

Huawei Enterprise Storage Operations & Maintenance (O&M) Technical White Paper

Issue 01
Date 2017-06-06

Copyright © Huawei Technologies Co., Ltd. 2017 All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



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

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

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: <http://e.huawei.com>

Email: support@huawei.com

Contents

1 Overview.....	1
1.1 Overview of Huawei Enterprise Storage O&M System	1
1.2 Components of Huawei Enterprise Storage O&M System.....	1
2 Easy Delivery	3
2.1 Overview	3
2.2 Automated Compatibility Evaluation	3
2.2.1 Background.....	3
2.2.2 Specific Solution and Feature Description.....	3
2.2.3 Specifications.....	5
2.3 Visualized Plan and Design	5
2.3.1 Background.....	5
2.3.2 Specific Solution and Feature Description.....	5
2.3.3 Specifications.....	6
2.4 One-Click Configuration Import.....	7
2.4.1 Background.....	7
2.4.2 Specific Solution and Feature Description.....	7
2.4.3 Specifications.....	7
2.5 Automatic Cable Detection	7
2.5.1 Background.....	7
2.5.2 Specific Solution and Feature Description.....	7
2.5.3 Specifications.....	8
2.6 Data Migration.....	8
2.6.1 Background.....	8
2.6.2 Specific Solution and Feature Description.....	8
2.6.3 Specifications.....	11
2.7 One-click Device Archive Collection	12
2.7.1 Background.....	12
2.7.2 Specific Solution and Feature Description.....	12
2.7.3 Specifications.....	14
2.8 SmartConfig.....	15
2.8.1 Introduction.....	15
2.8.2 Function Features.....	15

2.8.3 Specifications.....	15
2.9 DeviceManager.....	16
2.9.1 Introduction.....	16
2.9.2 Function Features.....	17
2.9.3 Specifications.....	17
2.10 DJ.....	18
2.10.1 Introduction.....	18
2.10.2 Function Features.....	20
2.10.3 Specifications.....	22
3 Routine Maintenance	23
3.1 Overview	23
3.2 One-click Device Health Check.....	23
3.2.1 Background.....	23
3.2.2 Specific Solution and Feature Description.....	23
3.2.2.2 Scheduled Task	25
3.2.2.3 Remote Inspection	27
3.2.3 Specifications.....	27
3.3 Performance Statistics and Optimization.....	27
3.3.1 Background.....	27
3.3.2 Feature Description.....	28
3.3.3 Specifications.....	28
4 Troubleshooting	29
4.1 Overview	29
4.2 Hardware Fault Prediction.....	29
4.2.1 Background.....	29
4.2.2 Specific Solution and Feature Description.....	29
4.2.3 Specifications.....	30
4.3 Fault Detection.....	30
4.3.1 Background.....	30
4.3.2 Specific Solution and Feature Description.....	30
4.3.3 Specifications.....	31
4.4 Call Home.....	32
4.4.1 Background.....	32
4.4.2 Specific Solution and Feature Description.....	32
4.4.3 Specifications.....	32
4.5 One-click Fault Data Collection	32
4.5.1 Background.....	32
4.5.2 Specific Solution and Feature Description.....	33
4.5.3 Specifications.....	33
4.6 End-to-End Visual Fault Management.....	34
4.6.1 Background.....	34

4.6.2 Specific Solution and Feature Description.....	34
4.6.3 Specifications.....	36
4.7 Intelligent Fault Analysis System	37
4.7.1 Background.....	37
4.7.2 Specific Solution and Feature Description.....	37
4.7.3 Specifications.....	37
4.8 Remote Access.....	38
4.8.1 Background.....	38
4.8.2 Specific Solution and Feature Description.....	38
4.8.3 Specifications.....	38
4.9 Metadata Recovery	38
4.9.1 Background.....	38
4.9.2 Specific Solution and Feature Description.....	38
4.9.3 Specifications.....	40
4.10 FRU/CRU Replacement	40
4.10.1 Background.....	40
4.10.2 Specific Solution and Feature Description.....	40
4.10.3 Specifications.....	41
4.11 Backup and Recovery Configuration	41
4.11.1 Background.....	41
4.11.2 Specific Solution and Feature Description.....	41
4.11.3 Specifications.....	41
5 Upgrade and Capacity Expansion.....	43
5.1 Overview	43
5.2 Upgrade	43
5.2.1 Background.....	43
5.2.2 Specific Solution and Feature Description.....	43
5.2.3 Specifications.....	45
5.3 Capacity Expansion	45
5.3.1 Background.....	45
5.3.2 Specific Solution and Feature Description.....	45
5.3.3 Specifications.....	48
6 Disaster Recovery and Backup.....	49
6.1 BCManager eBackup.....	49
6.1.1 Introduction.....	49
6.1.2 Function Features.....	50
6.1.3 Specifications.....	51
6.2 BCManager eReplication.....	51
6.2.1 Introduction.....	51
6.2.2 Function Features.....	51
6.2.3 Specifications.....	52

