CSPN Secure Access Control and Management of Huawei OceanStor Dorado Storage System

Security Target

Issue	**3.7**
Date	**2022-10-13**

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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	Revision Version	Change description	Author
2022-10-13	3.7	Update by reviewed comments on Oct 13.	Wai Yan WONG
2022-09-21	3.6	Update by reviewed comments on Sept 21.	Wai Yan WONG
2022-09-20	3.5	Update by reviewed comments on Sept 20.	Wai Yan WONG
2022-09-20	3.4	Updated the assumption on Sept 20.	Wai Yan WONG
2022-06-09	3.3	Updated by reviewed comments on June 09.	Wai Yan WONG
2022-06-01	3.2	Updated by reviewed comments on June 01.	Wai Yan WONG
2022-05-18	3.1	Update the title of this certification and the scope of data user on May 18.	Wai Yan WONG
2022-05-03	3.0	Update the SED on May 3.	Wai Yan WONG
2021-09-27	2.2	Updated by reviewed comments on Sept 27.	Luo Weihua
2021-09-24	2.1	Updated by reviewed comments on Sept 24.	Luo Weihua
2021-09-21	2.0	Updated Chapter 2.4.1, 2.4.2, 4.4, and 5.2 by pre-test issues, and update Chapter 1.1 and Chapter 2 for new model on Sept 21.	Luo Weihua
2021-07-16	1.0	File name changed	Jianyong LI
2021-07-16	0.4	Updated by reviewed comments on July 16.	Luo Weihua
2021-07-13	0.3	Updated by reviewed comments on July 8.	Luo Weihua
2021-07-05	0.2	Updated by reviewed comments on July 1.	Luo Weihua
2021-06-30	0.1	This is the initial draft.	Luo Weihua

Contents

Figures & Tables

1 Introduction

1.1 Product Identification

This Security Target is for the CSPN evaluation ([PROC_CSPN], [CRIT_CSPN]) of the Secure Access Control and Management of Huawei OceanStor Dorado Storage System.

Manufacturer	Huawei Technologies Co., Ltd
Organization URL	https://www.huawei.com/en/
Product's commercial name	Huawei OceanStor Dorado Storage System
Product software's version	6.1.2
Product's range	Data Storage
Reference model	OceanStor Dorado 5000 V6
Additional models for the range	OceanStor Dorado 3000 V6 OceanStor Dorado 6000 V6 OceanStor Dorado 8000 V6 OceanStor Dorado 18000 V6
Guidance document	[OceanStor Dorado_GUIDE]

1.2 Abbreviations

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

WWN	World Wide Name
RBAC	Role Based Access Control
SSH	Secure Shell
SFTP	Secure File Transfer Protocol
FTP	File Transfer Protocol
NTP	Network Time Protocol
DNS	Domain Name System
ACL	Access Control List
TOE	Target of Evaluation
SED	Self-Encryption Disk
OTP	One Time Password
FRU	Field Replaceable Unit
BBU	Backup Battery Unit
SSD	Solid-State Drive
RDMA	Remote Direct Memory Access
NDMP (out of scope)	Network Data Management Protocol

1.3 Reference

[PROC_CSPN]	First Level Security Certification For Information Technology Products, ANSSI-CSPN-CER-P-01/1.1
[CRIT_CSPN]	Criteria for Evaluation in View of a First Level Security Certification, ANSSI-CSPN-CER-P-02_v4.0
[OceanStor Dorado_GUIDE]	OceanStor Dorado 6.1.x Security Configuration Guide v5

2 Product and TOE description

2.1 Product Overview

The OceanStor Dorado Storage System (OceanStor Dorado for short) is Huawei's brand-new all-flash storage products designed for medium- and large-size enterprise storage environments, including the Entry-level, Mid-range and High-end. The storage systems leverage the flash-dedicated FlashLink® technique to provide mass data storage, fast data access, high availability, and excellent utilization in the ease-of-use and energy saving form factor.

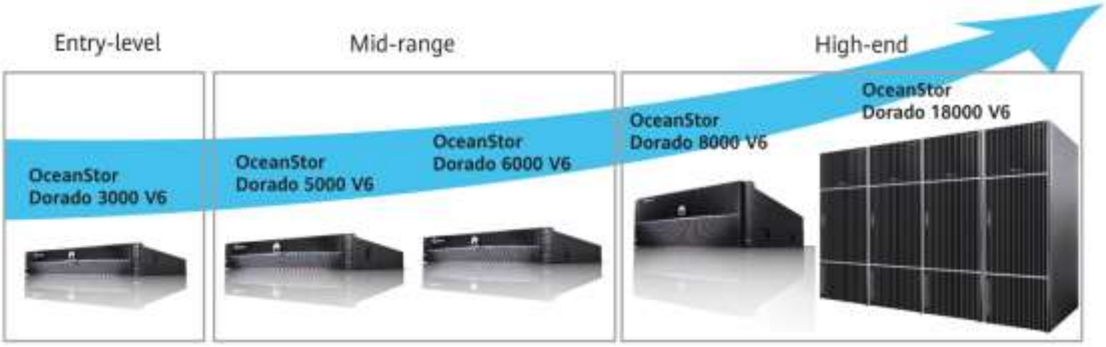

Figure 2-1 OceanStor Dorado V6

The OceanStor Dorado offers comprehensive and superb solutions by using diverse efficiency boost mechanisms to provide industry-leading performance. Those solutions help customers maximize their return on investment (ROI) and meet the requirements of different application scenarios such as online transaction processing (OLTP), online analytical processing (OLAP), high-performance computing (HPC), server virtualization, and virtual desktop infrastructure (VDI).

In addition to providing enterprise users with high-performance and efficient storage services, OceanStor Dorado supports advanced data backup and disaster recovery technologies, ensuring secure and smooth operation of data services. Furthermore, the storage systems also offer easy-to-use management and convenient local/remote maintenance, greatly decreasing the management and maintenance costs.

