CC Huawei OceanStor Dorado V6 Series Storage System Software 6.0.1

Security Target

Issue	**0.18**
Date	**2021-03-10**

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: https://e.huawei.com

About This Document

Change History

Date	Issue	Change Description	Author
2021-03-10	0.18	list the non-TOE software	Wu Yong
2021-01-29	0.17	update guidance version	Wu Yong, Hu pan
2021-01-15	0.16	add documentation signature files in 1.4.1	Wu Yong, Hu pan
2020-12-23	0.15	Updated the ST reference and some minor issue	Wu Yong, Hu pan
2020-09-23	0.14	Updated the ST reference	Wu Yong, Hu pan
2020-08-11	0.13	Updated the rationale for unsatisfied dependencies	Wu Yong, Hu pan
\2020-07-29	0.12	1. Added the reference documentation. 2. Modify the feedbacks in Sector 5.1.3.6 3. Clarify the dependencies description of FCS_COP.1/SHA256 and FCS_COP.1/PBKDF2 in Sector 5.2.2 4. Update the attributes in 5.1.3.1	Wu Yong, Hu pan
2020-07-17	0.11	1. Fixed issues reported on July 10.	Wu Yong
2020-07-03	0.10	1. Added suffix to the product guidance documentations.	Wu Yong
2020-07-01	0.9	1. Added the product guidance documentation. 2. Fixed issues reported on June 30.	Wu Yong
2020-06-12	0.8	1. Added the table title. 2. Fixed issues reported on June 5.	Wu Yong
2020-05-27	0.7	1. Modified the formats of some sections in the document.	Wu Yong

Date	Issue	Change Description	Author
2020-05-13	0.6	1. Added the mapping between security features and modules in Section 1.4.2. 2. Modified the Figure 1-3 Physical TOE boundary. 3. Modified the formats of some sections in the document.	Wu Yong
2020-03-18	0.5	1. In Section 5.3 and 2, the EAL is modified to 3+. 2. Added FCS_COP.1/PBKDF2 and FCS_COP.1/SHA256 in Table 5-1. 3. In Section 5.1, identified correctly each operation in the SFRs to avoid misunderstandings. 4. In Section 5.2.2, explained why the FCS_COP.1's dependency is not met, and add KMC platform as a part of Non-TOE Software in Section 1.3.3. 5. Corrected some typos.	Hu Pan, Wu Yong
2020-03-10	0.4	1. In section 2.1, deleted the desciption "extended by security functional components as defined in chapter 5" 2. In section 3.4 and 4.3, added the security objective of OE.Hardware. 3. In section 5.1, added a paragraph to describe the format of each operation. 4. In section 6, added the security function corresponding to FMT_SMF.1/USER and the detailed description. 5. In section 1.4.1, added the format of the reference documents.	Hu Pan, Wu Yong
2020-02-10	0.3	1.Modified version to 0.3 2.Modified objective (O.Manage) to O.SecurityManagement In section 4.3 Table1、section 5.2.1 Table1 3.Modified EAL 2 to EAL 3 in section 5.4;	Li Qiang, Hu Pan, Wu Yong
2019-04-20	0.2	Modified the document according to the internal review comments.	Li Qiang, Hu Pan, Wu Yong
2019-04-16	0.1	This is the initial draft.	Li Qiang, Hu Pan, Wu Yong

Contents

1 Introduction

This chapter contains the ST identification, TOE identification, TOE overview, and TOE description of Huawei OceanStor Dorado V6 Series Storage System. All of them are consistent with each other.

1.1 ST Reference

Title: CC Huawei OceanStor Dorado V6 Series Storage System Software 6.0.1 Security Target

Version: 0.18

Date: 2021-03-10

Developer: Huawei Technologies Co., Ltd.

1.2 TOE Reference

The TOE is identified as bellow:

TOE name: Huawei OceanStor Dorado V6 Series Storage System Software

TOE version: 6.0.1

Developer: Huawei Technologies Co., Ltd.

1.3 TOE Overview

This section provides the usage and major security features of the TOE, as well as the TOE type and major non-TOE hardware/software required by the TOE.

1.3.1 TOE Usage and Major Security Features

- Usage

  The Huawei OceanStor Dorado V6 Series Storage System is a new-generation storage system developed by Huawei Technologies Co., Ltd. It is purpose-built for enterprise-class mission-critical business and equipped with comprehensive SAN features, and is ideal for use with databases, virtual desktop infrastructure (VDI), virtual server infrastructure (VSI), and SAP HANA. OceanStor Dorado V6 facilitates the transition to all-flash storage for customers in the finance, manufacturing, telecom, and other sectors.

- TOE major security features

  The major security features implemented by the TOE are:

  - Identification and authentication
  - Authorization
  - Access control
  - Auditing
  - Security management

1.3.2 TOE type

Storage system software

1.3.3 Non-TOE Hardware, Software, and Firmware Required by the TOE

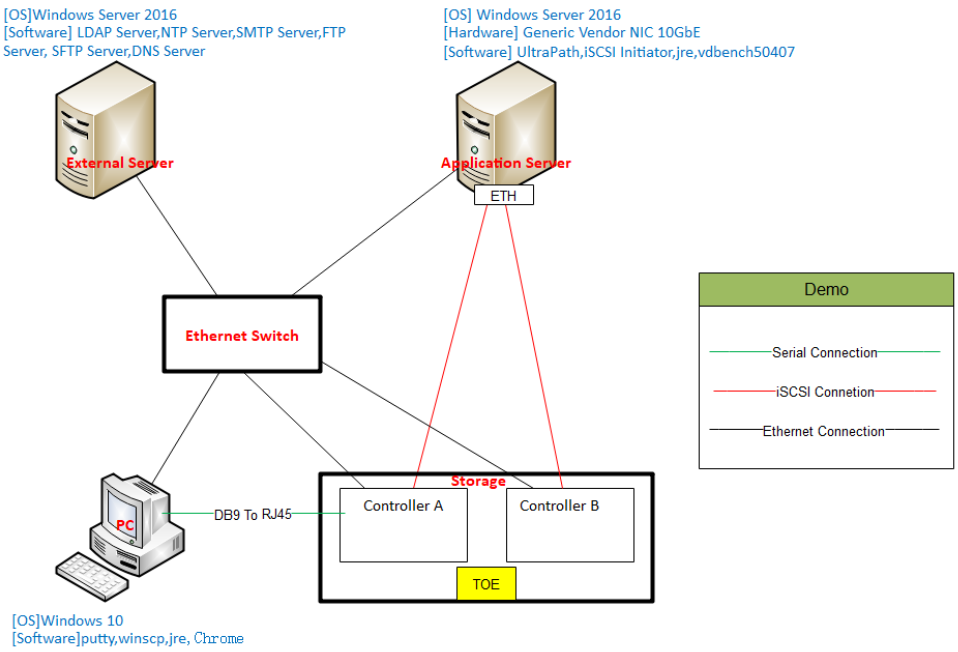
The TOE is a piece of software that provides storage functions to application servers.

The TOE is running on the OceanStor Dorado V6 series hardware models, which are OceanStor Dorado 3000 V6, OceanStor Dorado 5300 V6, OceanStor Dorado 5000 V6, OceanStor Dorado 5500 V6, OceanStor Dorado 6000 V6, OceanStor Dorado 5600 V6, OceanStor Dorado 5800 V6, OceanStor Dorado 8000 V6, OceanStor Dorado 6800 V6, OceanStor Dorado 18000 V6, OceanStor Dorado 18500 V6, and OceanStor Dorado 18800 V6. More information about the hardware models can be found in the following links:

https://support.huawei.com/carrier/navi?coltype=product#allProduct=true&col=product&path=PBI1-21430725/PBI1-251363742/PBI1-250389226/PBI1-21462728

If not all the hardware types are shown on this page, switch the language into Chinese and then all the types are included. The TOE is running on the customized Linux operating system (Euler OS V200R008C00) based on kernel 4.19.36. The OS、driver and KMC platform(version 2.0) are not covered by the TOE, see red frame in Figure 1-4. In addition, the software upgrade tool SmartKit (V2R6C00RC9SPC300 or later) and the software package integrity verification tool GnuPG are not parts of the TOE. Figure 1-1 shows the real environment for running the TOE.

