshot SFP**].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**rules as defined by the Volume/Snapshot SFP**].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**none**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**none**].

6.1.3.3 Subset residual information protection (FDP_RIP.1)

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

6.1.4 Identification and authentication (FIA)

6.1.4.1 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [

- **Client I&A:**
  - **User name**
  - **User password**
  - **User role**
- **Group I&A:**
  - **Group name**
  - **Group membership password**
  - **Group member's IP address**

].

Application Note: *When the TOE is configured to use a RADIUS server, Client I&A security attributes for iSCSI Clients may be stored in this server. Group I&A security attributes are always maintained within each array. Client I&A includes both Administrators and iSCSI Clients (see section 7.1.2 for more detail).*

6.1.4.2 User authentication before any action (FIA_UAU.2)

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

6.1.4.3 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.

6.1.4.4 User-subject binding (FIA_USB.1)

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [

- **Client I&A:**
  - **User name**
  - **User role**
- **Group I&A:**
  - **Group member's IP address**

].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [**none**].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [**none**].

6.1.5 Security management (FMT)

6.1.5.1 Management of security functions behaviour (FMT_MOF.1)

FMT_MOF.1.1 The TSF shall restrict the ability to [**modify the behavior of**] the functions [**time synchronization source**] to [**Group Administrator**].

6.1.5.2 Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1 The TSF shall enforce the [**Volume/Snapshot SFP**] to restrict the ability to [**modify**] the security attributes [**object ACL**] to [**Group Administrator, Pool Administrator, and Volume Administrator**].

6.1.5.3 Static attribute initialisation (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the [**Volume/Snapshot SFP**] to provide [**permissive**] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow ~~the~~ [**none**] to specify alternative initial values to override the default values when an object or information is created.

6.1.5.4 Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to [**add, modify, delete**] the [**user accounts and user account data**] to [**Group Administrator**].

6.1.5.5 Specification of management functions (FMT_SMF.1)

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

- **Management of ACLs**
- **Management of users including user role assignments**
- **Management of the time synchronization source**

].

6.1.5.6 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles [

- **Group Administrator**
- **Pool Administrator**
- **Volume Administrator**
- **Read-only Administrator**
- **iSCSI Client**

].

Application Note: *The iSCSI Client role is an implicit role. See section 7.1.4 for more information.*

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

6.1.6 Protection of the TSF (FPT)

6.1.6.1 Reliable time stamps (FPT_STM.1)

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

6.1.7 Trusted path/channels (FTP)

6.1.7.1 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1 The TSF shall provide ~~a~~ *an administrative* communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

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

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**none**].

6.2 Security Functional Requirements Rationale

6.2.1 Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

Security Functional Requirements	Objectives
FAU_GEN.1	O.Event.Logged
FAU_GEN.2	O.Event.Logged
FAU_SAR.1	O.Event.Viewable
FCS_CKM.1	O.AdmCom.Protected
FCS_CKM.2	O.AdmCom.Protected
FCS_COP.1-hmac	O.AdmCom.Protected
FCS_COP.1-sym	O.AdmCom.Protected
FCS_RNG.1	O.AdmCom.Protected
FDP_ACC.1	O.Object.Protected
FDP_ACF.1	O.Object.Protected
FDP_RIP.1	O.Object.Zeroed
FIA_ATD.1	O.User.Authenticated
FIA_UAU.2	O.User.Authenticated
FIA_UID.2	O.User.Authenticated
FIA_USB.1	O.User.Authenticated
FMT_MOF.1	O.Event.Logged
FMT_MSA.1	O.Object.Protected
FMT_MSA.3	O.Object.Protected
FMT_MTD.1	O.User.Managed
FMT_SMF.1	O.Event.Logged, O.Object.Protected, O.User.Managed
FMT_SMR.1	O.User.Managed
FPT_STM.1	O.Event.Logged
FTP_ITC.1	O.AdmCom.Protected

Table 9: Mapping of security functional requirements to security objectives

6.2.2 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives:

