Huawei OceanStor Dorado Storage System Software 6.1.2

Security Target

Issue	**0.21**
Date	**2024-11-26**

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
2024-11-26	0.21	Updated based on “20240919 [SGS] OceanStor TOE Identification issues”	Zeng Jie
2024-08-14	0.20	Removed hardware models except Dorado6000 V6 and updated the link in 1.3.3.	Zeng Jie
2024-07-24	0.19	Updated based on the ‘To update in ST and guidance’	Zeng Jie
2024-04-28	0.18	Updated based on the ‘21-RPT-611 Action Item List ASE v10.0’	Zeng Jie
2024-03-19	0.17	Updated based on the ‘21-RPT-616 Action Item List ASE v8.0’	Zeng Jie
2023-09-26	0.16	Updated based on the ‘21-RPT-616 Action Item List ATE v2.1’	Zeng Jie
2023-02-06	0.15	Updated based on the ‘21-RPT-616 Action Item List ATE v1.0’	Zeng Jie
2022-09-19	0.14	Updated based on the 'Actin Item list ASE v6.0 '	Yan Lei, Zeng Jie
2022-08-01	0.13	Updated based on the 'Action Item list ASE v5.0 '	Yan Lei, Zeng Jie
2022-07-04	0.12	Delete FAU_STG.4 Updated based on the 'Action Item list ASE v5.0 '	Yan Lei
2022-05-04	0.11	Addressed evaluator’s feedback	Huawei
2022-04-12	0.10	Updated TOE logical scope	Huawei
2021-10-14	0.9	Updated TOE logical scope	Luo Weihua
2021-09-23	0.8	Updated based on the 'Action Item list ASE v3.0 '	Luo Weihua

2021-09-01	0.7	Updated based on the 'Action Item list ASE v2.0 '	Luo Weihua
2021-07-06	0.6	Updated based on the 'Action Item list ASE v1.3 '	Luo Weihua
2021-06-30	0.5	Add table 5-6 5-7	Luo Weihua
2021-06-16	0.4	Updated based on the 'Action Item list ASE v1.1 '	Luo Weihua
2021-06-16	0.3	Updated based on the 'Action Item list ASE v1.0 '	Luo Weihua
2021-04-26	0.2	Updated by reviewed internally	Luo Weihua
2021-03-21	0.1	This is the initial draft.	Luo Weihua, Li Qiang

Contents

1 Introduction

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

1.1 ST Reference

Title: CC Huawei OceanStor Dorado Storage System Software 6.1.2 Security Target

Version: 0.21

Date: 2024-11-26

Developer: Huawei Technologies Co., Ltd.

1.2 TOE Reference

The TOE is identified as follows:

TOE name: Huawei OceanStor Dorado Storage System Software

TOE version: 6.1.2

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 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 is ideal for use with databases, virtual desktop infrastructure (VDI), virtual server infrastructure (VSI), SAP HANA, and file sharing services. OceanStor Dorado 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

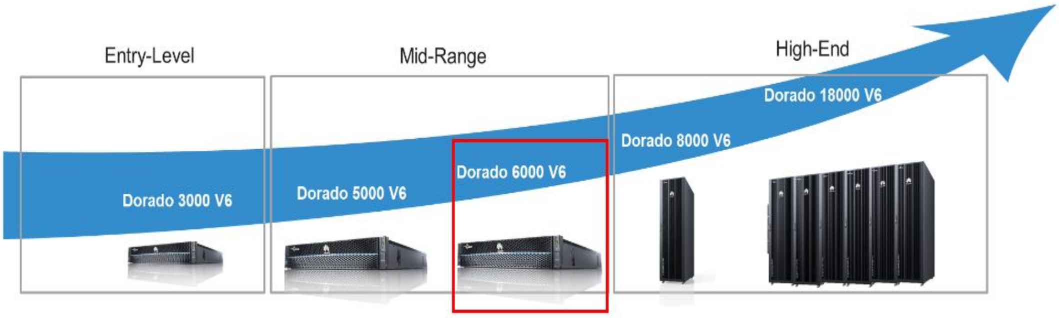
Storage system software

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

The TOE is a piece of software that manages the Huawei OceanStor Dorado storage application servers .

The TOE is running on the OceanStor Dorado 6000 V6 hardware model, which is a mid-range storage server as shown in the red box of Figure 1-1. Although the TOE can run on multiple OceanStor Dorado models, ONLY OceanStor Dorado 6000 V6 hardware model is considered as the non-TOE hardware model in this evaluation

Figure 1-1 OceanStor Dorado hardware models.

