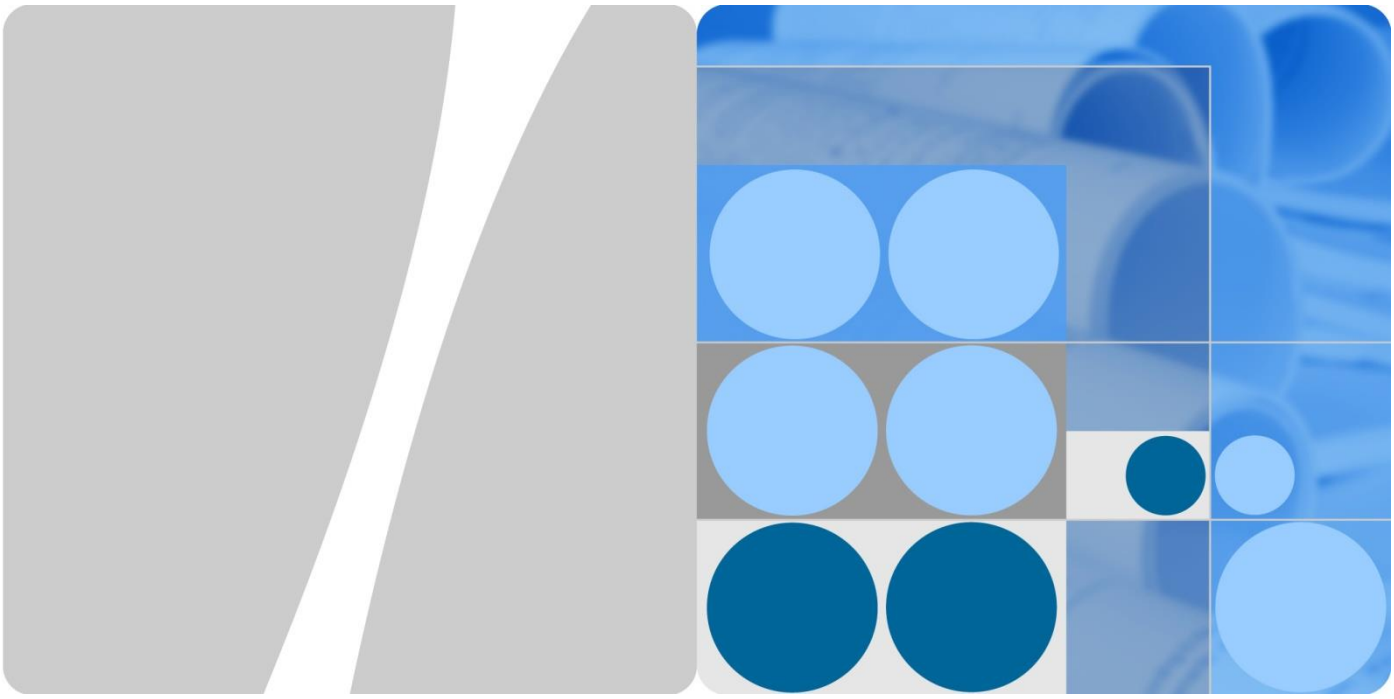


CC Huawei OceanStor 100D Storage System Software 8.0.3 ST

Version 2.3

Date 2021-10-29

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

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

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: http://www.huawei.com

Contents

Revision Record

Date	Revision Version	Change Description	Author
2021-10-29	2.3	Modified sections 1.4.1.	Zhang Ying
2021-10-20	2.2	Modified sections 1.4.1.	Zhang Ying
2021-07-30	2.1	Modified section 1.3.3 and 1.4.1.	Zhang Ying
2021-07-15	2.0	Modified sections 1.4.1.	Zhang Ying
2021-07-08	1.9	Modified sections 1.4.1.	Zhang Ying
2021-06-18	1.8	Modified sections 1.4.1.	Zhang Ying
2021-05-26	1.7	Modified sections 1.4.1.	Zhang Ying
2021-05-13	1.6	Modified sections 5.2.3.10.	Zhang Ying
2021-04-26	1.5	Modified sections 1.3.3 and 1.4.3.	Zhang Ying
2021-04-21	1.4	Modified the description of audit record dump.	Zhang Ying
2021-04-13	1.3	Change the number of built-in roles to 6.	Zhang Ying
2021-04-12	1.2	Modified version to 1.2 according to the comments of the evaluation laboratory. Update Product guidance in Section 1.4.1.	Zhang Ying
2021-03-31	1.1	Modified version to 1.1 according to the comments of the evaluation laboratory. The built-in role Machine-machine account is added.	Zhang Ying
2021-03-10	1.0	Modified version to 1.0 according to the comments of the evaluation laboratory	Zhang Ying
2021-02-18	0.9	Modified version to 0.9 according to the comments of the evaluation laboratory	Zhang Ying
2021-01-04	0.8	1. Changed 8.0.RC1 to 8.0.3 2. Modified section 1.3.3 3. Modified section 1.4.1	Zhang Ying
2020-12-18	0.7	1. Added Table 1-1 to section 1.3.3 and modified the hardware node model. 2. Modified section 1.4.1 and added the description of delivery and deployment modes. 3. Changed 8.0.2 to 8.0.RC1.	Zhang Ying
2020-07-21	0.6	Standardize the document name and TOE name.	Zhang Ying
2020-07-10	0.5	Modified version to 0.5 according to the comments of the evaluation laboratory	Zhang Ying

2020-06-24	0.4	Modified version to 0.4 according to the comments of the evaluation laboratory	Zhang Ying
2020-05-15	0.3	Modified according to the comments of the evaluation laboratory	Zhang Ying
2019-10-28	0.2	Internal review before delivery	Zhang Chunli, Zhang Ying
2019-9-10	0.1	Initial Draft	Zhang Chunli, Zhang Ying

1 Introduction

This section contains the ST Identification, TOE Identification, TOE overview and TOE description of Huawei OceanStor 100D 8.0.3 Storage System. All of them are consistent with each other. This Security Target is for the evaluation of OceanStor 100D 8.0.3 Storage system software.

1.1 ST Reference

Title: CC Huawei OceanStor 100D Storage System Software 8.0.3 ST

Version: 2.3

Date: 2021-10-29

Developer: Huawei Technologies Co., Ltd.

1.2 TOE Reference

The TOE is identified as bellow

TOE name: Huawei OceanStor 100D Storage System Software

TOE version: 8.0.3

Developer: Huawei Technologies Co., Ltd.

1.3 TOE Overview

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

1.3.1 TOE Usage and Major Security Features

OceanStor 100D is an intelligent distributed storage product that can be scaled horizontally or elastically. Based on the unique elastic erasure coding (EC) technology, as well as the dynamic deduplication and compression technology based on automatic load control, OceanStor 100D provides more available space for customers while ensuring service performance. In addition, it provides the ever new capability to support smooth software upgrade. Hardware can coexist for multiple generations without service interrupting caused by software and hardware updates.

OceanStor 100D uses storage system software to integrate local storage resources from common hardware into a distributed storage pool. OceanStor 100D provides distributed Block Service, distributed Object Service, and distributed File Service for upper-layer applications. Each storage service provides various functions and value-added features. In addition, OceanStor 100D supports flexible purchase and deployment of multiple storage services based on service requirements, helping enterprises cope with flexible and efficient data access requirements when services change rapidly.

OceanStor 100D provides highly efficient, highly available, and scalable intelligent distributed storage to meet higher performance, capacity, and scalability requirements of complex service loads in the cloud and AI era. It is widely applicable to cloud resource pools, mission-critical databases, big data analysis, content storage, and backup archiving in industries such as finance, carriers, and government public utilities.

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

- **Identification and Authentication**
- **Authorization and Access Control**
- **Auditing**

- **Security Management**
- **User Data Protection**
- **Protection of The TSF**
- **Resource Utilisation**
- **TOE Access**

1.3.2 TOE Type

Software of storage system

1.3.3 Non-TOE Hardware/Software/Firmware Required by the TOE

The TOE software is designed to run on OceanStor 100D series hardware nodes. The below table list hardware node model for OceanStor 100D. The TOE software is installed on the hardware nodes (see Table 1-1). At least three same hardware nodes are required for the TOE to run properly. If there are three hardware nodes, the active and standby management systems must be deployed on the same hardware node as the storage system. It is recommended that the active and standby management systems be installed on two independent hardware nodes. In this case, at least five nodes are required.

Table 1-1 The Hardware node model for OceanStor 100D

Hardware node model	Nameplate	Description
P100	DPE30101	Functions as a 2 U 12-slot passthrough node equipped with two Kunpeng 920 CPUs (48-core 2.6 GHz).
C100	DPE30102	Functions as a 4 U 36-slot passthrough node equipped with two Kunpeng 920 CPUs (48-core 2.6 GHz).
P110	H22H-05 (2288H V5)	Functions as a 2 U 12-slot node equipped with x86 CPUs. Cache disks: Huawei-developed NVMe SSD RAID controller card: SR130 (LSI3008) Onboard NICs: One 4-port GE NIC and one dual-port 25GE/10GE NIC (Huawei-developed NIC)
C110	H52H-05 (5288H V5)	Functions as a 4 U 36-slot node equipped with x86 CPUs. Cache disks: Huawei-developed NVMe SSD RAID controller card: SR130 (LSI3008) Onboard NICs: One 4-port GE NIC and one dual-port 25GE/10GE NIC (Huawei-developed NIC)

2288X V5	H22X-05	Functions as a 2 U 12-slot node equipped with x86 CPUs. Cache disks: NVMe SSD RAID controller card: 3508 standard card (9460-8i 2 GB cache, optional) Onboard NICs: Two dual-port 10GE Intel 82599 interface cards
5288X V5	H52X-05	Functions as a 4 U 36-slot node equipped with x86 CPUs. Cache disks: NVMe SSD RAID controller card: 3508 standard card (9460-8i 2 GB cache, optional) Onboard NICs: Two dual-port 10GE Intel 82599 interface cards

The following description mainly includes non-TOE servers or clients. Switches and cables are used for network connection. LDAP, NTP, AD, DNS, and Syslog service software can be installed on the server to provide services for the TOE. You can also install NFS, S3, or iSCSI client software to access the TOE.

