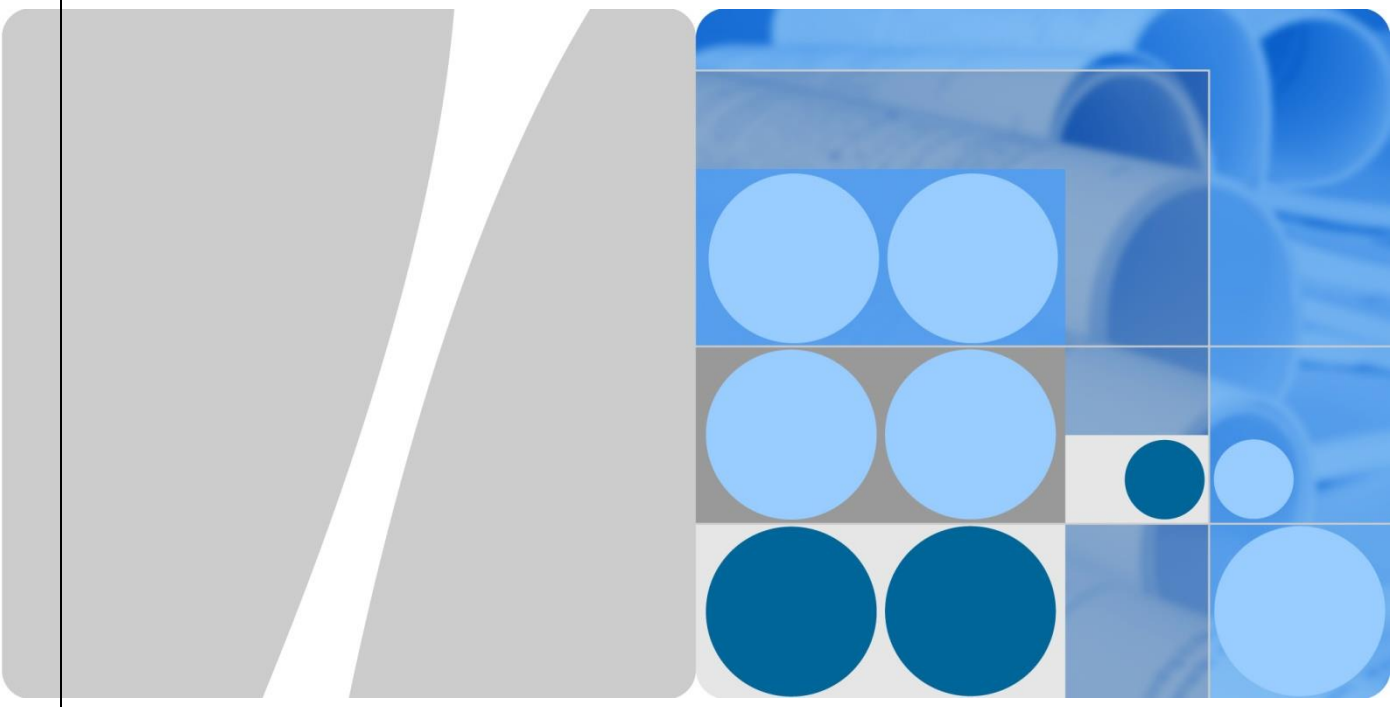

Security Target for Huawei OceanStor T&SX900 Series Storage System Software

Version 3.5

Date 2015-08-13

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

 and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Contents

Revision Record

Date	Revision Version	Change Description	Author
2013-3-6	0.1	Initial template	Yao Junning
2013-7-2	1.0	Fist version	Jiang Hongbin Zheng Xu Yao Junning
2013-08-19	1.1	TOE identification	
2013-9-5	1.2	TOE update according to E&E review result	Jiang Hongbin
2013-9-29	1.3	Second update according to E&E review result	Jiang Hongbin
2013-11-15	1.4	Revised according to Observation Report of HUA-STOR-OR-001 and HUA-STOR-OR-002	Yao Junning
2013-11-21	1.5	Revised according to E&E review result	Jiang Hongbin
2013-11-21	1.6	Revised according to E&E comments	Yao Junning
2013-12-5	1.7	Revised according to E&E comments HUA-STOR-OR-003	Jiang Hongbin
2013-12-18	1.8	Revised according to E&E observation report of HUA-STOR-OR-004 and HUA-STOR-OR-005	Jiang Hongbin
2013-12-28	1.9	Revised according to E&E comments of HUA-STOR-OR-001 to HUA-STOR-OR-005	Jiang Hongbin Chen ke
2014-1-13	2.0	Revised according to E&E comments of HUA-STOR-OR-001 to HUA-STOR-OR-005	Jiang Hongbin Chen ke
2014-1-20	2.1	Revised according to E&E comments	Jiang Hongbin Chen ke
2014-1-28	2.2	Revised according to E&E comments	Jiang Hongbin Chen ke
2014-2-12	2.3	Revised according to E&E comments	Jiang Hongbin Chen ke
2014-3-6	2.4	Revised according to E&E	Chen ke

		comments	
2014-4-29	2.5	Revised according to E&E comments	Jiang Hongbin
2014-5-8	2.6	Revised according to E&E comments	Jiang Hongbin
2014-5-27	2.7	Revised according to E&E comments	Jiang Hongbin
2014-7-1	2.8	Revised according to E&E comments	Jiang Hongbin
2014-7-24	2.9	Revised according to E&E comments	Jiang Hongbin
2014-11-18	3.0	Revised according to E&E comments	Jiang Hongbin
2015-05-26	3.1	Revised according to E&E comments	Jiang Zhifa
2015-06-05	3.2	Revised according to E&E comments	Jiang Zhifa
2015-07-03	3.3	Revised according to E&E comments	Jiang Zhifa
2015-08-05	3.4	Revised according to E&E comments	Jiang Zhifa
2015-08-13	3.5	Revised according to E&E comments	Jiang Zhifa

1 Introduction

This section contains the ST reference, TOE reference, TOE overview and TOE description of Huawei OceanStor T&SX900 Series Storage System. All of them are consistent with each other.

NOTE: SX900&SXX00T are the same product with different nomenclature depending on the final customer. The relation is as follows:

Enterprise users	**Operator user**
S2200T	NA
S2600T	S2900
S5500T	S3900
S5600T	S5900
S6800T	S6900

1.1 ST reference

This ST is uniquely identified as below,

Title: Huawei OceanStor T&SX900 Series Storage System V100R005 Security Target

Version: V3.5

Publication date: 2015-08-13

1.2 TOE reference

The TOE is identified as bellow,

TOE name: Huawei OceanStor T&SX900 Series Storage System Software

TOE version: V100R005C30SPC300

Developer: Huawei Technologies Co., Ltd.