2.2 Hardware Architecture

The OceanStor Dorado employs a full-mesh architecture. All FRUs, such as front-end interface modules, controllers, back-end interface modules, power modules, BBUs, fan modules, and SSDs, are redundant and protected against single points of failure. All FRUs are hot-swappable and can be replaced online.

The RDMA high-speed network implements shared access to the global memory at a low latency. The smart disk enclosures (equipped with CPUs and memory to provide computing power) at the back end offload disk reconstruction tasks from controllers to save controller resources.

2.2.1 Differences Between OceanStor 3000, 5000, 6000, 8000 and 18000 V6

Table 2-1 lists the differences between the product models of OceanStor Dorado.

Table 2-1 Differences between the reference model and the additional models

Product Model	OceanStor Dorado 3000 V6	OceanStor Dorado 5000 V6 OceanStor Dorado 6000 V6	OceanStor Dorado 8000 V6 OceanStor Dorado 18000 V6
Controller enclosure	2U enclosure with 25 disk slots (for SAS SSDs) 2U enclosure with 25 disk slots (for NVMe SSDs)	2U enclosure with 25 disk slots (for SAS SSDs) 2U enclosure with 36 disk slots (for NVMe SSDs)	4U enclosure without disk slots
Architecture	Active-Active	Active-Active	Active-Active
Number of controllers per enclosure	2	2	2 or 4
Disk type	SAS SSD NVMe SSD	SAS SSD NVMe SSD	SAS SSD NVMe SSD

2.2.2 Entry-level Device

The OceanStor Dorado 3000 V6 is an entry-level device. It uses a 2U controller enclosure that has two controllers and 25 SAS or NVMe SSDs (the enclosure with NVMe SSDs uses a self-defined physical form). The two controllers work in symmetric active-active mode for load balancing. All FRUs are redundant and can be replaced online.

Each controller enclosure of Huawei OceanStor Dorado 3000 V6 all-flash storage system supports a maximum of six hot-swappable interface modules.

Each controller of OceanStor Dorado 3000 V6 has four onboard GE ports, four onboard 10GE ports, two GE management and maintenance ports, and one serial port. The two controllers in a controller enclosure are interconnected through RDMA mirror channels, and two controller enclosures can be directly connected through the scale-out interface modules. The SAS product model provides onboard SAS back-end ports to connect to SAS disk enclosures. The NVMe product model does not provide onboard 100 Gbit/s RDMA back-end ports. The 100 Gbit/s RDMA interface modules must be deployed for connecting to smart NVMe disk enclosures.