- Description
  - The external servers, application server, NFS clients, S3 clients, management server or PC, and TOE (storage) are connected to each other by the Ethernet switch.
- Application server
  - Hardware

    Rack servers or PCs with at least one 10G/25G NIC
  - Software
    - Windows Server 2016 OS
    - Multipathing software UltraPath 21.06.060
    - Microsoft iSCSI Software Initiator in Windows Server 2016
    - JRE (Java Runtime Environment 1.8)
    - Vdbench5040x
    - LDAP Admin 1.8.3
- External servers
  - Hardware

    Rack servers or PCs with at least one 100M/1G Ethernet port
  - Software
    - Windows Server 2016 OS
    - OpenLDAP for Windows 2.4.42
    - AD Server, NTP server, SFTP/FTP server, DNS server in Windows Server 2016
    - rsyslog-8.24.0 or other version
    - SMTP Server
    - JRE(Java Runtime Environment 1.8)
- Management Server (or PC)
  - Hardware

Rack servers or PCs with at least one 100M/1G Ethernet port

- Software
  - Windows Server 2016 OS
  - Brower Google Chrome 63+
  - JRE (Java Runtime Environment 1.8), PuTTY 0.73, WinSCP 5.15, Postman, Python 2.79, Notepad ++
  - GnuPG

- Client
  - Hardware

    Rack servers with at least two 10G/25G Ethernet port
  - Software
    - CentOS 7.x for x86_64;
    - NFS Client(nfs-utils-*2*.3.3 or other version)
    - S3 Client(s3curl)
    - Vdbench5040x

1.4 TOE description

1.4.1 Physical scope

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.

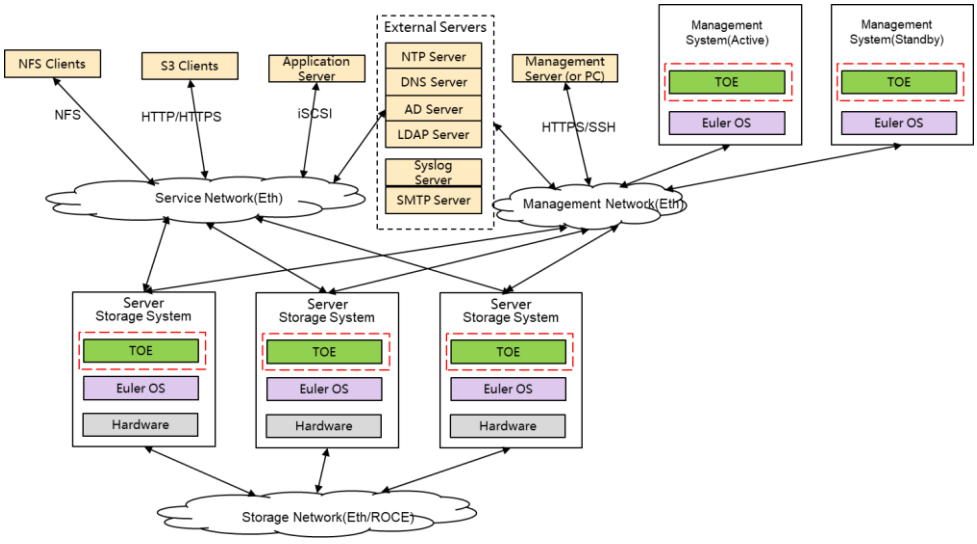


Figure 1-1 Shows the physical scope and physical boundary of the TOE environment

TOE contains two main software packages, a basic storage software package, and an object service setup package. The basic storage software package provides OAM management services, and IO services such as Block Service, File Service and their security functions. The object service setup package provides only Object Service and its security functions. For

Block Service, TOE supports standard iSCSI interface to provide volume access service for application server. For File Service, TOE supports standard NFS interfaces and provides file sharing services for NFS clients. For Object Service, TOE Support standard Amazon S3 API to provide object data access services for S3 clients.

Software and hardware integration is the recommended purchase or sales mode of OceanStor 100D. Software and hardware integration indicates that operating systems and drivers have been installed before delivery. You can directly install OceanStor 100D software using DeviceManager Client. In addition, hardware nodes that do not integrate operating systems and drivers can also be delivered. The operating system image and driver must be installed onsite. Then you can install OceanStor 100D software using DeviceManager Client.

The management system can be on the same server with the storage server system or different servers. Different deployment modes of the management system and storage system do not affect security. However, the responsibilities of each node are clearer when the nodes are deployed separately.

Table 1-2 The Physical TOE Scope

Type	Delivery Item	Version	Download Link
Software	Basic storage software package: OceanStor-100D-8.0.3.tar.gz	8.0.3	https://support.huawei.com/enterprise/en/software/251193663-ESW2000292557
Digital signature file	OceanStor-100D-8.0.3.tar.gz.asc	8.0.3	
Software	Object service setup package: OceanStor-100D-8.0.3-OBS.tar.gz	8.0.3	https://support.huawei.com/enterprise/en/software/251193663-ESW2000292577
Digital signature file	OceanStor-100D-8.0.3-OBS.tar.gz.asc	8.0.3	
Product guidance	OceanStor 100D 8.0.3 Event Reference	V01	https://support.huawei.com/enterprise/en/doc/EDOC1100200606?idPath=7919749%7C251364444%7C21430817%7C251366260%7C251192351
	OceanStor 100D 8.0.3 CLI Command Reference	V02	https://support.huawei.com/enterprise/en/doc/EDOC1100200603?idPath=7919749%7C251364444%7C21430817%7C251366260%7C251192351
	OceanStor 100D 8.0.3 Error Code Reference	V01	https://support.huawei.com/enterprise/en/doc/EDOC1100200607?idPath=7919749%7C251364444%7C21430817%7C251366260%7C251192351
	OceanStor 100D 8.0.3 REST Interface Reference	V02	https://support.huawei.com/enterprise/en/doc/EDOC1100200602?idPath=7919749%7C251364444%7

			C21430817%7C251366260%7C251192351
	OceanStor 100D 8.0.3 Object Service API Reference	V03	https://support.huawei.com/enterprise/en/doc/EDOC1100200604?idPath=7919749%7C251364444%7C21430817%7C251366260%7C251192351
	OceanStor 100D 8.0.3 Object Service Account Management API Description	V03	https://support.huawei.com/enterprise/en/doc/EDOC1100200605?idPath=7919749%7C251364444%7C21430817%7C251366260%7C251192351
	OceanStor 100D 8.0.3 Software Installation Guide	V04	https://support.huawei.com/enterprise/en/doc/EDOC1100200608?idPath=7919749%7C251364444%7C21430817%7C251366260%7C251192351
	CC Huawei OceanStor 100D Storage System Software 8.0.3 AGD_OPE	V12	https://support.huawei.com/enterprise/en/doc/EDOC1100200695?idPath=7919749%7C251364444%7C21430817%7C251366260%7C251192351
	CC Huawei OceanStor 100D Storage System Software 8.0.3 AGD_PRE	V14	https://support.huawei.com/enterprise/en/doc/EDOC1100200694?idPath=7919749%7C251364444%7C21430817%7C251366260%7C251192351
Product guidance	OceanStor 100D 8.0.3 Administrator Guide	V05	https://support.huawei.com/enterprise/en/doc/EDOC1100171252/426cffd9/about-this-document
	OceanStor 100D 8.0.3 Basic Object Service Configuration Guide	V05	https://support.huawei.com/enterprise/en/doc/EDOC1100171245?idPath=7919749%7C251364444%7C21430817%7C251366260%7C251192351
	OceanStor 100D 8.0.3 Security Configuration Guide	V05	https://support.huawei.com/enterprise/en/doc/EDOC1100171246?idPath=7919749%7C251364444%7C21430817%7C251366260%7C251192351

1.4.2 Logical Scope of the TOE

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

1.4.2.1 Identification and Authentication

The TOE works with multiple identity management systems to authenticate users and control access to storage data.

- In management 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, and one time password (OTP) sent through email. The TOE supports 2 kinds of combinations: password and OTP, password only.

  In remote authentication mode, the identities are stored in a remote LDAP server. When the identification begins, the input password is sent forward to the remote LDAP server through the standard LDAP protocol and identified by the LDAP server.
- For Block Service data access, the available Volume is limited by the initiator. CHAP authentication is supported for connecting to the TOE over an iSCSI network. Target Volumes on the TOE can be accessed only when CHAP authentication is passed.
- For File Service data access via NFS interface, the TOE provides local and remote authentication modes LDAP or NIS.
- For Object Service data access via S3 interface, the TOE provides local authentication mode. Each object account or user has an AK and an SK, and the identities information stored in the TOE. An operation request sent by a client contains a user's AK and a signature calculated based on the user's SK. After receiving the request, the object data can be accessed only when the TOE authentication AK and the signature calculation based on SK are passed.

1.4.2.2 Authorization

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

The TOE controls access by the RBAC (Role Based Access Control) model. In RBAC, a permission is an approval to perform an operation on one or more RBAC protected objects (i.e. the commands in TOE), a role is a set of permissions and an account can be assigned with only one role. The TOE support only 6 built-in roles (listed in table below) which cannot be modify or delete.

Table 1-3 Role permission definition

Role	Authority
Super administrator	All permissions.
Administrator	All permissions except user management, security management, and high-risk maintenance operations.
Security administrator	System security configuration permissions, including security policy configuration, access control, certificate management, KMC configuration, and time configuration.
SAN resource administrator	SAN resource management permissions, including management of storage pools, Volumes, mappings, hosts, Initiator, CHAP, iSCSI service.

Role	Authority
System viewer	Permission to query information and change the password of the account itself.
Machine-machine account	Has all permissions except session management and access control. A machine-machine account has the permission to view security policies.

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

1.4.2.3 Access Control

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

The TOE supports two Access Control mechanisms for Administrative Users:

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

1.4.2.4 Auditing

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

- By default all configured commands along with a timestamp when they are executed are logged.
- Attempts to login regardless success or failure are logged, along with user id, source IP address, timestamp, operation description, result (ok or error), and ID of the log..
- If the alarm dump function is enabled, the oldest logs will be dumped to the specified FTP/SFTP server when the log entries exceed a specified number.
- Review functionality is provided via the CLI and GUI interface, which allows administrative users to inspect the audit log.
- If the Alarm notification (Syslog) is enabled and successfully set, the system will automatically send audit logs to specified servers in real time.

1.4.2.5 Security management

Security functionality management include not only authentication, access level, but also managing security related data consisting of configuration profile and runtime parameters. According to security functionality management, customized security is provided.

- Management of users and roles
- Management of security policies and access control
- Management of users sessions
- Management of domain authentication
- Management of the TOE's time setting

- Management of certificates
- Management of audit and alarm notification
- Block Service Management
- Object Service Management
- File Service Management

All security management functions (i.e. commands related to security management) require sufficient user level for execution.