1.3 Product overview

The product is a new generation storage system developed by Huawei Technologies Co., Ltd. based on the current industry environment and development trend. The storage system combines files and blocks, various protocols, and diversified management interfaces. It is based on the industry-leading hardware specifications and integrates such high-end technologies as high density disk design, TurboModule flexible interface module and hot swap design, TurboBoost three-level performance boost technology, and multi-layer data protection technology. The storage system satisfies the increasingly complicated storage requirements of various service applications at a low cost, such as database online transaction processing, digital media, Internet operation, centralized storage, backup, disaster recovery, and data migration, effectively ensuring the security and continuity of user services.

CHAP authentication is supported when connecting to the TOE with a iSCSI network. The target LUN on the TOE can be accessed only when the CHAP authentication is passed.

All these security features belongs to the product surrounding the TOE and not to the TOE itself, and therefore no assurance is claimed over them.

1.4 TOE overview

In this section, the TOE usage and its major security features, including the TOE type and major non-TOE hardware/software required by the TOE are summarized.

1.4.1 TOE usage and major security features

- **Usage**

The TOE is responsible for the authentication, access control and auditing of the management tasks (which are also part of the TOE) needed for the correct operation of the entire product. The TOE also implements a synchronization system in order to obtain timestamps used in the audit records.

- **TOE major security features**

Then, the major security features implemented by the TOE subject to evaluation are:

- **Authentication and Identification**
- **Access Control**
- **Auditing**
- **Security functionality management**
- **NTP management**

1.4.2 TOE type

The TOE is a management software running in a Storage system.

1.4.3 Non-TOE hardware/software/firmware required by the TOE

The TOE is running on T Series Hardware Model OceanStor S2200T, OceanStor S2600T, OceanStor S5500T, OceanStor S5600T, OceanStor S5800T, and OceanStor S6800T and SX900 Series Hardware Model OceanStor S2900, OceanStor S3900-M200, OceanStor S3900-M300, OceanS5900-M100, OceanStor S5900-M200 and OceanStor S6900-M100.

The TOE is running on customized Linux operative system based on kernel 2.6.32.

The figure 1 shows the real environment for the TOE running.

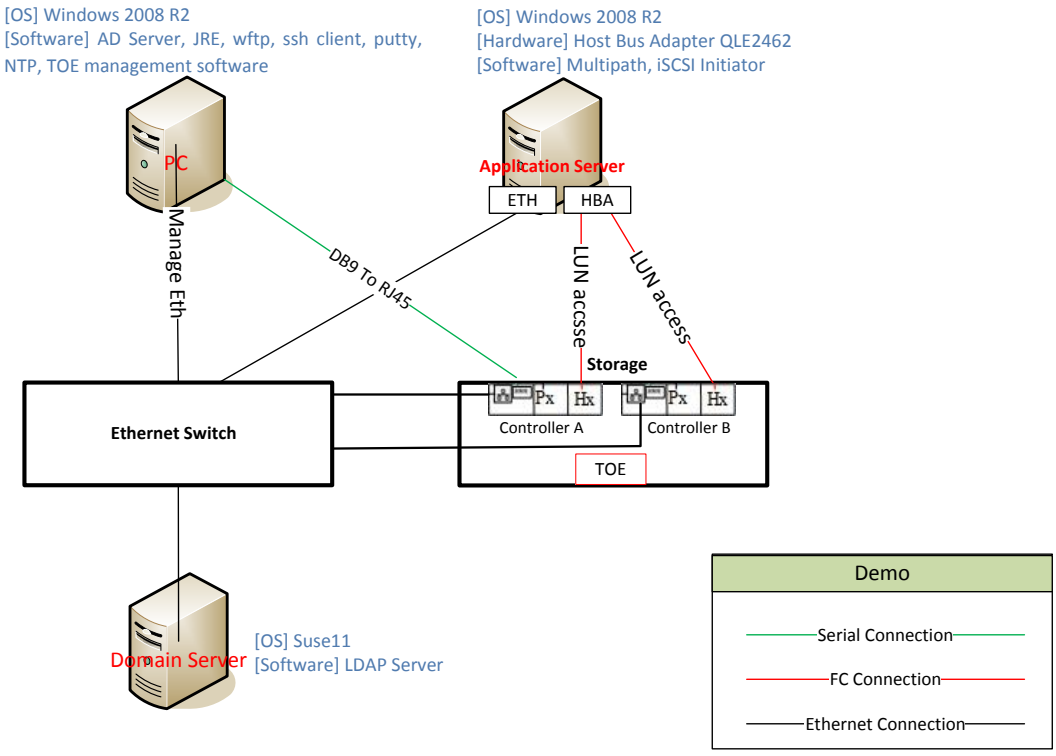

Figure 1 The Real environment of the TOE

- Description
  - Domain Server, Application Server, PC and the TOE (Storage) are connected with each other by an Ethernet Switch. The TOE ETH management will be accessed only through an independent local network. The fiber channel connection of the TOE is only used for LUN access.
  - There's a HBA (Host Bus Adapter) card installed on the Application Server, which has 2 FC ports; One of the FC ports connect to TOE's Controller_A and another one connect to Controller_B with FC cables.
  - The PC must have 1 serial port (DB9) and connect to the TOE with DB9_to_RJ45 cable, the serial port will be used for the AGD_PRE installation but after this, the serial port connection will not be accessible.
- Application server
  - Hardware
    - Rack Servers or PCs with at least 1 FC HBA (Host Bus Adapter) card and 2 100M/1G Ethernet Interface
  - Software
    - Multi-path software UltraPath V100R006C00SPC200
    - Windows Server 2008 R2 Operative System
    - Microsoft iSCSI Software Initiator Version 2.08
- Domain Server
  - Hardware
    - Personal Computer with at least 1 100M/1G Ethernet Interface
  - Software
    - PC operative system: Suse11
    - Application layer software: LDAP server (openldap 2) in Suse 11
- PC
  - Hardware
    - Rack Servers or PC with at least 1 100M/1G Ethernet Interface and 1 Serial DB9 Interface.
  - Software
    - Server operative system Windows Server 2008 R2
    - Windows AD (Active Directory) in Windows Server 2008 R2 service installed
    - JRE (Java Runtime Environment 1.6.0_10), WFTP server (wftpd 2.03), SSH client (SSH Secure Shell 3.2.9), Putty software (PuTTY 0.61).
    - Application layer software: NTP server in Windows Server 2008 R2
    - Manage software for the TOE (ISM V100R006C00SPCe00)

