Huawei OceanStor Hybrid Flash Storage System 6.1.8

Security Target

Issue 0.15

Date 2026-09-07



HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2020. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of 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
2025-11-15	0.1	This is the initial version
2025-11-20	0.2	Text error correction
2025-12-04	0.3	Some models and related descriptions removal
2025-12-12	0.4	Issue fixed
2026-03-11	0.5	Issue fixed
2026-04-19	0.6	Issue fixed
2026-05-11	0.7	Issue fixed
2026-06-02	0.8	Modified section 2.1.
2026-06-30	0.9	1. Modified Figure 1-4 in section 1.4.2; 2. Modified Table 1-2 in section 1.4.3.2; 3. Modified section 5.1.3.2.
2026-07-10	0.10	Modified Table 1-1 in section 1.4.1.
2026-07-13	0.11	Update Figure 1-4.
2026-08-03	0.12	Modified Table 1-1 in section 1.4.1.
2026-08-12	0.13	Modified Table 1-1 in section 1.4.1.
2026-08-28	0.14	Modified Table 1-1 in section 1.4.1.
2026-09-07	0.15	Modified Table 1-1 in section 1.4.1.

 Copyright © Huawei Technologies Co., Ltd.

Contents

About This Document ii

1 Introduction 4

1.1 ST Reference 4
1.2 TOE Reference 4
1.3 TOE Overview 4
1.3.1 TOE Usage and Major Security Features 4
1.3.2 TOE type 5
1.3.3 Non-TOE Hardware, Software, and Firmware Required by the TOE 5
1.4 TOE Description 7
1.4.1 Physical Scope 7
1.4.2 Logical Scope of the TOE 9
1.4.3 Summary of Security Features 10
1.4.3.1 Identification and Authentication 10
1.4.3.2 Authorization 11
1.4.3.3 Access Control 12
1.4.3.4 Auditing 12
1.4.3.5 Security Management 12

2 Conformance Claims 14

2.1 CC Conformance Claim 14

3 Security Problem Definition 15

3.1 Assets 15
3.2 Threats 16
3.2.1 Threat Components 16
3.3 Organizational Security Policies 16
3.4 Assumptions 16

4 Security Objectives 18

4.1 Security Objectives for the TOE 18
4.2 Security Objectives for the Operational Environment 19
4.3 Security Objective Rationale 19

5 Security Requirements for the TOE 22

5.1 TOE Security Functional Requirements 22

 Copyright © Huawei Technologies Co., Ltd.

5.1.1 Security Audit (FAU)....23
5.1.1.1 FAU_GEN.1 Audit Data Generation....23
5.1.1.2 FAU_GEN.2 User Identity Association....24
5.1.1.3 FAU_SAR.1 Audit Review....24
5.1.1.4 FAU_SAR.2 Restricted Audit Review....25
5.1.1.5 FAU_SAR.3 Selectable Audit Review....25
5.1.1.6 FAU_STG.2 Protected Audit Data Storage....25
5.1.1.7 FAU_STG.4 Action in Case of Possible Audit Data Loss....25
5.1.2 User Data Protection (FDP)....25
5.1.2.1 FDP_ACC.1/LUN Subset Access Control....25
5.1.2.2 FDP_ACC.1/NAS Subset Access Control....25
5.1.2.3 FDP_ACC.1/USER Subset Access Control....26
5.1.2.4 FDP_ACF.1/LUN Security Attribute Based Access Control....26
5.1.2.5 FDP_ACF.1/NAS Security Attribute Based Access Control....26
5.1.2.6 FDP_ACF.1/USER Security Attribute Based Access Control....28
5.1.3 Identification and Authentication (FIA)....29
5.1.3.1 FIA_ATD.1/USER User Attribute Definition....29
5.1.3.2 FIA_ATD.1/NAS User Attribute Definition....30
5.1.3.3 FIA_ATD.1/LUN User Attribute Definition....30
5.1.3.4 FIA_UAU.2/password mechanism: User authentication before any action....30
5.1.3.5 FIA_UAU.2/SSH key pair mechanism: User authentication before any action....30
5.1.3.6 FIA_UAU.2/password+OTP mechanism:User authentication before any action....30
5.1.3.7 FIA_UAU.6 Re-authenticating....30
5.1.3.8 FIA_UAU.7 Protected Authentication Feedback....31
5.1.3.9 FIA_UID.2 User Identification Before Any Action....31
5.1.3.10 FIA_USB.1 User-Subject Binding....31
5.1.3.11 FIA_AFL.1 Authentication Failure Handling....32
5.1.4 Security Management (FMT)....32
5.1.4.1 FMT_MSA.1/LUN Management of Security Attributes....32
5.1.4.2 FMT_MSA.1/NAS Management of Security Attributes....32
5.1.4.3 FMT_MSA.1/USERa Management of Security Attributes....33
5.1.4.4 FMT_MSA.1/USERb Management of Security Attributes....33
5.1.4.5 FMT_MSA.1/USERc Management of Security Attributes....33
5.1.4.6 FMT_MSA.1/USERd Management of Security Attributes....33
5.1.4.7 FMT_MSA.3 Management of Security Attributes....33
5.1.4.8 FMT_MTD.1 Management of TSF Data....33
5.1.4.9 FMT_SMF.1/LUN Specification of Management Functions....33
5.1.4.10 FMT_SMF.1/NAS Specification of Management Functions....34
5.1.4.11 FMT_SMF.1/USER Specification of Management Functions....34
5.1.4.12 FMT_SMR.1 Security Roles....34
5.1.4.13 FMT_MOF.1 Management of Security Function Behaviour....34
5.1.5 TOE Access (FTA)....34