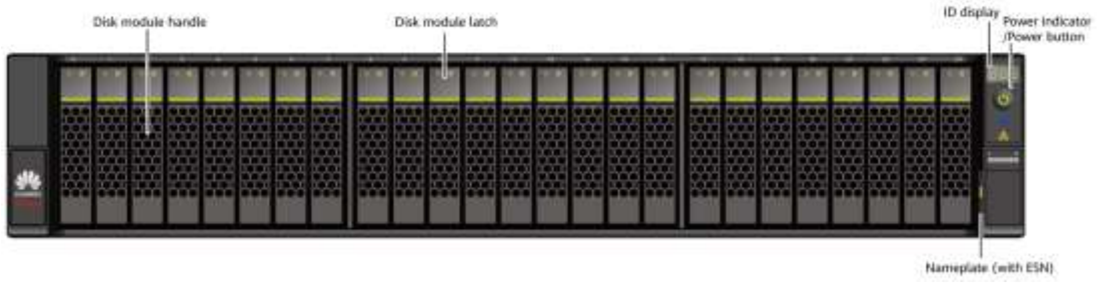

Figure 2-2 Front view of a 2U controller enclosure with 25 SAS SSDs

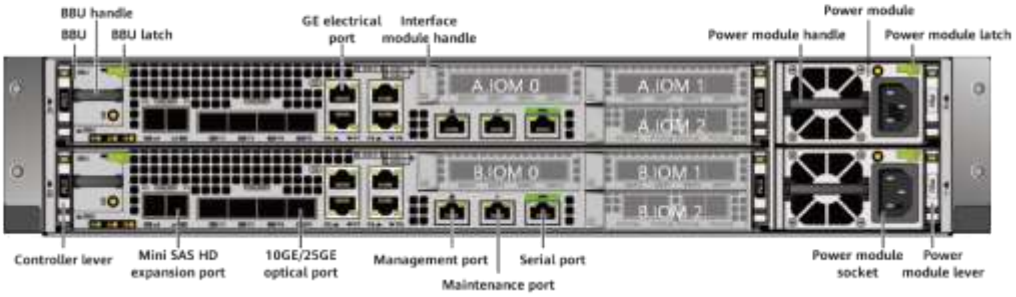

Figure 2-3 Rear view of a 2U controller enclosure with 25 SAS SSDs

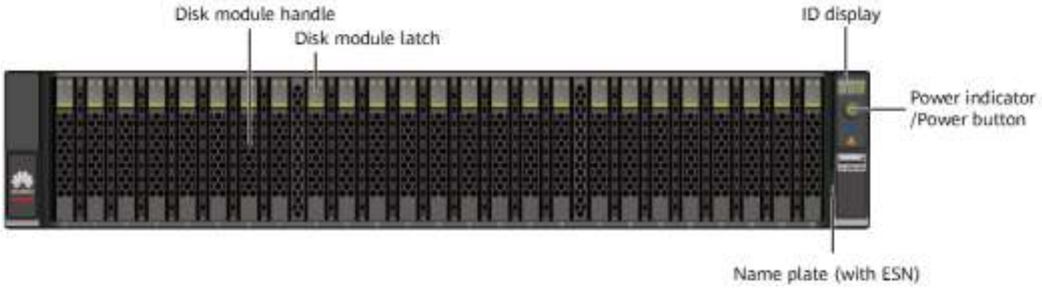

Figure 2-4 Front view of a 2 U controller enclosure with 25 NVMe SSDs

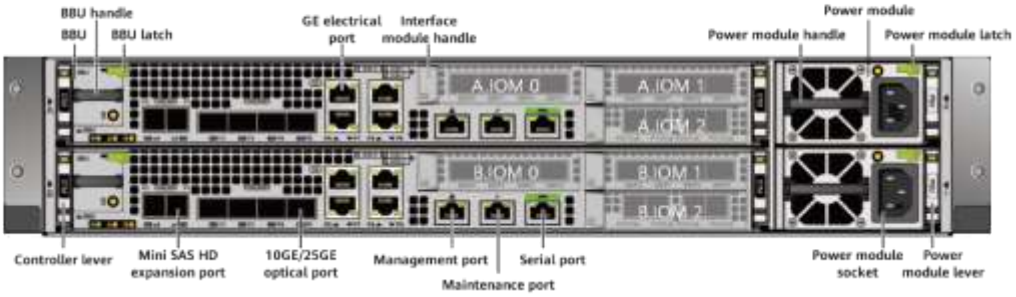

Figure 2-5 Rear view of a 2 U controller enclosure with 25 NVMe SSDs

2.2.3 Mid-range Devices

OceanStor Dorado mid-range devices include OceanStor Dorado 5000 V6 and Dorado 6000 V6. They use a 2U controller enclosure that has two controllers and 25 SAS SSDs or 36 NVMe SSDs. The NVMe SSD adopts a customized physical form, which allows an enclosure to house 40% more NVMe SSDs than 2.5-inch SAS SSDs. All FRUs are redundant and can be replaced online.

OceanStor Dorado mid-range devices provide SAN storage services. The devices use end-to-end low-latency SAN front-end protocols. Each controller enclosure supports up to 12 hot-swappable interface modules.

The two controllers in a controller enclosure of OceanStor Dorado mid-range device are interconnected through RDMA mirror channels, and multiple controller enclosures can be directly connected through the scale-out interface modules. Each controller has two GE management and maintenance ports and one serial port.

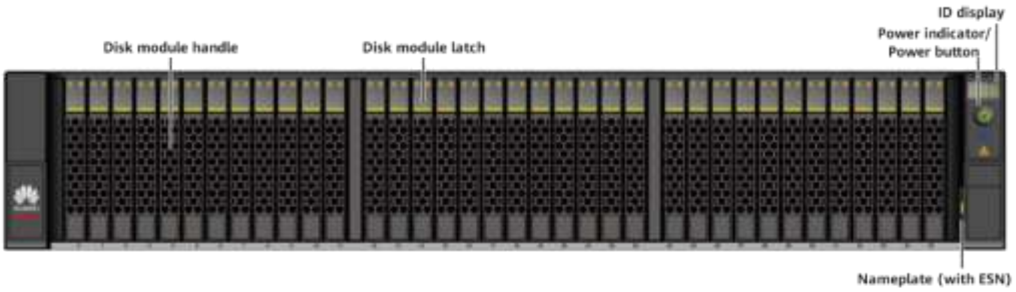

Figure 2-6 Front view of a 2U controller enclosure (with 36 NVMe SSDs)

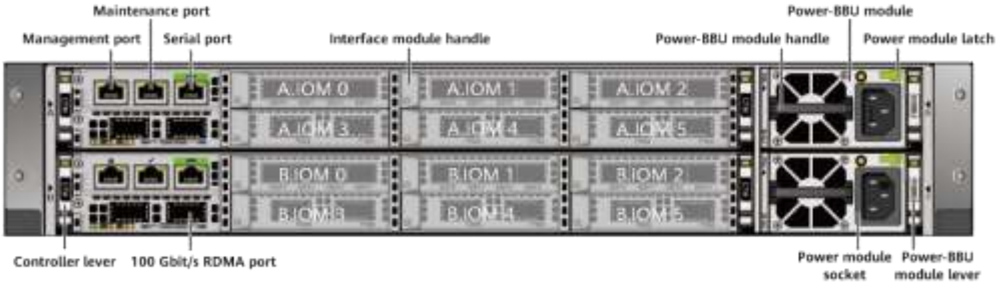

Figure 2-7 Rear view of a 2 U controller enclosure (with 36 NVMe SSDs)

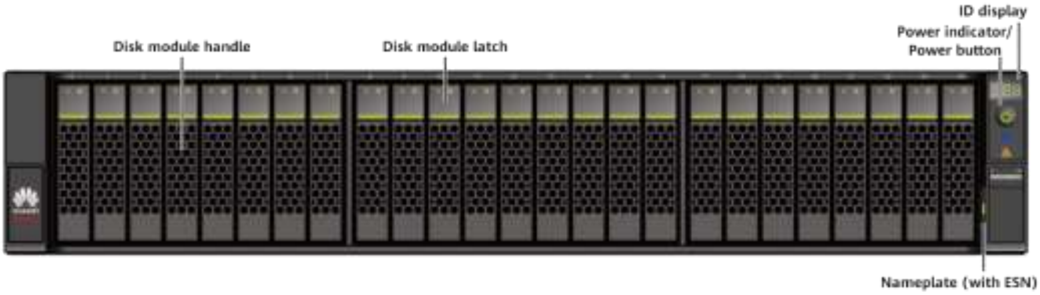

Figure 2-8 Front view of a 2U controller enclosure (with 25 SAS SSDs)

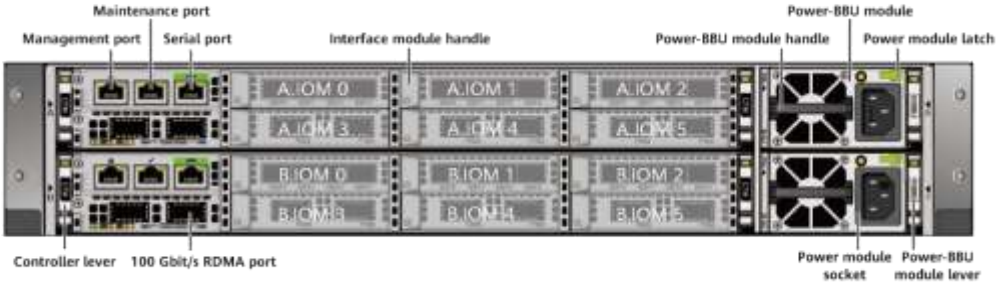

Figure 2-9 Rear view of a 2 U controller enclosure (with 25 SAS SSDs)