Figure 1-1 Real environment of the TOE



- Description
  - The external server, application server, PC, and TOE (storage) are connected to each other by the Ethernet switch.
  - The NIC on the application server has two Ethernet ports. One connects to the TOE's controller_A, and the other connects to controller_B through optical fibers.
  - The PC must have one port (DB9), and connects to the TOE through a DB9-to-RJ45 cable.
- Application server
  - Hardware

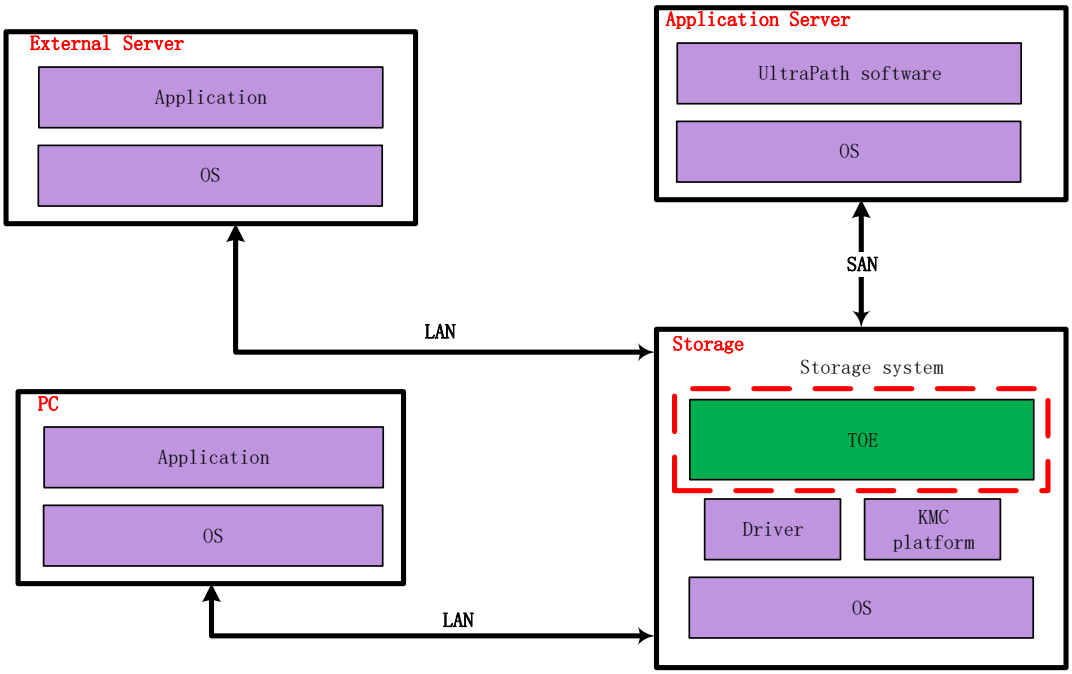
    Rack servers or PCs with at least one 10G/25G NIC
  - Software
    - Windows Server 2016 OS
    - Multipathing software UltraPath 21.06.060
    - Microsoft iSCSI Software Initiator in Windows Server 2016
    - JRE (Java Runtime Environment 1.8)
    - Vdbench50407
- External server
  - Hardware

    Rack servers or PCs with at least one 100M/1G Ethernet port
  - Software
    - Windows Server 2016 OS
    - OpenLDAP for Windows 2.4.42
    - NTP server, FTP server, DNS server in Windows Server 2016
    - OpenSSH v8.0.0.0p1

- PC
  - Hardware

    Rack servers or PCs with at least one 100M/1G Ethernet port and one Serial DB9 port
  - Software
    - Windows 10 OS
    - Brower Google Chrome 64+
    - JRE (Java Runtime Environment 1.8), PuTTY 0.73, WinSCP 5.17, Python 2.79, notepad ++, Postman, Foxmail
- Note: Please notice that the hardware and software types are not limited to certain types. If only the stated conditions above are fulfilled, the TOE can run on the environment with all the functionalities claimed.

Figure 1-2 Software environment of the TOE

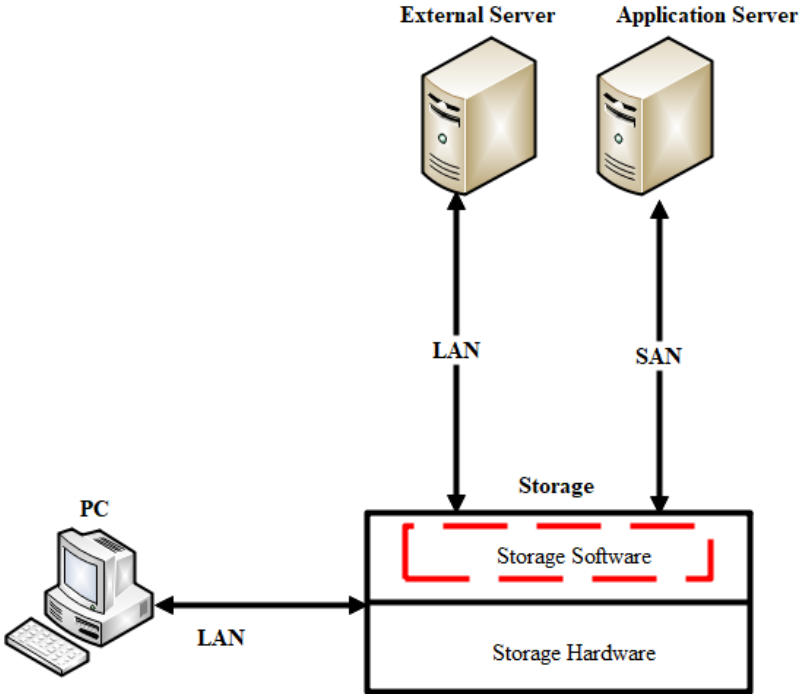


1.4 TOE Description

1.4.1 Physical Scope

Figure 1-3 shows the physical scope and physical boundary of the TOE environment.

Figure 1-3 Physical TOE boundary



The TOE is a 'software only', does not contain hardware. To be exact, the TOE is only part of the software, and its boundary will be described in more detail in the next chapter. In addition, the software package, signature file, and the guidance documentation are delivered to the customer site by downloading from support website.

Table 1-1 Document list

Type	Delivery Item	Version	Download Link
Software	OceanStor_Dorado_V6_Software_6.0.1.tgz (including TOE and OS)	6.0.1	https://support.huawei.com/enterprise/en/software/251142570-ESW2000213625
Software signature file	OceanStor_Dorado_V6_Software_6.0.1.tgz.asc	-	
Product guidance	OceanStor Dorado V6 Series 6.0.1 Error Code Reference.zip	V0.1	https://support.huawei.com/enterprise/en/centralized-storage/oceanstor-dorado-5000-v6-pid-22784062?category=other&subcategory=other
	OceanStor Dorado V6 Series 6.0.1 Error Code Reference.zip.asc		
	OceanStor Dorado V6 Series 6.0.1 Command Reference.zip	V0.1	
	OceanStor Dorado V6 Series 6.0.1 Command Reference.zip.asc		

Type	Delivery Item	Version	Download Link
	OceanStor Dorado V6 Series 6.0.1 REST Interface Reference.zip	V0.1	
	OceanStor Dorado V6 Series 6.0.1 REST Interface Reference.zip.asc		
	OceanStor Dorado V6 Series 6.0.1 Administrator Guide. zip	V0.1	
	OceanStor Dorado V6 Series 6.0.1 Administrator Guide. zip.asc		
	OceanStor Dorado V6 Series 6.0.1 Event Reference. zip	V0.1	
	OceanStor Dorado V6 Series 6.0.1 Event Reference. zip.asc		
	OceanStor Dorado V6 Series 6.0.1 Initialization Guide. zip	V0.1	
	OceanStor Dorado V6 Series 6.0.1 Initialization Guide. zip.asc		
	OceanStor Dorado V6 Series 6.0.1 Security Configuration Guide. zip	V0.1	
	OceanStor Dorado V6 Series 6.0.1 Security Configuration Guide. zip.asc		
	CC Huawei OceanStor Dorado V6 Series Storage System Software 6.0.1 AGD_OPE. zip	V1.0	
	CC Huawei OceanStor Dorado V6 Series Storage System Software 6.0.1		

Type	Delivery Item	Version	Download Link
	AGD_OPE. zip.asc		
	CC Huawei OceanStor Dorado V6 Series Storage System Software 6.0.1 AGD_PRE_User. zip	V0.11	
	CC Huawei OceanStor Dorado V6 Series Storage System Software 6.0.1 AGD_PRE_User. zip.asc		
	CC Huawei OceanStor Dorado V6 Series Storage System Software 6.0.1 AGD_PRE_Production. zip	V0.4	
	CC Huawei OceanStor Dorado V6 Series Storage System Software 6.0.1 AGD_PRE_Production. zip.asc		

1.4.2 Logical Scope of the TOE

The TOE boundary from a logical point of view is represented by the elements that are displayed with a red dotted box within the rectangle in the figure. The TOE consists of I/O Service, OMM and SYS CTRL, and is running underlying OS and hardware. The TOE provides several security functions, which are described in more detail in chap.1.4.3 .