 Copyright © Huawei Technologies Co., Ltd.

5.1.5.1 FTA_SSL.3 TSF-initiated Termination 34
5.1.5.2 FTA_TSE.1 TOE Session Establishment 34
5.1.6 Cryptographic Support (FCS) 35
5.1.6.1 FCS_COP.1/SHA256 Cryptographic Operation 35
5.1.6.2 FCS_COP.1/PBKDF2 Cryptographic Operation 35
5.2 Security Functional Requirement Rationale 35
5.2.1 Coverage 35
5.2.2 Security Requirement Dependency Rationale 41
5.3 Security Assurance Requirements 43
5.4 Security Assurance Requirement Rationale 44
6 TOE Summary Specification 45
6.1 Identification and Authentication 45
6.2 Authorization 47
6.3 Access Control 47
6.4 Auditing 48
6.5 Security Management 48
7 Glossary 50
7.1 Abbreviations and Terminology 50
7.2 References 51

 Copyright © Huawei Technologies Co., Ltd.

1 Introduction

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

1.1 ST Reference

1.2 TOE Reference

1.3 TOE Overview

1.4 TOE Description

1.1 ST Reference

Title: Huawei OceanStor Hybrid Flash Storage System 6.1.8 Security Target

Version: 0.15

Date: 2026-09-07

Developer: Huawei Technologies Co., Ltd.

1.2 TOE Reference

The TOE is identified as follows:

TOE name: Huawei OceanStor Hybrid Flash Storage System

TOE version: 6.1.8

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 Hybrid Flash Storage System is a new-generation storage system developed by Huawei Technologies Co., Ltd. It is designed to carry mission-critical and general-purpose services of enterprises, financial institutions, and data centers (DCs).

 Copyright © Huawei Technologies Co., Ltd.

They fully meet current data storage requirements, innovatively converge multiple databases, compute and storage, different generations of storage systems, cloud services, and warm and hot data storage, and provide customers with an ideal choice for agile service deployment in the future.

- TOE is an internal component supporting the Huawei OceanStor Hybrid Flash Storage System, providing the following 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 functionalities are part of the Huawei OceanStor Hybrid Flash, which the TOE supports through security features.

The TOE is running on the OceanStor Hybrid Flash hardware models, which are OceanStor 18510, OceanStor 18810, OceanStor 6810, OceanStor 5310, OceanStor 5510,OceanStor 5310 capacity flash, OceanStor 5510 capacity flash, OceanStor 5610, OceanStor 5210, OceanStor 5120, OceanStor 5220, Oceanstor 2600 and OceanStor 2620.