Security objectives	Rationale
O.AdmCom.Protected	The objective: ● The TOE shall protect network administrative communication channels from disclosure and modification. is satisfied by: ● FCS_CKM.1: Specifying the type of cryptographic keys generated by the TOE. ● FCS_CKM.2: Specifying the cryptographic key distribution methods used by the TOE. ● FCS_COP.1-hmac: Specifying the HMAC algorithms used for administrative communication security. ● FCS_COP.1-sym: Specifying symmetric key algorithms used for administrative communication security. ● FCS_RNG.1: Specifying the random number generator characteristics used in symmetric key generation and secret key generation. ● FTP_ITC.1: Specifying the protection of network administrative communication channels.
O.Event.Logged	The objective: ● The TOE shall offer a recording mechanism that provides an audit trail of TOE usage. Security-relevant events shall be logged and the logs maintained and protected from unauthorized disclosure or alteration within this audit trail. is satisfied by: ● FAU_GEN.1: Specifying the audit events generated by the TOE. ● FAU_GEN.2: Specifying the association of user identities with events. ● FMT_MOF.1: Specifying the management of the mechanism used for time synchronization. ● FMT_SMF.1: Specifying that the time synchronization source can be managed by the TOE. ● FPT_STM.1: Specifying that reliable time stamps exist for use in the audit events.
O.Event.Viewable	The objective: ● The TOE shall provide a mechanism for authorized administrators to view audit records in a human readable format. is satisfied by: ● FAU_SAR.1: Specifying a mechanism for authorized users to review audit records.
O.Object.Protected	The objective: ● The TOE shall ensure that users are authorized to access the protected objects of the TOE and ensure that users can perform only the actions allowed by the user's User Role in accordance to the security policy of the TOE. is satisfied by:

Security objectives	Rationale
	• FDP_ACC.1: Specifying the Volume/Snapshot ACL policy. • FDP_ACF.1: Specifying the Volume/Snapshot ACL rules. • FMT_MSA.1 & FMT_MSA.3: Specifying how the Volume/Snapshot ACLs are managed by the identified role(s). • FMT_SMF.1: Specifying that the Volume/Snapshot ACLs can be managed by the TOE.
O.Object.Zeroed	The objective: • The TOE shall remove residual information from deallocated array pages before the array pages are made available. is satisfied by: • FDP_RIP.1: Specifying that residual information can be removed from array pages upon allocation.
O.User.Authenticated	The objective: • The TOE shall require identification and authentication of users before allowing them to use the TOE. is satisfied by: • FIA_ATD.1: Specifying the user security attributes associated with a TOE user. • FIA_UAU.2: Specifying the authentication of TOE users. • FIA_UID.2: Specifying the identification of TOE users. • FIA_USB.1: Specifying the binding of the identified user to the connection.
O.User.Managed	The objective: • The TOE shall provide for the creation, deletion, and management of authorized users and the assigning of administrative roles to administrative users. is satisfied by: • FMT_MTD.1: Specifying how user accounts are managed by the identified role(s). • FMT_SMF.1: Specifying that user accounts can be managed by the TOE. • FMT_SMR.1: Specifying the user roles supported by the TOE.

Table 10: Security objectives for the TOE rationale

6.2.3 Security requirements dependency analysis

The following table demonstrates the dependencies of SFRs modeled in CC Part 2 and how the SFRs for the TOE resolve those dependencies:

Security Functional Requirement	Dependencies	Resolution
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1	FAU_GEN.1
	FIA_UID.1	FIA_UID.2
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1]	FCS_CKM.2 FCS_COP.1-hmac FCS_COP.1-sym
	FCS_CKM.4	This dependency is unresolved. The keys used for authentication are not formally destroyed. The object reuse mechanisms in the runtime environment prevent their use except for in the intended context.
FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
	FCS_CKM.4	This dependency is unresolved. The distributed symmetric keys are not formally destroyed. The object reuse mechanisms in the runtime environment prevent their use except for in the intended context.
FCS_COP.1-hmac	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
	FCS_CKM.4	This dependency is unresolved. The keys used for authentication are not formally destroyed. The object reuse mechanisms in the runtime environment prevent their use except for in the intended context.
FCS_COP.1-sym	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
	FCS_CKM.4	This dependency is unresolved. The keys used for authentication are not formally destroyed. The object reuse mechanisms in the runtime environment prevent their use except for in the intended context.
FCS_RNG.1	No dependencies.	
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1	FDP_ACC.1
	FMT_MSA.3	FMT_MSA.3
FDP_RIP.1	No dependencies.	
FIA_ATD.1	No dependencies.	

