Dell EqualLogic PS4000 Series Storage Array Firmware Version 7.1.1 Security Target

Version:	**3.22**
Status:	**Final**
Last Update:	**2017-04-06**

Trademarks

The following are trademarks of Dell Inc. in the United States, other countries, or both:

- Dell™
- DELL™ logo
- EqualLogic®

The following terms are trademarks of Microsoft Corporation in the United States, other countries, or both:

- Active Directory®
- Microsoft®

The following are trademarks of Oracle Corporation in the United States, other countries, or both:

- Java®
- Oracle®

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

Legal Notice

Revision History

Revision	Date	Author(s)	Changes to Previous Revision
3.22	2017-04-06	Scott Chapman, Jeremy Powell	Final Security Target.

Table of Contents

List of Tables

1 Introduction

1.1 Security Target Identification

Title: Dell EqualLogic PS4000 Series Storage Array Firmware Version 7.1.1 Security Target

Version: 3.22

Status: Final

Date: 2017-04-06

Sponsor: Dell Inc.

Developer: Dell Inc.

Certification Body: BSI

Certification ID: BSI-DSZ-CC-1008

Keywords: Dell, EqualLogic, SAN

1.2 TOE Identification

The TOE is Dell EqualLogic PS4000 Series Storage Array Firmware Version 7.1.1.

1.3 TOE Type

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

1.4 TOE Overview

The Dell EqualLogic PS4000 Series Storage Array is a high performance, enterprise-level 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 can 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 (ACLs)) 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 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 model number. This hardware model contains one to two controller cards.

- PS4000 - E, X, XV

The model suffixes in this hardware model number have the following definitions:

- E - Serial Advanced Technology Attachment (SATA) drives or Nearline Serial Attached SCSI (NL SAS) drives
- X - 10,000 RPM Serial Attached SCSI (SAS) drives
- XV - 15,000 RPM SAS drives

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

- iSCSI initiator software
- SAN Headquarters (SAN HQ) application, remote client to the TOE's SAN HQ service

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

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

Other Operational Environment hardware and/or software (e.g., Virtual Private Network (VPN)) may be required to secure the network communication between the TOE and other Operational Environment components. Section 1.4.2 contains more information on this. The method used to secure the network communication is environment specific; therefore, it cannot be detailed in this document.

1.4.2 Intended method of use

The arrays in which the TOE runs, including all physical connectors on an array, are intended to be located in a restricted access room (e.g., a server room) and accessible only by administrative personnel. This is to prevent physical tampering by non-administrative personnel.

Each array has an administrative serial connection that supports a terminal or terminal emulator and contains an administrative command line interface (CLI). If a terminal device is connected to this serial port, it is intended that the terminal device reside in the restricted access room with the array because the communication protocol that the TOE uses to communicate with the terminal device cannot be secured by the TOE.

The TOE also supports the same administrative CLI using the SSH/SCP protocol. Since this protocol protects the communication between the SSH/SCP client and TOE, the SSH/SCP client can be located either inside the restricted access room or outside the restricted access room.

The network traffic between remote components of the TOE and between trusted IT entities and the TOE (excluding the SSH/SCP client) is <u>not</u> protected by the TSF. It is intended that the administrator will provide other means (e.g., VPN, restricted physical access, organizational policies) to protect the network traffic between the TOE and the following supported Operational Environment components:

- Web browser GUIs
- SAN HQ clients
- iSCSI Clients
- Active Directory server
- RADIUS server
- NTP server
- Other Group member arrays

1.4.3 Major security features

The major security features of the TOE are:

- Auditing
- User data protection
- Identification and authentication (I&A)
- Security management
- Reliable time stamps
- Trusted channel
- Default access banners

1.5 TOE Description

1.5.1 TOE introduction and logical boundary

The TOE is the firmware 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. In addition, the TOE supports multipath input/output (MPIO) allowing iSCSI initiators to open multiple channels to the TOE over multiple physical connections in order to increase the data bandwidth between the iSCSI initiator and the TOE. 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 ACLs and Access Policies. Each volume has its own ACL and may be associated with zero or more Access Policies.

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) and a CLI. 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 GUI's network communication is not protected from disclosure and modification in the evaluated configuration. The CLI resides in the firmware, is accessible using an SSH/SCP client, and provides similar functionality as the GUI. The CLI protects its network communication from disclosure and modification using SSH/SCP. The web browser and SSH/SCP client are part of the Operational Environment.

The TOE provides another administrative interface to a service called SAN HQ that allows administrators to collect health data about the members of the array. The TOE authenticates SAN HQ users using the same authentication database as the other administrative interfaces. Users only have read access to the health data; no write access is provided. The remote applications that access this interface are outside the TOE boundary in the Operational Environment.

In addition, the TOE supports the Volume Shadow Copy Service (VSS) and Virtual Disk Service (VDS) network protocols (a.k.a. VSS/VDS) found on Microsoft Windows platforms using the iSCSI protocol. These services appear as a volume know as the "vss-control" pseudo volume. By default, access to the "vss-control" pseudo volume by iSCSI Clients is disabled.

The TOE supports the following authentication databases:

- Local
- RADIUS
- Active Directory

A local authentication database is stored on the local storage drives of the array by the TOE. The RADIUS server and Active Directory are remote authentication databases that are 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 I&A.

1.5.2 TOE structure

The operating software of the array consists of two major parts, a network stack and a storage stack, which are executed in parallel. Memory protection is used for separation. Dedicated memory regions are used for the stacks to communicate. The network stack implements high speed network

protocols (e.g., iSCSI) as well as the lower layers of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol. The storage stack implements the high speed storage algorithms and provides the execution environment for low speed background operations that are implemented as user mode processes. These user mode processes provide the administration algorithms and system monitoring functions.

1.5.3 TOE security features

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

1.5.3.1 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.

1.5.3.2 User data protection

1.5.3.2.1 Access control

The TOE uses ACLs and Access Policies to protect iSCSI access to individual volumes and snapshots. iSCSI Clients must pass the object's ACL and Access Policy check in order to gain access to data in the object.

Similarly, the TOE uses ACLs and Access Policies to control access to the "vss-control" pseudo volume. iSCSI Clients must pass the pseudo volume's ACL and Access Policy check in order to access the TOE's VSS/VDS services.

1.5.3.2.2 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.