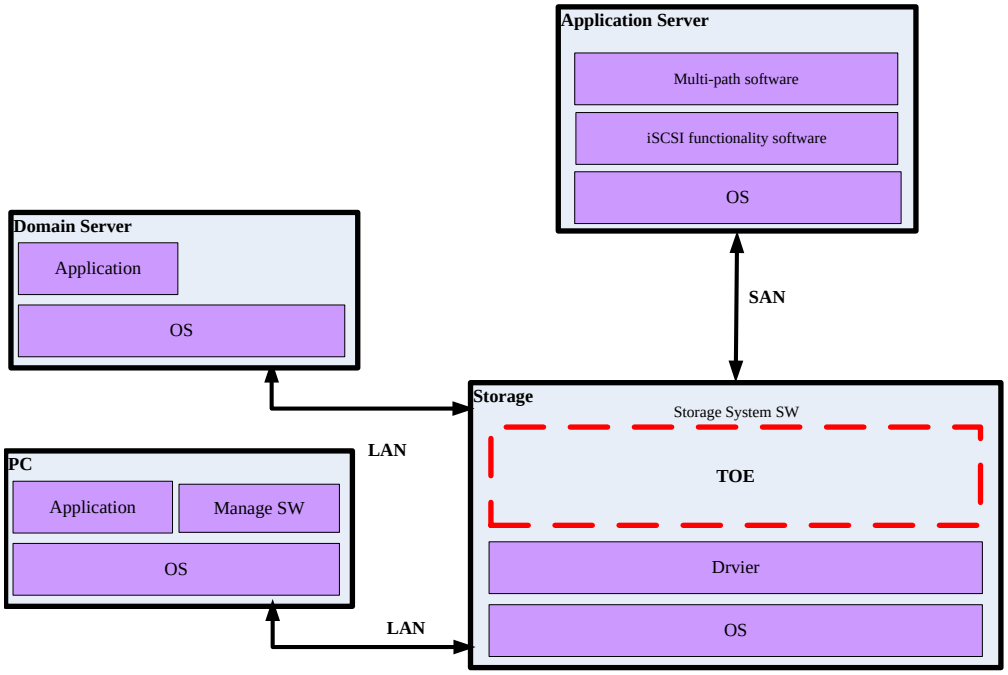

Figure 2 The software environment of the TOE

1.5 TOE description

1.5.1 Physical scope

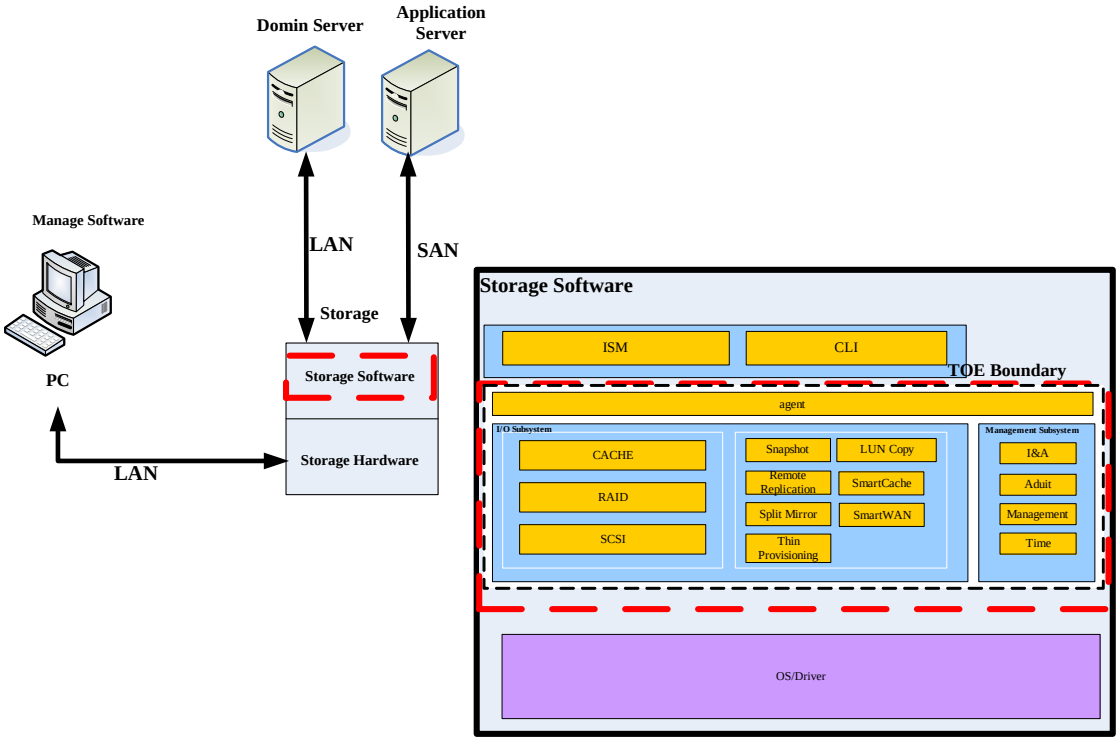

Figure 3: Physical TOE Boundary

The Figure shows the physical scope and the physical boundary of the TOE Environment.

The physical components of the TOE are:

- Storage System software:
  The TOE is installed in the Storage Server products and delivered to the customer site. The format of the software parts of TOE is a binary software package which contains the storage system software.

- Guidance:
  The format of the guidance is electronic (doc, chm, hdx) which contains product description, hardware description, installation and upgrade, configuration, operation and maintenance, fault management, and references. Such guidance is contained within the files:

  - OceanStor S2200T&S2600T&S5500T&S5600T&S5800T&S6800T_V100R005_07_en_3118G2D8.hdx
  - Huawei OceanStor T Serials Test Environment Buliding.doc (last version).
  - Storage Controller Software Upgrade Guide 01.chm

The guidance is also printed into books that are sent to the customers along with the storage equipment.

1.5.2 Logical scope of the TOE

The TOE logical boundary is defined by the security functions that it implements. The security functions implemented by the TOE are usefully grouped under the following Security Function Classes.

1.5.2.1 Authentication and Identification

1. The TOE can authenticate administrative users by user name and password. The authentication is always enforced for virtual terminal sessions via SSH sessions. The authentication for access via the console is always enabled. It supports login of two type of users, local users and domain users via remote LDAP (always using LDAPS)/AD server.