Figure 1-4 TOE logical scope

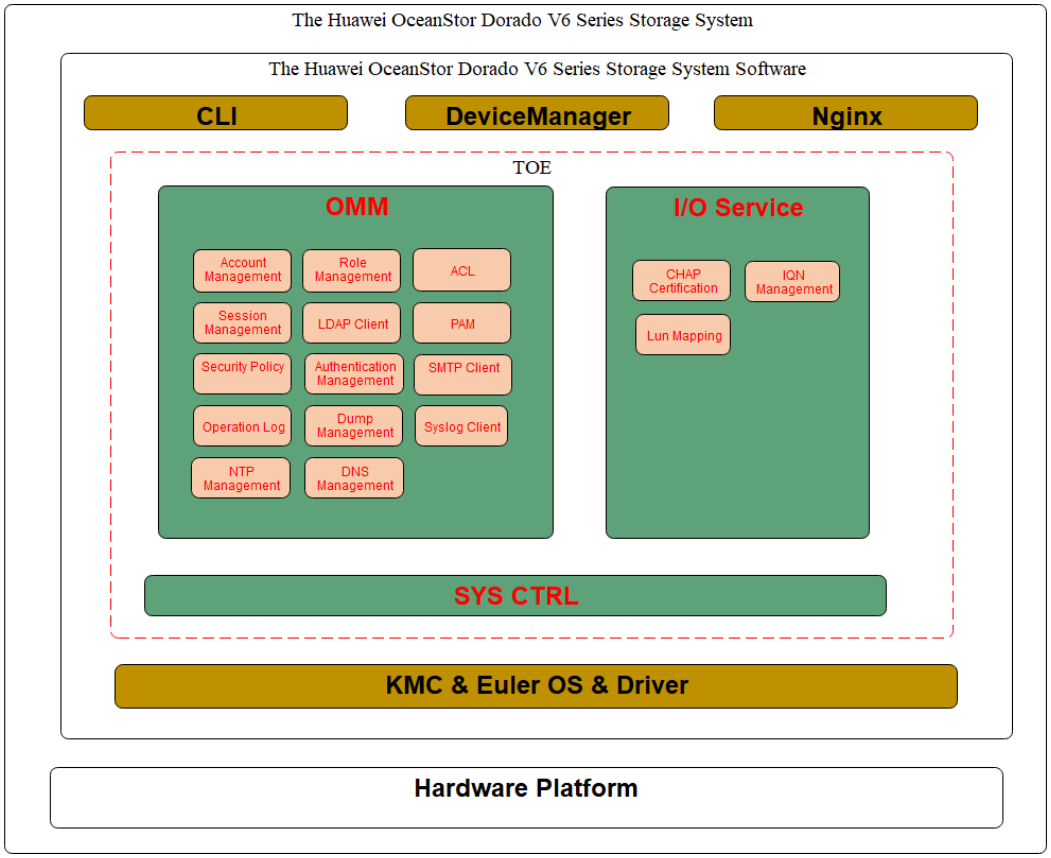


Figure 1-4 reflects the basic structure of the TOE with respect to subsystems and modules. The TOE provides all the security features. Security features are implemented through one or more modules.

1.4.3 Summary of Security Features

1.4.3.1 Identification and Authentication

- In user access, the TOE provides local and remote authentication modes.

  In local authentication mode, the identities are stored in the TOE. Identification is passed only if the input identities match the ones stored in the TOE. The identification factors include the password, SSH key pair, and one time password (OTP) sent through email. The TOE supports 3 kinds of combinations: password and OTP, password only, and SSH key pair only.

  In remote authentication mode, the identities are stored in a remote LDAP server. When the identification begins, the input password is sent forward to the remote LDAP server through the standard LDAP protocol and identified by the LDAP server.
- In data access, the available LUN is limited by the initiator. CHAP authentication is supported for connecting to the TOE over an iSCSI network. Target LUNs on the TOE can be accessed only when CHAP authentication is passed.

1.4.3.2 Authorization

Authorization indicates that devices assign operation authorities to accounts according to their validity.

The TOE implements authorization by the Role Based Access Control (RBAC) model. In RBAC, a permission is an approval to perform an operation on one or more RBAC protected objects (i.e. the commands in the TOE). A role is a set of permissions and an account can be assigned with only one role. The TOE supports not only built-in roles (listed in table below), which cannot be modified or deleted, but also customized roles whose permissions can be modified or deleted by users whose role holds a permission to modify other roles.

Table 1-2 Role permission definition

Role	Permission
Super administrator	All permissions
Administrator	All permissions except user management and high-risk maintenance operations
Security administrator	System security configuration permissions, including management of security rules, certificates, and data destruction
SAN resource administrator	SAN resource management permissions, including management of storage pools, LUNs, mappings, hosts, ports, and background configuration tasks
Data protection administrator	Data protection management permissions, including management of LUNs, local data protection, remote data protection, HyperMetro, and background configuration tasks
Remote device administrator	Cross-device data protection management permissions, including management of remote replication, HyperMetro, 3DC, LUNs, and mappings. This role is used for remote authentication in cross-device data protection scenarios.
Empty role	None permission except those allow query of information about itself.
Monitor	The role is used to monitor the TOE and to view the audit records.

When an account is created, it is authorized to perform certain operations and is not allowed to perform unauthorized operations. This is achieved by comparing the permissions held by the account's role and the permissions of the operations (i.e. commands). If an account attempts to perform any unauthorized operation, an error message is displayed and the attempt is audited.

1.4.3.3 Access Control

The TOE supports filtering of incoming access to management interfaces. An administrative user with a proper role can set the IP whitelist to limit access from IP addresses out of the list. The login method (SSH, SFTP, RESTful, Serial Port, etc) can be configured to limit an account's access methods.

A user whose role has proper permissions can control access to specific LUNs. The user adds a LUN and maps it to a host. The TOE controls access to the LUN from the host by host WWN.

1.4.3.4 Auditing

The TOE generates audit records for security-relevant management actions and stores the audit records in the TOE.

- By default, all configured commands along with a timestamp when they are executed are logged.
- Access attempts, regardless of success or failure, are logged, along with the user ID, source IP address, timestamp, etc.
- If the dump function is enabled, the oldest logs will be dumped to the specified FTP server when the log entries exceed a specified number.
- Review functionality is provided via the command line interface and GUI, which allows administrative users to inspect the audit logs.

1.4.3.5 Security Management

Security functionality management includes authentication, access level, and management of security related data, including configuration profile and runtime parameters. According to security functionality management, customized security is provided.

- Management of accounts and account attributes, including account credentials
- Management of the account policy, including account name length, password complexity, failure policy, and lockout policy
- Management of IP whitelist and login method
- Configuration of network services used by the TOE, such as NTP, Syslog, LDAP, SFTP, DNS, SMTP
- Management of the TOE's time

All security management functions (i.e. commands related to security management) require proper user roles for execution (see the description of access control in section 1.4.2.2 Authorization).