1.5.3.3 Identification and authentication (I&A)

1.5.3.3.1 Client I&A

The TOE supports I&A of all client users. Users are required to authenticate when connecting via the iSCSI protocol, the network administrative interfaces (i.e., GUI, SAN HQ, SSH/SCP), 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.

Both the iSCSI Client accounts and the administrative user accounts can be defined in the local user account database or in a RADIUS server. Only administrative user accounts can be defined in Active Directory. For each administrator, the TOE maintains the following user attributes:

- User name
- User password
- User role
- Kerberos ticket (when using Active Directory and single-sign on GUI sessions)

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	✔	✔
Active Directory		✔

Table 1: Authentication databases and supported user types

The TOE supports the following authentication database configurations:

- Local only
- Local and RADIUS
- Local and Active Directory

The TOE does not support the use of RADIUS and Active Directory simultaneously.

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 administrative user accounts, the TOE always checks the local database first for an account and then, if the administrative user account is not found, it checks the remote database (RADIUS, Active Directory), if one is configured. If Active Directory is configured and an administrator logs on to his computer using his Active Directory ID, when the administrator uses the TOE's administrative GUI, the GUI will use the Active Directory single sign-on feature (using Kerberos tickets) to automatically log the administrator onto the TOE.

The TOE will terminate administrative sessions on the CLI and GUI interfaces after an administrator configurable period of inactivity. It will also terminate SAN HQ sessions after 60 seconds of inactivity.

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.

A second type of iSCSI Client account exists, known as a transient iSCSI Client account. A transient account is the same as a non-transient iSCSI Client account except that the TOE automatically deletes the transient account after 24 hours of inactivity. An iSCSI initiator requests the creation of a transient iSCSI Client account for accessing a specific snapshot or volume when using multipath input/output (MPIO) connections. The TOE assigns the same access rights to the transient account as those assigned to the requesting iSCSI Client account for that snapshot or volume. Each transient account has its own CHAP user name and password that are stored in the local user account database.

1.5.3.3.2 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 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 and Active Directory are 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 Internet protocol (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".

1.5.3.4 Security management

The TOE supports the following authorized user roles:
- Group Administrator
- Pool Administrator
- Volume Administrator
- Read-only Administrator
- iSCSI Client
- SAN HQ 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, by default, 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). An iSCSI Client can be given the ability to perform administrative tasks by allowing the iSCSI Client access to the VSS/VDS services.

The SAN HQ Client role provides access to the TOE's SAN HQ service. This role allows read-only access to the configuration database, low-level system statistics, and crash-dumps of any failed daemon processes.

In addition, the TOE provides management interfaces for managing users including user role assignments, managing volume and snapshot ACLs, managing the time synchronization source, modifying the session inactivity timeout value, and modifying the access banner.

1.5.3.5 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 NTP to synchronize the TOE's internal time source.

1.5.3.6 Trusted channel

The TOE uses SSH to protect the CLI network communication and provides for protection of the transferred data from disclosure and modification as well as assured identification of both end points.

1.5.3.7 Default access banner

The TOE presents an access banner to all users before authenticating to the administrative interfaces.

1.5.4 Security policy data

This section describes the security policy model for the TOE.

1.5.4.1 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.
- **SAN HQ Client**- Administrator computer (i.e., user) used to monitor the health of the TOE.

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. This also includes the "vss-control" pseudo volume.

1.5.4.2 TSF data and security attributes

The following TSF data and security attributes are maintained by the TOE:
- Audit records
- Time synchronization source setting
- Administrator account data, including the following security attributes:
  - ○ User name
  - ○ User password

- ○ User role
- ○ Kerberos ticket (when using Active Directory with single-sign on GUI sessions)
- ● Group account data, including the following security attributes:
  - ○ Group name
  - ○ Group membership password
  - ○ Group member's IP address
- ● Snapshot and volume (including the "vss-control" pseudo volume) ACLs and Access Policies.
- ● Open Secure Shell (OpenSSH) RSA host key
- ● Access banners
- ● Inactivity timeouts
- ● SAN HQ readable objects:
  - ○ Configuration database
  - ○ Low-level statistics
  - ○ Core dumps of failed daemon processes

1.5.4.3 User data

The following user data are maintained by the TOE:

- ● Data contained in a volume or snapshot

1.5.5 Physical boundary

The TOE consists of the firmware and the guidance documentation.

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

- ● 32-bit image:
  - ○ kit_V7.1.1-R400572_351401522.tgz

Each firmware installation image 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 CLI that is used by administrators when they connect to the array using SSH/SCP or the serial connection.

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

- ● Updating Firmware for Dell EqualLogic PS Series Storage Arrays and FS Series Appliances
- ● EqualLogic Master Glossary Version 7.0
- ● Dell EqualLogic PS Series Storage Arrays iSCSI Initiator and Operating System Considerations
- ● Dell EqualLogic PS Series Storage Arrays Release Notes and Fix List PS Series Firmware 7.1.1

- Dell EqualLogic Group Manager Administrator's Manual PS Series Firmware 7.0, FS Series Firmware 3.0
- Dell EqualLogic Group Manager Online Help PS Series Firmware Version 7.0 FS Series Firmware Version 3.0
- Dell EqualLogic Group Manager CLI Reference Guide PS Series Firmware 7.0, FS Series Firmware 3.0
- PS Series Storage Arrays Common Criteria Configuration Guide Version 7.1
- Dell EqualLogic Events Guide PS Series Firmware 7.0, FS Series Firmware 3.0

1.5.6 Evaluated configuration

The evaluated configuration consists of the firmware and guidance documentation as specified in section 1.5.5 for the hardware model listed in section 1.4.1. It includes the optional use of a RADIUS server or Active Directory as authentication servers, both of which reside 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 1.5.5. 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 FTP daemon (ftpd) and the Telnet daemon (telnetd) must be disabled.
- All certificates created and issued by the Operational Environment for use with the TOE must be signed using the SHA-1 hash algorithm or stronger (e.g., SHA-2).

1.5.7 Operational Environment

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

1.5.7.1 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 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 following networks must be located in a non-hostile environment:
- iSCSI network
- Group network
- the RADIUS and Active Directory server networks
- the management network containing the SAN HQ Client and GUI client
- the NTP server network

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 VPN (e.g., non-TSF supplied IPsec) between enterprise sites
- Providing resources with up-to-date anti-virus tools and applying security updates regularly

2 CC Conformance Claim

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

This Security Target does not claim conformance to any Protection Profile.