2. The LUN access is limited by the LUN ID and WWN of the initiator for FC or by the custom name for iSCSI. Such WWN (FC)/custom name(iSCSI) are the unique identification methods for hosts.

1.5.2.2 Access Control

The TOE controls access to the storage system for management and configuration by user roles. Three hierarchical access control levels are offered that can be assigned to individual user accounts:

Table 1: Access Levels

User role	Purpose	Commands for access
Super Administrator	The system has only one super administrator who has full access permission for storage system. The super	Has all access and operation rights and can modify other levels of users.

	administrator can create administrators and read-only users.	
Administrator	Administrators are created by the super administrator. An administrator cannot only add, modify, or delete its own information.	Has certain permissions to manage the storage device, but cannot manage users, perform upgrade, import a License file, activate License, or import a configuration file.
Read-Only	Read-only user has only the access permission for the storage system and can perform queries only.	Only has the right to access a storage device. For example “showlun” to list the configuration of LUNs on storage.

The TOE checks the user role when the user access the storage system and refuse the action if the user has no right.

The user who has super administrator right can manage the LUN access control. The user adds LUN and map to hosts. The TOE controls access LUN from host by LUN ID and WWN of initiator (FC) or custom name (iSCSI).

1.5.2.3 Auditing

The TOE generates audit records for security-relevant management actions and stores the audit records in memory vault or manage board in the TOE.

- By default all configuration commands along with a timestamp when they are executed are logged.
- Attempts to access regardless success or failure are logged, along with user id, source IP address and timestamp.
- Oldest log will be deleted and dumped to the specified FTP server (always using SFTP) after the dump function is enabled when the log entry exceed its capacity.
- Review functionality is provided via the command line interface and GUI interface which allows users with rights to inspect the audit log.

1.5.2.4 Security management

Security functionality management includes authentication, authorization, user management, defining IP addresses and address ranges for clients.

1.5.2.5 NTP

NTP (Network Time Protocol) is an application layer protocol used on the internet to synchronize clock among a set of distributed time servers and clients. In this manner, the clock of the host is synchronized with certain time standards.

NTP synchronizes all the clocks of devices (switches, PCs, and routers) on the network so that these devices can provide multiple applications based on the uniform time. The TOE supports this protocol in order to maintain timestamps in the audit records.

2 Conformance claims

This ST and the TOE claim conformance to CC as below:

Part 1: Introduction and general model Version 3.1 Revision 4

Part 2: Security functional components Version 3.1 Revision 4

Part 3: Security assurance components Version 3.1 Revision 4

This ST does not claim conformance to any Protection Profile.

This ST claims conformance to EAL3 augmented with ALC_CMC.4 and ALC_CMS.4 with no other package.

This ST conforms to CC Part 2 conformant.

This ST conforms to CC Part 3 conformant.

3 Security Problem Definition

The security problem addressed by the TOE and its operational environment is defined in this section. The security problem definition shows the threats that are to be countered by the TOE, its operational environment, or a combination of the two.

3.1 Assets

All data from and to the interfaces available on the TOE is categorized into TSF data and non-TSF data. The integrity and confidentiality of all this data is to be protected and considered as assets.

TSF data:

- User account data, including the following security attributes:
  - User identities.
  - Locally managed passwords.
  - Locally managed access levels.
- Audit configuration data.
- Audit records.
- Configuration data of security feature and functions.

Non-TSF data:

- User data in disks.
- Configuration data destined to the TOE processed by non-security feature and functions.
  - Operation configuration data.
  - Device management configuration data.

3.2 Threats

3.2.1 Threats Components

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

- Non-TOE user or application without rights for accessing the TOE.
- TOE user (a human user, SERVER or application using the functionality of the TOE).

Threats:

- **T.UnauthenticatedAccess:**
  - **Threat agent:** Non-TOE user or application without rights for accessing the TOE.
  - **Asset:** all assets
  - **Adverse action:** The threat agent gains access to the TOE through the LAN interface.

- **T.UnauthorizedAccess:**
  - **Threat agent:** TOE user (a user or application using the functionality of the TOE).
  - **Asset:** all assets
  - **Adverse action:** The threat agent gains access to commands or information he is not authorized for through the LAN interface.

- **T.DataCorruption**
  - **Threat agent**: all threat agents
  - **Asset:** all assets
  - **Adverse action:** Data corruption due to hardware failure caused by incorrect system

access by threat agents performing unauthorized data modification and/or inadequate configuration actions through the LAN interface.

- **T.UnauthorizedServer**
  - **Threat agent**: Non-TOE user or application without rights for accessing the TOE.
  - **Asset:** User data in disks.
  - **Adverse action:** A system connected to the TOE could access data that was not intended to be accessed by unauthorized read and write through the SAN interface.

3.3 Organizational Security Policies

This ST does not declare any Organizational Security Policy.

3.4 Assumptions

A.Manage

Users with Super administrator or Administrator role are non-hostile, appropriately trained, and follow all administrator guidance.

A.Physical

It is assumed that the TOE is protected against unauthorized physical access.

A.I&A

The TOE environment will provide identification and authentication of users before allowing any actions.

A.DataProtection

The TOE environment will provide a secure place to store user data.

A.TrustedServers

The SFTP an LDAPS server are always trusted servers whose certificates are confidents too.

A.NetworkSegregation

It is assumed that the ETH management interface in the TOE will be accessed only through an independent local network. This network is separated from the networks that use the other ETH interfaces of the TOE (and is not source of attacks).

4 Security Objectives

The security objectives are divided into two sets: security objectives for the TOE and security objectives for the operational environment. These security objectives are provided by two different entities: the TOE and the operational environment.

4.1 Security Objectives for the TOE

- **O.Authorization** The TOE shall implement different authorization levels that can be assigned to administrative users in order to restrict the functionality that is available to individual administrators. The TOE must also implement authorization function in order to restrict the servers that connect to the storage. Servers are also considered as users.
- **O.Authentication** The TOE shall require each user/server to be successfully authenticated before allowing any action.
- **O.Audit** The TOE shall provide functionality to generate audit records for all configuration actions and shall provide ability to review audit records for authorized users.
- **O.Manage** The TOE shall provide a method for authorized users properly and safely manage the TOE.