Note: TOE's time is managed by NTP. NTP (Network Time Protocol) is an application layer protocol used on the internet to synchronize clock among a set of distributed time servers and clients. In this manner, the clock of the host is synchronized with certain time standards. NTP synchronizes all the clocks of devices (switches, PCs, and routers) on the network so that these devices can provide multiple applications based on the uniform time.

1.4.2.6 User Data Protection

The TOE uses account or user authentication, access control list (ACL) and bucket policy control object storage data access. Users must be authenticated before the ACL will be evaluated. Authentication occurs locally.

The TOE uses authentication and ACLs to control file data access. The file data access SFP relies on ACL and UNIX permissions, collectively called authorization data, to protect data at the file level. The root role is, by default, the owner of all files and directories. The file owner can assign permissions to the file. An authorized administrator or owner can change the file permissions. The TOE can translate UNIX permissions into ACLs and vice versa.

1.4.2.7 Protection of the TSF

The TOE protects user data against disk and node failure. For the main storage disk/cache disk, the system performs periodic detection on the disk, based on the detection results of key indicators, the slow disk/failed disk is identified, the system actively sends an alarm, and automatically isolates the disk in the background and triggers data reconstruction.

The TOE detects node failures through a heartbeat mechanism. When a node failure is detected (such as operating system reset, CPU failure), it will trigger node failover and switch the services carried on it to other normal nodes. To ensure that the failure within the redundancy range of the system design does not affect the availability of the storage system.

The TOE also includes a sys clock, which provides the TOE with a reliable timestamp. The system performs the synchronization of ACLs, logs, and user data to ensure inter-TSF data consistency.

1.4.2.8 Resource Utilization

The storage system protects data against failures using the multi-copy mechanism or erasure coding (EC). Data can be properly accessed even if a limited number of physical devices in the storage system become faulty, and data on the faulty devices will be automatically restored.

- **Multi-copy Mechanism**

The storage system supports two or three copies. Table 1-4 details the Multi-copy mode.

1. When a piece of data is written, the storage system generates two copies for the data.

2. The storage system writes the data and its copies into three storage nodes separately.

Table 1-4 Multi-copy modes

Mode	Description	Minimum Number of Nodes
Two copies	One copy is created for each piece of data. Data integrity will not be compromised when one storage node (server-level security) or cabinet (cabinet-level security) is faulty.	3 (NOTE1)
Three copies	Two copies are created for each piece of data. Data integrity will not be compromised when two storage nodes (server-level security) or cabinets (cabinet-level security) are faulty.	3

NOTE 1: The Minimum number of Nodes is 3 because less than 3 nodes cannot promise all the functions work well. This minimum number doesn't depend on the number of copies.

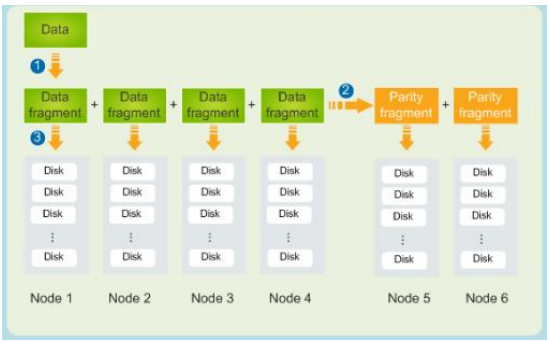
- **EC**

EC schemes are expressed in N+M mode. N indicates the number of data fragments (data strips) and M indicates the number of parity fragments (parity strips). The storage system supports N+2, N+3, and N+4 EC schemes. Table 1-5 details the EC schemes.

Figure 1-2 shows how data protection is implemented when the number of storage nodes is greater than or equal to N+2.

When the number of storage nodes is greater than or equal to (N+2)/2 and less than N+2, the following uses three storage nodes configured with 4+2 as an example to describe the basic principles.

Figure 1-2 Data protection in the 4+2 EC scheme



1. Divides data into four data fragments.

2. Groups the four data fragments and calculates two parity fragments.

3. Writes the data and parity fragments into six storage nodes.

Table 1-5 EC schemes

Mode	Description	Minimum Number of Nodes
N+2	Node-level security	Node-level security

Mode	Description	Minimum Number of Nodes
	If the number of nodes is greater than or equal to (N+2)/2 (rounded up) and less than N+2, the system can tolerate the failure of one storage node or two main storage disks at a time. If the number of nodes is greater than or equal to N+2, the system can tolerate the failure of two storage nodes or two main storage disks at the same time. Cabinet-level security If the number of cabinets is greater than or equal to (N+2)/2 (rounded up) and less than N+2, the system can tolerate the failure of one cabinet or two storage nodes at a time. If the number of cabinets is greater than or equal to N+2, the system can tolerate the failure of two cabinets or storage nodes at a time. N can be 4, 6, 8, 10, 12, 14, 16, 18, 20, or 22.	Minimum number of nodes: (N+2)/2 rounded up Cabinet-level security Minimum number of cabinets: (N+2)/2 rounded up
N+3	Node-level security If the number of nodes is greater than or equal to (N+3)/3 (rounded up) and less than N+3, the system can tolerate the failure of one storage node or three main storage disks at a time. N can be 6, 8, 12, 14, 18, or 20. If the number of nodes is greater than or equal to N+3, the system can tolerate the failure of three storage nodes or main storage disks at a time. N can be 6, 8, 10, 12, 14, 16, 18, or 20. Cabinet-level security If the number of cabinets is greater than or equal to (N+3)/3 (rounded up) and less than N+3, the system can tolerate the failure of one cabinet or three storage nodes at a time. N can be 6, 8, 12, 14, 18, or 20. If the number of cabinets is greater than or equal to N+3, the system can tolerate the failure of three cabinets or three storage nodes at a time. N can be 6, 8, 10, 12, 14, 16, 18, or 20.	Node-level security Minimum number of nodes: (N+3)/3 rounded up Cabinet-level security Minimum number of cabinets: (N+3)/3 rounded up
N+4	Node-level security If the number of nodes is greater than or equal to (N+4)/4 (rounded up) and less than N+4, the system can tolerate the failure of one storage node or four main storage disks at a time. N can be 8, 12, 16, or 20. If the number of nodes is greater than or equal to N+4, the system can tolerate the failure of four storage nodes or main storage disks at a time. N can be 8, 10, 12, 14, 16, 18, or 20. Cabinet-level security If the number of cabinets is greater than or equal to (N+4)/4 (rounded up) and less than N+4, the system can tolerate the failure of one cabinet or four storage nodes at a time. N can be 8, 12, 16, or 20. If the number of cabinets is greater than or equal to N+4, the system can tolerate the failure of four cabinets or four storage nodes at a time. N can be 8, 10, 12, 14, 16, 18, or 20.	Node-level security Minimum number of nodes: (N+4)/4 rounded up Cabinet-level security Minimum number of cabinets: (N+4)/4 rounded up
Note 1: An EC scheme is expressed in the format of N+M, wherein: N indicates the number of data		

Mode	Description	Minimum Number of Nodes
fragments. M indicates the number of parity fragments. Note 2: In the same scheme, a larger N indicates a higher disk utilization. Note 3: The TOE storage system provides support for flexible data layout strategies, including node-level security layout and cabinet-level security layout. Note 4: A node means a server, a cabinet means a group of servers placing on the Cabinet. • Node-level security layout Distribute the data and its redundancy to different nodes. As long as the number of failed nodes is less than or equal to the number of redundant nodes at the same time, the data can be automatically restored without interruption of business and without loss of data. • Cabinet-level security layout Distribute the data and its redundancy to different cabinets. As long as the number of failed cabinets is less than or equal to the number of redundant cabinets, the data can be automatically restored without interruption of business or loss of data.		

1.4.2.9 TOE Access

- TOE can coexist up to 32 sessions at the same time. The current system has reached the maximum number of sessions (32). If the super administrator does not have the super administrator login session, the super administrator can obtain a session.
- An administrator user can only obtain one session when “one session switch” is enabled.
- Within a specified period (the value ranges from 30 to 100 minutes and the default value is 30 minutes). If no operation is performed on the session, TOE will destroy the session. Once the session is destroyed, TOE must be re-login to obtain the access permission.
- The super administrator can forcibly destroy sessions of non-super administrators to release session resources.
- If the number of incorrect password inputs exceeds the upper limit, accounts will be locked. The super administrator will be automatically unlocked after being locked for 15 minutes. The non-super administrators is automatically unlocked after a specified period (the value ranges from 3 to 2000 minutes and the default value is 15 minutes).
- A system account will be locked if it has not been used for logging in to the system for a specified period of time (the value ranges from 1 to 999 days and the default value is 60 days).
- After a user login, information about the last login (including the login time and IP address) is displayed.

1.4.3 Evaluation Configuration

The hardware and the operating system installed on the hardware listed in the following table are used for the TOE evaluation.

Table 1-6 TOE evaluation configuration

Component	Hardware	Operating System	Software
Management System and Storage System	P110 (three nodes)	Euler OS (Euler version is V200R009C00SPC100B150, and kernel version is 4.18.0-147.5.0.5.h116)	TOE

- Application server
  - Hardware

    PC
  - Software
    - Windows Server 2016 OS
    - Multipathing software UltraPath 21.06.060
    - Microsoft iSCSI Software Initiator in Windows Server 2016
    - JRE (Java Runtime Environment 1.8)
    - Vdbench5040x
    - LDAP Admin 1.8.3
- External servers
  - Hardware

    PC
  - Software
    - Windows Server 2016 OS
    - OpenLDAP for Windows 2.4.42
    - AD Server, NTP server, SFTP/FTP server, DNS server in Windows Server 2016
    - rsyslog-8.24.0 or other version
    - SMTP Server
    - JRE (Java Runtime Environment 1.8)

- Management Server (or PC)
  - Hardware

    PC
  - Software
    - Windows Server 2016 OS
    - Brower Google Chrome 63+
    - JRE (Java Runtime Environment 1.8), PuTTY 0.73, WinSCP 5.15, Postman, Python 2.79, Notepad ++
- Client
  - Hardware

    Huawei 2288H V5 server
  - Software
    - CentOS 7.x for x86_64;

- NFS Client(nfs-utils-*2*.3.3 or other version)
- S3 Client(s3curl)
- Vdbench5040x

2 Conformance claims

2.1 CC Conformance Claim

This Security Target claims to be conformant to Version 3.1 of Common Criteria for Information Technology Security Evaluation according to:

• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017

• Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017

• Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

2.2 Protection Profile Conformance Claim

No conformance to a Protection Profile is claimed.