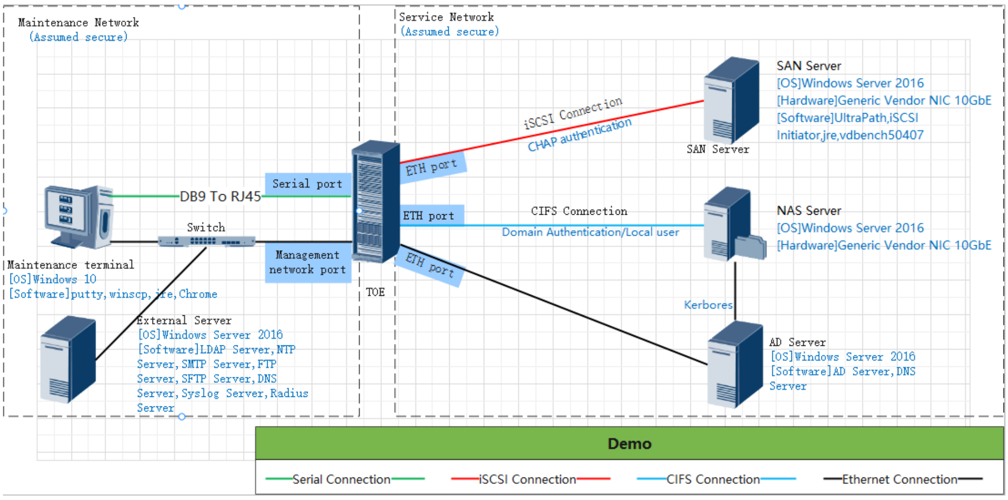


More information about the OceanStor Dorado 6000 V6 model can be found in the following links:

https://support.huawei.com/enterprise/en/flash-storage/oceanstor-dorado-6000-v6-pid-22784071

The TOE including Linux operating system (Euler OS V200R009C00) based on kernel 4.19.90 is running underlying hardware, see red frame in Figure 1-4. In addition, the software upgrade tool SmartKit (V200R007C00RC8 or later) and the software package integrity verification tool GnuPG are not parts of the TOE. Figure 1-2 shows the real environment for running the TOE.

Figure 1-2 Real environment of the TOE



- Description

  The external server, SAN server, NAS server, PC, and TOE (storage) are connected to each other by the Ethernet switch.

  The NIC on the SAN server, and NAS 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.

- SAN 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, SFTP server, DNS server, SMTP server, Syslog Server, Radius Server in Windows Server 2016
    - OpenSSH v8.0.0.0p1
- NAS server
  - Hardware
    - Rack servers or PCs with at least one 100M/1G Ethernet port

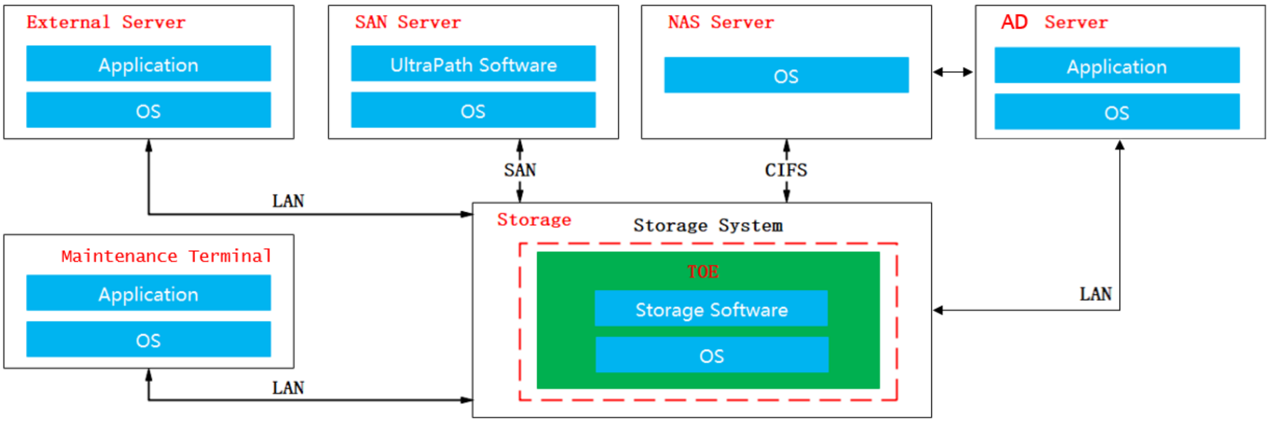
- Software
  - Windows Server 2016 OS
- Maintenance terminal
  - Hardware
    - Rack servers or PCs with at least one 100M/1G Ethernet port and one Serial DB9 port
  - Software
    - Windows 10 OS
    - Brower Google Chrome 64+
    - JRE (Java Runtime Environment 1.8), PuTTY 0.73, WinSCP 5.17, Python 3.9.5, notepad ++, Postman, Foxmail
- AD Server
  - Hardware

    Rack servers or PCs with at least one 100M/1G Ethernet port
  - Software
    - Windows Server 2016 OS
    - AD server, DNS server in Windows Server 2016

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 1-3 Software environment of the TOE