4.2 Security Objectives for the Operational Environment

- **OE.Manage** The TOE Environment must ensure that the super administrator and administrators are non-hostile, appropriately trained, and follow all administrator guidance.
- **OE.Physical** The TOE shall be protected against unauthorized physical access.
- **OE.I&A** The TOE Environment will uniquely identify users and will authenticate the claimed identity when requested to do so by the TOE.
- **OE.DataProtection** The TOE Environment must protects the data of TOE stored in secure place.
- **OE.TrustedServers** The SFTP an LDAPS server are always trusted servers whose certificates are confidents too.
- **OE.NetworkSegregation** The ETH management interface in the TOE will be accessed only through an independent local network. This network will be separated from the networks that use the other ETH interfaces of the TOE.

4.3 Security Objectives rationale

The tracing shows how the security objectives trace back to the threats, assumptions as described in the security problem definition. The security objectives rationale also demonstrates that all the given threats and assumption are addressed.

Objective	Threat / OSPs/Assumption	Rationale
O.Authentication	T.UnauthenticatedAccess	O.Authentication counters this threat by ensuring that all TOE actions can only be accessed after authentication.
	T.DataCorruption	O.Authentication couters this threat by ensuring that only authenticated user can manage user data.
	T.UnauthorizedServer	O.Authentication counters this threat by ensuring that only authenticated server can read and write the user data.

O.Authorization	T.UnauthorizedAccess	O.Authorization counters this threat by ensuring that all TOE actions can only be accessed after authorization.
	T.DataCorruption	O. Authorization counter this threat by ensuring that only authorized user can manage user data.
O.Audit	T.UnauthenticatedAccess	O.Audit counters this threat by ensuring that the TOE tracks all management actions taken against the TOE.
	T.UnauthorizedAccess	O.Audit counters this threat by ensuring that the TOE tracks all management actions taken against the TOE.
O.Manage	T.UnauthenticatedAccess	O.Manage counters this threat by allowing only a authenticated user to configure the TOE.
	T.UnauthorizedAccess	O.Manage counters this threat by allowing only a authorized user to configure the TOE.
	T.DataCorruption	O.Manage counters this threat by allowing a user to properly configure the TOE.
	T.UnauthorizedServer	O.Manage counters this threat by allowing a user to properly configure the TOE of LUN map to the servers.

The following table provides a mapping of the objectives for the operational environment to assumptions, threats and policies, showing that each objective is at least covered by one assumption, threat or policy.

Table 2: Mapping Objectives for the Environment to Assumptions

Environmental Objective	Assumption	Rationale
OE.Manage	A.Manage	OE.Manage directly upholds assumption A.Manage.
OE.Physical	A.Physical	OE.Physical directly upholds assumption A.Physical.
OE.I&A	A.I&A	OE.I&A directly upholds assumption A.I&A
OE.DataProtection	A.DataProtection	OE.DataProtection directly upholds assumption A.DataProtection.
OE.TrustedServers	A.TrustedServers	OE.TrustedServers directly upholds assumption A.TrustedServers
OE.NetworkSegregation	A.NetworkSegregation	OE.NetworkSegregation directly upholds assumption A.NetworkSegregation

5 Security Requirements for the TOE

This section provides functional and assurance requirements that satisfied by the TOE. These requirements consist of functional components from Part 2 of the CC and an Evaluation Assurance Level (EAL) containing assurance components from Part 3 of the CC.

5.1 TOE Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class.

Conventions

The following conventions are used for the completion of operations:

- ~~Strikethrough~~ indicates text removed as a refinement.
- (Underlined text in parentheses) indicates additional text provided as a refinement.
- [***Italicized and bold text in square brackets***] indicates the completion of an assignment.
- [Underlined text in square brackets] indicates the completion of a selection.
- Iteration/N indicates an element of the iteration, where N is the iteration number/character.

5.1.1 Security Audit (FAU)

5.1.1.1 FAU_GEN.1 Audit data generation

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) [***The following auditable events:***

a. user activity

1. login, logout

2. configuration change requests

b. user management

1. add, delete, modify

2. password change

3. offline user]

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, [***no other audit relevant information***]**.**

Application note: The startup and shutdown of the audit functions is associated with the startup and

shutdown of the entire TOE. The audit functionality will always be in active mode while the TOE is operative.

5.1.1.2 FAU_GEN.2 User identity association

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

5.1.1.3 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [***storage administrative user with super administrator role or administrator role or read-only role***] with the capability to read [***all information***] from the audit records.

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

5.1.1.4 FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

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

5.1.1.5 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall [overwrite the oldest stored audit records] and [***dump the oldest stored audit records to the specified FTP server after the event dump function has been enabled and set***] if the audit trail is full.

5.1.2 User Data Protection (FDP)

5.1.2.1 FDP_ACC.1/a Subset access control

FDP_ACC.1.1/a The TSF shall enforce the [***Discretionary Access Control policy for LUNs***] on

[

a) Subjects: Application servers

b) Objects: LUNs

c) Operations: Read and write

].

5.1.2.2 FDP_ACC.1/b Subset access control

FDP_ACC.1.1/b The TSF shall enforce the [***Discretionary Access Control policy for Commands***] on

[

a) Subjects: Super administrator and Administrator

b) Objects: the commands to configure and manage the TOE

c) Operations: execute the commands

].

5.1.2.3 FDP_ACF.1/a Security attribute based access control

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

[

Subjects: Application servers

subjects attributes:

a. Custom Name

object: LUNs

object attributes:

a. LUN ID

b. LUN World Wide Name

].

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

[***An application server is allowed to read and write to a LUN if the LUN ID and LUN World Wide Name is mapped to the application server***].

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

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

5.1.2.4 FDP_ACF.1/b Security attribute based access control

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

[

Subjects: Administrative user

subjects attributes:

a. User role

object: Commands

object attributes:

Command Level.

].

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

[

An administrative user of the TOE is allowed to execute a command if the role of the administrative user has rights to execute commands of the level of such command.

Role	***Command Level***	***Description***
Super administrator	***All Commands (Level 1, Level 2, Level 3)***	***Has all command rights and can modify other levels of user.***
Administrator	***Level 2 and Level 3 Commands***	***Has certain command rights, but cannot execute manage users, perform upgrade, import a License file, activate License, or import a configuration file command.***
Read-only	***Only Level 3 Commands***	***Only has the right to execute the type of show command. For example "showlun" to list the configuration of LUNs on storage.***

].

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

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

5.1.3 Identification and Authentication (FIA)

5.1.3.1 FIA_ATD.1/a User attribute definition

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

[

a) user ID

b) user role

c) password

d) unsuccessful authentication attempt since last successful authentication attempt counter

]

Application Note: if the user is a domain user, the password attribute is not a security attribute belonging to the TOE because of the password of the user is not maintained.