NOTE

The TOE's time is managed by the Network Time Protocol (NTP). NTP is an application layer protocol used on the internet to synchronize clocks 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.

2 Conformance Claims

2.1 CC Conformance Claim

This ST is *CC Part 2 conformant* [CC], and *CC Part 3 conformant* [CC]. The version of [CC] is 3.1 R5.

The ST claims conformance to the EAL3+ ALC_FLR.2 assurance package.

No conformance to a Protection Profile is claimed.

3 Security Problem Definition

The security problems addressed by the TOE and the operational environment of the TOE are defined in this chapter. 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 following is an enumeration of the subjects and objects participating in the policy.

TSF data:

- Authentication data: The data which is used by the TOE to identify and authenticate the external entities which interact with the TOE.
  - User identities.
  - Locally managed passwords.
  - Locally managed access levels.
- Audit data: The data which is provided by the TOE during security audit logging.
  - Audit configuration data.
  - Audit records.
- Configuration data for the TOE, which is used for configuration data of security features and functions.

Non-TSF data:

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

- Device management configuration data.

3.2 Threats

3.2.1 Threat Components

This section specifies the threats that are addressed by the TOE and the TOE 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).

T.UnauthenticatedAccess

- **Threat agent:** Non-TOE user or application without rights for accessing the TOE.
- **Asset:** All assets.
- **Adverse action:** A non-TOE user gains access to the TOE through LAN.

T.UnauthorizedAccess

- **Threat agent:** TOE user (a user or application using the functionality of the TOE).
- **Asset:** All assets.
- **Adverse action:** A user of the TOE authorized to perform certain actions and access certain information gains access to unauthorized commands or information through LAN.

T.DataCorruption

- **Threat agent**: TOE user (a user or application using the functionality of the TOE).
- **Asset:** All assets.
- **Adverse action:** Data could become corrupted due to incorrect system access by users of the TOE or attackers of unauthorized data modification, and inadequate configuration actions through LAN.

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 it was not intended to gain access by unauthorized read and write on user data through SAN.

3.3 Organizational Security Policies

No organizational security policy.

3.4 Assumptions

- **A.Manage**

It is assumed that the TOE users are non-hostile, sufficiently trained, and follow all administrator guidance. They will not write down their passwords.

- **A.Physical**

  It is assumed that the TOE and its operational environment are protected against unauthorized physical access.

- **A.I&A**

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

- **A.DataProtection**

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

- **A.Hardware**

  It is assumed that the underlying hardware (including the operating system) of OceanStor Dorado V6, which is outside the scope of the TOE, works correctly.

4 Security Objectives

The security objectives are divided into two solutions, which are the security objectives for the TOE and the security objectives for the operational environment. These solutions are provided by two entities: the TOE and the operational environment.

4.1 Security Objectives for the TOE

- **O.Authorization**

  The TOE should implement different authorization levels that can be assigned to administrators in order to restrict the functionality available to individual administrators. The TOE must also implement authorization functions to restrict the servers that connecting to the storage. Servers are also considered as users.

- **O.Authentication**

  The TOE must require each user/server to be successfully authenticated before allowing any action.

- **O.AccessControl**

  The TOE must require each user/server to be added to the whitelist before allowing any action.

- **O.Audit**

  The TOE should provide functionality to generate audit records for all configuration actions and should provide the ability to review audit records for authorized users.

- **O.SecurityManagement**

  The TOE should provide functionality to manage security functions provided by the TOE.

4.2 Security Objectives for the Operational Environment

The following security objectives, in addition to those assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation

of functions in the TOE hardware or software. They will be satisfied largely through application of procedural or administrative measures.

- **OE.Manage**

  The TOE environment must ensure that the administrative control of the TOE is non-hostile, appropriately trained, and follows all administrator guidance.

- **OE.Physical**

  The TOE should 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 protect the data of the TOE stored in a secure place.

- **OE.Hardware**

  The TOE environment must ensure that underlying hardware (including the operating system) of OceanStor Dorado V6, which is outside the scope of the TOE, works correctly.

4.3 Security Objective Rationale

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

Table 4-1 Mapping objectives to threats and OSPs

Objective	Threat, OSP, Assumption	Rationale
O.Authentication	T.UnauthenticatedAccess	O.Authentication counters this threat by ensuring that all actions must be after authentication.
	T.DataCorruption	O.Authentication counters this threat by ensuring that only authenticated users can manage user data.
	T.UnauthorizedServer	O.Authentication counters this threat by ensuring that only authenticated servers can read and write the user data.
O.Authorization	T.UnauthorizedAccess	O.Authorization counters this threat by ensuring that all actions must be after authorization.
	T.DataCorruption	O.Authorization counters this threat by ensuring that only authorized users can manage user data.

Objective	Threat, OSP, Assumption	Rationale
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.SecurityManagement	T.UnauthenticatedAccess	O.SecurityManagement counters this threat by allowing only authenticated users to configure the TOE.
	T.UnauthorizedAccess	O.SecurityManagement counters this threat by allowing only authorized users to configure the TOE.
	T.DataCorruption	O.SecurityManagement counters this threat by allowing a user to properly configure the TOE.
	T.UnauthorizedServer	O.SecurityManagement counters this threat by allowing a user to properly configure the TOE to map LUNs to the servers.
O.AccessControl	T.UnauthenticatedAccess	O.AccessControl counters this threat by allowing only whitelist users to access the TOE.
	T.UnauthorizedServer	O.AccessControl counters this threat by allowing only whitelist servers to access the TOE of the mapped LUNs.

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 4-2 Mapping objectives for the environment to assumptions

Environment 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.

Environment Objective	Assumption	Rationale
OE.DataProtection	A.DataProtection	OE.DataProtection directly upholds assumption A.DataProtection.
OE.Hardware	A.Hardware	OE.Hardware directly upholds assumption A.Hardware.

5 Security Requirements for the TOE

This chapter provides the functional and assurance requirements that are 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. Table 5-1 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

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.

Bold text indicates the completion of an assignment.

Italicised and bold text indicates the completion of a selection.Iteration/N indicates an element of the iteration, where N is the iteration number/character.

Table 5-1 TOE security functional requirements

Name	S	A	R	I
FAU_GEN.1	√	√		
FAU_GEN.2				
FAU_SAR.1		√		
FAU_SAR.2				

Name	S	A	R	I
FAU_SAR.3		√		
FAU_STG.1	√			
FAU_STG.3		√		
FAU_STG.4	√	√		
FDP_ACC.1		√		√
FDP_ACF.1		√		√
FIA_ATD.1		√		√
FIA_UAU.2				
FIA_UAU.5		√		
FIA_UAU.6		√		
FIA_UAU.7		√		
FIA_UID.2				
FIA_USB.1		√		
FIA_AFL.1	√	√		
FMT_MSA.1	√	√		√
FMT_MSA.3	√	√		
FMT_MTD.1	√	√		
FMT_SMF.1		√		√
FMT_SMR.1		√		
FMT_MOF.1	√	√		
FPT_STM.1				
FTA_SSL.3		√		
FTA_TSE.1		√		
FCS_COP.1		√	√	√

NOTE

S = Selection; A = Assignment; R = Refinement; I = Iteration

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:

- Start-up and shutdown of the audit functions
- All auditable events for the ***not specified*** level of audit; and
- **The following auditable events:**
  - **User activity**
    - **Login and logout**
    - **Configuration change requests**
  - **User management**
    - **Adding, deleting, or modifying users**
    - **User password change**
    - **User lock and unlock**
    - **User offline**

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

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event.
- 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**.

NOTE

The startup and shutdown of the audit functions are associated with the startup and shutdown of the entire TOE. The audit functionality will always be active 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 users with a role which contains alarm_R permission** 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_SAR.2 Restricted Audit Review

FAU_SAR.2.1: The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

5.1.1.5 FAU_SAR.3 Selectable Audit Review

FAU_SAR.3.1: The TSF shall provide the ability to apply **methods of selection** of audit data based on **the record type, record number, record sequence, record level, record status and record object**.

5.1.1.6 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.