1.4 TOE Description

1.4.1 Physical Scope

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	link
Software	OceanStor_Dorado_V6_Software_6.1.2.tgz	6.1.2	https://support.huawei.com/enterprise/en/software/262802692-ESW2000380282
Software signature file	OceanStor_Dorado_V6_Software_6.1.2.tgz.asc		
Product guidance	OceanStor Dorado 6.1.2 Error Code Reference.zip	V0.2	https://support.huawei.com/enterprise/en/doc/EDOC1100194728?idPath=7919749%7C251366268%7C250389224%7C261066246%7C22784071
	OceanStor Dorado 6.1.2 Error Code Reference.zip.asc		
	OceanStor Dorado 6.1.2 Command Reference.zip	V0.2	https://support.huawei.com/enterprise/en/doc/EDOC1100194663?idPath=7919749%7C251366268%7C250389224%7C261066246%7C22784071
	OceanStor Dorado 6.1.2 Command Reference.zip.asc		
	OceanStor Dorado 6.1.2 REST Interface Reference.zip	V0.2	https://support.huawei.com/enterprise/en/doc/EDOC1100196921?idPath=7919749%7C251366268%7C250389224%7C261066246%7C22784071
	OceanStor Dorado 6.1.2 REST Interface Reference.zip.asc		
	OceanStor Dorado 6.1.2 Administrator Guide. zip	V0.2	https://support.huawei.com/enterprise/en/doc/EDOC1100194693?idPath=7919749%7C251366268%7C250389224%7C261066246%7C22784071
	OceanStor Dorado 6.1.2 Administrator Guide. zip.asc		
	OceanStor Dorado 6.1.2 Event Reference. zip	V0.2	https://support.huawei.com/enterprise/en/doc/EDOC1100194708?idPath=7919749%7C251366268%7C250389224%7C261066246%7C22784
	OceanStor Dorado 6.1.2 Event Reference. zip.asc		

Type	Delivery Item	Version	link
			071
	OceanStor Dorado 6.1.2 Initialization Guide. zip	V0.2	https://support.huawei.com/enterprise/en/doc/EDOC1100194740?idPath=7919749%7C251366268%7C250389224%7C261066246%7C22784071
	OceanStor Dorado 6.1.2 Initialization Guide. zip.asc		
	OceanStor Dorado 6.1.2 Security Configuration Guide. zip	V0.1	https://support.huawei.com/enterprise/en/doc/EDOC1100194656?idPath=7919749%7C251366268%7C250389224%7C261066246%7C22784071
	OceanStor Dorado 6.1.2 Security Configuration Guide. zip.asc		
	CC Huawei OceanStor Dorado Storage System Software 6.1.2 AGD_OPE.pdf	V0.9	https://support.huawei.com/enterprise/en/doc/EDOC1100401173
	CC Huawei OceanStor Dorado Storage System Software 6.1.2 AGD_OPE.pdf.asc		
	CC Huawei OceanStor Dorado Storage System Software 6.1.2 AGD_PRE_User.pdf	V0.15	https://support.huawei.com/enterprise/en/doc/EDOC1100401624
	CC Huawei OceanStor Dorado Storage System Software 6.1.2 AGD_PRE_User.pdf.asc		
	CC Huawei OceanStor Dorado Storage System Software 6.1.2 AGD_PRE_Production.pdf	V0.4	https://support.huawei.com/enterprise/en/doc/EDOC1100401625
	CC Huawei OceanStor Dorado Storage System Software 6.1.2 AGD_PRE_Production.pdf.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， SYS CTRL and Euler OS, and is running underlying hardware. The TOE provides several security functions, which are described in more detail in chap 1.4.3