Common Criteria [CC] version 3.1 revision 4 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 basic level of expertise and effort. The TOE protects against straightforward or intentional breach of TOE security by attackers possessing a basic 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.

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 GUI network traffic, SAN HQ network traffic, iSCSI network traffic, the Group network traffic, the NTP network traffic, and the RADIUS and Active Directory server network traffic from disclosure to 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 Logical

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 and Active Directory, if used by the TOE, provide protection against unauthorized access to TSF data stored within them.

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 supports in the protection of the integrity and confidentiality of user and TSF data (including cryptographic material, user databases, and trusted certificates) 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

Any Network Time Protocol server the TOE uses to synchronize the realtime clock is a reliable time source.

A.SSHServerKeys.Authenticated

Any SSH client used to administer the TOE authenticates the TOE each time a secure channel is established.

3.3 Organizational Security Policies

P.Event.Logged

To preserve operational accountability and security, records that provide an audit log of security-relevant events will be created and reviewed by authorized personnel.

P.Credentials.Complex

All secrets used to construct credentials imported into the TOE shall be generated using a sufficient amount of entropy. Cryptographic secrets must be generated from at least 100 bits of entropy. Passwords must be complex enough such that the probability that the password can be obtained by an attacker during the lifetime of the secret is less than 2^{-20}.

P.Credentials.SafelyGenerated

All secrets used to construct credentials imported into the TOE shall be generated on a system that employs security controls that counter threats commensurate with the threats countered by the TOE itself.

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.

P.SSHServerKeys.Distributed

The administrator is responsible for acquiring and distributing SSH key fingerprints in a secure manner.

P.CertHash.Strong
Administrative users shall ensure that all certificates created and issued by the Operational Environment for use with the TOE are signed using the SHA-1 hash algorithm or stronger (e.g., SHA-2).

4 Security Objectives

4.1 Objectives for the TOE

O.AdmCom.Protected

The TOE shall protect the administrative network traffic over SSH from disclosure to and modification from non-administrative personnel.

O.Event.Logged

The TOE shall offer a recording mechanism that provides an audit trail of
- Successful and unsuccessful logon and logoff attempts on the TOE interactive administrative interfaces
- Successful and unsuccessful logon and logoff attempts on the TOE iSCSI interface
- Unsuccessful logon and logoff attempts on the TOE SAN HQ interface.

These 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.

O.Session.Locking

The TOE shall lock (or terminate) inactive sessions.

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 and Active Directory, if used by the TOE, shall provide protection against unauthorized access to TSF data stored within them.

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 support in the protection of the integrity and confidentiality of user and TSF data (including cryptographic material, user databases, and trusted certificates) 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 GUI network traffic, SAN HQ network traffic, iSCSI network traffic, the Group network traffic, the NTP network traffic, and the RADIUS and Active Directory server network traffic from disclosure to and modification by non-administrative personnel.

OE.Credentials.Complex

All secrets used to construct credentials imported into the TOE shall be generated using a sufficient amount of entropy. Cryptographic secrets must be generated from at least 100 bits of entropy. Passwords must be complex enough such that the probability that the password can be obtained by an attacker during the lifetime of the secret is less than 2^{-20}.

Note: *Passwords are allowed be less complex than cryptographic secrets because the TOE implements mitigating security mechanisms to rate limit the guessing of passwords.*

OE.Credentials.SafelyGenerated

All secrets used to construct credentials imported into the TOE shall be generated on a system that employs security controls that counter threats commensurate with the threats countered by the TOE itself.

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.

OE.NTP.Reliable

Any Network Time Protocol server the TOE uses to synchronize the realtime clock shall be reliable time source.

OE.RealtimeClock.Reliable

The real time clock of the underlying hardware platform shall provide reliable time stamps.

OE.SSHServerKeys.Distributed

The administrator acquire and distribute SSH key fingerprints in a secure manner.

OE.SSHServerKeys.Authenticated

Any SSH client used to administer the TOE shall authenticate the TOE each time a secure channel is established.

OE.CertHash.Strong

All certificates created and issued by the Operational Environment for use with the TOE shall be signed using the SHA-1 hash algorithm or stronger (e.g., SHA-2).

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	P.Event.Logged
O.Event.Viewable	P.Event.Logged
O.Object.Protected	T.Access.Unauthorized
O.Object.Zeroed	T.Access.Unauthorized
O.User.Authenticated	T.Access.Unauthorized P.SNMP.Unaccessible
O.User.Managed	T.Access.Unauthorized
O.Session.Locking	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.Credentials.Complex	P.Credentials.Complex P.SNMP.Unaccessible
OE.Credentials.SafelyGenerated	P.Credentials.SafelyGenerated
OE.Physical.Protected	A.Physical.Protected
OE.SNMP.Unaccessible	P.SNMP.Unaccessible
OE.TOE.Authenticated	P.TOE.Authenticated
OE.User.Trained	A.User.Trained
OE.NTP.Reliable	A.NTP.Reliable P.Event.Logged

Objective	Assumptions / Threats / OSPs
OE.RealtimeClock.Reliable	P.Event.Logged
OE.SSHServerKeys.Distributed	P.SSHServerKeys.Distributed
OE.SSHServerKeys.Authenticated	A.SSHServerKeys.Authenticated
OE.CertHash.Strong	P.CertHash.Strong

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	Unauthorized access to TSF and user data stored and processed by the TOE is countered by O.Object.Protected, where the TSF enforces an access control policy on all objects in the TOE. Unauthorized access to TSF and user data transmitted by the TOE is countered by O.AdmCom.Protected, where the TSF prevents the data from unauthorized disclosure and modification using SSH. All data contained in the storage array will be zeroed by the TSF before reallocation (O.Object.Zeroed) to prevent accidental unauthorized disclosure of TSF or user data. The TSF requires authentication of users so that authorization for access to TSF or user data can be determined (O.User.Authenticated). The TSF mitigates the risk of unauthorized users gaining access to an authorized user's session by terminating sessions after a period of inactivity (O.Session.Locking). Administrators can manage users' authorization through management functions of the TSF (O.User.Managed).