7 Interfaces and the Ecosystem.....	54
7.1 Overview	54
7.2 CLI.....	54
7.2.1 Introduction.....	54
7.2.2 Function Features.....	54
7.2.3 Specifications.....	55
7.3 SNMP	56
7.3.1 Introduction.....	56
7.3.2 Function Features.....	56
7.3.3 Specifications.....	57
7.4 REST	58
7.4.1 Introduction.....	58
7.4.2 Function Features.....	58
7.4.3 Specifications.....	59
7.5 syslog.....	59
7.5.1 Introduction.....	59
7.5.2 Function Features.....	59
7.5.3 Specifications.....	59
7.6 SMIS.....	59
7.6.1 Introduction.....	59
7.6.2 Function Features.....	59
7.6.3 Specifications.....	62
7.7 OpenStack.....	62
7.7.1 Introduction.....	62
7.7.2 Function Features.....	62
7.7.3 Specifications.....	66
7.8 Easy to Be Integrated.....	66
7.8.1 Introduction.....	66
7.8.2 Function Features.....	66
7.8.3 Specifications.....	67
A Acronyms and Abbreviations.....	69

1 Overview

1.1 Overview of Huawei Enterprise Storage O&M System

Enterprise storage operation and maintenance (O&M) scenarios are as follows:

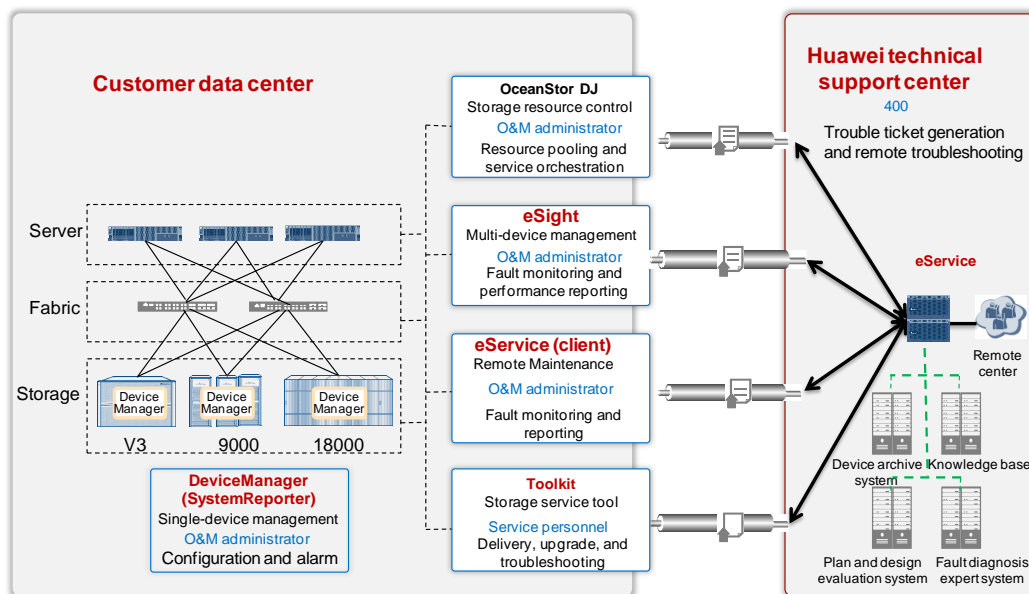
- Delivery scenario: engineering survey, planning and design, soft and hard installation, service commissioning, data migration, acceptance, and training
- Maintenance scenario: fault report, troubleshooting, and parts replacement, patch upgrade, maintenance prevention, and service optimization.

Enterprise storage products include: OceanStor V3 series、OceanStor V5 series、OceanStor F V5 series、OceanStor Dorado V3 series storage.

In general, the O&M system of enterprise storage is constructed in the product level, data center level, and cloud level. The three-level O&M system simplifies operations and improves operation efficiency, thereby reducing operating expense (OPEX).

1.2 Components of Huawei Enterprise Storage O&M System

The following figure shows the components of the enterprise storage O&M system.