Figure 1-1 OceanStor Hybrid Flash



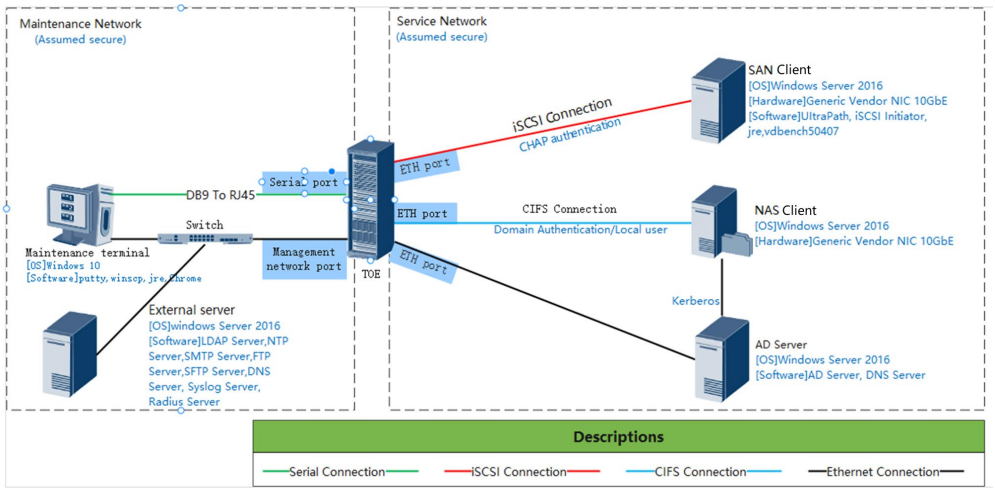
The TOE runs on the Linux operating system (Euler OS V200R012C00) based on kernel 5.10.0 running underlying hardware, see red frame in Figure 1-4. In addition, the software upgrade tool SmartKit (23.0.3 or later) and the software package integrity verification tool GnuPG are not parts of the TOE. Figure 1-2 shows the real environment for running the TOE.

NOTE

Different product models have different appearances and hardware configurations, but these differences do not affect the security functions and quality of the product. The operating systems of different software packages are the same, and there is no difference in basic software capabilities. Different software packages are only adapted to different hardware bases and devices.

 Copyright © Huawei Technologies Co., Ltd.

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.

  As shown in the preceding figure, the SAN server, NAS server and AD Server are connected through Ethernet cables.

  The maintenance 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
    - 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
- NAS server
  - Hardware
    - Rack servers or PCs with at least one 100M/1G Ethernet port
  - Software
    - Windows Server 2016 OS

 Copyright © Huawei Technologies Co., Ltd.

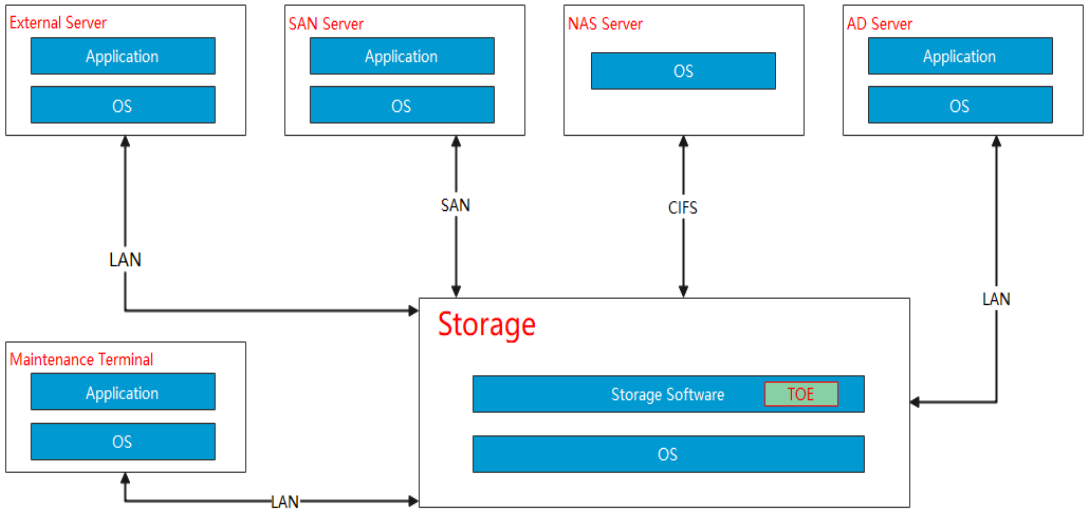
- Maintenance terminal
  - Hardware
    - Rack servers or PCs with at least one 100M/1G Ethernet port and one Serial DB9 port
  - Software
    - Windows 10 OS
    - Brower Google Chrome 64+
    - JRE (Java Runtime Environment 1.8), PuTTY 0.73, WinSCP 5.17, Python 3.9.5, notepad ++, Postman, Foxmail
-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