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	This assumption is directly upheld by OE.Network.Protected.
A.Physical.Protected	This assumption is directly upheld by OE.Physical.Protected.
A.Admin.Trained	This assumption is directly upheld by OE.Admin.Trained.
A.Admin.Trusted	This assumption is directly upheld by OE.Admin.Trusted.
A.User.Trained	This assumption is directly upheld by OE.User.Trained.
A.AdminClient.Trusted	This assumption is directly upheld by OE.AdminClient.Trusted.
A.AuthServers.Protected	This assumption is directly upheld by OE.AuthServers.Protected.
A.DNS.Trusted	This assumption is directly upheld by OE.DNS.Trusted.
A.Logical.Protected	This assumption is directly upheld by OE.Logical.Protected.
A.NTP.Reliable	This assumption is directly upheld by OE.NTP.Reliable.
A.SSHServerKeys.Authenticated	This assumption is directly upheld by OE.SSHServerKeys.Authenticated.

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 (OSP), 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.Event.Logged	The TOE maintains an audit log through O.Event.Logged, and allows authorized personnel to review the logs through O.Event.Viewable. The time stamps in the log are supported by the environment with OE.NTP.Reliable and OE.RealtimeClock.Reliable.
P.Credentials.Complex	This policy is directly enforced by OE.Credentials.Complex.
P.Credentials.SafelyGenerated	This policy is directly enforced by OE.Credentials.SafelyGenerated.
P.SNMP.Unaccessible	The TSF will restrict the SNMP interface to only those who authenticate (O.User.Authenticated). Administrators will not use the interface (OE.SNMP.Unaccessible) and will set its password to be sufficiently complex as required in OE.Credentials.Complex.
P.TOE.Authenticated	This policy is directly enforced by OE.TOE.Authenticated.
P.SSHServerKeys.Distributed	This policy is directly enforced by OE.SSHServerKeys.Distributed.

OSP	Rationale for security objectives
P.CertHash.Strong	This policy is directly enforced by OE.CertHash.Strong.

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*].**

Rationale

The quality of the random number generator is defined using this SFR. The quality metric required in FCS_RNG.1.2 is detailed in the German Scheme AIS20 and AIS31.

6 Security Requirements

6.1 TOE Security Functional Requirements

The following table shows the SFRs 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 Cryptographic operation		CC Part 2	No	No	Yes	No
	FCS_RNG.1-COMPOSED Composed random number generation	FCS_RNG.1	ECD	Yes	No	Yes	Yes
	FCS_RNG.1-KERNEL Kernel random number generation	FCS_RNG.1	ECD	Yes	Yes	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	Yes	No	No
FTA - TOE access	FTA_SSL.3-SANHQ TSF-initiated termination of SAN HQ sessions	FTA_SSL.3	CC Part 2	Yes	Yes	Yes	No
	FTA_SSL.3-ADMIN TSF-initiated termination of administrative sessions	FTA_SSL.3	CC Part 2	Yes	Yes	Yes	No
	FTA_TAB.1 Default TOE access banners		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: SFRs 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) [

- **Successful and unsuccessful logon and logoff attempts on the TOE interactive administrative interfaces**

- **Successful and unsuccessful logon and logoff attempts on the TOE iSCSI interface**

- **Unsuccessful logon and logoff attempts on the TOE SAN HQ interface.**

].

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)

Cryptographic key generation				
Protocol	**Key generation algorithm**	**Cryptographic algorithm**	**Key size**	**Standard**
SSH-2	RSA key generation using probable primes	RSA	2048 bits	[FIPS186-2] Chapter 7
	Diffie-Hellman key agreement and key derivation	AES	128, 192, and 256 bits	[RFC4253] SSH-2
		TDEA	168 bits	
		HMAC-SHA-1	160 bits	

Table 8: SSH-2 cryptographic key generation

FCS_CKM.1.1   The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**defined in Table 8 with a specified random number generator FCS_RNG.1-COMPOSED**] and specified cryptographic key sizes [**defined in Table 8**] that meet the following: [**the standard(s) defined in Table 8**].

6.1.2.2 Cryptographic key distribution (FCS_CKM.2)

Cryptographic key distribution		
Protocol	**Key distribution method**	**Standard**
SSH-2	Diffie-Hellman key exchange with the following method: ● diffie-hellman-group14-sha1	[RFC4253] SSH-2; [RFC3526] SSH Group 14

Table 9: SSH-2 cryptographic key distribution

FCS_CKM.2.1   The TSF shall distribute *symmetric* cryptographic keys in accordance with a specified cryptographic key distribution method [**defined in Table 9**] that meets the following: [**the standard(s) defined in Table 9**].

6.1.2.3 Cryptographic operation (FCS_COP.1)

Cryptographic operations					
Protocol	**Implemen-tation**	**Operation**	**Algorithm**	**Key size**	**Standard**
SSH-2	Software	Signature creation	RSA	2048 bits	[RFC3447] RSA algorithm, RSASSA-PKCS1-v1_5; [RFC4253] In SSH-2, the server signs the Diffie-Hellman parameters with its RSA private key for server authentication by the client
			SHA-1	N/A	
		Symmetric encryption and decryption	AES (CBC mode and CTR mode)	128, 192, and 256 bits	[RFC4253] SSH-2 using TDEA with CBC mode and AES with CBC mode; [RFC4344] SSH-2 using AES with CTR mode; [SP800-38A] Block cipher modes; [FIPS197] AES algorithm; [SP800-67] TDEA algorithm
			TDEA with three independent keys (CBC mode)	168 bits	

Cryptographic operations					
Protocol	**Implemen-tation**	**Operation**	**Algorithm**	**Key size**	**Standard**
		Data authentication	HMAC-SHA-1	160 bits	[RFC4251]🔗 SSH-2 general HMAC support; [RFC4253]🔗 SSH-2 detailed HMAC support; [FIPS198-1]🔗 HMAC; [FIPS180-4]🔗 SHA-1 and SHA-2
			HMAC-SHA-1-96	160 bits	

Table 10: SSH-2 cryptographic operations

FCS_COP.1.1   The TSF shall perform [**the operations defined in Table 10**] in accordance with a specified cryptographic algorithm [**defined in Table 10**] and cryptographic key sizes [**defined in Table 10**] that meet the following: [**the standard(s) defined in Table 10**].

6.1.2.4 Composed random number generation (FCS_RNG.1-COMPOSED)

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 the Kernel RNG defined by FCS_RNG.1-KERNEL 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.