2.2.4 High-end Devices

The OceanStor Dorado high-end devices are OceanStor Dorado 8000 V6 and Dorado 18000 V6. They use independent controller enclosures, each with 28 interface module slots. All interface modules are shared among all controllers. A single controller enclosure can tolerate failure of three out of four controllers without service interruption (if two controller enclosures are deployed, the system can tolerate failure of seven out of eight controllers). A modular design is adopted for key components. All FRUs are redundant and can be replaced online. Each controller enclosure has two power planes. On each power plane, the power modules are in 1+1 redundancy.

OceanStor Dorado high-end devices provide SAN storage services. The devices use end-to-end low-latency SAN front-end protocols on various service interface modules.

The Controllers in a controller enclosure are interconnected through RDMA channels. Different controller enclosures can be interconnected directly or through switches. In direct connection mode, two controller enclosures are directly connected without a switch using scale-out interface modules. In switched connection mode, two controller enclosures are connected to switches using scale-out interface modules to achieve interconnection of up to 32 controllers on dual switching planes. Each controller enclosure has two management modules. Each management module has three GE ports (management or maintenance), one USB port, and one serial port.

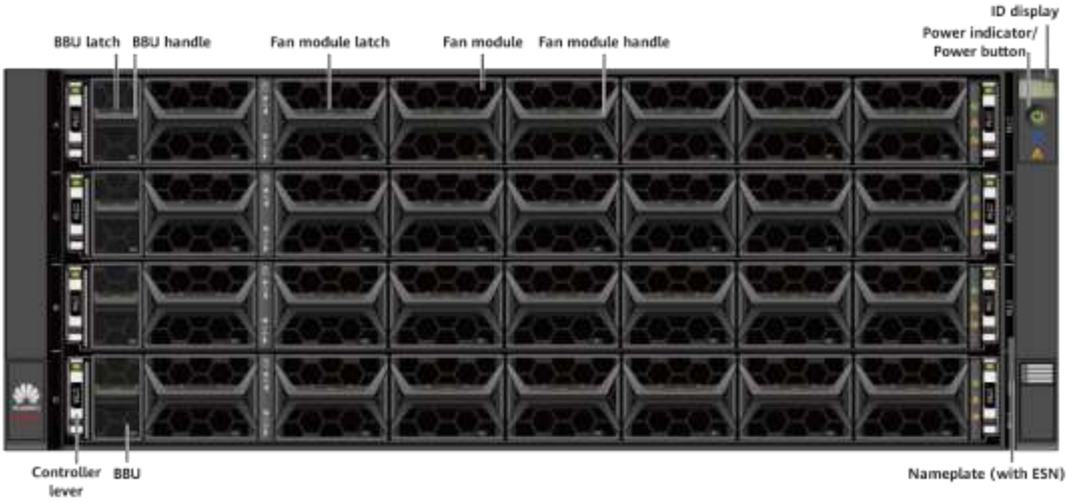

Figure 2-10 Controller enclosure front view

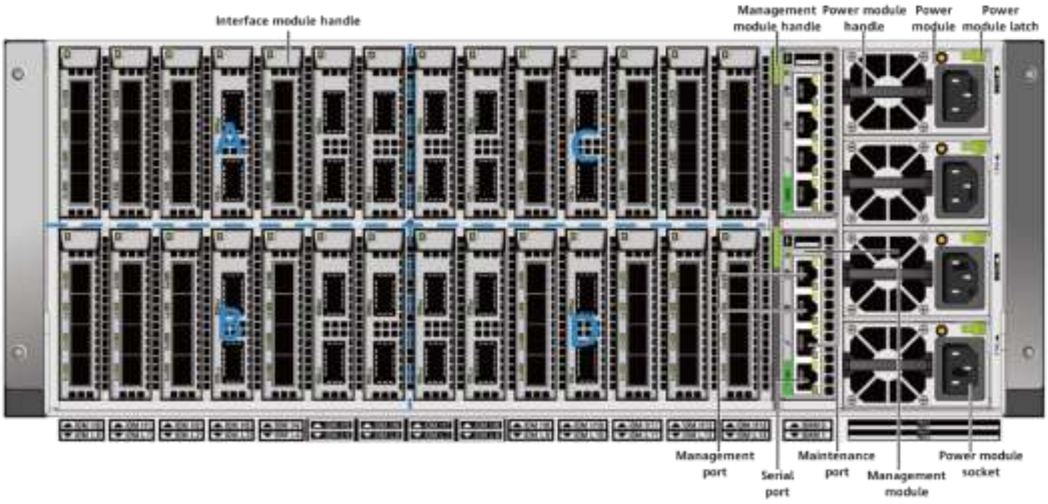

Figure 2-11 Controller enclosure rear view

2.3 Software Architecture

The OceanStor Dorado software architecture consists of I/O Service, OMM and SYS CTRL, and is running underlying OS and hardware, as shown in Figure 2-12. It provides several security functions, which are described in more detail in chap 5.

The I/O Service is responsible for providing data access service.

The OMM is responsible for managing and controlling the communication, configuration and security features in Huawei OceanStor Dorado Storage System.

The SYS CTRL is responsible for system initialization and startup, failover and recovery.