Figure 1-3 Software environment of the TOE



1.4 TOE Description

1.4.1 Physical Scope

The TOE is a 'software only' without hardware and is installed within the hardware for delivery. To be exact, the TOE is only part of the software, and its boundary will be described in more detail in 1.4.2 Logical Scope of the TOE.

 Copyright © Huawei Technologies Co., Ltd.

Table 1-1 The Physical TOE Scope

Type	Delivery Item	Version	Download Link
TOE Software	OceanStor_6.1.8_Software.tgz	6.1.8	The TOE is preinstalled on the hardware appliances, including following models: OceanStor 18510 OceanStor 18810 OceanStor 6810 OceanStor 5310 OceanStor 5510 QceanStor 5310 capacity flash OceanStor 5510 capacity flash OceanStor 5610
	OceanStor_lite_converged_6.1.8_Software.tgz	6.1.8	The TOE is preinstalled on the hardware appliances, including following models: OceanStor 5210 OceanStor 5120 QceanStor 5220 OceanStor 2620 OceanStor 2600
Signature file	OceanStor_6.1.8_Software.tgz.asc	6.1.8	Customers who have purchased the product can obtain the permission to download the PGP file from this link: https://support.huawei.com/enterprise/en/flash-storage/oceanstor-series-pid-262794302/software/263098039?idAbsPath=fixnode01|7919749|251366268|250389224|262794302&subModel=254051637&subModelName=OceanStor+5310
	OceanStor_lite_converged_6.1.8_Software.tgz.asc	6.1.8	Customers who have purchased the product can obtain the permission to download the PGP file from this link: https://support.huawei.com/enterprise/en/flash-storage/oceanstor-entry-level-series-pid-262794303/software/263098041?idAbsPath=fixnode01|7919749|251366268|250389224|262794303&subModel=256016845&subModelName=OceanStor+2220

 Copyright © Huawei Technologies Co., Ltd.

Type	Delivery Item	Version	Download Link
Product guidance	OceanStor 6.1.8 Error Code	01	Error Code/Command/Event can be queried on the support website of Huawei OceanStor Dorado Storage (https://info.support.huawei.com/storage/refer/#/home, and choose corresponding tab, Product & Version: **OceanStor / 6.1.8,** then select the corresponding Product Model and export.).
	OceanStor 6.1.8 Command Reference Manual	01	
	OceanStor 6.1.8 Event	01	
	OceanStor 6.1.8 REST Interface Reference	03	https://support.huawei.com/enterprise/en/doc/EDOC1100375526?idPath=7919749|251366268|250389224|262794302
	OceanStor 6.1.x & V700R001 Administrator Guide	14	https://support.huawei.com/enterprise/en/doc/EDOC1100233723?idPath=7919749|251366268|250389224|262794302
	OceanStor 6.1.x & V700R001 Initialization Guide	14	https://support.huawei.com/enterprise/en/doc/EDOC1100233736?idPath=7919749|251366268|250389224|262794302
	OceanStor 6.1.x & V700R001 Security Configuration Guide	15	https://support.huawei.com/enterprise/en/doc/EDOC1100247956/426cffd9?idPath=7919749|251366268|250389224|262794302
	Huawei OceanStor Hybrid Flash Storage System 6.1.8 AGD_PRE_User	0.4	Provided together with the Security Target documents via email.
	Huawei OceanStor Hybrid Flash Storage System 6.1.8 AGD_OPE	0.7	

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 is running on the operation system and the underlying hardware. The TOE provides several security functions, which are described in more detail in chap 1.4.3