Security Functional Requirement	Dependencies	Resolution
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UID.2	No dependencies.	
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MOF.1	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1
	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.3	FMT_MSA.1	FMT_MSA.1
	FMT_SMR.1	FMT_SMR.1
FMT_MTD.1	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_SMF.1	No dependencies.	
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_STM.1	No dependencies.	
FTP_ITC.1	No dependencies.	

Table 11: TOE SFR dependency analysis

6.3 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 2 components as specified in [CC] part 3, augmented by ALC_FLR.1.

The following table shows the Security assurance requirements, and the operations performed on the components according to CC part 3: iteration (Iter.), refinement (Ref.), assignment (Ass.) and selection (Sel.).

Security assurance class	Security assurance requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
ADV Development	ADV_ARC.1 Security architecture description	CC Part 3	No	No	No	No
	ADV_FSP.2 Security-enforcing functional specification	CC Part 3	No	No	No	No

Security assurance class	Security assurance requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
	ADV_TDS.1 Basic design	CC Part 3	No	No	No	No
AGD Guidance documents	AGD_OPE.1 Operational user guidance	CC Part 3	No	No	No	No
	AGD_PRE.1 Preparative procedures	CC Part 3	No	No	No	No
ALC Life-cycle support	ALC_CMC.2 Use of a CM system	CC Part 3	No	No	No	No
	ALC_CMS.2 Parts of the TOE CM coverage	CC Part 3	No	No	No	No
	ALC_DEL.1 Delivery procedures	CC Part 3	No	No	No	No
	ALC_FLR.1 Basic flaw remediation	CC Part 3	No	No	No	No
ASE Security Target evaluation	ASE_INT.1 ST introduction	CC Part 3	No	No	No	No
	ASE_CCL.1 Conformance claims	CC Part 3	No	No	No	No
	ASE_SPD.1 Security problem definition	CC Part 3	No	No	No	No
	ASE_OBJ.2 Security objectives	CC Part 3	No	No	No	No
	ASE_ECD.1 Extended components definition	CC Part 3	No	No	No	No
	ASE_REQ.2 Derived security requirements	CC Part 3	No	No	No	No
	ASE_TSS.1 TOE summary specification	CC Part 3	No	No	No	No
ATE Tests	ATE_COV.1 Evidence of coverage	CC Part 3	No	No	No	No
	ATE_FUN.1 Functional testing	CC Part 3	No	No	No	No
	ATE_IND.2 Independent testing - sample	CC Part 3	No	No	No	No
AVA Vulnerability assessment	AVA_VAN.2 Vulnerability analysis	CC Part 3	No	No	No	No

Table 12: Security assurance requirements

6.4 Security Assurance Requirements Rationale

The evaluation assurance level has been chosen to match a basic attack potential commensurate with the threat environment that is experienced by typical consumers of the TOE. In addition, the evaluation assurance level has been augmented with ALC_FLR.1 commensurate with the augmented flaw remediation capabilities offered by the developer beyond those required by the evaluation assurance level.

7 TOE Summary Specification

7.1 TOE Security Functionality

The following subsections explain how the security functions are implemented. The TOE security functionality (TSF) described in these subsections cover the various SFR classes defined in this ST.

The primary security features of the TOE are:

- Auditing
- Identification and authentication
- User data protection
- Security management
- Reliable time stamps
- Trusted channel

7.1.1 Auditing

The TOE generates audit records for logon and logoff events for both successful and failure attempts. It also generates records for start-up and shutdown of the audit functions. The records include the following attributes:

- event date and time
- event type
- subject identity (if applicable)
- event outcome
- event level (audit, info, warning, error, fatal).

The TOE also provides the ability for authorized users to view audit records via either a web browser or SSH. For each audit record, the interfaces display the following attributes:

- event date and time
- event description (including event type and event outcome)
- subject identity (if applicable)
- event level (audit, info, warning, error, fatal)

The roles authorized to view audit records are:

- Group Administrator
- Pool Administrator
- Volume Administrator
- Read-only Administrator

This section maps to the following SFR(s):

- FAU_GEN.1 - Audit data generation
- FAU_GEN.2 - User identity association
- FAU_SAR.1 - Audit review

7.1.2 Identification and authentication (I&A)

7.1.2.1 Client I&A

The TOE supports identification and authentication of all client users. Users are required to authenticate when connecting via the iSCSI protocol, the network administrative interface, and the serial connection. No actions can be performed by a user until after the user has been successfully identified and authenticated.