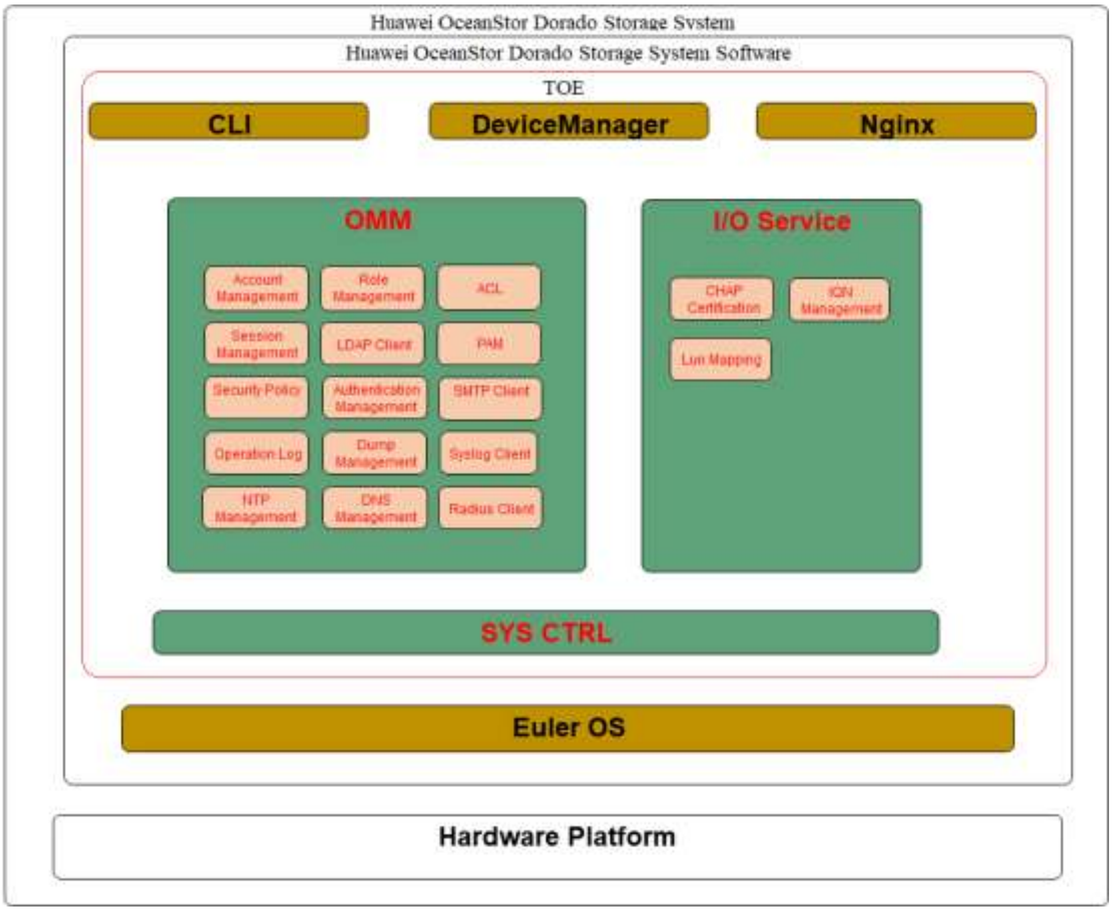

Figure 2-12 OceanStor Dorado software architecture

Figure 2-12 reflects the basic structure of the OceanStor Dorado software with respect to subsystems and modules. It provides all the security features. Security features are implemented through one or more modules.

NOTE

The different models including OceanStor Dorado 3000, 5000, 6000, 8000 and 18000 V6 share the same software architecture as Figure 2-12.

2.4 TOE Features

2.4.1 Identification and Authentication

Identification and authentication includes user access, data access and related security management.

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 for CLI.
- 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.

In data access, the available LUN is limited by the initiator. CHAP authentication is supported for connecting to the TOE over an iSCSI network. Target LUNs on the TOE can be accessed only when CHAP authentication is passed.

In security management, the TOE provides identification and authentication parameters configuration.

- Management of accounts and account attributes, including account credentials
- Management of the account policy, including account name length, password complexity, failure policy, and lockout policy
- Configuration of network services used by the TOE, such as LDAP, SFTP, DNS, SMTP.

NOTE

The user authentication method could be selected during user creation and can be modified later. Only the super administrator with the user management permission can create users and modify user authentication methods.

2.4.2 Authorization

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

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

Table 2-2 Role permission definition

Role	Permission
Super administrator	All permissions, including user management, security configuration (management of security rules, certificates, KMC, and data destruction), SAN resource management (management of storage pools, LUNs, mapping views, hosts, ports, and background configuration tasks), data protection management (anagement of LUNs, local data protection, remote data protection, HyperMetro, and background configuration tasks), cross-device data protection management (cross-device management of remote replication, HyperMetro, 3DC, LUNs, and mapping views), and O&M (information collection, performance collection, inspection, batch configuration, rebooting or powering off the TOE, rebooting the controller of the TOE, etc).
Administrator	All permissions except user management, batch configuration, and high-risk maintenance operations (including rebooting or powering off the TOE, rebooting the controller of the TOE).
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.
NDMP backup administrator	Management rights for NDMP backup services, including local data protection management, remote data protection management, HyperMetro management, and resource optimization management.
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**. The Empty role is a read-only role provided by the TOE.

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

2.4.3 Access Control

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

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

2.4.4 Auditing

The TOE generates audit records for security-relevant management actions and stores the audit records in the TOE, or transmits the audit records to syslog server.

- 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/FTP server when the log entries exceed a specified number.
- Review functionality is provided via the command line interface and GUI, which allows administrative users to inspect the audit logs.
- The audit records are transmitted to syslog server, if the transmit function is enable and the syslog server is configured.
- The NTP server must be configured to ensure accurate audit records timestamp.

2.5 Product Usage

The TOE is (part of) the software of the Data Storage product. Figure 2-13 shows the typical application scenarios of OceanStor Dorado, including active-active, replication, backup, and archiving.