5.1.3.2 FIA_ATD.1/b User attribute definition

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

[

a) Custom Name (for Application servers)

b) LUN ID (for LUNs)

]

5.1.3.3 FIA_UAU.2 User authentication before any action

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.

5.1.3.4 FIA_UID.2 User identification before any action

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.

Application Note: The domain users are identified and authenticated by a remote LDAP server (always using LDAPS). The TOE allows access to domain users depending on the pass/fail verdict provided by such remote LDAP server once the domain user performs an authentication attempt.

5.1.4 Security Management (FMT)

5.1.4.1 FMT_MSA.1/a Management of security attributes

FMT_MSA.1.1/a The TSF shall enforce the [***Discretionary Access Control policy for LUNs***] to restrict the ability to [query] the security attributes [***identified in FDP_ACF.1.1/a***] to [***administrative users with read-only role, administrator role or super administrator role***].

5.1.4.2 FMT_MSA.1/b Management of security attributes

FMT_MSA.1.1/b The TSF shall enforce the [***Discretionary Access Control policy for Commands***] to restrict the ability to [query] the security attributes [***"user ID" and "user role" identified in FIA_ATD.1/a***] to [***administrative users with read-only role, administrator role or super administrator role***].

5.1.4.3 FMT_MSA.1/b2 Management of security attributes

FMT_MSA.1.1/b2 The TSF shall enforce the [***Discretionary Access Control policy for Commands***] to restrict the ability to [modify] the security attributes [***"user role" of others identified in FIA_ATD.1/a***] to [***administrative users with super administrator role***].

5.1.4.4 FMT_MSA.1/b3 Management of security attributes

FMT_MSA.1.1/b3 The TSF shall enforce the [***Discretionary Access Control policy for Commands***] to restrict the ability to [modify] the security attributes [***"password" of self identified in FIA_ATD.1/a***] to [***administrative users with read-only role, administrator role or super administrator role***].

5.1.4.5 FMT_MSA.3/a Static attribute initialization

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

FMT_MSA.3.2/a The TSF shall allow the [***administrative users with administrator role or super administrator role***] to specify alternative initial values (except of LUN ID and WWN) to override the default values when an object or information is created.

5.1.4.6 FMT_MSA.3/b Static attribute initialization

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

FMT_MSA.3.2/b The TSF shall allow [***administrative users with super administrator role****]* to specify alternative initial values to override the default values when an object or information is created.

5.1.4.7 FMT_MTD.1/a Management of TSF data

FMT_MTD.1.1/a The TSF shall restrict the ability to [***manage***] the [***attributes of Security Management Functions identified in FMT_SMF.1/a***] to [***administrative users with administrator role or super administrator role***].

5.1.4.8 FMT_MTD.1/a2 Management of TSF data

FMT_MTD.1.1/a2 The TSF shall restrict the ability to [query] the [***attributes of Security Management Functions identified in FMT_SMF.1/a***] to [***administrative users with read-only role, administrator role or super administrator role***].

5.1.4.9 FMT_MTD.1/b Management of TSF data

FMT_MTD.1.1/b The TSF shall restrict the ability to [***manage***] the [***configuration of Security Management Functions identified in FMT_SMF.1/b***] to [***administrative users with super administrator role***].

5.1.4.10 FMT_MTD.1/b2 Management of TSF data

FMT_MTD.1.1/b2 The TSF shall restrict the ability to [query] the [***configuration of Security Management Functions identified in FMT_SMF.1/b***] to [***administrative users with read-only role, administrator role or super administrator role***].

5.1.4.11 FMT_SMF.1/a Specification of Management Functions

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

[

a) Logic host and host group management

b) LUN map

].

5.1.4.12 FMT_SMF.1/b Specification of Management Functions

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

[

a) user management

b) access control management

c) definition of IP addresses and address ranges that will be accepted as source addresses in client session establishment requests

d) time management

].

5.1.4.13 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles: [***the authorized roles identified in Table 4***

Table 3: TOE Security Roles Definition

Role	***Description***
Super administrator	***Unlimited access to the storage system, and the ability to create administrators and read-only users***

Administrator	***Limited access to the storage system, but no permission to create a user, upgrade the storage system, or import a configuration file.***
Read-only	***Permissions to log in to the storage device and query information such as the storage system's operating status and health status.***

].

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

5.1.5 Protection of the TSF (FPT)

5.1.5.1 FPT_STM.1 Reliable time stamps

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

Application Note: the security function calls NTP function to provide reliable time stamps.

5.1.6 TOE access (FTA)

5.1.6.1 FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after [***a specific time (5 minutes) interval of user inactivity***].

5.1.6.2 FTA_TSE.1 TOE session establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on

[

a) Authentication failure

b) Source IP address

c) Three time attempts due to authentication failure within certain period of time

].

5.2 Security Assurance Requirements

The security assurance requirements for the TOE are taken from the CC Part 3 and are EAL3 (Evaluation assurance level 3 (EAL3) - methodically tested and checked) augmented with ALC_CMC.4.

Table 4: TOE Security Assurance Requirements

Assurance Class	Assurance components
Class ADV: Development	ADV_ARC.1
	ADV_FSP.3
	ADV_TDS.2
Class AGD: Guidance documents	AGD_OPE.1
	AGD_PRE.1
Class ALC : Life Cycle Support	ALC_CMC.4
	ALC_CMS.4
	ALC_DEL.1
	ALC_DVS.1
	ALC_LCD.1
Class ASE: Security Target evaluation	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
Class ATE: Tests	ATE_COV.2
	ATE_DPT.1
	ATE_FUN.1
	ATE_IND.2
Class AVA: Vulnerability assessment	AVA_VAN.2