5.1.1.7 FAU_STG.3 Action in Case of Possible Audit Data Loss

FAU_STG.3.1: The TSF shall **dump the oldest 10,000 stored audit records to the specified FTP server after the event dump function has been enabled and set** if the audit trail exceeds **50,000 records**.

5.1.1.8 FAU_STG.4 Prevention of Audit Data Loss

FAU_STG.4.1: The TSF shall ***ignore audited events*** and **none other actions** if the audit trail is full.

5.1.2 User Data Protection (FDP)

5.1.2.1 FDP_ACC.1/LUN Subset Access Control

FDP_ACC.1.1/LUN: The TSF shall enforce the **Attribute Based Access Control policy for LUNs** on:

- **Subjects: Application servers**
- **Objects: LUNs**
- **Operations: Read and write**

5.1.2.2 FDP_ACC.1/USER Subset Access Control

FDP_ACC.1.1/USER: The TSF shall enforce the **Role Based Access Control policy for Commands** on:

- **Subjects: the user of the TOE with the roles defined in FMT_SMR.1**
- **Objects: the commands to configure and manage the TOE**
- **Operations: configure and manage**

5.1.2.3 FDP_ACF.1/LUN Security Attribute Based Access Control

FDP_ACF.1.1/LUN: The TSF shall enforce the **Attribute Based Access Control policy for LUNs** to objects based on the following:

- **Subjects: Application servers**

  Subject attributes:

  - **World Wide Name**
- **Objects: LUNs**

Object attributes:

- **LUN ID**
- **LUN World Wide Name**

FDP_ACF.1.2/LUN: 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 a LUN if the LUN ID and LUN World Wide Name have been mapped to the application server**.

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

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

5.1.2.4 FDP_ACF.1/USER Security Attribute Based Access Control

FDP_ACF.1.1/USER: The TSF shall enforce the **Role Based Access Control policy for Commands** to objects based on the following:

- **Subjects: Administrative user**

  Subject attributes:
  - **Account password**
  - **Account role ID (a role stands for a specified set of permissions)**
- **Objects: Commands**

  Object attributes:
  - **Permissions to execute the commands**

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

- **Only authorized users are permitted to access commands.**
- **Users can be assigned with different roles to control the TOE access permission.**
- **There are 8 built-in roles (listed in FMT_SMR.1.1) and at most 56 customized roles.**
- **Each role stands for a specified set of permissions.**
- **Each command has its corresponding permissions and the correspondence is defined by the software which cannot be changed.**
- **Commands are allowed to be accessed and executed by an account only if the permission set of the account's role has the command's corresponding permissions.**

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

FDP_ACF.1.4/USER: 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/USER User Attribute Definition

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

- **Account Name**
- **Account Password**
- **Account Type (Local, Domain User, Domain Group)**
- **Account Lock Status (Unlocked, Locked)**
- **Account Role ID**
- **Password Status (Normal, Expired, Initialization, About to expire, Unsafe, Never expire)**
- **Account Status (Online, Offline)**
- **Account Login Method**

NOTE

- If the user is a domain user, the **Account Password** and **Password Status** are not security attributes belonging to the TOE because the password of the user is not maintained.
- **Account Login Method** defines the login method (SSH, SFTP, RESTful, Serial Port, etc) allowed for the account.

5.1.3.2 FIA_ATD.1/LUN User Attribute Definition

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

- **Host World Wide Name**
- **LUN ID**

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_UAU.5 Multiple Authentication Mechanisms

FIA_UAU.5.1: The TSF shall provide the **password mechanism, SSH key pair mechanism, and OTP mechanism** to support user authentication.

FIA_UAU.5.2: The TSF shall authenticate any user's claimed identity according to the **following rules:**

- **Authentication is passed only if the hash values of input username and password are the same as those stored in the TOE or remote LDAP server when the password authentication mechanism is used.**
- **Authentication is passed only if the private key that the user's SSH client holds matches the public key stored in the TOE.**
- **Authentication is passed only if the input OTP is the same as that generated by the TOE and sent to the recipient email box.**

5.1.3.5 FIA_UAU.6 Re-authenticating

FIA_UAU.6.1: The TSF shall re-authenticate the user under the conditions: **rebooting or powering off the TOE, initializing a user's password, unlocking a user, and clearing or importing configuration data.**

5.1.3.6 FIA_UAU.7 Protected Authentication Feedback

FIA_UAU.7.1: The TSF shall provide only **obscured following feedback:**

- **Obscured input password for example:**
  a. **Asterisks to represent password while login through DeviceManager.**
  b. **Asterisks or hidden characters to represent password while login through SSH, the specific type depends on the SSH client.**
  c. **Hidden characters to represent password while login through Serial Port.**
  d. **Asterisks to represent password while re-authentication in DeviceManager or CLI**
- **Obscured authentication failure feedback for example:**
  a. **When login through unsupported login method, the feedback is "The account does not support this login method. 1. Configure a correct login method list for this account as the super administrator. 2. Log in using an allowed method."**
  b. **When login with incorrect username or password, and the Account Lockout is disable, the feedback is "The user name or password is incorrect. Check the user name and password, and try again."**
  c. **When login with incorrect username or password, and the Account Lockout is enable, the feedback is "The user name or password is incorrect. Enter the correct user name and password. You can try for X times." where X stands for the number of tries left. And once the attempts exhausted, the feedback is "The user account has been locked. Try again after Y seconds." where Y stands for the locked time of this account.**
  d. **When re-authenticating with incorrect password, the feedback is "XXX. Description: the password is incorrect. Suggestion: check the password and try again." Where XXX describes the failure of the specific operation such as "Restarting the device failed".**

to the user while the authentication is in progress.

NOTE

The feedbacks above are just examples, which is a subset of the TOE.

5.1.3.7 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.

NOTE

The domain users are identified and authenticated by a remote LDAP server. The TOE allows access of a domain user depending on the pass/failure verdict provided by such remote LDAP server once the domain user performs an authentication attempt.

5.1.3.8 FIA_USB.1 User-Subject Binding

FIA_USB.1.1: The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: **Account Name and Account Role ID**.

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**.

5.1.3.9 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1: The TSF shall detect when ***an administrator configurable positive integer from 1 to 9 (consecutive within 5 minutes)*** unsuccessful authentication attempts occur related to **user login and other conditions that need re-authentication**.

FIA_AFL.1.2: When the defined number of unsuccessful authentication attempts has been ***met***, the TSF shall:

- **Lock the offending account for Temporary and set minutes from 3 to 2000, which can be configured by an administrator**.
- **Lock the offending account for Permanent, which can be configured by an administrator**.
- **Audit the event in the security log**.

NOTE

The locking action will only be taken if the failure occurs in login.

5.1.4 Security Management (FMT)

5.1.4.1 FMT_MSA.1/LUN Management of Security Attributes

FMT_MSA.1.1/LUN: The TSF shall enforce the **Role Based Access Control policy for LUNs** to restrict the ability to ***query, modify, delete*** the security attributes **defined in FDP_ACF.1.1/LUN** to **the administrative users with roles in FMT_SMR.1.1 that have the proper permissions**.

5.1.4.2 FMT_MSA.1/USERa Management of Security Attributes

FMT_MSA.1.1/USERa: The TSF shall enforce the **Role Based Access Control policy for Commands** to restrict the ability to ***query*** the security attributes **which is users' own attributes defined in FIA_ATD.1/USER except Account Password** to **the administrative users with all roles in FMT_SMR.1.1.**

5.1.4.3 FMT_MSA.1/USERb Management of Security Attributes

FMT_MSA.1.1/USERb: The TSF shall enforce the **Role Based Access Control policy for Commands** to restrict the ability to ***modify and query*** the security attributes **which is other users' attributes except Account Password defined in FIA_ATD.1/USER** to **the administrative users with roles in FMT_SMR.1.1 that have the proper permissions.**

5.1.4.4 FMT_MSA.1/USERc Management of Security Attributes

FMT_MSA.1.1/USERc: The TSF shall enforce the **Role Based Access Control policy for Commands** to restrict the ability to ***change_default*** the security attributes **which is other users' Account Password defined in FIA_ATD.1/USER** to **the administrative users with roles in FMT_SMR.1.1 that have the proper permissions.**

5.1.4.5 FMT_MSA.1/USERd Management of Security Attributes

FMT_MSA.1.1/USERd: The TSF shall enforce the **Role Based Access Control policy for Commands** to restrict the ability to ***modify*** the security attributes **which is users' own**

Account Password defined in FIA_ATD.1/USER to **the administrative users with roles in FMT_SMR.1.1 that have the proper permissions.**

5.1.4.6 FMT_MSA.3 Management of Security Attributes

FMT_MSA.3.1: The TSF shall enforce the **Role Based Access Control policy for Commands** to provide ***permissive*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2: The TSF shall allow the **authorized roles as defined in FMT_SMR.1** to specify alternative initial values to override the default values when an object or information is created.