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

- DRG.2.4: The RNG initialized with a random seed [**holding 160 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: *This RNG is used to generate SSH keys and the SSH host key pair (RSA key generation).*

6.1.2.5 Kernel random number generation (FCS_RNG.1-KERNEL)

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

- ~~DRG.2.1~~ *DRG.3.1*: If initialized with a random seed [**using a vendor specific RNG as random source**], the internal state of the RNG shall [**have a minimum entropy of 180 bits**].
- ~~DRG.2.2~~ *DRG.3.2*: The RNG provides forward secrecy.
- ~~DRG.2.3~~ *DRG.3.3*: The RNG provides backward secrecy *even if the current internal state is known*.

    Application Note: *The vendor specific RNG uses timing information from external input signals such as network and disk Input/Output interrupts.*

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

- ~~DRG.2.4~~ *DRG.3.4*: The RNG initialized with a random seed [**holding 256 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~~ *DRG.3.5*: 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: *Refinements were used to make the FCS_RNG.1 ECD conform to Class DRG.3.*

6.1.3 User data protection (FDP)

6.1.3.1 Subset access control (FDP_ACC.1)

Volume/Snapshot/VSS SFP (Part 1 of 2: Subject/object access control)		
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	Snapshot - A point-in-time copy of a volume.
	O_Volume	Volume - A set of array pages commonly used to house a single filesystem.
	O_Vss	The "vss-control" pseudo volume.
Operations	Admin	Perform VSS/VDS services.
	Read	Read the contents within a snapshot or volume.
	Write	Modify (including creating and deleting) the contents within a snapshot or volume.
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_VolAcl	The snapshot or volume's ACL.
	AO_VolPolicy	A snapshot or volume's Access Policy.
	AO_VssAcl	The "vss-control" pseudo volume's ACL.
	AO_VssPolicy	A "vss-control" pseudo volume's Access Policy.
Rules	R_Empty	All subjects are denied access to an object when no ACL entries exist in that object's ACL and it has no Access Policies associated with it.

Volume/Snapshot/VSS SFP (Part 1 of 2: Subject/object access control)		
Type	**Short name**	**Definition**
	R_VolAcl	A subject can read and write the contents within a snapshot or volume when the subject's security attributes match all specified subject security attributes (CHAP user name and/or iSCSI initiator name and/or IP address) of one or more ACL entries in that snapshot or volume's ACL.
	R_VolPolicy	A subject can read and write the contents within a snapshot or volume when the subject's security attributes match all specified subject security attributes (CHAP user name and/or iSCSI initiator name and/or IP address) of one or more Access Policies of that snapshot or volume.
	R_VssAcl	A subject can perform VSS/VDS services when the subject's security attributes match all specified subject security attributes (CHAP user name and/or iSCSI initiator name and/or IP address) of one or more ACL entries in the "vss-control" pseudo volume's ACL.
	R_VssPolicy	A subject can perform VSS/VDS services when the subject's security attributes match all specified subject security attributes (CHAP user name and/or iSCSI initiator name and/or IP address) of one or more Access Policies of the "vss-control" pseudo volume.

Table 11: Volume/Snapshot/VSS SFP (Part 1 of 2: Subject/object access control)

FDP_ACC.1.1   The TSF shall enforce the [**Volume/Snapshot/VSS SFP**] on [**subjects, objects, and operations as defined in Table 11**].

6.1.3.2 Security attribute based access control (FDP_ACF.1)

FDP_ACF.1.1   The TSF shall enforce the [**Volume/Snapshot/VSS SFP**] to objects based on the following: [**subjects and objects as defined in Table 11, and for each, the security attributes as defined in Table 11**].

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 in Table 11**].

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**
  - ○ **User Kerberos Ticket (When using Active Directory with single-sign on GUI sessions)**

- **Group I&A:**
  - ○ **Group name**
  - ○ **Group membership password**
  - ○ **Group member's IP address**

].

Application Note: *When the TOE is configured to use either the RADIUS server or Active Directory, Client I&A security attributes for iSCSI Clients may be stored in these servers. 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.

Application Note: *This SFR applies to the administrative interfaces (GUI, CLI, and SAN HQ) and the iSCSI CHAP interfaces.*

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)

Volume/Snapshot/VSS SFP (Part 2 of 2: Security attribute management)		
Operation	**Security attribute**	**Authorized user or role**
Modify	ACLs on snapshots and volumes (AO_VolAcl)	The following roles: ● Group Administrators (for all snapshots and volumes) ● Pool Administrators of snapshots and volumes for the pools in which the user is a Pool Administrator ● Volume Administrators of snapshots and volumes for which the user is a Volume Administrator
Modify	ACL on the "vss-control" pseudo volume (AO_VssAcl)	Group Administrators
Create, modify, delete	Access Policies (AO_VolPolicy and AO_VssPolicy)	Group Administrators
Bind (Bind an Access Policy to a snapshot or volume)	Access Policies on snapshots and volumes (AO_VolPolicy)	The following roles: ● Group Administrators (for all snapshots and volumes) ● Pool Administrators of snapshots and volumes for the pools in which the user is a Pool Administrator ● Volume Administrators of snapshots and volumes for which the user is a Volume Administrator
Bind (Bind an Access Policy to the "vss-control" pseudo volume)	Access Policies on the "vss-control" pseudo volume (AO_VssPolicy)	Group Administrators

Table 12: Volume/Snapshot/VSS SFP (Part 2 of 2: Security attribute management)

FMT_MSA.1.1   The TSF shall enforce the [**Volume/Snapshot/VSS SFP**] to restrict the ability to [**perform operations as defined in Table 12 on**] the security attributes [**as defined in Table 12**] to [**the authorized users or roles as defined in Table 12**].

6.1.5.3 Static attribute initialisation (FMT_MSA.3)

FMT_MSA.3.1   The TSF shall enforce the [**Volume/Snapshot/VSS 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~~ [**no one**] 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)

TSF data management		
Operation	**TSF data**	**Authorized user and role**
Modify, delete, add	User accounts and user account data (except transient iSCSI Client accounts)	Group Administrator
Add	Transient iSCSI Client accounts for MPIO	iSCSI Client
Modify	Inactivity timeout	Group Administrator
Modify, delete, add	Access Banner	Group Administrator
Read	Configuration database, low-level system statistics, crash-dumps of any failed daemon processes	SAN HQ Client
Perform VSS/VDS services on	Snapshots and volumes	iSCSI Clients who have been granted access by a Group Administrator

Table 13: TSF data management

FMT_MTD.1.1   The TSF shall restrict the ability to [**perform the operations in Table 13 on**] the [**TSF data in Table 13**] to [**the authorized users and roles in Table 13**].