Figure 1-4 TOE logical scope

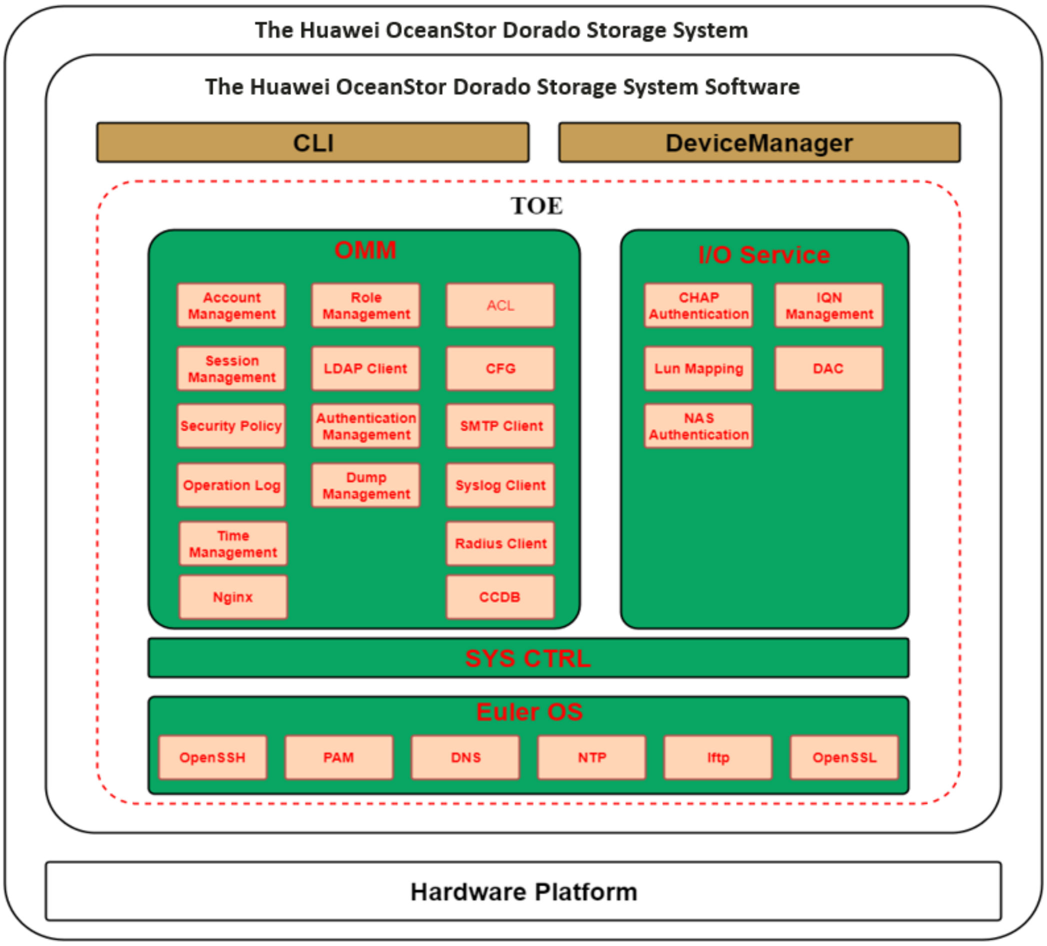


Figure 1-4 reflects the basic structure of the TOE with respect to subsystems and modules. The TOE provides all the security features. Security features are implemented through one or more modules.

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 or a remote radius server. The identification factors include the password, and OTP. The input password is sent forward to the remote LDAP server through the standard LDAP protocol and identified by the LDAP server. The input OTP is sent forward to the remote radius server through the standard radius protocol and identified by the radius server. The TOE supports 2 kinds of combinations: password and OTP, and password only.
- In data access, the TOE provides SAN service and NAS service.

In data access for SAN service, 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.

In data access for NAS service, the TOE maintains NTFS-Style files and provides CIFS protocol for access. Local authentication and AD domain authentication (Kerberos) are supported for file access in the TOE. In local authentication, the accessible users and passwords are verified by the TOE. In AD domain authentication, the accessible users are authenticated by the AD server.

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 a user 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, batch configuration and high-risk maintenance operations
Security administrator	System security configuration permissions, including management of security rules, certificates, KMC, and data destruction
SAN resource administrator	SAN resource management permissions, including management of storage pools, LUNs, mapping views, 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 mapping views. This role is used for remote authentication in cross-device data protection scenarios.
Monitor	Routine O&M permissions, such as information collection, performance collection, and inspection. This role does not have permission to manage SAN resources, data protection, and security configuration.
Non-privileged administrator	Basic system permissions, including querying information about the system, users, and roles. This role can be queried or used only on the CLI. On the CLI, this role is **Empty role**.

When a user 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 a user attempts to perform any unauthorized operation, an error message is displayed.

1.4.3.3 Access Control

The TOE supports filtering of incoming access to management interfaces. An user whose role has proper permissions can set the IP whitelist to limit access from IP addresses out of the list. The login method (CLI, SFTP, DeviceManager, RESTful, Serial Port) 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 mapping list configured before.

The TOE assigns different file access permissions to different users. DAC policies are used to control file access through CIFS protocol.

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 SFTP server when the log entries exceed a specified number.
- Review functionality is provided via the command line interface and DeviceManager (a customized web tool designed by Huawei), which allows users whose role has proper permissions 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 users and user attributes, including user credentials
- Management of the user policy, including user 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 1.4.3.2 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 EAL4+ 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.

3.3 Organizational Security Policies

P.DataCorruption

In order to prevent data corruption:

- TOE users should avoid incorrect system access to prevent data to become corrupted;
- Non-TOE users or applications should avoid unauthorized data modification, and Inadequate configuration actions through LAN should be avoided.

P.UnauthorizedSubject

In order to prevent unintended access user data within the local network, a user, application or server without access rights should not be able to read and write user data through SAN or NAS.

3.4 Assumptions

- **A.Manage**

  It is assumed that the administrators of the TOE 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.DataProtection**

  The TOE environment will provide a secure network communication to protect user data that is sent to and received from the TOE.

- **A.Hardware**

  It is assumed that the underlying hardware of OceanStor Dorado, 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 from user access.
- **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 administrators of the TOE is non-hostile, appropriately trained, and follows all administrator guidance. Also, users, applications and servers must be trustworthy when they access the TOE within the local network.
- **OE.Physical**

  The TOE environment should be protected against unauthorized physical access.
- **OE.DataProtection**

  The TOE environment will protect user data sent to and received from the TOE with a secure network communication.
- **OE.Hardware**

  The TOE environment must ensure that underlying hardware of OceanStor Dorado, 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.
	P.DataCorruption	O.Authentication enforces this policy by ensuring that only authenticated users can manage user data.
	P.UnauthorizedSubject	O.Authentication enforces this policy 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.
	P.DataCorruption	O.Authorization enforces this policy by ensuring that only authorized users 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