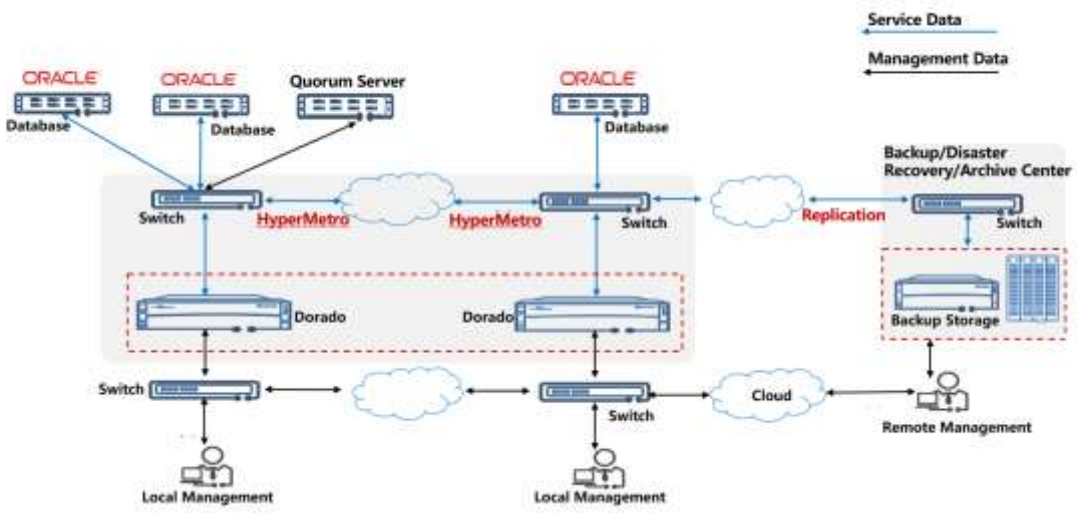

Figure 2-13 Product usage

- **Service Data Read/Write**： The service data read/write process from the host to the OceanStor Dorado includes the following two processes: 1) The host initiates a write request until the data is written to the disk and a write success message is returned. 2) The host initiates a read process until the read process is successful.
- **Active-active/Replication:** The OceanStor Dorado are deployed to implement disaster recovery. The implementation mode is that both the active and standby data centers take over user services at the same time. In this case, data in the active and standby data centers is synchronized and mirrored in real time. This ensures that service continuity is not affected when any one side is faulty. Replication refers to synchronous or asynchronous replication of data from the primary end to the secondary end.
- **Local O&M:** Maintenance is performed through the maintenance network connected to the customer's data center.
- **Local O&M**： Maintenance is performed through the maintenance network connected to the customer's data center.
- **Remote O&M**： Maintenance is performed after being authorized by the customer, through secure and encrypted network which is used to remotely access the customer's maintenance network through the Internet

2.6 TOE Environment

The TOE environment is made of:

- The external server connected the TOE is used for LDAP server, NTP server, SMTP server, SFTP/FTP server, and DNS server.
- The application server connected the TOE is used for SAN server, which access LUNs in TOE through iSCSI protocol.

- The local PC connected to the TOE though the CLI interface either through TOE’s console interface or TOE’s ETH interface via a secure channel enforcing SSH, and though web browser via a secure channel enforcing HTTPs.
- Remote PCs connected to the TOE either though the CLI interface through TOE’s ETH interface via a secure channel enforcing SSH or though web browser via a secure channel enforcing HTTPs.

3 TOE Evaluated Configuration

3.1 Test Environment

The topology of the test equipment is illustrated below:

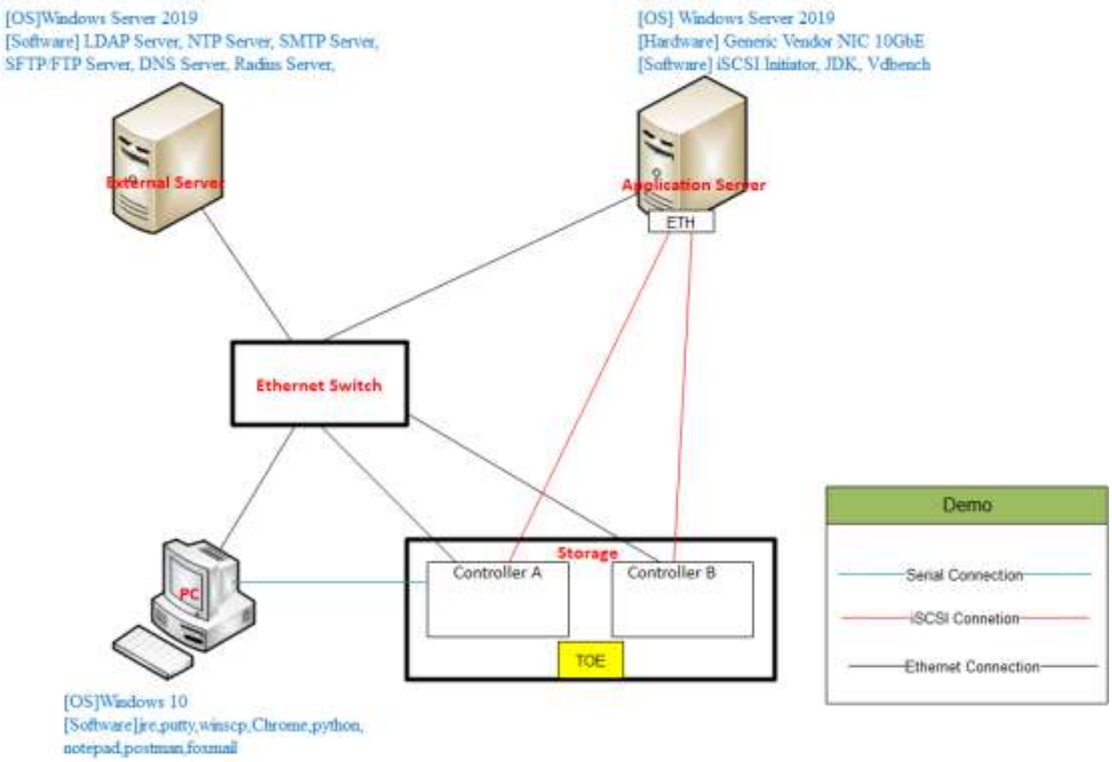
[OS]Windows Server 2019
[Software] LDAP Server, NTP Server, SMTP Server, SFTP/FTP Server, DNS Server, Radius Server,
External Server
[OS] Windows Server 2019
[Hardware] Generic Vendor NIC 10GbE
[Software] iSCSI Initiator, JDK, Vdbench
Application Server
ETH
Ethernet Switch
Storage
Controller A
Controller B
TOE
PC
[OS]Windows 10
[Software]jre,putty,winscp,Chroeme,python, notepad,postman,foxmail
Demo
Serial Connection
iSCSI Connetion
Ethernet Connection