The iSCSI Client interface uses CHAP for authenticating users. The network administrative interfaces prompt for the administrator name and password and pass the responses to the TOE.

The iSCSI Client accounts can be defined in the local user account database and/or a RADIUS server. In the evaluated configuration, the administrative user accounts must be defined in the local user account database only.

For iSCSI Client user accounts, if both the local and RADIUS databases are configured, the TOE will accept the user's credentials if there is a credential match in either database.

For all client interface types (i.e., iSCSI protocol, network administrative interface, and serial connection) and client authentication mechanism types, the TOE maintains the following security attributes belonging to individual users:

- User name
- User password
- User role

Once a client user is successfully authenticated, the TOE associates the following user security attributes with subjects acting on behalf of that user:

- User name
- User role

The evaluated configuration requires the iSCSI Clients to authenticate the TOE, thus, providing mutual authentication of the iSCSI connections.

This section maps to the following SFR(s):

- FIA_ATD.1 - User attribute definition
- FIA_UAU.2 - User authentication before any action
- FIA_UID.2 - User identification before any action
- FIA_USB.1 - User-subject binding

7.1.2.2 Group I&A

Multiple arrays can be grouped together by a Group Administrator to function as a single array. Each array that joins a Group is known as a Group member. Each Group has an array that acts as the Group leader. As each array joins a Group, it is required to mutually authenticate to the Group leader. The TOE in the Group leader and the TOEs in the other Group members perform the Group I&A. No Group-related actions can be performed by a Group member until after the Group member has been successfully identified and authenticated by the TOE of the Group leader. An array can only be a member of one Group.

Each Group has a single Group name and a single Group membership password defined by the Group Administrator and stored locally by each TOE; hence, RADIUS is not used for Group I&A. As Group members authenticate to the Group leader and detach from the Group leader, the Group

leader dynamically grows and shrinks its authenticated Group members table to accommodate these changes. The TOE in the Group leader propagates this table to the other Group members so that the other Group member TOEs know which arrays are an active part of the Group in case the Group leader becomes inactive.

Each Group member's IP address is used to uniquely identify the Group member in the Group. Each TOE uses CHAP to mutually authenticate to the Group leader using the Group name as the CHAP "User name" and the Group membership password as the CHAP "User password".

The TOE maintains the following security attributes belonging to individual Groups:

- Group name
- Group membership password

Once a Group member is successfully authenticated by the TOE, the TOE associates the following security attribute with that Group member:

- Group member's IP address

This section maps to the following SFR(s):

- FIA_ATD.1 - User attribute definition
- FIA_UAU.2 - User authentication before any action
- FIA_UID.2 - User identification before any action
- FIA_USB.1 - User-subject binding

7.1.3 User data protection

7.1.3.1 Access control

The TOE implements access control lists (ACLs) to protect access to volumes and snapshots by iSCSI Clients. Each ACL consists of zero or more records. Each record contains one or more of the following security attributes:

- CHAP user name
- IP address
- iSCSI initiator name

In order for a subject to match a record, the subject's security attributes must match all specified security attributes in the record. In order for the TOE to grant access, the subject must match at least one record in the ACL. If no records exist in an ACL, access is denied to the object that the ACL protects.

When an ACL is first created, it contains no records. This restrictive default behavior cannot be modified. Members of the Group Administrator role can modify any volume and snapshot ACL. Members of the Pool Administrator role can modify volume and snapshot ACLs in the pools for which they are the Pool Administrator. Members of the Volume Administrator role can modify volume and snapshot ACLs of the volumes and snapshots for which they are the Volume Administrator.

This section maps to the following SFR(s):

- FDP_ACC.1 - Subset access control
- FDP_ACF.1 - Security attribute based access control
- FMT_MSA.1 - Management of security attributes
- FMT_MSA.3 - Static attribute initialisation

7.1.3.2 Residual information protection

The TOE zeroizes (write zeros in every byte of) a page of disk space at page allocation time. This prevents unintended access to residual data that may exist on a page from prior usage.