The system contains the following components:

- **DeviceManager:** single-device O&M software
- **SystemReporter:** collects performance statistics of a single device.
- **Toolkit:** professional toolkit intended for Huawei technical support engineers. It includes a collection of tools for compatibility assessment, plan and design, one-click fault information collection, preventive maintenance inspection, upgrade, and field replaceable unit (FRU) replacement.
- **eSight:** multi-device maintenance suite provided for customers. It allows fault monitoring and visualized O&M.
- **DJ:** intended for customers. It offers unified management of storage resources, service catalog orchestration, on-demand supply of storage services and data application services.
- **eService client:** deployed on a customer's equipment room. It can discover exceptions of storage devices in real time and report them to Huawei maintenance center.
- **eService:** deployed on the Huawei maintenance center. It monitors devices in the network in real time and changes passive maintenance to active maintenance, or even implements maintenance for customers.

2 Easy Delivery

2.1 Overview

A delivery process involves the stages of engineering survey, plan and design, and delivery implementation. This section describes tools and management software used in device delivery, data migration, and disaster recovery and backup projects.

2.2 Automated Compatibility Evaluation

2.2.1 Background

Before a storage array upgrade, host information needs to be collected upgrade risks need to be evaluated. However, manual evaluation is inefficient and not performed in a timely manner, thereby blocking on-site maintenance personnel in performing upgrade tasks and deteriorating upgrade efficiency and quality.

2.2.2 Specific Solution and Feature Description

The compatibility evaluation system is easy to use, efficient, accurate, and flexible. It provides a platform for automatically analyzing host information collected by the InfoGrab tool. In the compatibility automatic evaluation, the InfoGrab host information collection package is imported and the compatibility evaluation report is exported.

Easy-to-use: easy to upload InfoGrab host information collection package; one-click startup of automatic compatibility evaluation

Efficient: For a large number of evaluation tasks, the compatibility evaluation system allows concurrent evaluation.

Accurate: The evaluation results are correct because the compatibility evaluation system evaluates each item by following the evaluation rule provided by each service field where the item belongs.

Flexible: Compatibility evaluation rules are dynamically expandable to meet different service requirements.

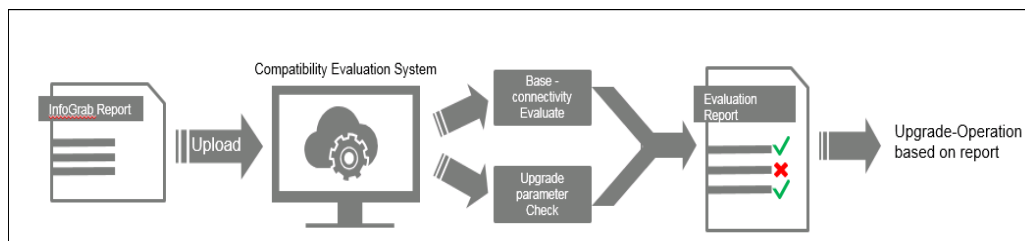


Table 2-1 lists the evaluation rules of the compatibility evaluation system.

Table 2-1 Evaluation rules of the compatibility evaluation system

Evaluation Item	Feature Evaluation	Details
Basic compatibility	Check basic host connectivity.	Basic host connectivity
	Check cluster software features.	Cluster software feature
	Check switch features.	Switch feature
Upgrade-related items	Check HBA timeout duration.	Check the HBA timeout duration in a Fibre Channel network environment where UltraPath for Linux is used.
		Check the timeout duration in an iSCSI network environment where UltraPath for Linux is used.
		Set HBA attributes in a Fibre Channel network environment where UltraPath for AIX is used.
		Check the HBA timeout duration in a Fibre Channel network environment where UltraPath for Windows is used.
		Check the initiator timeout duration in an iSCSI network environment where UltraPath for Windows is used.
	Check host multipathing status.	Check the path status of a Linux host.
		Check the path status of a Solaris host.
		Check the path status of an AIX host.
		Check the path status of an HP-UX host.
		Check the path status of a VMware host.
	Check the path status of a Windows host.	
Check Oracle timeout parameters.	Check Oracle database timeout parameters.	

Tool to get the address:

Offline version: <http://support.huawei.com/onlinetoolsweb/itexpress/itvd/cn.html>

Online version: <http://eservice-lld.huawei.com:8080/#/lld/overview>

2.2.3 Specifications

Information packages collected by InfoGrab in ToolBox V1R1C00RC2 and later support compatibility evaluation.