Figure 3-1 Test Environment

- Description
  - The external server, application server, PC, and TOE (storage) are connected to each other by the Ethernet switch S6720.
  - The NIC on the application server has two Ethernet ports. One connects to the TOE's controller_A, and the other connects to controller_B through optical fibers.
  - The configuration of storage does not contain self-encrypted disk, and therefore the SED is deactivated.
- Application server
  - Hardware
    - ✓ Rack servers or PCs with at least one 10G/25G NIC
  - Software

    - ✓ Windows Server 2019 OS
    - ✓ Microsoft iSCSI Software Initiator in Windows Server 2019
    - ✓ JDK 8
    - ✓ Vdbench50406

- External server
  - Hardware
    - ✓ Rack servers or PCs with at least one 100M/1G Ethernet port
  - Software
    - ✓ Windows Server 2019 OS
    - ✓ LDAP(AD) server, NTP server, SFTP/FTP server, DNS server, Radius server in Windows Server 2019
- PC
  - Hardware
    - ✓ Rack servers or PCs with at least one 100M/1G Ethernet port and one Serial port
  - Software
    - ✓ Windows 10 OS
    - ✓ Brower Google Chrome 64+
    - ✓ JDK 8, PuTTY 0.73, WinSCP 5.17, Python 3.9.5, notepad ++, Postman, Foxmail

3.2 Initial Configuration

For details about the initial configuration of Dorado, see the configuration guide at http://support.huawei.com.

Table 3-1 Support website

Product Model	Support website
OceanStor Dorado 3000 V6	https://support.huawei.com/enterprise/en/centralized-storage/oceanstor-dorado-3000-v6-pid-24030129
OceanStor Dorado 5000 V6	https://support.huawei.com/enterprise/en/centralized-storage/oceanstor-dorado-5000-v6-pid-22784062
OceanStor Dorado 6000 V6	https://support.huawei.com/enterprise/en/centralized-storage/oceanstor-dorado-6000-v6-pid-22784071
OceanStor Dorado 8000 V6	https://support.huawei.com/enterprise/en/centralized-storage/oceanstor-dorado-8000-v6-pid-24030109
OceanStor Dorado 18000 V6	https://support.huawei.com/enterprise/en/centralized-storage/oceanstor-dorado-18000-v6-pid-24030083

4 Security Perimeter

4.1 Typical Users

The OceanStor Dorado defines different management accounts and built-in accounts as well as allocates different configuration and maintenance permissions to these accounts. The following table describes default accounts and usage of these accounts.

Table 4-1 Default accounts

Default account	User Role	Usage
_super_admin	Root administrator	Used to initialize the password of the super administrator when the super administrator forgets its password. (The old password is required when the super administrator wants to set a new password.) The user can only be logged in to using a serial port.
admin	Super administrator	The user has full control over the storage system. It can manage users and initialize the passwords users.

NOTE

The default account named _super_admin is a near-end user and cannot be added, deleted or modified. It is used only to initialize the password of the super administrator but not to manage the TOE. Therefore, it is not within the scope of the RBAC.

The previous roles can be given to a human being or an application.

4.2 TOE Assets

All data 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.

4.3 Threat Model

4.3.1 Threat Agents

The following attackers are considered:

- 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).

4.3.2 Threats

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

- **T.UnauthenticatedAccess**
  - **Threat agent**: Non-TOE user or application without rights for accessing the TOE.
  - **Asset**: All assets.
  - **Adverse action**: A non-TOE user gains access to the TOE through LAN.
- **T.UnauthorizedAccess**
  - **Threat agent**: TOE user (a user or application using the functionality of the TOE).
  - **Asset**: All assets.
  - **Adverse action**: A user of the TOE authorized to perform certain actions and access certain information gains access to unauthorized commands or information through LAN.
- **T.DataCorruption**
  - **Threat agent**: TOE user (a user or application using the functionality of the TOE) and Non-TOE user or application without rights for accessing the TOE.
  - **Asset**: All assets.
  - **Adverse action**: Data could become corrupted due to incorrect system access by the TOE users, Non-TOE users or applications of unauthorized data modification, and inadequate configuration actions through LAN.

4.4 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.

- **A.ExternalServices**

  It is assumed that the following services provided by the external server are considered as secure, such as LDAP server, NTP server and Radius server.

- **A.Password**

  Password policy needs to follow the state of the art (see https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_MDP_NoteTech.pdf for recommendations).

NOTE

The TOE sends or receives user data through the iSCSI protocol. Currently, the TOE provides only CHAP authentication and does not encrypt transmission. Therefore, it is assumed that user data is transmitted over a secure network.

CHAP with mutual authentication is not activated by default and it’s up to the user to activate it.

- **A.NDMP**

  It is assumed that the NDMP Administrator is not within the TOE.

  The MD5 algorithm is adopted to meet protocol compliance requirements of NDMP based on the fact that NDMP is usually used on a LAN with limited security risks. Therefore, it is assumed that the authentication mode of NDMP is secure.

  The NDMP feature does not encrypt data, it is assumed that NDMP data is transmitted over a secure network.