Objective	Threat, OSP, Assumption	Rationale
		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.
	P.DataCorruption	O.SecurityManagement enforces this policy by allowing a user to properly configure the TOE.
	P.UnauthorizedSubject	O.SecurityManagement enforces this policy by allowing a user to properly configure the TOE to map LUNs to the servers and DAC policies of file systems in the TOE.
O.AccessControl	T.UnauthenticatedAccess	O.AccessControl counters this threat by allowing only whitelist users to access the TOE.
	P.UnauthorizedSubject	O.AccessControl enforces this policy by allowing only whitelist servers to access the TOE of the mapped LUNs and only servers to access file systems in the TOE through DAC policies.
OE.Manage	P.UnauthorizedSubject	OE.Manage enforces this policy by ensuring that administrators are trustworthy and competent to operate the TOE and its environment. Also, users, applications and servers are trustworthy while within the local network.
OE.Physical	P.UnauthorizedSubject	OE.Physical enforces this policy by ensuring that the environment prevents physical access to unauthorized subjects.
OE.DataProtection	P.DataCorruption	OE.DataProtection enforces this policy by protecting data in transit

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.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		√		
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**
  - **Authentication users management**
    - **Adding, deleting, enable, disable or modifying Windows users**
    - **Adding deleting, or modifying Windows groups**

NOTE

NAS client accesses NAS services provided by TOE through **Authentication user**. It is named **Windows user**. So **Authentication user** is a NAS services related user, not an OS user.

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 **the users whose role is Super administrator, Administrator, SAN resource administrator or Monitor as defined in FMT_SMR.1.1 or customized roles having permission of alarm_R** 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.

NOTE

The **alarm** is a permission group for accessing audit logs. If a user has the **alarm** permission, the user can add, delete, modify, and query audit logs. The **alarm_R** is a read-only permission in the **alarm** permission group.

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 Severity, ID, Object, Occurred, Type and Status**.

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: When one specific type of the audit trail exceeds **50,000 records** the TSF shall **dump the oldest 10,000 stored audit records to the specified SFTP server after the event dump function has been set enabled**.

NOTE

Audit trail include three types: alarm log, running log and operation log.

The upper limit number of one specific type of audit records is 55,000. Once the number of audit records exceeds 50,000, the oldest logs are dumped to reserve sufficient space for receiving the new records.

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 **Security Attribute Based Access Control policy for LUNs** on:

- **Subjects: SAN clients**
- **Objects: LUNs**
- **Operations: Read and write**

5.1.2.2 FDP_ACC.1/NAS Subset Access Control

FDP_ACC.1.1/NAS: The TSF shall enforce the **Security Attribute Based Access Control policy for files** on **the subjects, objects, and operations among subjects and objects listed in Table 5-2**.

Table 5-2 FDP_ACC.1/NAS detail

Subject	Object		Operations among subjects and objects
	File Style	File Type	
CIFS Client	NTFS-Style File	Directory, Regular File	Open, create, read, write, delete, obtain properties, set properties,

Subject	Object		Operations among subjects and objects
	File Style	File Type	
			obtain permissions, and set permissions

5.1.2.3 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 table 1-2 or customized roles.**
- **Objects: the commands to configure and manage the TOE**
- **Operations: configure and manage**

5.1.2.4 FDP_ACF.1/LUN Security Attribute Based Access Control

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

- **Subjects: SAN clients**
- **Subject attributes: Initiator IQN**
- **Objects: LUNs**
- **Object attributes: LUN ID**

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:

- **A SAN client can access a LUN if the LUN ID has been mapped to the initiators of the client.**

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**.

NOTE

IQN is the format most commonly used for iSCSI names, which uniquely identify nodes in an iSCSI network.

5.1.2.5 FDP_ACF.1/NAS Security Attribute Based Access Control

FDP_ACF.1.1/NAS: The TSF shall enforce the **Security Attribute Based Access Control policy for files** to objects based on the following: **the subjects, objects, operations, and associated security attributes listed in Table 5-3.**

Table 5-3 FDP_ACF.1.1/NAS detail

Operation	Subject	Object (File)	Subject (Security Attribute)	Object (Security Attribute)	Other Security Attributes used for DAC
Open	CIFS Client	NTFS-Style File	Windows User SID, Windows Group SID	SID and ACEs	None
Create	CIFS Client	NTFS-Style File	Windows User SID, Windows Group SID	N/A	Parent directory’s ACEs
Delete	CIFS Client	NTFS-Style File	Windows User SID, Windows Group SID	SID and ACEs	Parent directory’s ACEs
Read, write	CIFS Client	NTFS-Style File	Windows User SID, Windows Group SID	SID and ACEs	None
Obtain properties, set properties	CIFS Client	NTFS-Style File	Windows User SID, Windows Group SID	SID and ACEs	Parent directory’s SID and ACEs
Obtain permissions, set permissions	CIFS Client	NTFS-Style File	Windows User SID, Windows Group SID	SID and ACEs	Parent directory’s SID and ACEs

FDP_ACF.1.2/NAS: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **access is granted if one of the following conditions listed in Table 5-4 is satisfied.**

Table 5-4 FDP_ACF.1.2/NAS detail

Operation	Subject	Object (File)	Rule Id	Rule Detail
Open	CIFS Client	NTFS-Style File	1	There is no ACE that denies access to the subject for the specific operation and an ACE exists that grants permission to the subject for the specific operation.
			2	There is no ACE that denies access for the specific operation to any group that the subject is a member of and an ACE exists that grants permission to any group the subject is a member of for the specific operation.