This section maps to the following SFR(s):

- FDP_RIP.1 - Subset residual information protection

7.1.4 Security management

The TOE supports the following authorized user roles:

- Group Administrator
- Pool Administrator
- Volume Administrator
- Read-only Administrator
- iSCSI Client (an implicit role)

The Group Administrator role is the most powerful of the roles and is used to manage the TOEs including the users assigned to the other roles. The Pool Administrator role is an administrative role used to manage pools of virtual storage space, but the role has less power than the Group Administrator role. The Volume Administrator role is an administrative role used to manage volumes within a pool, but the role has less power than the Pool Administrator role. The Read-only Administrator can monitor administrative information, but cannot modify the information. The iSCSI Client role is the least powerful role and is implicitly assigned to any computer connection that connects to the TOE through the iSCSI network connection(s).

Only a Group Administrator user can create and manage other Group Administrator users, Pool Administrator users, Volume Administrator users, and Read-only Administrator users. Pool Administrator users, Volume Administrator users, and Read-only Administrator users cannot create or manage other user accounts.

In addition, the TOE provides management for managing users including user role assignments, managing volume and snapshot ACLs, and managing the time synchronization source.

This section maps to the following SFR(s):

- FMT_MTD.1 - Management of TSF data
- FMT_SMF.1 - Specification of management functions
- FMT_SMR.1 - Security roles

7.1.5 Reliable time stamps

The TOE uses an internal time source to provide reliable time stamps for audit records. The Group Administrator can optionally configure the TOE to use the Network Time Protocol (NTP) to synchronize the TOE's internal time source.

This section maps to the following SFR(s):

- FMT_MOF.1 - Management of security function behaviour
- FPT_STM.1 - Reliable time stamps

7.1.6 Trusted channel

The TOE establishes a trusted channel for administrative communication between itself and SSH/SCP clients and between itself and web browsers (TLS). In the case of the web browser, the web browser initially connects using HTTP and downloads a Java program from the TOE into the web browser. The Java program then establishes a TLS connection with the TOE. The versions of SSH/SCP and TLS supported in the evaluated configuration are:

- SSH-2 (for both SSH and SCP)
- TLSv1.0

In all cases, these Operational Environment products (i.e., the SSH/SCP client and web browser) initiate communication by contacting the TOE. The TOE requires the web browsers and SSH/SCP clients to provide an administrative user name and password for identification and authentication. (The user name and password are typically supplied by the web browser user and SSH/SCP user.)

For TLS, the following cipher suites are supported in the evaluated configuration (where 3DES means TDEA and DH_anon means ADH):

- TLS_DH_anon_WITH_AES_256_CBC_SHA (a.k.a. ADH-AES256-SHA)
- TLS_DH_anon_WITH_AES_128_CBC_SHA (a.k.a. ADH-AES128-SHA)
- TLS_DH_anon_WITH_3DES_EDE_CBC_SHA (a.k.a. ADH-DES-CBC3-SHA)

For TLS, the following MAC (Message Authentication Code) algorithm is supported in the evaluated configuration:

- hmac-sha1 (160 bits)

For SSH/SCP, the following encryption algorithms are supported in the evaluated configuration:

- aes256-cbc
- aes192-cbc
- aes128-cbc
- aes256-ctr
- aes192-ctr
- aes128-ctr
- 3des-cbc

For SSH/SCP, the following MAC (Message Authentication Code) algorithms are supported in the evaluated configuration:

- hmac-sha1 (160 bits)
- hmac-sha1-96 (96 bits)

For SSH/SCP, the following key exchange algorithms are supported in the evaluated configuration:

- diffie-hellman-group1-sha1
- diffie-hellman-group14-sha1
- diffie-hellman-group-exchange-sha1
- diffie-hellman-group-exchange-sha256

For both TLS and SSH/SCP, TDEA uses three independent keys.

The TOE includes a software-based deterministic random number generator (DRNG) for generating TLS and SSH-2 session keys used in trusted channel communication. The DRNG has a minimum entropy of 40 bits and provides both forward secrecy and backward secrecy.