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-4 TOE logical scope

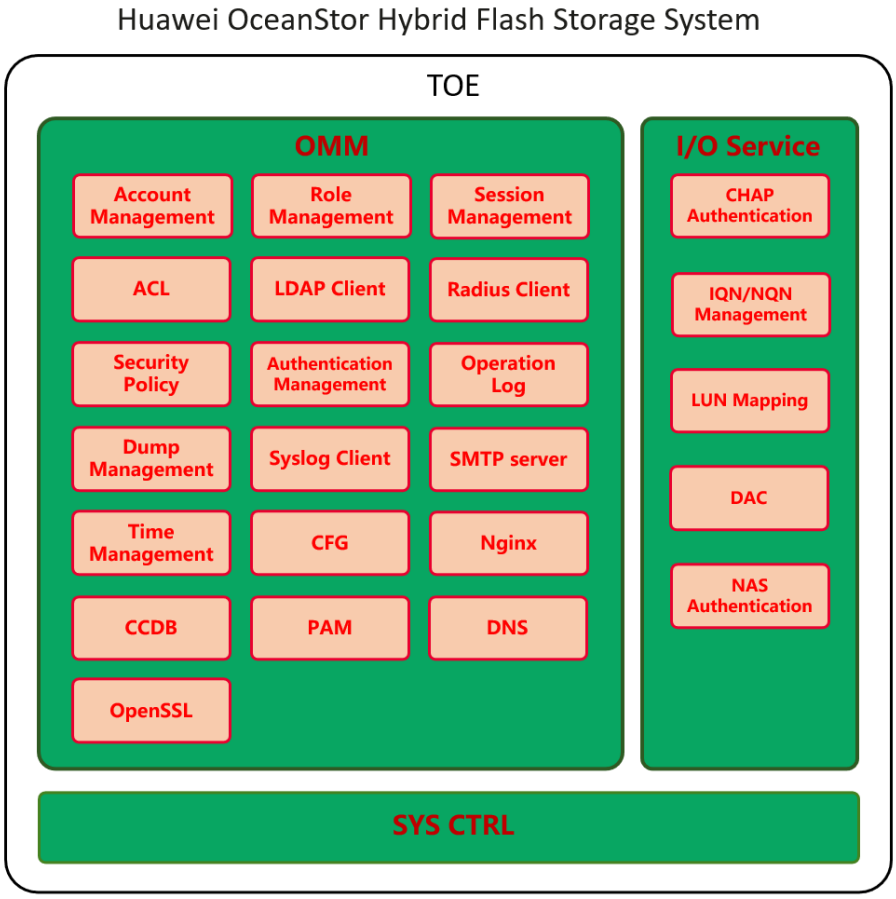


Figure 1-4 reflects the basic structure of the TOE with respect to subsystems and modules. The TOE provides all the security features. Security features are implemented through one or more modules.

1.4.3 Summary of Security Features

1.4.3.1 Identification and Authentication

- In user access, the TOE has two authentication modes, TOE provides identification and authentication support in case of local authentication. In remote authentication mode, the TOE does not support authentication and only obtains authentication results from the domain server.

  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 AD server or a remote radius server. The identification factors include the password, and OTP. The input password is sent forward to the remote AD server through the standard LDAP protocol and identified by the AD 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.

 Copyright © Huawei Technologies Co., Ltd.

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 upon successful CHAP authentication when enabled, and without authentication when disabled.

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 related to the TSF

Role	Permission
Root administrator	All permissions
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
NAS resource administrator	NAS resource management permission, including disk domain management, storage pool management, port management.
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 maintenance inspection such as system logs, configuration information. This role does not have permission to manage SAN resources, data protection, and

 Copyright © Huawei Technologies Co., Ltd.

Role	Permission
	security configuration.

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 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 commands for configuring along with a timestamp when they are executed are logged, see the auditable events list in 5.1.1.1 for details.
- 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 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
- 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).

 Copyright © Huawei Technologies Co., Ltd.

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

2.1 CC Conformance Claim

This Security Target and the TOE described are in accordance with the requirements of [CC].

This Security Target claims conformance with the following parts of Common Criteria:

- Conformant to [CC40R1P1].
- Conformant to [CC40R1P2].
- Conformant to [CC40R1P3].
- Conformant to [CC40R1P5].
- Conformant to [Errata].