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 and Access Policies**
- **Management of users including user role assignments**
- **Management of the time synchronization source**
- **Management of session timeout**
- **Management of the access banner**

- **Reading of the SAN HQ health monitoring data**
- **VSS/VDS services**

].

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**
- **SAN HQ Client**

].

Application Note: *The iSCSI Client and SAN HQ Client roles are implicit roles. 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 *by synchronizing the real time clock using the Network Time Protocol.*

Application Note: *The real time clock is in the environment and is assumed to be reliable. See OE.RealtimeClock.Reliable. When used by the TOE, the Network Time Protocol servers are also assumed to be reliable. See OE.NTP.Reliable*

6.1.7 TOE access (FTA)

6.1.7.1 TSF-initiated termination of SAN HQ sessions (FTA_SSL.3-SANHQ)

FTA_SSL.3.1   The TSF shall terminate ~~an interactive session~~ *the session between the SAN HQ client and the TOE's SAN HQ service* after a [**60 second period of inactivity**].

6.1.7.2 TSF-initiated termination of administrative sessions (FTA_SSL.3-ADMIN)

FTA_SSL.3.1   The TSF shall terminate ~~an interactive~~ *an administrative* session after ~~a~~ [**an administrator defined amount of inactivity**].

Application Note: *This SFR only applies to administrative interfaces of the TOE.*

6.1.7.3 Default TOE access banners (FTA_TAB.1)

FTA_TAB.1.1   Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

6.1.8 Trusted path/channels (FTP)

6.1.8.1 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1   The TSF shall provide a~~a~~ *an administrative* communication channel *using SSH-2* between itself and ~~another trusted IT product~~ *an administrator's SSH client* 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~~ *and* disclosure.

FTP_ITC.1.2   The TSF shall permit [**~~another trusted IT product~~ *an administrator's SSH client***] to initiate communication via the trusted channel.

FTP_ITC.1.3   The TSF shall initiate communication via the trusted channel for [**management functions**].

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	O.AdmCom.Protected
FCS_RNG.1-COMPOSED	O.AdmCom.Protected
FCS_RNG.1-KERNEL	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

Security functional requirements	Objectives
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.Session.Locking, O.User.Managed
FMT_SMF.1	O.Event.Logged, O.Object.Protected, O.Session.Locking, O.User.Managed
FMT_SMR.1	O.User.Managed
FPT_STM.1	O.Event.Logged
FTA_SSL.3-SANHQ	O.Session.Locking
FTA_SSL.3-ADMIN	O.Session.Locking
FTA_TAB.1	O.Object.Protected
FTP_ITC.1	O.AdmCom.Protected

Table 14: 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 the administrative network traffic over SSH from disclosure to and modification from non-administrative personnel. 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: Specifying the symmetric key algorithms and HMAC algorithms used for administrative communication security.

Security objectives	Rationale
	● FCS_RNG.1-COMPOSED: Specifying the random number generator characteristics used in symmetric key generation and secret key generation. ● FCS_RNG.1-KERNEL: Specifying the random number generator characteristics used by FCS_RNG.1-COMPOSED. ● FTP_ITC.1: Specifying the protection of administrative SSH channels.

O.Event.Logged	The objective:
	● The TOE shall offer a recording mechanism that provides an audit trail of
	    ○ Successful and unsuccessful logon and logoff attempts on the TOE interactive administrative interfaces
	    ○ Successful and unsuccessful logon and logoff attempts on the TOE iSCSI interface
	    ○ Unsuccessful logon and logoff attempts on the TOE SAN HQ interface.
	These 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: ● FDP_ACC.1: Specifying the Volume/Snapshot security policy. ● FDP_ACF.1: Specifying the Volume/Snapshot security policy rules. ● FMT_MSA.1 & FMT_MSA.3: Specifying how the Volume/Snapshot security attributes are managed by the identified role(s).

Security objectives	Rationale
	● FMT_SMF.1: Specifying that the Volume/Snapshot security policy can be managed by the TOE. ● FTA_TAB.1: Providing a warning to users about unauthorized access
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.
O.Session.Locking	The objective: ● The TOE shall lock (or terminate) inactive sessions is satisfied by: ● FMT_MTD.1: Specifying how the inactivity timeout can be managed. ● FMT_SMF.1: Specifying that the inactivity timeout can be managed. ● FTA_SSL.3-SANHQ: Specifying that the TOE will terminate inactive SAN HQ sessions. ● FTA_SSL.3-ADMIN: Specifying that the TOE will terminate inactive administrative sessions.

Table 15: 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
	FCS_CKM.4	This dependency is unresolved. The generated keys 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	[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 encryption, decryption, and data 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-COMPOSED	No dependencies.	
FCS_RNG.1-KERNEL	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.	
FTA_SSL.3-SANHQ	No dependencies.	
FTA_SSL.3-ADMIN	No dependencies.	
FTA_TAB.1	No dependencies.	
FTP_ITC.1	No dependencies.	

Table 16: TOE SFR dependency analysis

6.3 Security Assurance Requirements

The security assurance requirements (SARs) 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 SARs, 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

Security assurance class	Security assurance requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
	ADV_FSP.2 Security-enforcing functional specification	CC Part 3	No	No	No	No
	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 17: SARs

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
- Default access banners

7.1.1 Auditing

The TOE generates audit records for:
- Successful and unsuccessful logon and logoff attempts on the TOE interactive administrative interfaces
- Successful and unsuccessful logon and logoff attempts on the TOE iSCSI interface
- Unsuccessful logon and logoff attempts on the TOE SAN HQ interface.

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 SFRs:
- 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 I&A of all client users. Users are required to authenticate when connecting via the iSCSI protocol, the network administrative interfaces (i.e., GUI, SAN HQ, SSH/SCP), 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.

Both the iSCSI Client accounts and the administrative user accounts can be defined in the local user account database and/or a RADIUS server. Only administrative user accounts can be defined in Active Directory. The TOE does not support the use of RADIUS and Active Directory simultaneously.