2.3 Package Claim

This ST claims conformance to EAL3+ ALC_FLR.2 assurance package.

3 Security Problem Definition

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

3.1 Assets

All data from and to the interfaces available on the TOE is categorized into TSF data and non-TSF data. The following is an enumeration of the subjects and objects participating in the policy.

TSF data:

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

Non-TSF data:

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

3.2 Threats

3.2.1 Threats Components

This section 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 of assets.
  - **Adverse action:** A user who is not a user of the TOE gains access to the TOE through the interface of LAN.

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

- **T.DataCorruption**
  - **Threat agent**: TOE user (a user or application using the functionality of the TOE).
  - **Asset:** all of assets.
  - **Adverse action:** Data could become corrupted due to hardware failure that cause by

incorrect system access by users of the TOE or attackers of unauthorized data modification, and inadequate configure actions through interface of LAN.

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

3.3 Organizational Security Policies

No organizational security policy.

3.4 Assumptions

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

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

A.NETWORK The operational environment will provide a secure network communication to protect data that is sent to and received from the TOE. The network and all the services running on it are trustworthy, such as NFS service, S3 service and iSCSI service.

A.Hardware It is assumed that the underlying hardware (including Operating system) of OceanStor 100D, which is outside the scope of the TOE, works correctly.

4 Security Objectives

The security objectives, are divided into two solutions. These solutions are called the security objectives for the TOE and the security objectives for the operational environment. It reflects that these solutions are provided by two different entities: the TOE, and the operational environment.

4.1 Security Objectives for the TOE

- **O.Authorization**

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

- **O.Authentication**

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

- **O.Audit**

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

- **O.SecurityManagement**

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

- **O.**DataProtection

  The TOE shall provide functionality to reconstruct user data when nodes or disks are damaged within a certain proportion.

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. Thus, they will be satisfied largely through application of procedural or administrative measures.

- **OE.Manage**

  The TOE Environment must ensure the administrative control of the TOE are non-hostile, appropriately trained, and follow all administrator guidance.

- **OE.Physical**

  The TOE shall be protected against unauthorized physical access.

- **OE.COMMS**

  Communications with the TOE are appropriately protected by the operational environment through the use of physical and network security.

- **OE.HARDWARE**

  The Operational environment shall ARM Servers (including Euler operating system)

4.3 Security Objectives 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 objectives rationale also demonstrates that all the given threats, OSPs and assumption are addressed.

Table 4-1 Mapping Objectives for the Environment to Assumptions

Objective	Threat / OSPs/Assumption	Rationale
O.Authentication	T.UnauthenticatedAccess	O.Authentication counters this threat by ensuring that all of actions must be after authentication.
	T.UnauthorizedAccess	O.Authentication counters this threat by ensuring that all of actions must be after authentication.
	T.DataCorruption	O.Authentication couters this threat by ensuring that only authenticated user could manage user data.
	T.UnauthorizedServer	O.Authentication counters this threat by ensuring that only authenticated server could read and write the user data.
O.Authorization	T.UnauthorizedAccess	O.Authorization counters this threat by ensuring that all of actions must be after authorization.
	T.UnauthorizedServer	O. Authorization counters this threat by ensuring that only authorized server could read and write the user data.
	T.DataCorruption	O.Authorization couters this threat by ensuring that only authorized user could 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 a authenticated user to configure the TOE.
	T.UnauthorizedAccess	O. SecurityManagement counters this threat by allowing only a authorized user to configure the TOE.

	T.DataCorruption	O. SecurityManagement counters this threat by allowing a user to properly configure the TOE.
	T.UnauthorizedServer	O. SecurityManagement counters this threat by allowing a user to properly configure the TOE of Volume map to the servers.
O.DataProtection	T.DataCorruption	O.DataProtection counters this threat by reconstructing user data when nodes or disks are damaged within a certain proportion.

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

Environmental Objective	Assumption	Rationale
OE.Manage	A.Manage	OE.Manage directly upholds assumption A.Manage.
OE.Physical	A.Physical	OE.Physical directly upholds assumption A.Physical.
OE.COMMS	A.NETWORK	OE.COMMS directly upholds assumption A.NETWORK.
OE.HARDWARE	A.Hardware	OE.HARDWARE directly upholds assumption A.Hardware

5 Security Requirements for the TOE

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

5.1 Conventions

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. The following conventions are used for the completion of operations:

- Selection: Indicated by using bold text, e.g., **selected item**.
- Assignment: Indicated by surrounding brackets, e.g., [assigned item].
- Refinement: Indicated by surrounding brackets and italics, e.g., [*refined item*].
- Iteration: Iteration/N indicates an element of the iteration, where N is the iteration number/character.

5.2 TOE Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. The following table identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 5-1 TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit Data Generation	√	√		
FAU_GEN.2	User Identity Association				
FAU_SAR.1	Audit Review		√		
FAU_SAR.2	Restricted Audit Review				
FAU_SAR.3	Selectable Audit Review		√		
FAU_STG.1	Protected Audit Trail Storage	√			
FAU_STG.3	Action in Case of Possible Audit Data Loss		√		
FAU_STG.4	Prevention of Audit Data Los	√	√		
FDP_ACC.1/ VOLUME	Subset access control		√		√
FDP_ACC.1/ OBJECT	Subset access control		√		√
FDP_ACC.1/FILE	Subset access control		√		√
FDP_ACC.1/USER	Subset access control		√		√
FDP_ACF.1/ VOLUME	Security attribute based access control		√		√
FDP_ACF.1/ OBJECT	Security attribute based access control		√		√
FDP_ACF.1/FILE	Security attribute based access control		√		√
FDP_ACF.1/USER	Security attribute based access control		√		√

Name	Description	S	A	R	I
FAU_GEN.1	Audit Data Generation	√	√		
FIA_ATD.1/USER	User attribute definition		√		√
FIA_ATD.1/ VOLUME	User attribute definition		√		√
FIA_ATD.1/ OBJECT	User attribute definition		√		√
FIA_ATD.1/FILE	User attribute definition		√		√
FIA_UAU. 2	User authentication before any action				
FIA_UAU.5	Multiple Authentication Mechanisms		√		
FIA_UAU.6	Re-authenticating		√		
FIA_UAU.7	Protected authentication feedback		√		
FIA_UID.2	User identification before any action				
FIA_AFL.1	Authentication failure handling	√	√		
FIA_USB.1	User-Subject Binding		√		
FIA_SOS.2	Specification of secrets		√		
FMT_MSA.1/ VOLUME	Management of security attributes	√	√		√
FMT_MSA.1/ OBJECT	Management of security attributes	√	√		√
FMT_MSA.1/FILE	Management of security attributes	√	√		√
FMT_MSA.1/ USERa	Management of security attributes	√	√		√
FMT_MSA.1/ USERb	Management of security attributes	√	√		√
FMT_MSA.3/ VOLUME	Static attribute initialization	√	√		√
FMT_MSA.3/ OBJECT	Static attribute initialization	√	√		√
FMT_MSA.3/FILE	Static attribute initialization	√	√		√
FMT_MSA.3/USER	Static attribute initialization	√	√		√

Name	Description	S	A	R	I
FAU_GEN.1	Audit Data Generation	√	√		
FMT_SMF.1	Specification of Management Functions		√		
FMT_SMR.1	Security roles		√		
FPT_STM.1	Reliable time stamps				
FPT_FLS.1	Failure with preservation of secure state		√		
FRU_FLT.1	Degraded fault tolerance		√		
FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions		√		
FTA_SSL.3	TSF-initiated termination		√		
FTA_TAH.1	TOE access history	√			
FTA_TSE.1	TOE session establishment		√		
FCS_COP.1/SHA256	Cryptographic Operation		√		√
FCS_COP.1/ PBKDF2	Cryptographic Operation		√		√

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

5.2.1 Security Audit (FAU)

5.2.1.1 FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

1. Start-up and shutdown of the audit functions;
2. All auditable events for the **not specified** level of audit; and
3. [login and logout, configuration changes made through Web Administration GUI, CLI and RESTful]:

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event;

b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, [no other audit relevant information].

Application note: The startup and shutdown of the audit functions is associated with the startup and shutdown of the entire TOE. The audit functionality will always be in active mode while the TOE is operative.

5.2.1.2 FAU_GEN.2 User Identity Association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

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.

5.2.1.3 FAU_SAR.1 Audit Review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [Super administrator, Administrator, Security administrator, SAN resource administrator, System viewer] with the capability to read [all audit information generated by user Id] from the audit records.

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

5.2.1.4 FAU_SAR.2 Restricted Audit Review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 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.

5.2.1.5 FAU_SAR.3 Selectable Audit Review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

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

5.2.1.6 FAU_STG.1 Protected Audit Trail Storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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

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

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

Hierarchical to: No other components.

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.3.1: The TSF shall [dump at least 10000 oldest audit records which type is operation log to the specified FTP server after the event dump function has been enabled and set] if the audit trail exceeds [The minimum value is 50000] records.

5.2.1.8 FAU_STG.4 Prevention of Audit Data Loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1: The TSF shall **overwrite the oldest stored audit records** and [send to Syslog] if the audit trail is full.

5.2.2 User Data Protection (FDP)

5.2.2.1 FDP_ACC.1/VOLUME Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1/VOLUME Security attribute based access control

FDP_ACC.1.1/VOLUME The TSF shall enforce the [Volume Access Control SFP] on [

Subjects: Application servers,

Objects: Volume,

Operations: Read and write].

5.2.2.2 FDP_ACC.1/OBJECT Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1/OBJECT Security attribute based access control

FDP_ACC.1.1/OBJECT The TSF shall enforce the [Object Storage Data Access Control SFP] on [

Subjects: Users and client systems accessing object data,

Objects: Objects storage data,

Operations: Read, write, execute]

5.2.2.3 FDP_ACC.1/FILE Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1/FILE Security attribute based access control

FDP_ACC.1.1/FILE The TSF shall enforce the [File Storage Data Access Control SFP] on [

Subjects: users and client systems accessing file storage data

Objects: file, directory, share

Operations: read, write, create, delete, execute, access].