The methodology to be used for the evaluation is described in the [CEM] with an evaluation assurance level of EAL2 augmented with ALC_FLR.2.

The chosen assurance level for this Evaluation is EAL2 augmented with ALC_FLR.2, which the vulnerability analysis level is AVA_VAN.2 and conforms the assurance security requirements:ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.2, ALC_FLR.2, ALC_CMS.2, ALC_DEL.1, ATE_COV.1, ATE_FUN.1, ATE_IND.2which are defined in [CC40R1P5] .

This Security Target does not claim conformance with any protection profile.

 Copyright © Huawei Technologies Co., Ltd.

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

3.2 Threats

3.3 Organizational Security Policies

3.4 Assumptions

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.

 Copyright © Huawei Technologies Co., Ltd.

- 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**

 Copyright © Huawei Technologies Co., Ltd.

It is assumed that the TOE and its operational environment are protected against unauthorized physical access. Assuming that the SAN server, NAS server, NTP server, Maintenance terminal, FTP server, DNS server etc. are in a physically authorized environment.

- **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, which is outside the scope of the TOE, works correctly. At the same time, this assumes that there is no direct vulnerability in the hardware, so that the attacker cannot attack the system through the hardware.

- **A.ExternalServer**

  It is assumed that the external servers, such as the NTP server, syslog server, AD server, RADIUS server, DNS server, and SMTP server, provide related functions

 Copyright © Huawei Technologies Co., Ltd.

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

4.2 Security Objectives for the Operational Environment

4.3 Security Objective Rationale

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 should also implement the function of the authorization to restrict the servers that is 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 commands for configuring 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.

 Copyright © Huawei Technologies Co., Ltd.

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 are 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, which is outside the scope of the TOE, works correctly.

- **OE.ExternalServer**

  The TOE environment must ensure that external servers, such as the NTP server, syslog server, AD server, RADIUS server, DNS server, and SMTP server, must properly provide related functions.

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.

 Copyright © Huawei Technologies Co., Ltd.

Objective	Threat, OSP, Assumption	Rationale
	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 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.

 Copyright © Huawei Technologies Co., Ltd.

Objective	Threat, OSP, Assumption	Rationale
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.
OE.ExternalServer	A.ExternalServer	OE. ExternalServer directly upholds assumption A. ExternalServer.

 Copyright © Huawei Technologies Co., Ltd.

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

5.2 Security Functional Requirement Rationale

5.3 Security Assurance Requirements

5.4 Security Assurance Requirement Rationale

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				

 Copyright © Huawei Technologies Co., Ltd.

Name	S	A	R	I
FAU_SAR.3		√		
FAU_STG.2	√			
FAU_STG.4		√		
FDP_ACC.1		√		√
FDP_ACF.1		√		√
FIA_ATD.1		√		√
FIA_UAU.2				√
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	√	√		
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 data 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. The NAS service administrator creates a **Windows user** who can use the NAS service on the storage system.

FAU_GEN.1.2: The TSF shall record within each audit data 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, PP-Module, functional package or 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 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.

Copyright © Huawei Technologies Co., Ltd.

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.2 Protected Audit Data Storage

FAU_STG.2.1: The TSF shall protect the stored audit data in the audit trail from unauthorized deletion.

FAU_STG.2.2: The TSF shall be able to ***prevent*** unauthorized modifications to the stored audit data in the audit trail.

5.1.1.7 FAU_STG.4 Action in Case of Possible Audit Data Loss

FAU_STG.4.1: 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 50,000. 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,

 Copyright © Huawei Technologies Co., Ltd.

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

NOTE

A CIFS (Common Internet File System) client is a device or application that uses the CIFS protocol to access shared resources hosted on CIFS servers.

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.

 Copyright © Huawei Technologies Co., Ltd.

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 7, or 8 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:

 Copyright © Huawei Technologies Co., Ltd.

- **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 9** TSF relevant **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

1. 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.

2. Regardless of whether the login authentication is set to **Password** or **Password+Email OTP**, the login authentication method is **Login password** through RESTful or SFTP.

 Copyright © Huawei Technologies Co., Ltd.