5.3 Security Functional Requirements Rationale

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

Table 5: Mapping SFRs to objectives

Objectives	Security Functional Requirements	Rationale
O.Audit	FAU_GEN.1 Audit data generation	The requirement meets the objective by ensuring that the TOE generates audit records of security related events.
	FAU_GEN.2 User identity association	The requirement meets the objective by ensuring that the audit functionality is able to associate audit records with the identity of the user whose actions generate such records.
	FAU_SAR.1 Audit review	The requirement meets the objective by ensuring that all audit records can be reviewed by authorized administrative users in a suitable format.
	FAU_STG.1 Protected audit trail storage	The requirement meets the objective by ensuring that the audit trail is protected against accesses performed by unauthorized users.
	FAU_STG.4 Prevention of audit data loss	The requirement meets the objective by ensuring the audit record integrity.
	FPT_STM.1 Reliable time stamps	The requirement meets the objective by ensuring that all audit records are associated with a reliable time stamp
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that the TOE identified each user before any actions and such identity is written in the audit records.
	FMT_SMF.1/a Specification of Management Functions	The requirement meets the objective by ensuring that the TOE manages the audit configuration of servers.
	FMT_SMF.1/b Specification of Management Functions	The requirement meets the objective by ensuring that the TOE manages audit configuration of users.
O.Authentication	FIA_ATD.1/a User attribute definition	The requirement meets the objective by ensuring that the TOE maintains security attributes for each local or LDAP users.
	FIA_ATD.1/b User attribute definition	The requirement meets the objective by ensuring that the TOE maintains security attributes for each server.
	FIA_UAU.2 User authentication	The requirement meets the objective by ensuring that the TOE authenticated each user

	before any action	before any action
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that the TOE identified each user before any action.
	FMT_SMF.1/a Specification of Management Functions	The requirement meets the objective by ensuring that the TOE manages the authentication policy of servers.
	FMT_SMF.1/b Specification of Management Functions	The requirement meets the objective by ensuring that the TOE manages the authentication policy of users.
	FTA_TSE.1 TOE session establishment	The requirement meets the objective by ensuring that the TOE should deny the connection based on specific conditions.
O.Authorization	FDP_ACC.1/a Subset access control	The requirement meets the objective by ensuring that the TOE has an access control policy that ensures that only authorized servers can gain data from the TOE.
	FDP_ACC.1/b Subset access control	The requirement meets the objective by ensuring that the TOE has an access control policy that ensures that only authorized users can gain access to the TOE.
	FDP_ACF.1/a Security attribute based access control	The requirement meets the objective by ensuring that only authorized servers gain access to data protected by the TOE.
	FDP_ACF.1/b Security attribute based access control	The requirement meets the objective by ensuring that only authorized users gain access to the TOE.
	FIA_ATD.1/a User attribute definition	The requirement meets the objective by ensuring that the TOE maintains security attributes for each local user.
	FIA_ATD.1/b User attribute definition	The requirement meets the objective by ensuring that the TOE maintains security attributes for each server.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that the TOE identified each user before any action.
	FMT_MSA.1/a Management of security attributes	The requirement meets the objective by ensuring that the security attribute of LUNs in TOE can only be changed by authorized user.
	FMT_MSA.1/b Management of security attributes	The requirement meets the objective by ensuring that the security attribute of users in TOE can only be changed by authorized user.
	FMT_MSA.1/b2 Management of security attributes	The requirement meets the objective by ensuring that the security attribute of users in TOE can only be changed by authorized user.

	FMT_MSA.1/b3 Management of security attributes	The requirement meets the objective by ensuring that the security attribute of users in TOE can only be changed by authorized user.
	FMT_MSA.3/a Static attribute initialization	The requirement meets the objective by ensuring that the default values for security attribute of LUNs in TOE should be provided and overriddenby authorized user.
	FMT_MSA.3/b Static attribute initialization	The requirement meets the objective by ensuring that the default values for security attribute of users in TOE should be provided by authorized user.
	FMT_SMF.1/a Specification of Management Functions	The requirement meets the objective by ensuring that the TOE manages the authentication policy of servers.
	FMT_SMF.1/b Specification of Management Functions	The requirement meets the objective by ensuring that the TOE manages the authentication policy of users.
	FMT_SMR.1 Security roles	The requirement meets the objective by ensuring that specific roles are defined to management of the TOE.
	FTA_SSL.3 TSF-initiated termination	The requirement meets the objective by ensuring that the interactive session should be terminated by TOE after a specific time.
O.Manage	FAU_SAR.1 Audit review	This requirement meets the objective by ensuring that the audit review functionality can be managed.
	FMT_MSA.1/a Management of security attributes	The requirement meets the objective by ensuring that the security attribute of LUNs can be managed.
	FMT_MSA.1/b Management of security attributes	The requirement meets the objective by ensuring that the security attribute of users can be managed.
	FMT_MSA.1/b2 Management of security attributes	The requirement meets the objective by ensuring that the security attribute of users can be managed.
	FMT_MSA.1/b3 Management of security attributes	The requirement meets the objective by ensuring that the security attribute of users can be managed.
	FMT_MSA.3/a Static attribute initialization	The requirement meets the objective by ensuring that the default values for security attribute of LUNs can be managed.
	FMT_MSA.3/b Static attribute initialization	The requirement meets the objective by ensuring that the default values for security attribute of users in TOE can be managed.
	FMT_MTD.1/a	The requirement meets the objective by

	Management of TSF data	ensuring that the attributes of security management functions can be managed.
	FMT_MTD.1/a2 Management of TSF data	The requirement meets the objective by ensuring that the attributes of security management functions can be managed.
	FMT_MTD.1/b Management of TSF data	The requirement meets the objective by ensuring that the configuration of security management functions can be managed.
	FMT_MTD.1/b2 Management of TSF data	The requirement meets the objective by ensuring that the configuration of security management functions can be managed.
	FMT_SMF.1/a Specification of Management Functions	The requirement meets the objective by ensuring that the TOE manage the authentication policy of servers.
	FMT_SMF.1/b Specification of Management Functions	The requirement meets the objective by ensuring that the TOE manage the authentication policy of users.
	FTA_SSL.3 TSF-initiated termination	The requirement meets the objective by ensuring that the interactive session can be managed.

5.4 Security Assurance Requirements Rationale

The evaluation assurance level EAL3 + ALC_CMC.4 + ALC_CMS.4 has been chosen commensurate with the threat environment that is experienced by typical consumers of the TOE.

6 TOE Summary Specification

The objective for the TOE summary specification is to provide a description of how the TOE satisfies all the SFRs.

6.1 TOE Security Functional Specification

6.1.1 Authentication and Identification

Authentication and Identification to administrative users and Data Users (Data User of TOE means the users of TOE's user data) are supported by the TOE. The purpose of authentication and identification to administrative users is to make sure administrative user can manage TOE only when TOE recognizes him as the right person. It's just the same to Data User's read and writes actions with user data.

6.1.1.1 Authentication and Identification of administrative user

Administrative users can manage TOE by two ways: ISM and CLI. ISM and CLI are not parts of the TOE. ISM is a manage software, providing GUI management functions. You can download the ISM client by typing the TOE IP address in internet browser. Administrative users can log-in and manage TOE through the ISM client with right username and password. CLI is a command line management tool. Administrative users can log-in to TOE through standard SSH client such as putty and manage the TOE.