5.2.2.4 FDP_ACC.1/USER Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1/USER Security attribute based access control

FDP_ACC.1.1/USER The TSF shall enforce the [Administrative User Access Control SFP**]** on [

Subjects: the user of the TOE with the roles defined in FMT_SMR.1

Objects: the commands to configure and manage the TOE

Operations: configure and manage]

5.2.2.5 FDP_ACF.1/VOLUME Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1/VOLUME Subset access control

FMT_MSA.3/VOLUME Static attribute initialization

FDP_ACF.1.1/VOLUME The TSF shall enforce the [Volume Access Control SFP] to objects based on the following: [

Subject attributes: World Wide Name

Objects: Volume ID, Volume World Wide Name]

FDP_ACF.1.2/VOLUME The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [An application server is allowed to read and write to a Volume if the Volume ID and Volume World Wide Name is mapped to the application server].

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

FDP_ACF.1.4/VOLUME The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [access is denied if the Volume is not mapped to the application server].

5.2.2.6 FDP_ACF.1/OBJECT Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1/OBJECT Subset access control

FMT_MSA.3/OBJECT Static attribute initialization

FDP_ACF.1.1/OBJECT The TSF shall enforce the [Object Storage Data Access Control SFP] to objects based on the following: [

Subject attributes: Username, Authentication status,

Objects: ACLs for each object]

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

A successful authenticate subject of the TOE is allowed to perform an operation if the content of the Access Control List for the object authorizes the Subject to perform the desired operation]**.**

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

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

5.2.2.7 FDP_ACF.1/USER Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1/USER Subset access control

FMT_MSA.3/USER Static attribute initialization

FDP_ACF.1.1/USER The TSF shall enforce the [Administrative User Access Control SFP] to objects based on the following: [

Subjects attributes: user password, user role ID;

Object attributes: permissions to execute the command]

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: [

a) Only authorized users are permitted to access to commands.

b) Users can be assigned with different role to control the TOE access permission.

c) There are 6 built-in roles (list in FMT_SMR.1.1).

d) Each role stands for a specified set of permissions.

e) Each command has it’s correspond permissions and the correspondence is defined by the software which cannot be changed.

f) Commands is allow to be accessed and executed by an account only if the permission set of the account’s role has the permissions match the commands correspond 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].

5.2.2.8 FDP_ACF.1/FILE Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1/FILE Subset access control

FMT_MSA.3/FILE Static attribute initialization

FDP_ACF.1.1/FILE The TSF shall enforce the [File Storage Data Access Control SFP] to objects based on the following: [

Subject attributes: UID, GID; Objects: rwx permissions]

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

A user perform the operations granted to their UID or GID according to the file or directory's rwx permissions]**.**

FDP_ACF.1.3/ FILE The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [An authorized administrator or super administrator has granted access for the client system on the export and share].

FDP_ACF.1.4/ FILE The TSF shall explicitly deny access of subjects to objects based on the

following additional rules :[

An authorized administrator or super administrator denies the client ip access to the export or share.]

5.2.3 Identification and Authentication (FIA)

5.2.3.1 FIA_ATD.1/USER User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_ATD.1.1/USER The TSF shall maintain the following list of security attributes belonging to individual users: [User Name, User Password, User Type, User Lock Status, User Role ID, Password Status, User Status, User Login Method]

Note:

If the user is a domain user, the User **Password and Password Status** attributes are not security attributes belong to the TOE because of the password of the user not maintained.

5.2.3.2 FIA_ATD.1/VOLUME User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_ATD.1.1/VOLUME The TSF shall maintain the following list of security attributes belonging to individual users: [Host World Wide Name, Volume ID].

5.2.3.3 FIA_ATD.1/OBJECT User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to

individual users: [Access Key ID，Secret Access Key]

5.2.3.4 FIA_ATD.1/FILE User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [FQDN, client IP Address, SUBNETWORK, NETGROUP].

5.2.3.5 FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

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.

5.2.3.6 FIA_UAU.5 Multiple Authentication Mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_UAU.5.1: The TSF shall provide [Local, Active Directory service] to support user authentication.

FIA_UAU.5.2: The TSF shall authenticate any user's claimed identity according to [authorized user-defined configuration and the external protocol’s rules]

5.2.3.7 FIA_UAU.6 Re-authenticating

Hierarchical to: No other components.

Dependencies: No dependencies

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

5.2.3.8 FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide [

a) Asterisks to represent password

b) “Claimned identity (User Name or User Password) is invalid.“ to represent authentication failure

] to the user while the authentication is in progress.

5.2.3.9 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

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

5.2.3.10 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

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

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

a) Lock the offending account for Temporary and set minutes from 3 to 2000, which can be configured by administrator

b) Lock the offending account for Permanent, which can be configured by an administrator.

c) Audit the event in the security log]

Note: In remote authentication mode, after the above authentication failures the domain users who are identified and authenticated by a remote LDAP server can't be locked by the TOE. The locking policy of domain users is set by the LDAP server, not the TOE.

5.2.3.11 FIA_USB.1 User-Subject Binding

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1: The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [User Name and User Role].

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: [attributes are bound to the user session upon successful login].

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: [attributes do not change during a user session].

5.2.3.12 FIA_SOS.2 TSF Generation of secrets

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_SOS.2.1: The TSF shall provide a mechanism to generate secrets that meet [the salt used in PBKDF2 is a 16-byte random number generated using the RAND_bytes function of the OpenSSL library].

FIA_SOS.2.2: The TSF shall be able to enforce the use of TSF generated secrets for [Administrative users login].

5.2.4 Security Management (FMT)

5.2.4.1 FMT_MSA.1/VOLUME Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1/VOLUME Subset access control or

FDP_IFC.1 Subset information flow control]

FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MSA.1.1 The TSF shall enforce the [Volume Access Control SFP] to restrict the ability to **query, modify, delete, [create]** the security attributes [defined in FIA_ATD.1/VOLUME] to the [Super administrator role, Administrator role, SAN resource administrator role, Machine-machine account role].

5.2.4.2 FMT_MSA.1/OBJECT Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1/OBJECT Subset access control or

FDP_IFC.1 Subset information flow control]

FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MSA.1.1 The TSF shall enforce the [Object Storage Data Access Control SFP] to restrict the ability to **query, modify, delete, [create]** the security attributes [defined in FIA_ATD.1/OBJECT] to the [Super administrator role, Administrator role].

5.2.4.3 FMT_MSA.1/FILE Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1/FILE Subset access control or

FDP_IFC.1 Subset information flow control]

FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MSA.1.1 The TSF shall enforce the [File Storage Data Access Control SFP] to restrict the ability to **query, modify, delete, [create]** the security attributes [defined in FIA_ATD.1/FILE] to the [Super administrator role, Administrator role, File or Directory owners].

5.2.4.4 FMT_MSA.1/USERa Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1/USER Subset access control or

FDP_IFC.1 Subset information flow control]

FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MSA.1.1 The TSF shall enforce the [Administrative User Access Control SFP] to restrict the ability to **query, modify, change_default, delete, [create]** the security attributes [all attributes identified in FIA_ATD.1/USER] to the [Super administrator role]**.**

5.2.4.5 FMT_MSA.1/USERb Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1/USER Subset access control or

FDP_IFC.1 Subset information flow control]

FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FMT_MSA.1.1 The TSF shall enforce the [Adminstrative User Access Control SFP] to restrict the ability to **modify** the security attributes [User Password] to the [all administrative users role].

5.2.4.7 FMT_MSA.3/VOLUME Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

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

FMT_MSA.3.2 The TSF shall allow the [Super administrator role, Administrator role, SAN resource administrator role, Machine-machine account role] to specify alternative initial values to override the default values when an object or information is created.

Application note: When creating a volume, set the default security attribute to prevent external application servers from accessing the volume. The application server can use the storage space of the volume only after the volume is mapped to the host or host group.

5.2.4.8 FMT_MSA.3/OBJECT Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [Object Storage Data Access Control SFP] to provide **permissive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [Super administrator role, Administrator role, *authorized account*] to specify alternative initial values to override the default values when an object or information is created.

Application note: permissive ACLs of object.

5.2.4.9 FMT_MSA.3/FILE Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [File Storage Data Access Control SFP] to provide **permissive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [Super administrator role, Administrator role, *authorized file owner*] to specify alternative initial values to override the default values when an object or information is created.

Application note: permissive FQDN, client IP Address, SUBNETWORK, NETGROU of NFS share.

5.2.4.10 FMT_MSA.3/USER Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [Administrative User Access Control SFP] to provide **permissive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [Super administrator role] to specify alternative initial values to override the default values when an object or information is created.

Application note: permissive of User Role of the administrative user.

5.2.4.11 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

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

[

a) Users and Roles management
b) Users Session Management
c) Security Policies and Access Control Management
d) Domain Authentication Management
e) Certificate Management
f) Audit and Alarm Management
g) Block Service Management, including logical host and host group management, Volume mapping, CHAP management;
h) Object Service Management
i) File Service Management
j) Time Setting

].

5.2.4.12 FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

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

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

Table 5-2 Role and Authority

Role	Authority
Super administrator	All permissions.

Role	Authority
Administrator	All permissions except user management, security management, and high-risk maintenance operations.
Security administrator	System security configuration permissions, including security policy configuration, access control, certificate management, KMC configuration, and time configuration.
SAN resource administrator	SAN resource management permissions, including management of storage pools, Volume and volume mappings, host and host group, ports, and background configuration tasks.
System viewer	Permission to query information and change the password of the account itself.
Machine-machine account	Has all permissions except session management and access control. A machine-machine account has the permission to view security policies.

5.2.5 Protection of the TSF (FPT)

5.2.5.1 FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [disk failures, node failures].

5.2.5.2 FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

5.2.6 Resource Utilization(FRU)

5.2.6.1 FRU_FLT.1 Degraded fault tolerance

Hierarchical to: No other components.

Dependencies: FPT_FLS.1 Failure with preservation of secure state

FRU_FLT.1.1 The TSF shall ensure the operation of [read and write operations] when the following failures occur: [loss of one node or one disk].

5.2.7 TOE access (FTA)

5.2.7.1 FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions

Hierarchical to: FTA_MCS.1 Basic limitation on multiple concurrent sessions.

Dependencies: FIA_UID.1 Timing of identification

FTA_MCS.2.1 The TSF shall restrict the only one session that belong to the same user according to the rules [“one session switch” of security policy attribute is enable]**.**

FTA_MCS.2.2 The TSF shall enforce, by default, a limit of [32] sessions per user.

5.2.7.2 FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [specific time (minutes from 30 to 100 which configured by administrator) interval of user inactivity].

5.2.7.3 FTA_TAH.1 TOE access history

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TAH.1.1 Upon successful session establishment, the TSF shall display the **date, time, location** of the last successful session establishment to the user**.**

FTA_TAH.1.2 Upon successful session establishment, the TSF shall display the **date, time, location** of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.