5.1.4.7 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1: The TSF shall restrict the ability to ***change_default, query, modify, delete, and clear*** the **configuration of Security Management Functions defined in FMT_SMF.1/LUN and FMT_SMF.1/USER** to **users with authorized roles as defined in FMT_SMR.1.1.**

5.1.4.8 FMT_SMF.1/LUN Specification of Management Functions

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

- **Logical host and host group management**
- **LUN mapping**

5.1.4.9 FMT_SMF.1/USER Specification of Management Functions

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

- **Management of accounts and account attributes, including account credentials**
- **Management of the account policy, including account name length, password complexity, failure policy, and lockout policy**
- **Management of ACLs and ACL parameters such as IP addresses or address ranges**
- **Configuration of network services used by the TOE, such as NTP, Syslog, LDAP, SFTP, DNS**
- **Management of the TOE's time**

5.1.4.10 FMT_SMR.1 Security Roles

FMT_SMR.1.1: The TSF shall maintain the roles: **the authorized roles identified in the table below.**

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

Table 5-2 Role permission definition

Role	Authority
Super administrator	All permissions
Administrator	All permissions except user management and high-risk

Role	Authority
	maintenance operations
Security administrator	System security configuration permissions, including management of security rules, certificates, and data destruction
SAN resource administrator	SAN resource management permissions, including management of storage pools, LUNs, mappings, hosts, ports, and background configuration tasks
Data protection administrator	Data protection management permissions, including management of LUNs, local data protection, remote data protection, HyperMetro, and background configuration tasks
Remote device administrator	Cross-device data protection management permissions, including management of remote replication, HyperMetro, 3DC, LUNs, and mappings. This role is used for remote authentication in cross-device data protection scenarios.
Empty role	None permission except those allow query of information about itself.
Monitor	The role is used to monitor the TOE and to view the audit records.

5.1.4.11 FMT_MOF.1 Management of Security Function Behaviour

FMT_MOF.1.1: The TSF shall restrict the ability to ***determine the behaviour of*** the functions **defined in FMT_SMF.1/USER and FMT_SMF.1/LUN** to **users with authorized roles as defined in FMT_SMR.1.1.**

5.1.5 Protection of the TSF (FPT)

5.1.5.1 FPT_STM.1 Reliable Timestamps

FPT_STM.1.1: The TSF shall be able to provide reliable timestamps.

NOTE

The security function calls the NTP function to provide reliable timestamps.

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 interval (minutes from 1 to 100, which can be configured by an administrator) 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:

- **Authentication failure**
- **User login IP address**
- **Max attempts due to authentication failure within certain period of time**

- **Login method**
- **Server IQN**

5.1.7 Cryptographic Support (FCS)

5.1.7.1 FCS_COP.1/SHA256 Cryptographic Operation

FCS_COP.1.1/SHA256: The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **SHA256** and cryptographic key sizes **None** that meet the following: **FIPS 180-4.**

NOTE

SHA256 is used in TLS communication.

5.1.7.2 FCS_COP.1/PBKDF2 Cryptographic Operation

FCS_COP.1.1/PBKDF2: The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **PBKDF2 (SHA256)** (with iteration number 10,000) and cryptographic key sizes **None** that meet the following: **RFC2898**.

NOTE

PBKDF2 is used for hashing passwords before storage in non-volatile memory. The salt used in PBKDF2 is a 16-byte random number obtained from the Euler OS deterministic random number generator.

5.2 Security Functional Requirement Rationale

5.2.1 Coverage

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

Table 5-3 Mapping SFRs to objectives

Objective	Security Functional Requirement	Rationale
O.Audit The TOE should provide functionality to generate audit records for all configuration actions and should provide the ability to review audit records for authorized users.	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_SAR.2	The requirement meets the objective by

Objective	Security Functional Requirement	Rationale
	Restricted audit review	prohibiting all unauthorized users from accessing the audit records.
	FAU_SAR.3 Selectable audit review	The requirement meets the objective by ensuring that authorized users have access to the audit records.
	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.3 Action in Case of Possible Audit Data Loss	The requirement meets the objective by ensuring the audit record integrality.
	FAU_STG.4 Prevention of audit data loss	The requirement meets the objective by ensuring the audit record integrality.
	FPT_STM.1 Reliable time stamps	The requirement meets the objective by ensuring that all audit records are associated with a reliable timestamp.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that the TOE identifies each user before any action.
	FMT_SMF.1/LUN Specification of Management Functions	The requirement meets the objective by ensuring that the TOE manages the audit configuration of servers.
	FMT_SMF.1/USER Specification of Management Functions	The requirement meets the objective by ensuring that the TOE manages audit configuration of users.
O.Authentication The TOE must require each user/server to be successfully authenticated before allowing any action.	FIA_ATD.1/USER User attribute definition	The requirement meets the objective by ensuring that the TOE maintains security attributes for each local user.
	FIA_ATD.1/LUN User attribute definition	The requirement meets the objective by ensuring that the TOE maintains security attributes for each server.
	FIA_UAU.2 User authentication before any action	The requirement meets the objective by ensuring that the TOE authenticates each user before any action.
	FIA_UAU.5 Multiple authentication mechanisms	The requirement meets the objective by ensuring that the TOE supports multiple authentication mechanisms for each user.

Objective	Security Functional Requirement	Rationale
	FIA_UAU.6 Re-authenticating	The requirement meets the objective by ensuring that the TOE requires re-authentication for important operations.
	FIA_UAU.7 Protected authentication feedback	The requirement meets the objective by ensuring that the TOE protects authentication feedback for each user.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that the TOE identifies each user before any action.
	FIA_USB.1 User-subject binding	The requirement meets the objective by ensuring that a user-subject is generate after successful authentication.
	FIA_AFL.1 Authentication failure handling	The requirement meets the objective by ensuring that the TOE handles authentication failure for each user.
	FMT_SMF.1/LUN Specification of Management Functions	The requirement meets the objective by ensuring that the TOE manages the authentication policy of servers.
	FMT_SMF.1/USER Specification of Management Functions	The requirement meets the objective by ensuring that the TOE manages the authentication policy of users.
	FCS_COP.1/SHA256 Cryptographic operation	The requirement meets the objective by ensuring that the TOE crypts the password with this algorithm.
	FCS_COP.1/PBKDF2 Cryptographic operation	The requirement meets the objective by ensuring that the TOE crypts the password with this algorithm.
	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 The TOE should implement different authorization levels that can be assigned to administrators in order to restrict the functionality available to individual administrators.	FDP_ACC.1/LUN Subset access control	The requirement meets the objective by ensuring that the TOE has an access control policy that allows only authorized servers to gain data from the TOE.
	FDP_ACC.1/USER Subset access control	The requirement meets the objective by ensuring that the TOE has an access control policy that allows only authorized users to gain access to the TOE.
	FDP_ACF.1/LUN Security attribute based	The requirement meets the objective by ensuring that only authorized servers gain