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 administrative user accounts for the CLI (both SSH/SCP and the serial connection), GUI, and SAN HQ interface, the TOE always checks the local database first for an account and then, if the administrative user account is not found, it checks the remote database (RADIUS or Active Directory), if one is configured. If Active Directory is configured and an administrator logs on to his computer using his Active Directory ID, when the user uses the TOE's administrative GUI, the GUI will use the Active Directory single sign-on feature to automatically log the user onto the TOE. This is done by providing the TOE a Kerberos ticket, which the TOE then validates with the Ticket Granting Server. The TOE prevents unauthorized yet authenticated access by comparing the authenticated user identity against the role stored in the Active Directory. Any users who do not have the administrative role associate with their identity are denied access.

SAN HQ authenticates users against the same authentication databases as the CLI and GUI. Any user account with read access to a group can be used to access the SAN HQ service.

The SAN HQ service terminates connections after 60 seconds of inactivity. If the client wishes to continue grabbing data, it must re-establish a connection.

For all client interface types (i.e., iSCSI protocol, network administrative interfaces, 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
- User kerberos Ticket (for use with Active Directory Single Sign On on the GUI only)

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.

As mentioned before, a second type of iSCSI Client account exists, known as a transient iSCSI Client account. A transient account is the same as a non-transient iSCSI Client account except that the TOE automatically deletes the transient account after 24 hours of inactivity. An iSCSI initiator requests the creation of a transient iSCSI Client account for accessing a specific snapshot or volume when using MPIO connections. The TOE assigns the same access rights to the transient account as those assigned to the requesting iSCSI Client account for that snapshot or volume. Each transient account has its own CHAP user name and password that are stored in the local user account database.

The TSF will terminate CLI and GUI sessions after an administrator defined amount of inactivity. The TSF will also terminate SAN HQ sessions when no traffic between the SAN HQ client and SAN HQ service is observed for a period of 60 seconds.

This section maps to the following SFRs:
- 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
- FTA_SSL.3-SANHQ- TSF-initiated termination of SAN HQ sessions
- FTA_SSL.3-ADMIN- TSF-initiated termination of administrative sessions

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 and Active Directory are 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 both access control lists (ACLs) and Access Policies to protect access to snapshots, volumes, and the "vss-control" pseudo volume by iSCSI Clients.

Each ACL consists of zero or more ACL entries. Each ACL entry contains one or more of the following security attributes:

- CHAP user name
- IP address
- iSCSI initiator name

In order for a subject to match an ACL entry, the subject's security attributes must match all specified security attributes in the entry. In order for the TOE to grant access, the subject must match at least one entry in the ACL. If no entries exist in an ACL, then the ACL mechanism does not grant the user access to the object.

When an ACL is first created, it contains no ACL entries. This default creation behavior cannot be modified.

An Access Policy is similar to an ACL except that it can be associated with multiple objects, which makes security management of subject permissions easier for the administrator. Access Policies can also be collected into Access Policy Groups which can be used to assign one or more Access Policies to objects en masse. Otherwise, Access Policies are functionally identical to ACLs. For purposes of this discussion, Access Policies and Access Policy Groups are simply called Access Policies.

An Access Policy contains entries called Access Points, each of which contain:

- CHAP user name
- A set of IP addresses
- iSCSI initiator name

In order for a subject to match an Access Point, the subject's security attributes must match all specified security attributes in the Access Point. In order for the TOE to grant access, the subject must match at least one Access Point in one of the Access Policies associated with the object. If no Access Points exist, then the Access Policy mechanism does not grant access to the object.

If neither the ACL nor the Access Policies grant the user access, then the user is denied access to the object.

For the management of snapshot and volume ACLs, members of the Group Administrator role can modify any ACL. Members of the Pool Administrator role can modify ACLs in the pools for which they are the Pool Administrator. Members of the Volume Administrator role can modify ACLs of the objects for which they are the Volume Administrator.

For the "vss-control" pseudo volume, only members of the Group Administrator role can modify the pseudo volume's ACL.

Unlike ACLs, Access Policies (and Access Policy Groups) are created independently of the object that they protect. Only members of the Group Administrator role can create, modify, and delete Access Policies (including Access Policy Groups).

For binding Access Policies to a snapshot and volume, members of the Group Administrator role can bind any Access Policy to any snapshot or volume. Members of the Pool Administrator role can bind any Access Policy to only a snapshot or volume in the pools for which they are the Pool Administrator. Members of the Volume Administrator role can bind any Access Policy to only a snapshot or volume for which they are the Volume Administrator.

For the "vss-control" pseudo volume, only members of the Group Administrator role can bind an Access Policy to the "vss-control" pseudo volume.

Granting access to a snapshot or volume implies that the iSCSI Client can read and write the contents of that snapshot or volume. Granting access to the "vss-control" pseudo volume implies that the iSCSI Client can perform VSS/VDS services on that array and gives Group Administrator access to the iSCSI Client for that array.

This section maps to the following SFRs:
- 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:
- 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)
- SAN HQ Client

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 typically the least powerful role and is implicitly assigned to any computer connection that connects to the TOE through the iSCSI network connection(s).

An iSCSI Client can also be used to perform management tasks using the VSS/VDS services. The iSCSI Client must be granted access to the "vss-control" pseudo volume in order to access these services. Granting an iSCSI Client access to this pseudo volume gives the iSCSI Client Group Administrator capabilities.

Only a Group Administrator user can setup SAN HQ, 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 security attributes, managing the time synchronization source, and modifying the session timeout value.

The SAN HQ user must have read access to the group in order to operate properly. In fact, it is recommended that the subject *only* have read access to the group. This is because the client used to access SAN HQ interacts with it without user direct interaction; therefore, the administrative account name and password are stored on the client. This access is part of the SAN HQ Client role. The SAN HQ Client role is implicitly assigned to any administrator who logs into the TOE through the SAN HQ interface.

This section maps to the following SFRs:

- 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 in the environment 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 SFRs:

- 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 a CLI client using SSH/SCP. The version of SSH/SCP supported in the evaluated configuration is:

- SSH-2 (for both SSH and SCP)

A CLI client initiates communication by contacting the TOE. The TOE requires the CLI client to provide an administrative user name and password for I&A. (The user name and password are supplied by the user of the CLI client.)

All SSH-2 cryptographic algorithms are implemented in software. 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 algorithm is supported in the evaluated configuration:

- diffie-hellman-group14-sha1

For SSH/SCP, TDEA (represented as "3des" above) uses three independent keys.