FTA_TAH.1.3 The TSF shall not erase the access history information from the user interface without giving the user an opportunity to review the information.

Note: TOE does not support the security functions defined in FTA_TAH.1.2.

5.2.7.4 FTA_TSE.1 TOE session establishment

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [Authentication failure, Source IP address, Login method, Max attempts due to authentication failure within certain period of time]

5.2.8 Cryptographic Support (FCS)

5.2.8.1 FCS_COP.1/SHA256 Cryptographic Operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction.

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

NOTE

SHA256 is used for integrity protection in TLS communication. And SHA256 is used for cryptographic algorithm PBKDF2.

5.2.8.2 FCS_COP.1/PBKDF2 Cryptographic Operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

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

NOTE

PBKDF2 is used for hashing passwords before storage in non-volatile memory. The salt used in PBKDF2 is a 16-byte random number obtained from the TOE's deterministic random number generator (defined in FIA_SOS.2).

5.3 Security Functional Requirements Rationale

5.3.1 Coverage

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

Table 5-3 Mapping SFRs to objectives

Objective	Security Functional Requirements	Rationale
O.Audit The TOE shall provide functionality to generate audit records for all configuration actions and shall provide ability to review audit records for authorized users.	FAU_GEN.1 Audit data generation	The requirement meets the objective by ensuring that the TOE generates audit records of security related events.
	FAU_GEN.2 User identity association	The requirement meets the objective by ensuring that the audit functionality is able to associate audit records with the identity of the user whose actions generate such records.
	FAU_SAR.1 Audit review	The requirement meets the objective by ensuring that all audit records can be reviewed by authorized administrative users in a suitable format.
	FAU_SAR.2 Restricted audit review	The requirement meets the objective by prohibiting all unauthorized users from accessing the audit records.
	FAU_SAR.3 Selectable audit review	The requirement meets the objective by ensuring that authorized users have access to the audit records.
	FAU_STG.1 Protected audit trail storage	The requirement meets the objective by ensuring that the audit trail is protected against accesses performed by unauthorized users.
	FAU_STG.3 Action in Case of Possible Audit Data Loss	The requirement meets the objective by ensuring that the audit trail is protected against loss.
	FAU_STG.4 Prevention of audit data loss	The requirement meets the objective by ensuring the audit record integrality.
	FPT_STM.1 Reliable time stamps	The requirement meets the objective by ensuring that all audit record are associated with a reliable timestamp
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that the TOE identified each user before any actions.

	FMT_SMF.1 Specification of Management Functions	The requirement meets the objective by ensuring that the TOE manages the audit configuration of servers.
O.Authentication The TOE must require each user/server/client 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 administrative user.
	FIA_ATD.1/VOLUME User attribute definition	The requirement meets the objective by ensuring that the TOE maintains security attributes for each application server.
	FIA_ATD.1/OBJECT User attribute definition	The requirement meets the objective by ensuring that the TOE maintains security attributes for each object account.
	FIA_ATD.1/FILE User attribute definition	The requirement meets the objective by ensuring that the TOE maintains security attributes for NFS account.
	FIA_UAU.2 User authentication before any action	The requirement meets the objective by ensuring that the TOE authenticated each user before any action
	FIA_UAU.5 Multiple authentication mechanisms	The requirement meets the objective by ensuring that TOE support Multiple authentication mechanisms for each user
	FIA_UAU.6 Re-authenticating	The requirement meets the objective by ensuring that the TOE need to Re-authenticating for Important Operations
	FIA_UAU.7 Protected authentication feedback	The requirement meets the objective by ensuring that the TOE Protected authentication feedback for each user
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that the TOE identified 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 handing Authentication failure for each user
	FIA_SOS.2 TSF Generation of secrets	The requirement meets the objective by ensuring that the TOE provide a mechanism to generate secrets.
	FMT_SMF.1Specification of Management Functions	The requirement meets the objective by ensuring that the TOE manages the authentication policy of servers or administrative 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_MCS.2 Per user attribute limitation on multiple concurrent sessions	The requirement meets the objective by ensuring that the TOE should restrict only one session that belong to an administrative user.
	FTA_TAH.1 TOE access history	The requirement meets the objective by ensuring that the TOE should display the last successful session establishment of the user**.**
	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 shall implement different authorization levels that can be assigned to administrators in order to restrict the functionality that is available to individual administrators	FDP_ACC.1/VOLUME Subset access control	The requirement meets the objective by ensuring that the TOE has an access control policy that ensures that only authorized servers can gain Block Service storage data from the TOE.
	FDP_ACC.1/OBJECT Subset access control	The requirement meets the objective by ensuring that the TOE has an access control policy that ensures that only authorized account or user can gain Object Service storage data from the TOE.
	FDP_ACC.1/FILE Subset access control	The requirement meets the objective by ensuring that the TOE has an access control policy that ensures that only authorized client can gain File Service storage data from the TOE.
	FDP_ACC.1/USER Subset access control	The requirement meets the objective by ensuring that the TOE has an access control policy that ensures that only authorized users can gain access to the TOE.
	FDP_ACF.1/VOLUME Security attribute based access control	The requirement meets the objective by ensuring that only authorized servers gain access to Block Service storage data protected by the TOE.
	FDP_ACF.1/OBJECT Security attribute based access control	The requirement meets the objective by ensuring that only authorized account or user gain access to Object Service storage data protected by the TOE.
	FDP_ACF.1/FILE Security attribute based access control	The requirement meets the objective by ensuring that only authorized clients gain

	access to File Service storage data protected by the TOE.
FDP_ACF.1/USER Security attribute based access control	The requirement meets the objective by ensuring that only authorized users gain access to the TOE.
FIA_ATD.1/USER User attribute definition	The requirement meets the objective by ensuring that the TOE maintains security attributes for each local user.
FIA_ATD.1/VOLUME User attribute definition	The requirement meets the objective by ensuring that the TOE maintains security attributes for each server.
FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that the TOE identified each user before any action.
FMT_MSA.1/VOLUME Management of security attributes	The requirement meets the objective by ensuring that the security attribute of Volumes in TOE can only be changed by authorized user.
FMT_MSA.1/USERa Management of security attributes	The requirement meets the objective by ensuring that the security attribute of users in TOE can only be changed by authorized user.
FMT_MSA.1/USERb Management of security attributes	The requirement meets the objective by ensuring that the security attribute of users in TOE can only be changed by authorized user.
FMT_MSA.3/VOLUME Static attribute initialization	The requirement meets the objective by ensuring that the default values for security attribute of Volumes in TOE should be provided and could be changed by authorized user.
FMT_MSA.3/OBJECT Static attribute initialization	The requirement meets the objective by ensuring that the default values for security attribute of object accounts or users in TOE should be provided and could be changed by authorized user.
FMT_MSA.3/USER Static attribute initialization	The requirement meets the objective by ensuring that the default values for security attribute of administrative users in TOE should be provided and could be changed by super administrator.
FMT_SMF.1 Specification of Management Functions	The requirement meets the objective by ensuring that the TOE manages the authentication policy of servers.
FMT_SMR.1 Security roles	The requirement meets the objective by ensuring that specific roles are defined to management of the TOE.

	FTA_SSL.3 TSF-initiated termination	The requirement meets the objective by ensuring that the interactive session should be terminated by TOE after a specific time.
O. SecurityManagement The TOE shall provide a method for authorized users 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_MSA.1/VOLUME Management of security attributes	The requirement meets the objective by ensuring that the security attribute of Volumes can be managed.
	FMT_MSA.1/OBJECT Management of security attributes	The requirement meets the objective by ensuring that the security attribute of object storage service can be managed.
	FMT_MSA.1/FILE Management of security attributes	The requirement meets the objective by ensuring that the security attribute of file storage service can be managed.
	FMT_MSA.1/USERa Management of security attributes	The requirement meets the objective by ensuring that the security attribute of administrative users can be managed.
	FMT_MSA.1/USERb Management of security attributes	The requirement meets the objective by ensuring that the security attribute of administrative users can be managed.
	FMT_MSA.3/VOLUME Static attribute initialization	The requirement meets the objective by ensuring that the default values for security attribute of Volumes in TOE can be managed.
	FMT_MSA.3/OBJECT Static attribute initialization	The requirement meets the objective by ensuring that the default values for security attribute of object in TOE can be managed.
	FMT_MSA.3/FILE Static attribute initialization	The requirement meets the objective by ensuring that the default values for security attribute of file share in TOE can be managed.
	FMT_MSA.3/USER Static attribute initialization	The requirement meets the objective by ensuring that the default values for security attribute of administrative users in TOE can be managed.
	FMT_SMF.1Specification of Management Functions	The requirement meets the objective by ensuring that the TOE manage the authentication policy of servers.
	FMT_SMR.1 Security roles	The requirement meets the objective by ensuring that the TOE manage the administrative users and roles

	FTA_SSL.3 TSF-initiated termination	The requirement meets the objective by ensuring that the interactive session can be managed.
O.DataProtection The TOE shall provide fouction to reconstructe user data when nodes or disks are damaged within a certain proportion.	FPT_FLS.1 Failure with preservation of secure state	The requirement meets the objective by ensuring that user data can be reconstructed from erasure coded data in order to keep user data availability when nodes or disks are damaged within a certain proportion.
	FRU_FLT.1 Degraded fault tolerance	The requirement meets the objective by ensuring that reading and writing operations can be normally provided when nodes or disks are damaged within a certain proportion.