Objective	Security Functional Requirement	Rationale
	access control	access to data protected by the TOE.
	FDP_ACF.1/USER Security attribute based access control	The requirement meets the objective by ensuring that only authorized users gain access to the TOE.
	FIA_ATD.1/USER User attribute definition	The requirement meets the objective by ensuring that the TOE maintains security attributes for each local user.
	FIA_ATD.1/LUN 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 identifies each user before any action.
	FMT_MSA.1/LUN Management of security attributes	The requirement meets the objective by ensuring that the security attributes of LUNs in the TOE can be changed only by authorized users.
	FMT_MSA.1/USERa Management of security attributes	The requirement meets the objective by ensuring that the security attributes of users in the TOE can be changed only by authorized users.
	FMT_MSA.1/USERb Management of security attributes	The requirement meets the objective by ensuring that the security attributes of users in the TOE can be changed only by authorized users.
	FMT_MSA.1/USERc Management of security attributes	The requirement meets the objective by ensuring that the security attributes of users in the TOE can be changed only by authorized users.
	FMT_MSA.1/USERd Management of security attributes	The requirement meets the objective by ensuring that the security attributes of users in the TOE can be changed only by authorized users.
	FMT_MSA.3 Static attribute initialization	The requirement meets the objective by ensuring that the default values for security attributes of LUNs or users in the TOE should be provided and can be changed by authorized users.
	FMT_SMF.1/LUN Specification of Management Functions	The requirement meets the objective by ensuring that the TOE manages the authentication policy of servers.
	FMT_SMF.1/USER	The requirement meets the objective by ensuring that the TOE manages the

Objective	Security Functional Requirement	Rationale
	Specification of Management Functions	authentication policy of users.
	FMT_SMR.1 Security roles	The requirement meets the objective by ensuring that specific roles are defined for 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 the TOE after a specific period of time.
O.SecurityManagement The TOE should provide a method for authorized users to properly and safely manage the TOE.	FAU_SAR.1 Audit review	This requirement meets the objective by ensuring that the audit review functionality can be managed.
	FMT_MOF.1 Management of Security Function Behaviour	This requirement meets the objective by ensuring that only authorized users can manage the Security Function.
	FMT_MSA.1/LUN Management of security attributes	The requirement meets the objective by ensuring that the security attributes of LUNs can be managed.
	FMT_MSA.1/USERa Management of security attributes	The requirement meets the objective by ensuring that the security attributes of users can be managed.
	FMT_MSA.1/USERb Management of security attributes	The requirement meets the objective by ensuring that the security attributes of users can be managed.
	FMT_MSA.1/USERc Management of security attributes	The requirement meets the objective by ensuring that the security attributes of users can be managed.
	FMT_MSA.1/USERd Management of security attributes	The requirement meets the objective by ensuring that the security attributes of users can be managed.
	FMT_MSA.3 Static attribute initialization	The requirement meets the objective by ensuring that the default values for security attributes of users and LUNs in the TOE can be managed.
	FMT_MTD.1 Management of TSF data	The requirement meets the objective by ensuring that the attributes and configuration of security management functions can be managed.
	FMT_SMF.1/LUN Specification of	The requirement meets the objective by ensuring that the TOE manages the

Objective	Security Functional Requirement	Rationale
	Management Functions	authentication policy of servers.
	FMT_SMF.1/USER Specification of Management Functions	The requirement meets the objective by ensuring that the TOE manages 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.
O.AccessControl The TOE must require each user/server to be added to the whitelist before allowing any action.	FIA_ATD.1/USER User attribute definition	The requirement meets the objective by ensuring that the TOE maintains login method for each local user.
	FTA_TSE.1 TOE session establishment	The requirement meets the objective by ensuring that the TOE should deny the access based on IP/IQN white list.

5.2.2 Security Requirement Dependency Rationale

The security functional requirements in this Security Target do not introduce dependencies on any security assurance requirement; neither do the security assurance requirements in this Security Target introduce dependencies on any security functional requirement.

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

Table 5-4 Dependencies of SFRs

Security Functional Requirement	Dependency	Resolution
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.2
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.3	FAU_STG.1	FAU_STG.1
FAU_STG.4	FAU_STG.1	FAU_STG.1
FDP_ACC.1/LUN	FDP_ACF.1	FDP_ACF.1/LUN
FDP_ACC.1/USER	FDP_ACF.1	FDP_ACF.1/USER

Security Functional Requirement	Dependency	Resolution
FDP_ACF.1/LUN	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/LUN FMT_MSA.3
FDP_ACF.1/USER	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/USER FMT_MSA.3
FIA_ATD.1/LUN	N/A	N/A
FIA_ATD.1/USER	N/A	N/A
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UAU.5	N/A	N/A
FIA_UAU.6	N/A	N/A
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2
FIA_UID.2	N/A	N/A
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FMT_MSA.1/LUN	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	FDP_ACC.1/LUN FMT_SMR.1 FMT_SMF.1/LUN
FMT_MSA.1/USERa	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	FDP_ACC.1/USER FMT_SMR.1 FMT_SMF.1/USER
FMT_MSA.1/ USERb	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	FDP_ACC.1/USER FMT_SMR.1 FMT_SMF.1/USER
FMT_MSA.1/ USERc	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	FDP_ACC.1/USER FMT_SMR.1 FMT_SMF.1/USER
FMT_MSA.1/ USERd	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	FDP_ACC.1/USER FMT_SMR.1 FMT_SMF.1/USER
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1/LUN FMT_SMF.1/USER
FMT_SMF.1/LUN	N/A	N/A

Security Functional Requirement	Dependency	Resolution
FMT_SMF.1/USER	N/A	N/A
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1/LUN FMT_SMF.1/USER
FPT_STM.1	N/A	N/A
FTA_SSL.3	N/A	N/A
FTA_TSE.1	N/A	N/A
FCS_COP.1/SHA256	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Unsupported: FCS_CKM.1, FCS_CKM.4
FCS_COP.1/PBKDF2	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Unsupported: FCS_CKM.1, FCS_CKM.4

NOTE

Rationale for Unsatisfied Dependencies:

The FCS_COP.1/SHA256 dependency on FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1; SHA256 is the Secure Hash Algorithm, and cryptographic hash algorithms do not need cryptographic keys to operate.

The FCS_COP.1/PBKDF2 dependency on FDP_ITC.1, FDP_ITC.2, or FCS_CKM.1; PBKDF2 is key derivation functions, used to reduce vulnerabilities to brute force attacks, and this cryptographic algorithms do not need cryptographic keys to operate.

5.3 Security Assurance Requirements

The security assurance requirements for the TOE are taken from the CC Part 3 and are EAL3+ALC_FLR.2 (Evaluation assurance level 3+ ALC_FLR.2).

Table 5-5 TOE security assurance requirements

Assurance Class	Assurance Component
Class ADV: Development	ADV_FSP.3
	ADV_TDS.2
	ADV_ARC.1
Class AGD: Guidance Documents	AGD_OPE.1
	AGD_PRE.1

Assurance Class	Assurance Component
Class ALC: Lifecycle Support	ALC_CMC.3
	ALC_CMS.3
	ALC_DEL.1
	ALC_DVS.1
	ALC_LCD.1
	ALC_FLR.2
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

5.4 Security Assurance Requirement Rationale

The evaluation assurance level 3+ALC_FLR.2 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 Identification and Authentication

The purpose of authentication and identification is to make sure a user can access the TOE only after the TOE has identified the user identity as the right account.

- The TOE supports authentication and identification on two types of users: Administrative Users and Data Users.
  - The Administrative User is an account that will manage or configure the TOE's functions, including but not limited to security functions.
  - The Data User is a subject that will access the data stored in the TOE through standard I/O protocols.
- To Administrative Users, the TOE provides local and remote authentication modes.
  - In local authentication mode, the user identities are stored locally in the TOE. The identification factors include the password, SSH key pair, and one time password (OTP) sent through email. The TOE supports 3 kinds of combinations: password and OTP, password only, and SSH key pair only. The combination of a user's identification factors can be chosen by another user whose role has the proper permissions.
    i. When the password is used, the result of identification is based on the comparison between the hash of the input password and the one stored in the TOE. The hash algorithm is PBKDF2, which iteratively performs SHA256 with the password for 10,000 times.
    ii. When the account SSH key pair is chosen, the result of identification is based on the match result between the SSH public key stored in the TOE and the

private key held by the SSH client. This type of identification can be chosen only for login through SSH or SFTP.

iii. When the OTP is used, an email with the OTP will be sent to the recipient configured by other administrative users with proper roles. The OTP is generated by the TOE randomly. A user is allowed to log in to the TOE only when the input OTP is same as the one generated by the TOE.