This section maps to the following SFR(s):

- FCS_CKM.1 - Cryptographic key generation
- FCS_CKM.2 - Cryptographic key distribution
- FCS_COP.1-hmac - Cryptographic operation
- FCS_COP.1-sym - Cryptographic operation
- FCS_RNG.1 - Random number generation
- FTP_ITC.1 - Inter-TSF trusted channel

8 Abbreviations, Terminology and References

8.1 Abbreviations

3DES
Triple Data Encryption Standard (a.k.a. TDEA)

ACL
Access Control List

ADH
Anonymous Diffie-Hellman

AES
Advanced Encryption Standard

ATA
Advanced Technology Attachment

CBC
Cypher-Block Chaining

CC
Common Criteria

CHAP
Challenge Handshake Authentication Protocol

CLI
Command Line Interface

CTR
Counter

DES
Data Encryption Standard

DH
Diffie-Hellman

DNS
Domain Name Service

DRNG
Deterministic Random Number Generator

EAL
Evaluation Assurance Level

FTP
File Transfer Protocol

GUI
Graphical User Interface

IP
Internet Protocol

IPsec
IP Security

iSCSI
Internet SCSI

MAC
Message Authentication Code

NAS
Network-Attached Storage

NL
Nearline

NL SAS
Nearline Serial Attached SCSI

NPTRNG
Non-Physical True Random Number Generator

NTP
Network Time Protocol

PPP
Point-to-Point Protocol

RADIUS
Remote Authentication Dial In User Service

RNG
Random Number Generator

RPM
Revolutions Per Minute

SAN
Storage Area Network

SAS
Serial Attached SCSI

SATA
Serial ATA

SCP
Secure Copy

SCSI
Small Computer System Interface

SFP
Security Function Policy

SFR
Security Functional Requirement

SSD
Solid State Drive

SSH
Secure Shell

ST
Security Target

TDEA
Triple Data Encryption Algorithm

TDES
Triple Data Encryption Standard (a.k.a. TDEA)

TLS
Transport Layer Security

TOE
Target of Evaluation

TSF
TOE Security Functionality

8.2 Terminology

This section contains definitions of technical terms that are used with a meaning specific to this document. Terms defined in the [CC] are not reiterated here, unless stated otherwise.

Client I&A
Identification and authentication of Administrators (via the network administrative interface and serial connection) and iSCSI Clients.

iSCSI initiator
A computer that attempts to connect to a volume or snapshot (iSCSI target) on a SAN device using the iSCSI protocol.

iSCSI target
A volume or snapshot on a SAN device that accepts iSCSI protocol connections.

8.3 References

CC **Common Criteria for Information Technology Security Evaluation**
Version 3.1R3
Date July 2009
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R3.pdf
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R3.pdf

RFC1994 **PPP Challenge Handshake Authentication Protocol (CHAP)**
Author(s) William Allen Simpson
Version IETF RFC 1994
Date August 1996
Location http://tools.ietf.org/rfc/rfc1994.txt

RFC2246 **The TLS Protocol Version 1.0**
Author(s) T. Dierks
Version IETF RFC 2246
Date January 1999
Location http://tools.ietf.org/rfc/rfc2246.txt

RFC3268 **Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)**
Author(s) P. Chown
Version IETF RFC 3268
Date June 2002
Location http://tools.ietf.org/rfc/rfc3268.txt

RFC4251 **The Secure Shell (SSH) Protocol Architecture**
Author(s) T. Ylonen
Version IETF RFC 4251
Date January 2006
Location http://tools.ietf.org/rfc/rfc4251.txt

RFC4253 **The Secure Shell (SSH) Transport Layer Protocol**
Author(s) T. Ylonen
Version IETF RFC 4253
Date January 2006
Location http://tools.ietf.org/rfc/rfc4253.txt

RFC4344 **The Secure Shell (SSH) Transport Layer Encryption Modes**
Author(s) M. Bellare, T. Kohno, C. Namprempre
Version IETF RFC 4344
Date January 2006
Location http://tools.ietf.org/rfc/rfc4344.txt

RFC4419 **Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol**
Author(s) M. Friedl, N. Provos, W. Simpson
Version IETF RFC 4419
Date March 2006
Location http://tools.ietf.org/rfc/rfc4419.txt

RFC5048 **Internet Small Computer System Interface (iSCSI) Corrections and Clarifications**
Author(s) Mallikarjun Chadalapaka, Ed.
Version IETF RFC 5048
Date October 2007
Location http://tools.ietf.org/rfc/rfc5048.txt