5 TOE Security Functions

5.1 SF.Identification and Authentication

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

- The TOE supports authentication and identification on two types of users: Administrative Users and Data Users.
    - The Administrative User is an account that will manage or configure the TOE's functions, including but not limited to security functions.
    - The Data User is a subject that will access the data stored in the TOE through standard I/O protocols.
- To Administrative Users, the TOE provides local and remote authentication modes
    - In local authentication mode, the user identities are stored locally in the TOE. The identification factors include the password, SSH key pair, and one time password (OTP) sent through email. The TOE supports 3 kinds of combinations: password and OTP, password only, and SSH key pair only. The combination of a user's identification factors can be chosen by another user whose role has the proper permissions.
        - ✓ 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.
        - ✓ When the account SSH key pair is chosen, the result of identification is based on the match result between the SSH public key stored in the TOE and the private key held by the SSH client. This type of identification can be chosen only for login through SSH or SFTP.
        - ✓ When the OTP is used, an email with the OTP will be sent to the recipient configured by other administrative users with proper roles. The OTP is generated by the TOE randomly. A user is allowed to log in to the TOE only when the input OTP is same as the one generated by the TOE.
    - In remote authentication mode, the user identities are stored in a remote LDAP server (which means a server in compliance with the standard LDAP protocol, such as the AD server and OpenLDAP server) or a remote radius server.
    - 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 account 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 an radius client. The input account 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, initializing the user password, unlocking a user, and clearing or importing configuration data. This is called re-authentication.
- If the identification is successful, information about the last successful login (including the IP address and time) will be displayed. This function can be enabled or disabled by proper Administrative Users.
- The input password is presented as asterisks, and no mater any reason the authentication or re-authentication fails with, the TOE will only give blurry feedback to prevent from brute-force cracking. In addition, after the authentication or re-authentication failure, the failure count is recorded in the TOE. After N consecutive authentication failures during 5 minutes, the account will be locked for M minutes, in which N is a positive integer from 1 to 9 and M is a positive integer from 3 to 2000. Both of the values can be configured by a user whose role has proper permissions and both take effect globally.
- After a successful identification, a session will be created to stand for the user dynamically. During the session's creation, a random unique number will be generated as an identifier of the session, and the user's account name, account role and other security attributes will be assigned to the session. A session will be terminated if it is inactive up to N minutes, in which N is a positive number from 1 to 100 and is configured by Administrative Users with proper permissions. A session will be denied after user authentication failed, IQN authentication failed.
- The Administrative User with proper permissions can configure a mapping, which contains relationships between an iSCSI initiator (World Wide Name, i.e. WWN) and an iSCSI target (LUN).
- The Data User whose initiator is in the mapping pre-configured in the TOE has rights to access the data (i.e. LUN) on the TOE, which is actually a simple Attribute Based Access Control model. Furthermore, if CHAP authentication is enabled, the target LUN on the TOE can be accessed only when CHAP authentication is passed. If CHAP authentication is disabled, the target LUN on the TOE can be accessed without authentication. All these above are similar to other SAN protocols.

This security function counters the threats: **UnauthenticatedAccess and DataCorruption.**

5.2 SF.Authorization

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

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

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

All roles and their permissions are defined in table Table 2-2.

This security function counters the threats: **UnauthorizedAccess and DataCorruption.**

5.3 SF.Access Control

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

The TOE supports two Access Control mechanisms for Administrative Users:

- The IP Whitelist is configured globally to limit access from IP addresses out of the list. The elements of the list are single IP addresses or ranges configured by proper Administrative Users. A user cann’t establish session to access the TOE if the IP address out of the list.
- Login Method is a list including SSH, SFTP, RESTful, Serial Interface, etc. A user can access the TOE only using the method/protocol included in this list configured for the user by other proper Administrative Users.

This security function counters the threat: **UnauthenticatedAccess.**

5.4 SF.Audit

The TOE provides an audit trail for all essential operations.

- All non-query operations will be recorded in the operation logs. Typically, these operations include login, logout, configuration change, user management, and security settings.
- An audit record is composed of 6 basic items: who (user name), where (user IP address), when (timestamp), what (operation description), result (success or specific error code), and ID (a unique number of this record).
- Review functionality is provided via the command line interface and GUI, which allows Administrative Users to inspect the audit logs. Administrative Users whose role has proper permissions can query or fetch the audit trail. Administrative 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, protected by ACL. If an SFTP/FTP server to dump audit records is configured and enabled, once the number of records exceeds 55,000, the oldest 10,000 records will be dumped to the SFTP/FTP server. If such an SFTP/FTP server is not configured or not enabled, the newer records will overwrite the oldest stored audit records once the number of records reaches 55,000.
- All audit trails are transmitted to syslog server for centralized log management, if an syslog server is configured and the transmission is enable
- The NTP service can synchronize all the clocks of devices on the network so that these devices can provide audit trails' timestamp with the uniform time.

This security function counters the threats: **UnauthenticatedAccess and UnauthorizedAccess.**

6 Rationale

6.1 Assets vs Security Needs

The following security needs of assets are:

		Availability	**Confidentiality**	**Integrity**
TSF data	Authentication data	X	X(*)	X
	Audit data	X		X
	Configuration data	X		X

NOTE

(*)The confidentiality of authentication data is guaranteed by HTTPS (Nginx)

6.2 Assets vs Threats

Threat Asset	T.UnauthenticatedAccess	T.UnauthorizedAccess	T.DataCorruption
Authentication data	Av, I	Av, I	Av, I
Audit data	Av, I	Av, I	Av, I
Configuration data (TSF)	Av, I	Av, I	Av, I
Av: Availability, I: Integrity			

6.3 Threats vs Security Functions

Threat Security Function	T.UnauthenticatedAccess	T.UnauthorizedAccess	T.DataCorruption
SF.Identification and Authentication	X		X
SF.Authorization		X	X
SF.Access Control	X		
SF.Audit	X	X	