NOTE: Before using ISM, the communication between the ISM and the TOE must be secured. A trusted certificate belonging to the ISM will be configured in the TOE so that the TOE, once the ISM connects to it, will be able to guarantee that the ISM is genuine.

NOTE: The port 5988 must be closed in the TOE before its first use.

The TOE can identify administrative users by a unique ID and enforces their authentication before granting them access to any TSF management interfaces.

Detailed functions include:

1) Authentication and Identification function supports login of two type of users, local users and domain users, the information of local users being saved in local, and the information of domain users being saved in remote LDAP server (always using LDAPS).
2) Support authentication via local password if the user is a local user. This function is achieved by comparing user information input with pre-defined user information stored in system.
3) Support authentication via remote LDAP (Lightweight Directory Access Protocol) server if the user is a domain user. This function is achieved by performing pass/fail action based on result from remote LDAP server, and the TOE checking the pass/fail action based on the result obtained from remote LDAP server. LDAP certification only support ISM logins. Support authenticate user login using SSH tool and client of ISM.
4) Support logout when no operation is performed on the user session within a given interval. This function is achieved by performing count-down through timing related to clock function.
5) Support max attempts due to authentication failure within certain period of time. This function is achieved by providing counts on authentication failure. User will be locked for a period of time and user will not be able to login when max attempts has been reached. Maximum online user is supported by TOE. New user will not be able to log in to system when maximum online user has been reached, until online user log-out.
6) Support limiting access by IP address. This function is achieved by comparing IP address of requesting session with configured value stored in memory.
7) Support for user individual attributes in order to achieve all the enumerated features: user ID, user role, password, unsuccessful authentication attempt since last successful authentication.

6.1.1.2 Authentication and Identification of Data User

"Data User" of TOE means the users of TOE's user data, for example, an application server or a NAS equipment. Generally speaking Data User is not an administrative user. Administrative user is the user of TOE's functionalities. Administrative user can configure a Data User through TOE's functionalities. One Data User can be recognized by TOE through proper attributes of Data User. Usually the "Data User" has several parts called initiators, FC initiator has an attribute called WWN, iSCSI initiator has attribute called custom name, the initiator can be recognized by the attribute and the LUN can only identification by WWN(FC) or custom name(iSCSI). The administrative user could map a LUN to a logic host and add the initiator of data user to the logic host, When the data user access the data, the authentication and identification of the user could be executed to check the WWN of initiator (FC) or custom name (iSCSI) that mapped to the logic host which the accessed LUN added to by TOE.

Detailed functions include:

1) Support LUN access limitation through WWN of initiator (FC) or custom name (iSCSI). Target LUN on TOE can be accessed by initiators granted by administrative user.

(FIA_ATD.1/a, FIA_ATD.1/b, FIA_UAU.2, FIA_UID.2, FTA_TSE.1)

6.1.2 Access Control

The TOE enforces a discretionary access control policy for commands by supporting following functionalities:

1) Support 3 access levels (super administrator, administrator, read-only). This function is achieved by storing number as level in memory.
2) Support assigning access level to commands. This function is achieved by associating access level number with commands registered.
3) Support assigning access level to user ID. This function is achieved by associating access level number with user ID.
4) Support manual session termination by username. This function is achieved by interpreting commands for username, locating and cleaning session information related to this username, forcing this username to re-authenticate.

The TOE enforces a discretionary access control policy for LUNs by supporting following functionalities:

1) Support assigning the access privilege of LUNs to the logic hosts. This function is achieved by creating the logic hosts and adding the WWN of initiators(FC) to the logic hosts, and then mapping the LUNs to the logic hosts.
2) Support setting the configuration of CHAP to initiators when the host connects to the TOE with iSCSI.

TOE Security Functional Requirements Satisfied: (FMT_MSA.1/a, FMT_MSA.1/b, FMT_MSA.1/b2, FMT_MSA.1/b3, FMT_MSA.3/a, FMT_MSA.3/b, FMT_MTD.1/a, FMT_MTD.1/a2, FMT_MTD.1/b, FMT_MTD.1/b2, FMT_SMR.1, FTA_SSL.3, FDP_ACC.1/a, FDP_ACC.1/b, FDP_ACF.1/a, FDP_ACF.1/b)

6.1.3 Auditing

The TOE can provide auditing ability by receiving all types of logs and processing them according to user's configuration:

1) Support 4 levels of log, include Event, Warning, Major, Critical. Support log recording when system configuration changes and system error occurs. Support log file auto-store in

memory and disk, oldest log will be deleted and dump to the specified FTP server (always using SFTP) after the dump function enabled when log entry exceed certain number.

2) Support log search by authorized user. Authorized user can search log entries through ISM client.

TOE Security Functional Requirements Satisfied: (FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_STG.1, FAU_STG.4)

6.1.4 Security Management

The TOE offers management functionality for its security functions, where appropriate. This is partially already addressed in more detail in the previous sections of the TSF, but includes:

1) User management, including user name, passwords, etc.
2) Access control management, including the association of users and corresponding privileged functionalities.
3) Defining IP addresses and address ranges for clients that are allowed to connect to the TOE.

All of these management options are typically available via the ISM GUI.

Detailed function specification include following:

1) Support configuration on limiting access by IP address;
2) Support LUN mapping, TOE will provide assignment mechanism to map LUN to proper servers.

TOE Security Functional Requirements Satisfied: (FMT_SMF.1/a, FMT_SMF.1/b)

6.1.5 NTP

The TOE supports Network Time Protocol (NTP) to synchronize all the clocks of devices on the network so that these devices can provide multiple applications based on the uniform time.

TOE Security Functional Requirements Satisfied: (FPT_STM.1)

A Acronyms and Abbreviations

CC	Common Criteria
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
PP	Protection Profile
SFR	Security Functional Requirement
EAL	Evaluation Assurance Level
CLI	Command Line Interface
GUI	Graphical User Interface
ISM	Integrated Storage Manager
SSH	Secure Shell
SNMP	Simple Network Management Protocol
NTP	Network Time Protocol
FTP	File Transfer Protocol
SFTP	Secure File Transfer Protocol
LDAP	Lightweight Directory Access Protocol
SAN	Storage Area Network
NAS	Network Attached Storage
RAID	Dundant Array of Independent Disks
LUN	Logical Unit Number
ID	Identifier
FC	Fiber Channel
iSCSI	Internet Small Computer Systems Interface
WWN	World Wide Name
IQN	iSCSI Qualified Name
CHAP	Challenge Handshake Authentication Protocol
SSL	Secure Sockets Layer

HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
HMAC	Hashed Message Authentication Code
MD5	Message Digest Algorithm 5