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) **Status (Disable, Enable)**
    e) **Password Expired Time**
    f) **Privileges (None, SeSecurityPrivilege)**

NOTE

The '**SeSecurityPrivilege**' of **Windows user** indicates the privilege of operating ACLs. Privileges include viewing and dumping security logs.

The '**SID**' (**Security Identifier**) is a number used in the **Windows operating system** to uniquely identify a user, group, and computer account.

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/password mechanism: 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.2/SSH key pair mechanism: 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.

5.1.3.6 FIA_UAU.2/password+OTP mechanism: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.

5.1.3.7 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.**

 Copyright © Huawei Technologies Co., Ltd.

5.1.3.8 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.

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

5.1.3.10 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**

 Copyright © Huawei Technologies Co., Ltd.

- **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**.

5.1.3.11 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**
  - **The system automatically logs out all active sessions of the user.**
  - **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 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**.

 Copyright © Huawei Technologies Co., Ltd.

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 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 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 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 permissions 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:

 Copyright © Huawei Technologies Co., Ltd.

- **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 TOE Access (FTA)

5.1.5.1 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 a user having system configuration permissions) of user inactivity.**

5.1.5.2 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**

Copyright © Huawei Technologies Co., Ltd.

- **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**

5.1.6 Cryptographic Support (FCS)

5.1.6.1 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.**

5.1.6.2 FCS_COP.1/PBKDF2 Cryptographic Operation

FCS_COP.1.1/PBKDF2: The TSF shall perform **password based key derivation** in accordance with a specified cryptographic algorithm **PBKDF2 (HMAC-SHA256)** (with iteration number 10,000 and 16-byte salt) and cryptographic key sizes **None** that meet the following: **SP800-132**.

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	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	The requirement meets the objective by ensuring that all audit records can be

Copyright © Huawei Technologies Co., Ltd.

Objective	Security Functional Requirement	Rationale
authorized users.	Audit review	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.2 Protected audit data storage	The requirement meets the objective by ensuring that the audit trail is protected against accesses performed by unauthorized users.
	FAU_STG.4 Action in Case of Possible Audit Data Loss	The requirement meets the objective by ensuring the audit record integrally.
	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.
	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.

 Copyright © Huawei Technologies Co., Ltd.

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.
	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 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	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.

 Copyright © Huawei Technologies Co., Ltd.

Objective	Security Functional Requirement	Rationale
that can be assigned to administrators in order to restrict the functionality available to individual administrators.	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.
	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	The requirement meets the objective by

 Copyright © Huawei Technologies Co., Ltd.

Objective	Security Functional Requirement	Rationale
	Management of security attributes	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 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.

 Copyright © Huawei Technologies Co., Ltd.

Objective	Security Functional Requirement	Rationale
	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 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.
	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	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	The requirement meets the objective by ensuring that the TOE should deny the

 Copyright © Huawei Technologies Co., Ltd.

Objective	Security Functional Requirement	Rationale
whitelist before allowing any action.	establishment	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	Through an external NTP server
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.2	FAU_GEN.1	FAU_GEN.1
FAU_STG.4	FAU_STG.2	FAU_STG.2
FDP_ACC.1/LUN	FDP_ACF.1	FDP_ACF.1/LUN
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

Copyright © Huawei Technologies Co., Ltd.

FIA_UAU.2	FIA_UID.1	FIA_UID.2
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/USER FIA_ATD.1/NAS FIA_ATD.1/LUN
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/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 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/NAS FMT_SMF.1/USER
FMT_SMF.1/LUN	N/A	N/A
FMT_SMF.1/NAS	N/A	N/A
FMT_SMF.1/USER	N/A	N/A
FMT_SMR.1	FIA_UID.1	FIA_UID.2

 Copyright © Huawei Technologies Co., Ltd.

FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1/LUN FMT_SMF.1/NAS FMT_SMF.1/USER
FTA_SSL.3	FMT_SMR.1	FMT_SMR.1
FTA_TSE.1	N/A	N/A
FCS_COP.1/SHA256	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1, or FCS_CKM.5] FCS_CKM.3	Unsupported: FCS_CKM.1, FCS_CKM.3
FCS_COP.1/PBKDF2	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1, or FCS_CKM.5] FCS_CKM.3	Unsupported: FCS_CKM.1, FCS_CKM.3

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 EAL2+ALC_FLR.2 (Evaluation assurance level 2+ ALC_FLR.2).