The TOE includes a software-based deterministic random number generator (DRNG) for generating SSH-2 session keys used in trusted channel communication. This DRNG has a minimum entropy of 40 bits and provides both forward secrecy and backward secrecy. This DRNG uses the Kernel RNG's output as seeding input for the OpenSSL SSLeay RNG. The Kernel RNG is seeded with random data generated by hardware sources. The Kernel RNG has at least 180 bits of entropy.

The SSH-2 server generates an asymmetric host key so that it can authenticate itself to its clients. Although SSH-2 supports several asymmetric encryption algorithms, in the evaluated configuration, only RSA with 2048 bit keys are allowed.

The SSH-2 server signs the Diffie-Hellman parameters with its RSA private key and sends this signature to the client. The client may then authenticate the server by verifying the signature and checking it against its local database of trusted certificates. This also anchors the trust to the symmetric keys exchanged during the Diffie-Hellman exchange. This is described in section 8 of [RFC4253].

This section maps to the following SFRs:

- FCS_CKM.1- Cryptographic key generation
- FCS_CKM.2- Cryptographic key distribution
- FCS_COP.1- Cryptographic operation
- FCS_RNG.1-COMPOSED- Composed random number generation
- FCS_RNG.1-KERNEL- Kernel random number generation
- FTP_ITC.1- Inter-TSF trusted SSH channel

7.1.7 Default access banners

The TOE displays an access banner to all users accessing the administrative interfaces to indicate that the system is trusted and no unauthorized personnel may use it. This banner appears on the CLI or GUI before the provides identification or authentication to the TOE.

A Group Administrator can modify the access banner arbitrarily for the group he or she administrates.

This section maps to the following SFRs:

- FTA_TAB.1- Default access banners
- FMT_MTD.1- Management of TSF data

8 Abbreviations, Terminology and References

8.1 Abbreviations

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

ACL
Access Control List

AD
Active Directory

AES
Advanced Encryption Standard

ATA
Advanced Technology Attachment

BSI
Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security)

CBC
Cypher-Block Chaining

CC
Common Criteria

CHAP
Challenge Handshake Authentication Protocol

CLI
Command Line Interface

CTR
Counter

DNS
Domain Name Service

DRNG
Deterministic Random Number Generator

EAL
Evaluation Assurance Level

ECD
Extended Components Definition

FTP
File Transfer Protocol

GUI
Graphical User Interface

HMAC
Hash-based Message Authentication Code

I&A
Identification and Authentication

IP
Internet Protocol

iSCSI
Internet SCSI

IT
Information Technology

MAC
Message Authentication Code

MPIO
Multipath Input/Output

NAS
Network-Attached Storage

NL
Nearline

NL SAS
Nearline Serial Attached SCSI

NPTRNG
Non-Physical True Random Number Generator

NTP
Network Time Protocol

OSP
Organizational Security Policy

PPP
Point-to-Point Protocol

PS
Peer Storage

RADIUS
Remote Authentication Dial In User Service

RNG
Random Number Generator

RPM
Revolutions Per Minute

SAN
Storage Area Network

SAN HQ
SAN Headquarters

SAS
Serial Attached SCSI

SATA
Serial ATA

SCP
Secure Copy

SCSI
Small Computer System Interface

SFP
Security Function Policy

SFR
Security Functional Requirement

SHA-1
Secure Hash Algorithm version 1

SHA-2
Secure Hash Algorithm version 2

SNMP
Simple Network Management Protocol

SSH
Secure Shell

SSLeay
Secure Sockets Layer Eric A. Young

ST
Security Target

TDEA
Triple Data Encryption Algorithm

TOE
Target of Evaluation

TSF
TOE Security Functionality

VDS
Virtual Disk Service

VPN
Virtual Private Network

VSS
Volume Shadow Copy Service

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   3.1R4
Date   September 2012
Location   http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf
Location   http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R4.pdf
Location   http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R4.pdf

FIPS180-4   **Secure Hash Standard (SHS)**
Version   FIPS PUB 180-4
Date   March 2012
Location   http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf

FIPS186-2   **DIGITAL SIGNATURE STANDARD (DSS)**
Version   FIPS PUB 186-2
Date   January 27, 2000
Location   http://csrc.nist.gov/publications/fips/archive/fips186-2/fips186-2.pdf

FIPS197   **Specification for the ADVANCED ENCRYPTION STANDARD (AES)**
Version   FIPS PUB 197
Date   November 26, 2001
Location   http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

FIPS198-1   **The Keyed-Hash Message Authentication Code (HMAC)**
Version   FIPS PUB 198-1
Date   July 2008
Location   http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf

RFC1994   **PPP Challenge Handshake Authentication Protocol (CHAP)**
Author(s)   W. Simpson
Date   1996-08-01
Location   http://www.ietf.org/rfc/rfc1994.txt

RFC3447   **Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1**
Author(s)   J. Jonsson, B. Kaliski
Date   2003-02-01
Location   http://www.ietf.org/rfc/rfc3447.txt

RFC3526   **More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)**
Author(s)   T. Kivinen, M. Kojo
Date   2003-05-01
Location   http://www.ietf.org/rfc/rfc3526.txt

RFC4251   **The Secure Shell (SSH) Protocol Architecture**
Author(s)   T. Ylonen, C. Lonvick
Date   2006-01-01
Location   http://www.ietf.org/rfc/rfc4251.txt

RFC4253   **The Secure Shell (SSH) Transport Layer Protocol**
Author(s)   T. Ylonen, C. Lonvick
Date   2006-01-01
Location   http://www.ietf.org/rfc/rfc4253.txt

RFC4344   **The Secure Shell (SSH) Transport Layer Encryption Modes**
Author(s)   M. Bellare, T. Kohno, C. Namprempre
Date   2006-01-01
Location   http://www.ietf.org/rfc/rfc4344.txt

RFC5048   **Internet Small Computer System Interface (iSCSI) Corrections and Clarifications**
Author(s)   M. Chadalapaka
Date   2007-10-01
Location   http://www.ietf.org/rfc/rfc5048.txt

SP800-38A   **Recommendation for Block Cipher Modes of Operation**
Author(s)   Morris Dworkin
Version   NIST Special Publication 800-38A 2001 Edition
Date   December 2001
Location   http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf

SP800-67   **NIST Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher**
Version   NIST Special Publication 800-67 Version 1.1
Date   May 19, 2008
Location   http://csrc.nist.gov/publications/nistpubs/800-67/SP800-67.pdf