Operation	Subject	Object (File)	Rule Id	Rule Detail
Create	CIFS Client	NTFS-Style File	3	There is no parent directory ACE that denies Write or Execute access to the subject and parent directory ACEs exist that grant Write and Execute permission to the subject.
			4	There is no parent directory ACE that denies Write or Execute access to any group that the subject is a member of and parent directory ACEs exist that grant Write and Execute permission to any group the subject is a member of.
Delete	CIFS Client	NTFS-Style File	5	Rule 1, or 2 above is true.
			6	The subject is not the owner and Rule 6, or 7 below are true.
			7	There is no parent directory ACE that denies Delete Child access to the subject or a parent directory ACE exists that grants Delete Child permission to the subject.
			8	There is no parent directory ACE that denies Delete Child access to any group that the subject is a member of and an object ACE exists that grants Delete Child permission to a group the subject is a member of.
Read, write	CIFS Client	NTFS-Style File	9	Rule 1, or 2 above is true.
Obtain properties, set properties	CIFS Client	NTFS-Style File	10	Rule 3, or 4 above is true and rule 1, or 2 above is true.
Obtain permissions, set permissions	CIFS Client	NTFS-Style File	11	Rule 3, or 4 above is true and rule 1, or 2 above is true.

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

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

5.1.2.6 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: User**

  Subject attributes User 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 7 built-in roles (listed in FMT_SMR.1 table 1-2) 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 a user only if the permission set of the user'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:

- **User security attributes**
  a) **Username**
  b) **Password**
  c) **Role**
  d) **Type (Local, LDAP User, LDAP Group)**
  e) **Status (Online, Offline)**
  f) **Password Status (Normal, Expired, Initialization, About to expire, Unsafe, Never expire)**
  g) **Login Method (CLI, SFTP, DeviceManager, RESTful, Serial port)**
  h) **Login Authentication (Password, SSH Key Pair, Password+Email OTP, Password+Radius OTP)**
  i) **Lock Status (Unlocked, Locked)**
  j) **Create Time**

NOTE

If the user **Type** is **LDAP User** or **LDAP Group**, the **Password** and **Password Status** are not security attributes belonging to the TOE because the password of the user is not maintained.

5.1.3.2 FIA_ATD.1/NAS User Attribute Definition

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

- **Authentication user security attributes**
  - **Windows User**
    a) **User Name**
    b) **SID**
    c) **Group Name**
    d) **GSID**
    e) **Status (Disable, Enable)**
    f) **Password Expired Time**
    g) **Privileges (None, SeSecurityPrivilege)**

NOTE

The '**SeSecurityPrivilege**' of **Windows user** indicates the privilege of operating ACLs.

5.1.3.3 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:

- **Initiator IQN**
- **LUN ID**

5.1.3.4 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.

5.1.3.5 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 local 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.**
- **Authentication is passed only if the input OTP is the same as that stored in the remote radius server**

5.1.3.6 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, rebooting the controller of the TOE, initializing a user's**

password, changing own password, unlocking a user, and clearing or importing configuration data to the TOE.

5.1.3.7 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 user does not support this login method. 1. Configure a correct login method list for this user as the super administrator. 2. Log in using an allowed method."**
  b) **When login with incorrect username or password, and the User 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 User 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.

5.1.3.8 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 or Radius server. The TOE allows access of a domain user depending on the pass/failure verdict provided by such remote LDAP or Radius server once the domain user performs an authentication attempt.

5.1.3.9 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:

- **User security attributes**
  - **User Name and User Role ID**
- **Authentication user security attributes**
  - **Windows User Name and User SID**
  - **Windows Group Name and User GID**

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**.

5.1.3.10 FIA_AFL.1 Authentication Failure Handling

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

NOTE

- The period of consecutive incorrect password attempts is 5 minutes for **user**.
- The period of consecutive incorrect password attempts is 1 minute for **Authentication user**.

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

- **User management**
  - **Lock the offending user for Temporary and set minutes from 3 to 2000, which can be configured by an administrator.**
  - **Lock the offending user for Permanent, which can be configured by an administrator.**
  - **Audit the event in the security log.**
- **Authentication user management**
  - **Lock the offending user for 1 minute.**

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, create*** the security attributes **defined in FDP_ACF.1.1/LUN** to **the users with roles in FMT_SMR.1 table 1-2 that have the proper permissions**.

5.1.4.2 FMT_MSA.1/NAS Management of Security Attributes

FMT_MSA.1.1/NAS: The TSF shall enforce the **Security Attribute Based Access Control policy for files** to restrict the ability to **access** the security attributes **defined in FDP_ACF.1.1/NAS** to **the subject as defined in the table 5-3**.

NOTE

Access operation include open, close, create, read, write, delete, obtain properties, set properties, obtain permissions, and set permissions as defined in the table 5-2.