5.3.2 Security Requirements Dependency Rationale

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

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

Table 5-4 Functional Requirements Dependencies

Security Fynctional Requirement	Dependency	Resolution
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.2
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.3	FAU_STG.1	FAU_STG.1
FAU_STG.4	FAU_STG.1	FAU_STG.1
FDP_ACC.1/VOLUME	FDP_ACF.1	FDP_ACF.1/VOLUME
FDP_ACC.1/OBJECT	FDP_ACF.1	FDP_ACF.1/ OBJECT
FDP_ACC.1/FILE	FDP_ACF.1	FDP_ACF.1/ FILE

Security Fynctional Requirement	Dependency	Resolution
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FDP_ACC.1/USER	FDP_ACF.1	FDP_ACF.1/USER
FDP_ACF.1/VOLUME	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/VOLUME FMT_MSA.3/VOLUME
FDP_ACF.1/OBJECT	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/OBJECT FMT_MSA.3/OBJECT
FDP_ACF.1/USER	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/USER FMT_MSA.3/USER
FDP_ACF.1/FILE	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/FILE FMT_MSA.3/FILE
FIA_ATD.1/VOLUME	NA	NA
FIA_ATD.1/USER	NA	NA
FIA_ATD.1/OBJECT	NA	NA
FIA_ATD.1/FILE	NA	NA
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UAU.5	NA	NA
FIA_UAU.6	NA	NA
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2
FIA_UID.2	NA	NA
FIA_USB.1	FIA_ATD.1	FIA_ATD.1/USER
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_SOS.2	NA	NA
FMT_MSA.1/VOLUME	FDP_ACC.1 FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	FDP_ACC.1/VOLUME FMT_SMR.1 FMT_SMF.1
FMT_MSA.1/OBJECT	FDP_ACC.1 FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	FDP_ACC.1/ OBJECT FMT_SMR.1 FMT_SMF.1

Security Fynctional Requirement	Dependency	Resolution
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FMT_MSA.1/FILE	FDP_ACC.1 FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	FDP_ACC.1/ FILE FMT_SMR.1 FMT_SMF.1
FMT_MSA.1/USERa	FDP_ACC.1 FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	FDP_ACC.1/USER FMT_SMR.1 FMT_SMF.1
FMT_MSA.1/ USERb	FDP_ACC.1 FDP_IFC.1FMT_SMR.1 FMT_SMF.	FDP_ACC.1/USER FMT_SMR.1 FMT_SMF.1
FMT_MSA.3/VOLUME	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/ VOLUME FMT_SMR.1
FMT_MSA.3/OBJECT	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/ OBJECT FMT_SMR.1
FMT_MSA.3/FILE	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/ FILE FMT_SMR.1
FMT_MSA.3/USER	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/USERa FMT_MSA.1/USERb FMT_SMR.1
FMT_SMF.1	NA	NA
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_FLS.1	NA	NA
FPT_STM.1	NA	NA
FRU_FLT.1	FPT_FLS.1	FPT_FLS.1
FTA_MCS.2	FIA_UID.1	FIA_UID.2
FTA_SSL.3	NA	NA
FTA_TAH.1	NA	NA
FTA_TSE.1	NA	NA
FCS_COP.1/SHA256	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Unsupported: FCS_CKM.1, FCS_CKM.4

Security Fynctional Requirement	Dependency	Resolution
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FCS_COP.1/PBKDF2	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Unsupported: FCS_CKM.1, FCS_CKM.4

NOTE

Rationale for Unsatisfied Dependencies:

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

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

5.4 Security Assurance Requirements

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

Table 5-5 TOE Security Assurance Requirements

Assurance Class	Assurance components
Class ADV: Development	ADV_ARC.1
	ADV_FSP.3
	ADV_TDS.2
Class AGD: Guidance documents	AGD_OPE.1
	AGD_PRE.1
Class ALC : Life Cycle Support	ALC_CMC.3
	ALC_CMS.3
	ALC_DEL.1 ALC_FLR.2
	ALC_DVS.1
	ALC_LCD.1
Class ASE: Security Target evaluation	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2

	ASE_SPD.1
	ASE_TSS.1
Class ATE: Tests	ATE_COV.2
	ATE_DPT.1
	ATE_FUN.1
	ATE_IND.2
Class AVA: Vulnerability assessment	AVA_VAN.2

5.5 Security Assurance Requirements Rationale

EAL3+ALC_FLR.2 has been chosen commensurate with the threat environment that is experienced by typical consumers of the TOE.

6 TOE Summary Specification

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

6.1 Identification and Authentication

The purpose of authentication and identification is to make sure the specified user can access TOE only when TOE recognizes it as the right account by verifying the identities.

1. The TOE supports authentication and identification to two kinds of users: Administrative Users and Data Users.

- The Administrative User is the account which will manage or configure the TOE's functions including but not limited to security functions.
- The Data User is the subject which will access the data stored in TOE through standard IO protocols.

2. To Administrative Users, the TOE provides local and remote authentication mode.

- In local authentication mode, the identities of the user is stored locally in TOE. The identification factors include the password, and one time password (OTP) sent through email. .

1) The type of a user's identities can be chosen by another user whose role contains the proper permissions.
2) 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.
3) 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 identities of the user is stored locally in a remote LDAP server (means a server obey standard LDAP protocol, such as AD server, OpenLDAP server).

1) The LDAP server's essential information (includes IP address, port, and protocol) is configured by a user whose role has the proper permissions.
2) In this type of identification, the TOE act as an LDAP client, the inputted user name and password is forwarded to the LDAP server through standard LDAP protocol and is verified by the LDAP server.

3. Authentication occurs not only in logging into the TOE, but also in executing some vital commands such as rebooting or powering off the TOE, initializing the user's password, unlocking a user, and clearing or importing configuration data. This is called re-authentication.

4. The input password is presented as asterisks and no mater any reason the authentication or re-authentication fails with, the TOE will only give a blurry feedback to prevent from brute-force cracking. In addition, after the authentication or re-authentication failure, the failure count is record in the TOE. After N consecutive authentication failures during 5 minutes, the account will be locked for M minutes, in which N stands for a positive integer from 1 to 9 and M stands for 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.

Note: In remote authentication mode, after the above authentication failures the domain users who are identified and authenticated by a remote LDAP server can't be locked. The locking policy of domain users is set by the LDAP server, not the TOE.

5. After a successful identification, a session will be create to stands 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 name, user role and other security attributes will assigned to the session. A session will be terminated if it's inactive up to N minutes, in which N is a positive number from 30 to 100 and is configured by Administrative users with proper permissions.

6. 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 (Volume). The Data User (application server which holds the initiator) whose initiator is in the mapping pre-configured in the TOE has rights to access the data (i.e. Volume) on the TOE. Furthermore, if CHAP authentication is enabled, the target Volume on the TOE can be accessed only when CHAP authentication is passed. All these above are similar to other SAN protocols.

7. The Administrative User with proper permissions can configure object account, bucket and user. The account can configure user ACL by S3 RESTful interface. The object account or user (which holds AK and SK) whose AK and SK is pre-configured in TOE has rights to access the object data (i.e.) in TOE.

8. NFS can set the authentication mode for each shared directory. The following authentication modes are supported:

i. FQDN: Fully qualified domain name, only the client IP address that belongs to the FQDN can access the shared directory. NFS clients and TOE must be added to the NIS or LDAP domain.
ii. IPADDR: Only the configured client IP address can access the shared directory.
iii. SUBNETWORK: Only the client IP address that belongs to the subnet can access the shared directory.
iv. NETGROUP: Only the client IP address that belongs to the NETGROUP can access the shared directory. NFS clients and TOE s must be added to the NIS or LDAP domain.
v. ANONYMOUS: Any client can access the shared directory.

Each authentication mode supports two types of access rights: Read-write or read-only.

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

6.2 Authorization

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

The TOE implements authorization according to core RBAC model modified slightly. The key points of the implementation of the core RBAC model is 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 TOE. A user can execute a command only if the user’s permission list contains the command's permission.
- A set of permissions composes a role. The TOE support 6 built-in roles which cannot be modify or delete.
- Only one role can be assigned to a user. The assignment can be done during the creation or modification of a user.
- A user is authorized to perform certain operations and is forbidden to perform certain operations, this is achieved by comparing the permissions held by the account's assigned role and the permissions of the commands which bearing the operations.

Table 6-1 Role permission definition

Role	Authority
Super administrator	All permissions.
Administrator	All permissions except user management, security management, and high-risk maintenance operations.
Security administrator	System security configuration permissions, including security policy configuration, access control, certificate management, KMC configuration, and time configuration.
SAN resource administrator	SAN resource management permissions, including management of storage pools, Volumes, mappings, hosts, Initiator, CHAP, iSCSI service.
System viewer	Permission to query information and change the password of the account itself.
Machine-machine account	Has all permissions except session management and access control. A machine-machine account has the permission to view security policies.

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

6.3 Access Control

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

The TOE supports two Access Control mechanisms for Administrative Users:

- IP White List is configured globally to limit access from IP addresses out of the list. The elements of the list are single IP addresses or ranges.
- Login Method is a list including CLI, DeviceManager, and RESTful. A user can access the TOE only using the method included in this list configured for the user by other proper Administrative Users

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

6.4 Auditing

The TOE provides an audit trail for all essential operations.

1. All non-query operations will be recorded in the operations logs. Typically these operations include login, logout, configuration change, user management and security settings.

2. An audit record is composed of 6 basic information: who (user name), where (user IP address), when (a corresponding timestamp), what (the operation description), result (success or specific error code), ID (an unique number of this record).

3. Review functionality is provided via the CLI and GUI interface, which allows Administrative Users to inspect the audit log. Administrative Users whose role has proper permissions can query or fetch the audit trail.

4. All audit trails are stored locally in TOE's persistent media.

5. If an FTP/SFTP server to dump audit records is configured and enabled, once a periodic dump task is polled and the number of records exceeds 50000 or more, at least 10000 oldest audit records which type is operation log will be dumped to the FTP/SFTP server. If such a FTP/SFTP server is not configured or enabled, once a periodic audit management task is polled and the number of records exceeds 50000 or more, at least 10000 oldest audit records which type is operation log are discard for storing new audit logs..

6. If the Alarm notification (Syslog) is enabled and successfully configured, the TOE will automatically send audit logs to specified servers in real time.

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

6.5 Security Management

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

1. The TOE's mainly security functions includes:

- Users and Role Management, including user password, user lock status, user's role and other credentials.
- Security Policies Management, including Username Policy, Password Policy, Password Validity, Login Policy, user lock policy.
- Access control Management, including IP Address and Address Segment List.

- Users sessions Management
- Domain Authentication Management
- Time Settings Management, including NTP and Time Zone.
- Certificate Management
- Alarm and Audit Management, including Alarm Dump, Alarm Severity, Alarm Masking, Alarm Notification (Syslog)
- Block Service Management, including Host, Host Group, Volume, mapping views, iSCSI Service.
- File Service Management, including Share and File System
- Object Service Management, including Account, DNS, Service Network, Global Namespace

2. Every security management function has corresponding permissions. Administrative Users whose role has proper permissions is permitted to manage the corresponding security functions.

TOE Security Functional Requirements Satisfied: (FMT_MSA.1/VOLUME, FMT_MSA.1/OBJECT, FMT_MSA.1/FILE, FMT_MSA.1/USERa, FMT_MSA.1/USERb, FMT_MSA.3/VOLUME, FMT_MSA.3/OBJECT, FMT_MSA.3/FILE, FMT_MSA.3/USER, FMT_SMF.1, FMT_SMR.1, FPT_STM.1).