– In remote authentication mode, the user identities are stored in a remote LDAP server (which means a server in compliance with the standard LDAP protocol, such as the AD server and OpenLDAP server).

iv. The LDAP server's essential information (including the IP address, port, and protocol) is configured by a user whose role has the proper permissions.

v. In this type of identification, the TOE acts as an LDAP client. The input account name and password are forwarded to the LDAP server through the standard LDAP protocol and are verified by the LDAP server.

- Authentication occurs not only in logging in to the TOE, but also in executing some vital commands such as rebooting or powering off the TOE, initializing the user password, unlocking a user, and clearing or importing configuration data. This is called re-authentication.
- If the identification is successful, information about the last successful login (including the IP address and time) will be displayed. This function can be enabled or disabled by proper Administrative Users.
- The input password is presented as asterisks, and no mater any reason the authentication or re-authentication fails with, the TOE will only give blurry feedback to prevent from brute-force cracking. In addition, after the authentication or re-authentication failure, the failure count is recorded in the TOE. After N consecutive authentication failures during 5 minutes, the account will be locked for M minutes, in which N is a positive integer from 1 to 9 and M is a positive integer from 3 to 2000. Both of the values can be configured by a user whose role has proper permissions and both take effect globally.
- After a successful identification, a session will be created to stand for the user dynamically. During the session's creation, a random unique number will be generated by Euler OS as an identifier of the session, and the user's account name, account role and other security attributes will be assigned to the session. A session will be terminated if it is inactive up to N minutes, in which N is a positive number from 1 to 100 and is configured by Administrative Users with proper permissions.
- The Administrative User with proper permissions can configure a mapping, which contains relationships between an iSCSI initiator (World Wide Name, i.e. WWN) and an iSCSI target (LUN). The Data User (application server which holds the initiator) whose initiator is in the mapping pre-configured in the TOE has rights to access the data (i.e. LUN) on the TOE, which is actually a simple Attribute Based Access Control model. Furthermore, if CHAP authentication is enabled, the target LUN on the TOE can be accessed only when CHAP authentication is passed. All these above are similar to other SAN protocols.

TOE Security Functional Requirements Satisfied: (FDP_ACC.1/LUN, FDP_ACF.1/LUN, FIA_ATD.1/USER, FIA_ATD.1/LUN, FIA_UAU.2, FIA_USB.1, FIA_UAU.5, FIA_UAU.6, FIA_UAU.7, FIA_UID.2, FIA_AFL.1, FTA_SSL.3, FTA_TSE.1, FCS_COP.1/SHA256, FCS_COP.1/PBKDF2)

6.2 Authorization

Authorization is to grant proper permissions to identify sessions which are generated with subset of identified users' attributes, so that the identified Administrative Users have rights to execute specified commands in the TOE.

The TOE implements authorization according to the core RBAC model modified slightly. The key points of the implementation of the core RBAC model are described as below:

- Every action of Administrative Users is achieved by a command, and every command has one or more permissions associated to it. This relationship is built in the TOE. A user can execute a command only if the user's permission list contains this command's permission.
- A set of permissions composes a role. The TOE supports up to 64 roles, among which 8 are built-in roles that cannot be modified or deleted, and the rest can be customized by users whose role has proper permissions.
- Only one role can be assigned to a user. The assignment can be done during the creation or modification of a user.
- A user is authorized to perform certain operations and is forbidden to perform certain operations. This is achieved by comparing the permissions held by the account's assigned role and the permissions of the commands which bearing the operations.

Table 6-1 Role permission definition

Role	Authority
Super administrator	All permissions
Administrator	All permissions except user management and high-risk maintenance operations
Security administrator	System security configuration permissions, including management of security rules, certificates, and data destruction
SAN resource administrator	SAN resource management permissions, including management of storage pools, LUNs, mappings, hosts, ports, and background configuration tasks
Data protection administrator	Data protection management permissions, including management of LUNs, local data protection, remote data protection, HyperMetro, and background configuration tasks
Remote device administrator	Cross-device data protection management permissions, including management of remote replication, HyperMetro, 3DC, LUNs, and mappings. This role is used for remote authentication in cross-device data protection scenarios.
Empty role	None permission except those allow query of information about itself.
Monitor	The role is used to monitor the TOE and to view the audit records.

TOE Security Functional Requirements Satisfied: (FDP_ACC.1/USER, FDP_ACF.1/USER, FIA_ATD.1/USER, FMT_SMR.1, FMT_MOF.1)

6.3 Access Control

Access Control indicates that rules can be formulated by proper Administrative Users to globally control the access of a specific user to the TOE.

The TOE supports two Access Control mechanisms for Administrative Users:

- The IP Whitelist is configured globally to limit access from IP addresses out of the list. The elements of the list are single IP addresses or ranges.
- Login Method is a list including SSH, SFTP, RESTful, Serial Interface, etc. A user can access the TOE only using the method/protocol included in this list configured for the user by other proper Administrative Users.

TOE Security Functional Requirements Satisfied: (FIA_ATD.1/USER, FTA_TSE.1)

6.4 Auditing

The TOE provides an audit trail for all essential operations.

- All non-query operations will be recorded in the operation logs. Typically, these operations include login, logout, configuration change, user management, and security settings.
- An audit record is composed of 6 basic items: who (user name), where (user IP address), when (timestamp), what (operation description), result (success or specific error code), and ID (a unique number of this record).
- Review functionality is provided via the command line interface and GUI, which allows Administrative Users to inspect the audit logs. Administrative Users whose role has proper permissions can query or fetch the audit trail.
- All audit trails are stored locally in the TOE's persistent media. If an FTP server to dump audit records is configured and enabled, once the number of records exceeds 50,000, the oldest 10,000 records will be dumped to the FTP server. If such an FTP server is not configured or not enabled, the newer records will be ignored once the number of records reaches 55,000.

TOE Security Functional Requirements Satisfied: (FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_STG.1, FAU_STG.3, FAU_STG.4, FPT_STM.1)

6.5 Security Management

The TOE allows management of security functions by Administrative Users. The TOE can be configured to grant user the access right to the resources that are required for user operations.

- The TOE's mainly security functions include:
  - Account Management, including the account password, account lockout status, account's role and other credentials.
  - Account Policy Management, including the account name length, password complexity, access failure policy, and account lockout policy.
  - Access Control List Management, including the login method list and IP whitelist.
  - Network Service Management, including Network Time Protocol (NTP), Syslog, Light Directory Access Protocol (LDAP), Secure File Transfer Protocol (SFTP) and

Domain Name System (DNS). The NTP service can synchronize all the clocks of devices on the network so that these devices can provide multiple applications (including audit trails' timestamp) based on the uniform time.

- Time Management, including time and time zone.
- Data Resource Management, including LUNs and mappings.

- Every security function has corresponding permissions. Administrative Users whose role has proper permissions are permitted to manage the corresponding security functions.

TOE Security Functional Requirements Satisfied: (FMT_MSA.1/LUN, FMT_MSA.1/USERa, FMT_MSA.1/USERb, FMT_MSA.1/USERc, FMT_MSA.1/USERd, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1/LUN, FPT_STM.1, FMT_MOF.1, FMT_SMF.1/USER)

7 Glossary

7.1 Abbreviations and Terminology

remote replication(out of scope)	Active Standby data center
HyperMetro(out of scope)	Active-Active Data Centers
3DC(out of scope)	Three Data Centers
LAN	Local Area Network
SAN	Storage Area Network
AD	Active Directory
LDAP	Lightweight Directory Access Protocol
iSCSI	Internet Small Computer System Interface
LUN	Logic Unit Number
CHAP	Challenge Handshake Authentication Protocol
WWN	World Wide Name

RBAC	Role Based Access Control
SSH	Secure Shell
SFTP	Secure File Transfer Protocol
FTP	File Transfer Protocol
REST	Representational State Transfer
NTP	Network Time Protocol
DNS	Domain Name System
PAM	Pluggable Authentication Module
ACL	Access Control List
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
CC	Common Criteria

7.2 References

[CC] Common Criteria for Information Technology Security Evaluation, Part 1-3, Version 3.1 Revision 5, April 2017