5.1.4.3 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 Password** to **the users with all roles in FMT_SMR.1 table 1-2.**

5.1.4.4 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 Password defined in FIA_ATD.1/USER** to **the users with roles in FMT_SMR.1 table 1-2 that have the proper permissions.**

5.1.4.5 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' Password defined in FIA_ATD.1/USER** to **the users with roles in FMT_SMR.1 table 1-2 that have the proper permissions.**

5.1.4.6 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 Password defined in FIA_ATD.1/USER** to **the users with roles in FMT_SMR.1 table 1-2 that have the proper permissions.**

5.1.4.7 FMT_MSA.3 Management of Security Attributes

FMT_MSA.3.1: The TSF shall enforce the **Role Based Access Control policy for Commands, Security Attribute Based Access Control policy for LUNs and Security Attribute Based Access Control policy for files** 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 table 1-2** to specify alternative initial values to override the default values when an object or information is created.

5.1.4.8 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, FMT_SMF.1/NAS and FMT_SMF.1/USER** to **users with authorized roles as defined in FMT_SMR.1.1**.

5.1.4.9 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**
- **Initiator management**
- **LUN mapping**

5.1.4.10 FMT_SMF.1/NAS Specification of Management Functions

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

- **Authentication user management**
- **File DAC**

5.1.4.11 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 users and user attributes, including user credentials**
- **Management of the user policy, including user 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**

5.1.4.12 FMT_SMR.1 Security Roles

FMT_SMR.1.1: The TSF shall maintain the roles: **the authorized roles identified in the table 1-2.**

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

5.1.4.13 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, FMT_SMF.1/LUN and FMT_SMF.1/NAS** to **users with authorized roles as defined in FMT_SMR.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 user having proper permissions) 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:

- **User session establishment**
  - **Authentication failure**
  - **User login IP address not in Authorized IP Addresses**
  - **Max attempts due to authentication failure within certain period of time**
  - **No corresponding login method**
- **LUN session establishment**
  - **Server IQN authentication failure**
- **Windows user session establishment**
  - **Windows user authentication failure**
  - **Max attempts due to authentication failure for Windows user within 1 minute**

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.**

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 5-5 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 users in a suitable format.
	FAU_SAR.2 Restricted audit review	The requirement meets the objective by 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 integrally.
	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/NAS Specification of Management Functions	The requirement meets the objective by ensuring that the TOE manages audit configuration of users.
	FMT_SMF.1/USER Specification of Management Functions	The requirement meets the objective by ensuring that the TOE manages audit configuration of users.

Objective	Security Functional Requirement	Rationale
	FIA_UAU.2 User Authentication Before Any Action	The requirement meets the objective by ensuring that the TOE authenticates each user before any action.
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_ATD.1/NAS User attribute definition	The requirement meets the objective by ensuring that the TOE maintains security attributes for each authentication user.
	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.
	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/NAS 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

Objective	Security Functional Requirement	Rationale
	Specification of Management Functions	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/NAS Subset access control	The requirement meets the objective by ensuring that the TOE has an access control policy that allows only authorized servers to access files in 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 access control	The requirement meets the objective by ensuring that only authorized servers gain access to data protected by the TOE.
	FDP_ACF.1/NAS Security attribute based access control	The requirement meets the objective by ensuring that only authorized servers gain access to files in 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_ATD.1/NAS User attribute definition	The requirement meets the objective by ensuring that the TOE maintains security attributes for each authentication user.

Objective	Security Functional Requirement	Rationale
	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/NAS Management of security attributes	The requirement meets the objective by ensuring that the security attributes of files 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/NAS 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.
	FMT_SMR.1	The requirement meets the objective by ensuring that specific roles are defined for

Objective	Security Functional Requirement	Rationale
	Security roles	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/NAS Management of security attributes	The requirement meets the objective by ensuring that the security attributes of files 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 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/NAS 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.
	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 IQN whitelist.

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 5-6 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
FDP_ACC.1/LUN	FDP_ACF.1	FDP_ACF.1/LUN

Security Functional Requirement	**Dependency**	**Resolution**
FDP_ACC.1/NAS	FDP_ACF.1	FDP_ACF.1/NAS
FDP_ACC.1/USER	FDP_ACF.1	FDP_ACF.1/USER
FDP_ACF.1/LUN	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/LUN FMT_MSA.3
FDP_ACF.1/NAS	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/ NAS 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_ATD.1/NAS	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.2	FIA_UAU.2
FIA_UID.2	N/A	N/A
FIA_USB.1	FIA_ATD.1	FIA_ATD.1/USER FIA_ATD.1/NAS
FIA_AFL.1	FIA_UAU.2	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/NAS	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	FDP_ACC.1/NAS FMT_SMR.1 FMT_SMF.1/NAS
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	FDP_ACC.1/USER FMT_SMR.1

Security Functional Requirement	Dependency	Resolution
	FMT_SMF.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
FMT_SMF.1	N/A	N/A
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 algorithm 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 EAL4+ALC_FLR.2 (Evaluation assurance level 4+ ALC_FLR.2).