6.6 User Data Protection

For Block Service, application servers are only permitted to access volumes for which a mapping has been explicitly configured.

For Object Service, the TOE controls access to object data via user policy (i.e. ACL) and bucket policy. Authorized administrators may create an account and obtain its AK and SK, and can create buckets, users and user policies (ACL). This ACL grant user permissions to access the bucket resources. The bucket policy controls one or multiple users' or accounts' permission to access buckets or bucket objects. A bucket policy applies to both accounts and users.

For File Service, the TOE uses the UNIX rwx model to control directory permissions for file data access.

TOE Security Functional Requirements Satisfied: (FDP_ACC.1/VOLUME, FDP_ACC.1/OBJECT, FDP_ACC.1/FILE, FDP_ACF.1/VOLUME, FDP_ACF.1/ OBJECT, FDP_ACF.1/ FILE).

6.7 Protection of the TSF

The TOE protects user data against disk and node failure.

For the main storage disk/cache disk, the system performs periodic detection on the disk, based on the detection results of key indicators, the slow disk/failed disk is identified, the system actively sends an alarm, and automatically isolates the disk in the background and triggers data reconstruction.

The TOE detects node failures through a heartbeat mechanism. When a node failure is detected (such as operating system reset, CPU failure), it will trigger node failover and switch the services carried on it to other normal nodes. To ensure that the failure within the redundancy range of the system design does not affect the availability of the storage system.

The TOE also includes a sys clock, which provides the TOE with a reliable timestamp. The system performs the synchronization of ACLs, logs, and user data to ensure inter-TSF data consistency.

TOE Security Functional Requirements Satisfied: (FPT_FLS.1, FPT_STM.1).

6.8 Resource Utilization

The storage system protects data against failures using the multi-copy mechanism or erasure coding (EC). Data can be properly accessed even if a limited number of physical devices in the storage system become faulty, and data on the faulty devices will be automatically restored. The number of disks and nodes that can be lost while still maintaining read and write functionality is dependent upon the number of disks and nodes implemented.

- **Multi-copy Mechanism**

The storage system supports two or three copies. Table 6-2 details the Multi-copy mode.

1. When a piece of data is written, the storage system generates two copies for the data.

2. The storage system writes the data and its copies into three storage nodes separately.

Table 6-2 Multi-copy modes

Mode	Description	Minimum Number of Nodes
Two copies	One copy is created for each piece of data. Data integrity will not be compromised when one storage node (server-level security) or cabinet (cabinet-level security) is faulty.	3 (NOTE1)
Three copies	Two copies are created for each piece of data. Data integrity will not be compromised when two storage nodes (server-level security) or cabinets (cabinet-level security) are faulty.	3

NOTE 1: The Minimum number of Nodes is 3 because less than 3 nodes cannot promise all the functions work well. This minimum number doesn't depend on the number of copies.

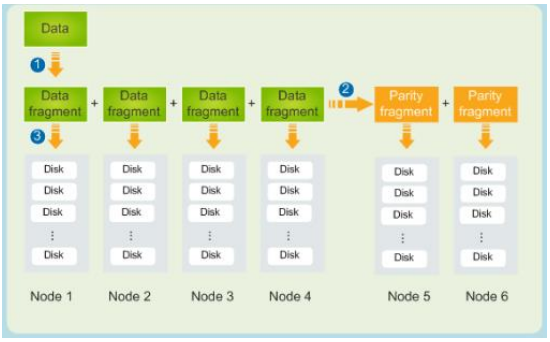
- **EC**

EC schemes are expressed in N+M mode. N indicates the number of data fragments (data strips) and M indicates the number of parity fragments (parity strips). The storage system supports N+2, N+3, and N+4 EC schemes. Table 6-3 details the EC schemes.

Figure 6-3 shows how data protection is implemented when the number of storage nodes is greater than or equal to N+2.

When the number of storage nodes is greater than or equal to (N+2)/2 and less than N+2, the following uses three storage nodes configured with 4+2 as an example to describe the basic principles.

Figure 6-3 Data protection in the 4+2 EC scheme



1. Divides data into four data fragments.
2. Groups the four data fragments and calculates two parity fragments.
3. Writes the data and parity fragments into six storage nodes.

Table 6-3 EC schemes

Mode	Description	Minimum Number of Nodes
N+2	Node-level security If the number of nodes is greater than or equal to (N+2)/2 (rounded up) and less than N+2, the system can tolerate the failure of one storage node or two main storage disks at a time. If the number of nodes is greater than or equal to N+2, the system can tolerate the failure of two storage nodes or two main storage disks at the same time. Cabinet-level security If the number of cabinets is greater than or equal to (N+2)/2 (rounded up) and less than N+2, the system can tolerate the failure of one cabinet or two storage nodes at a time. If the number of cabinets is greater than or equal to N+2, the system can tolerate the failure of two cabinets or storage nodes at a time. N can be 4, 6, 8, 10, 12, 14, 16, 18, 20, or 22.	Node-level security Minimum number of nodes: (N+2)/2 rounded up Cabinet-level security Minimum number of cabinets: (N+2)/2 rounded up
N+3	Node-level security If the number of nodes is greater than or equal to (N+3)/3 (rounded up) and less than N+3, the system can tolerate the failure of one storage node or three main storage disks at a time. N can be 6, 8, 12, 14, 18, or 20. If the number of nodes is greater than or equal to N+3, the system can tolerate the failure of three storage nodes or main storage disks at a time. N can be 6, 8, 10, 12, 14, 16, 18, or 20. Cabinet-level security If the number of cabinets is greater than or equal to (N+3)/3 (rounded up) and less than N+3, the system can tolerate the failure of one cabinet or three storage nodes at a time. N can be 6, 8, 12, 14, 18, or 20. If the number of cabinets is greater than or equal to N+3, the system	Node-level security Minimum number of nodes: (N+3)/3 rounded up Cabinet-level security Minimum number of cabinets: (N+3)/3 rounded up

Mode	Description	Minimum Number of Nodes
	can tolerate the failure of three cabinets or three storage nodes at a time. N can be 6, 8, 10, 12, 14, 16, 18, or 20.	
N+4	Node-level security If the number of nodes is greater than or equal to (N+4)/4 (rounded up) and less than N+4, the system can tolerate the failure of one storage node or four main storage disks at a time. N can be 8, 12, 16, or 20. If the number of nodes is greater than or equal to N+4, the system can tolerate the failure of four storage nodes or main storage disks at a time. N can be 8, 10, 12, 14, 16, 18, or 20. Cabinet-level security If the number of cabinets is greater than or equal to (N+4)/4 (rounded up) and less than N+4, the system can tolerate the failure of one cabinet or four storage nodes at a time. N can be 8, 12, 16, or 20. If the number of cabinets is greater than or equal to N+4, the system can tolerate the failure of four cabinets or four storage nodes at a time. N can be 8, 10, 12, 14, 16, 18, or 20.	Node-level security Minimum number of nodes: (N+4)/4 rounded up Cabinet-level security Minimum number of cabinets: (N+4)/4 rounded up
Note 1: An EC scheme is expressed in the format of N+M, wherein: N indicates the number of data fragments. M indicates the number of parity fragments. Note 2: In the same scheme, a larger N indicates a higher disk utilization. Note 3: The TOE storage system provides support for flexible data layout strategies, including node-level security layout and cabinet-level security layout. Note 4: A node means a server, a cabinet means a group of servers placing on the Cabinet. • Node-level security layout Distribute the data and its redundancy to different nodes. As long as the number of failed nodes is less than or equal to the number of redundant nodes at the same time, the data can be automatically restored without interruption of business and without loss of data. • Cabinet-level security layout Distribute the data and its redundancy to different cabinets. As long as the number of failed cabinets is less than or equal to the number of redundant cabinets, the data can be automatically restored without interruption of business or loss of data.		

TOE Security Functional Requirements Satisfied: (FRU_FLT.1).

6.9 TOE Access

- TOE must restrict the maximum number of concurrent sessions (32) that belong to the same user or the TOE system. The super administrator can obtain a session when TOE system has reached the maximum number of sessions (32).
- An administrator user can only obtain one session when the attribute of security policies **one session switch** is enabled.
- Within a specified period (the value ranges from 30 to 100 minutes and the default value is 30 minutes). If no operation is performed on the session, TOE will destroy the session.

Once the session is destroyed, TOE must be re-authenticated to obtain the access permission.

- The super administrator can forcibly destroy sessions of non-super administrators to release session resources.
- If the number of incorrect password inputs exceeds the upper limit, accounts will be locked. The super administrator will be automatically unlocked after being locked for 15 minutes. A non-super administrator is automatically unlocked after a specified period of time (the value ranges from 3 to 2000 minutes and the default value is 15 minutes).
- A system account will be locked if it has not been used for logging in to the system for a specified period of time (the value ranges from 1 to 999 days and the default value is 60 days).
- If the identification is successful, information about the last successful login (including the IP address, date and time) will be displayed. This function can be enabled or disabled by proper administrative users.

TOE Security Functional Requirements Satisfied: (FTA_MCS.2, FTA_SSL.3, FTA_TAH.1, FTA_TSE.1).

7 Acronyms and Terms

This section, Table 7-1, and Table 7-2 define the acronyms and terms used throughout this document.

7.1 Acronyms

Table 7-1 Acronyms

Acronym	Definition
ACL	Access Control List
AD	Active Directory
AK	Access Key
API	Application Programming Interface
CHAP	Challenge-Handshake Authentication Protocol
CLI	Command Line Interface
EAL	Evaluation Assurance Level
EC	Erasure Coding
FTP	File Transfer Protocol
GID	Group Identifier

GUI	Graphical User Interface
ID	Identifier
IP	Internet Protocol
iSCSI	Internet Small Computer System Interface
KMC	Key Management Component
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
NAS	Network-Attached Storage
NFS	Network File System
NIS	Network Information Service
NTP	Network Time Protocol
OAM	Operation Administration and Maintenance
OBS	Object Storage Service
OS	Operating System
PBKDF2	Password-Based Key Derivation Function
SFTP	Secure File Transfer Protocol
SAN	Storage Area Network
SID	Security Identifier
SK	Secret Access Key
SMB	Server Message Block
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
UID	User Identifier
WWN	World Wide Name

7.2 Terminology

Table 7-2 Terms

Term	Definition
rwx permissions	Unix permission flags of read, write, and execute