Table 5-7 TOE security assurance requirements

Assurance Class	Assurance Component
Class ADV: Development	ADV_FSP.2
	ADV_TDS.1
	ADV_ARC.1
Class AGD: Guidance Documents	AGD_OPE.1
	AGD_PRE.1
Class ALC: Lifecycle Support	ALC_CMC.2
	ALC_CMS.2

 Copyright © Huawei Technologies Co., Ltd.

Assurance Class	Assurance Component
	ALC_DEL.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.1
	ATE_FUN.1
	ATE_IND.2
Class AVA: Vulnerability Assessment	AVA_VAN.2

5.4 Security Assurance Requirement Rationale

The evaluation assurance level 2+ALC_FLR.2 has been chosen commensurate with the threat environment that is experienced by typical consumers of the TOE.

 Copyright © Huawei Technologies Co., Ltd.

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

6.2 Authorization

6.3 Access Control

6.4 Auditing

6.5 Security Management

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.
- In user access, the TOE has two authentication modes, TOE provides identification and authentication support in case of local authentication. In remote authentication mode, the TOE does not support authentication and only obtains authentication results from the domain server.
  - 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 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.

 Copyright © Huawei Technologies Co., Ltd.

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 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 AD server (which means a server in compliance with the standard LDAP protocol) 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 AD server's essential information (including the IP address, port, and protocol) is configured by a user whose role has the permissions. In this type of identification, the TOE acts as an client. The input user name and password are forwarded to the AD server through the standard LDAP protocol and are verified by the AD server. The radius server’s essential information (including the IP address, port, and protocol) is configured by a user whose role has the 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 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 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 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 permissions. A session will be denied after User authentication failed, IQN authentication failed, or Windows user authentication failed.
- The User with 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

 Copyright © Huawei Technologies Co., Ltd.

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 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.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 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 9 are TSF relevant built-in roles that cannot be modified or deleted as table 1-2, and the rest can be customized by users whose role has 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, Device Manager, 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.

 Copyright © Huawei Technologies Co., Ltd.

- The CIFS client can access files on the TOE through CIFS protocol, after AD domain authentication (Kerberos) passing, if the Windows user has 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. User can use the CLI tool to log in to the storage device through SSH v2 protocol or a local serial port, and also can use a browser to log in to the storage device using DeviceManager to view logs.Users whose role has permissions can query or fetch the audit trail. Users whose role has 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.2, FAU_STG.4)

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.
- 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 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,

 Copyright © Huawei Technologies Co., Ltd.

FMT_MSA.3, FMT_MTD.1, FMT_SMF.1/LUN, FMT_MOF.1, FMT_SMF.1/USER, FMT_SMF.1/NAS)

7 Glossary

7.1 Abbreviations and Terminology
7.2 References

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

 Copyright © Huawei Technologies Co., Ltd.

CC	Common Criteria
NAS	Network Attached Storage
CIFS	Common Internet File System
DAC	Discretionary Access Control
ACE	Access Control Entry
IQN	iSCSI Qualified Name
SID	Security Identifier
GSID	Group Security Identifier
OTP	One Time Password

7.2 References

Name	Description
[CC]	Common Criteria for Information Technology Security Evaluation. Part 1-5 November 2022 Version 4.0 Revision 1
[CC40R1P1]	Common Criteria (CC) Part 1: Introduction and general model November 2022 Version 4.0 Revision 1
[CC40R1P2]	Common Criteria (CC) Part 2: Security functional components November 2022 Version 4.0 Revision 1
[CC40R1P3]	Common Criteria (CC) Part 3: Security assurance components November 2022 Version 4.0 Revision 1

 Copyright © Huawei Technologies Co., Ltd.

Name	Description
[CC40R1P5]	Common Criteria (CC) Part 5: Pre-defined packages of security requirements November 2022 Version 4.0 Revision 1
[CEM]	Common Methodology for Information Technology Security Evaluation Evaluation methodology November 2022 Version 4.0 Revision 1
[Errata]	Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 Version: 1.2 Date of issue: 2025-10-15 Status: Final

 Copyright © Huawei Technologies Co., Ltd.