Table 5-7 TOE security assurance requirements

Assurance Class	Assurance Component
Class ADV: Development	ADV_FSP.4
	ADV_TDS.3
	ADV_ARC.1
	ADV_IMP.1
Class AGD: Guidance Documents	AGD_OPE.1
	AGD_PRE.1
Class ALC: Lifecycle Support	ALC_CMC.4
	ALC_CMS.4
	ALC_DEL.1
	ALC_DVS.1
	ALC_LCD.1
	ALC_TAT.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.3

5.4 Security Assurance Requirement Rationale

The evaluation assurance level 4+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: Users and Data Users.
  - The User is a user that will manage or configure the TOE's functions, including but not limited to security functions.
  - The Data User is a subject including SAN server and NAS server that will access the data stored in the TOE through standard I/O protocols.
- To 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 user 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 users with proper permissions. 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) or a remote radius server. The identification factors include the password, and one time password (OTP) sent through radius protocol. The TOE supports 2 kinds of combinations: password and OTP, and password only.
- The LDAP server's essential information (including the IP address, port, and protocol) is configured by a user whose role has the proper permissions. In this type of identification, the TOE acts as an LDAP client. The input user name and password are forwarded to the LDAP server through the standard LDAP protocol and are verified by the LDAP server. The radius server’s essential information (including the IP address, port, and protocol) is configured by a user whose role has the proper permissions. In this type of identification, the TOE acts as a radius client. The input user name and OTP are forwarded to the radius server through the standard radius protocol and are verified by the radius 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, rebooting the controller of the TOE, initializing a user's password, changing own password, unlocking a user, and clearing or importing configuration. 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 the users whose role has the proper permissions.
- 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 User authentication or User re-authentication failure, the failure count is recorded in the TOE. After N^u consecutive authentication failures during 5 minutes, the User will be locked for M minutes, in which N^u 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 User with proper permissions and both take effect for all Users. At the same time, after the Windows user authentication failure, the failure count is also recorded in the TOE. After N^d consecutive authentication failures during 1 minute, the Windows user will be locked for 1 minute, which N^d is a positive integer from 1 to 9. The value of N^d can be configured by User with proper permissions and take effect for the Windows users.
- 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 name, 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 Users with proper permissions. A session will be denied after User authentication failed, IQN authentication failed, or Windows user authentication failed.
- The User with proper permissions can configure a mapping, which contains relationships between an iSCSI initiator (IQN) and an iSCSI target (LUN). The Data User (SAN 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. The target LUN on the TOE can be accessed only when CHAP authentication is passed.

- The Data User (NAS server which uses Windows user) can access files on the TOE through CIFS protocol, if local authentication or AD domain authentication (Kerberos) is passed and has proper permissions to match DAC policies.

TOE Security Functional Requirements Satisfied: (FDP_ACC.1/LUN, FDP_ACC.1/NAS, FDP_ACF.1/LUN, FDP_ACF.1/NAS, FIA_ATD.1/USER, FIA_ATD.1/LUN, FIA_ATD.1/NAS, 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 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 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 as table 1-2, 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.

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 Users to globally control the access of a specific user to the TOE.

The TOE supports two Access Control mechanisms for 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. A user can’t establish session to access the TOE if the IP address out of the list.
- Login Method is a list including CLI, SFTP, DeviceManager, RESTful, Serial Port. A user can access the TOE only using the method/protocol included in this list configured for the user by other proper Users.

The TOE also supports Access Control mechanisms for SAN/NAS services at the same time.

- The SAN client whose initiator is in the mapping pre-configured in the TOE has rights to access the LUN on the TOE.
- The CIFS client can access files on the TOE through CIFS protocol, after AD domain authentication (Kerberos) passing, if the Windows user has proper permissions to match DAC policies.

TOE Security Functional Requirements Satisfied: (FDP_ACC.1/LUN, FDP_ACC.1/NAS, FDP_ACF.1/LUN, FDP_ACF.1/NAS, FIA_ATD.1/USER, FIA_ATD.1/LUN, FIA_ATD.1/NAS, 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 CLI and DeviceManager (a customized web tool designed by Huawei), which allows Users to inspect the audit logs. Users whose role has proper permissions can query or fetch the audit trail. Users whose role has proper permissions can also select the audit trail which he wants based the record type, record number, record sequence, record level, record status and record object
- All audit trails are stored locally in the TOE's persistent media. If a SFTP 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 SFTP server.

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)

6.5 Security Management

The TOE allows management of security functions by 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:
- User Management, including the user password, user lockout status, user's role and other credentials.
- User Policy Management, including the user name length, password complexity, access failure policy, and user 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), Simple Mail Transfer Protocol (SMTP). 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 mappings, and files DAC.
- Every security function has corresponding permissions. 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/NAS, 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, FMT_SMF.1/NAS)

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
RBAC	Role Based Access Control
SSH	Secure Shell
SFTP	Secure 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
NAS	Network Attached Storage
CIFS	Common Internet File System
DAC	Discretionary Access Control
ACE	Access Control Entry
IQN	iSCSI Qualified Name

7.2 References

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