2.3 Visualized Plan and Design

2.3.1 Background

As the unified storage market is booming, labors are mainly invested into the following aspects during the project delivery: plan and design, software installation and commissioning, and acceptance. To better understand challenges facing Huawei field service personnel/ASP/CSP in project plans and design, we made a survey with the results shown in the following:

1. No end-to-end plan and design solution is prepared for field users, and they only use their experience and the existing single-end guide to complete project planning.
2. Storage planning is time-consuming and tools or processes for guiding the storage planning are needed.
3. In configuring storage, tools are required to provide automated batch configurations to improve efficiency.



High communication costs for project information exchange



Long project design time due to a large amount of documents



Time- and labor-consuming and error-prone massive configurations



Complex logic in network planning



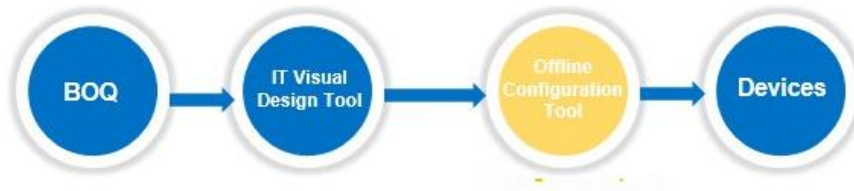
How can we help field users to plan projects quickly, efficiently, and correctly?

2.3.2 Specific Solution and Feature Description

Use tools to provide easy delivery for field personnel, helping them rapidly plan project information and configurations.

The visualized design tool provides "Visual display, high efficiency, anti-misoperations, export of the project LLD by one click." You do not need to fill in the complicated low level design (LLD) template.

You can use tool wizards to generate the following by one click: networking diagram, cabinet layout, equipment connection diagram, and switch zone planning. With a few manual modifications (filling in port IP addresses and storage service planning), end-to-end LLD files and offline configuration scripts are generated, reducing project planning duration to less than two hours.



Visual display, high efficiency, anti-misoperations, export of the project LLD by one click; no need to fill in the LLD template manually

- Visualized LLD: provides a visualized LLD tool for field users in storage project planning.
- End-to-end: provides end-to-end guidance in planning project information such as network cabling, equipment layout, and storage service planning.
- Anti-misoperation design: The tool's built-in logic designs and determination for planning items can prevent errors caused by manual operations.
- Easy and convenient: simplifies and optimizes the modes of setting planning items, saving 90% of time.
- One-click configuration: The offline configuration tool directly invokes the scripts exported by the LLD tool to complete project configurations.

2.3.3 Specifications



2.4 One-Click Configuration Import

2.4.1 Background

Currently, services in the site deployment are configured in the customer's site, which is time-consuming and has strict requirements for service personnel's skills. As the unified storage market is booming, labors are mainly invested into the following aspects during the project delivery: plan and design, software installation and commissioning, and acceptance.

Before on-site implementation, use the visualized plan tool to plan, design, and configure services in advance, and then generate a configuration file. In the on-site implementation, import the configuration file to take effect or complete production pre-installation, thereby effectively delivering site deployment.

2.4.2 Specific Solution and Feature Description

1. One-click configurations are imported and integrated in DeviceManager. After logging in to DeviceManager, you can use this function.
2. Users employ the visualized planning tool to complete service planning and configuration, and export the XML file of the service configuration. The file cannot be manually edited or modified. Log in to DeviceManager of a desired device and import the file by one click to complete the service configuration.

2.4.3 Specifications

- Size of the configuration file does not exceed 1 MB.
- In the service planning, configurations on arrays are completed within five minutes.

2.5 Automatic Cable Detection

2.5.1 Background

When you install and deploy high-end storage products, a large number of cables need to be connected and the connections are complicated, thereby bringing challenges for manual checks of cable connections. To cope with the challenges, automatic cable detection is provided, enabling fast deployment and reliable cable connection checks to ensure correct cable connections.

2.5.2 Specific Solution and Feature Description

Automatic cable detection applies to management network cables, power cables, mini SAS cables, and PCIe cables. Only when all of those cables pass the checks, you can ensure that devices' internal cables are connected correctly. If a cable connection error is detected, the tool will display error information and connection guide. In addition, the error can be located and displayed on the tool's high-fidelity graphics. After the error is rectified, you can perform the detection again.

Checking management network cables: Check the management network cable connections of storage systems, including SVP internal management network cables and network cables between engines.

Checking power cables: The tool automatically checks whether a device is in dual-power supply mode and its power cables are correctly connected.

Checking mini SAS cables: Check whether mini SAS cables meet the requirements of standard networking. After the check, confirm the disk enclosure location in the high-fidelity graphics and check whether the location is consistent with the actual location.

Checking PCIe cables: Only the multi-engine storage system requires PCIe cable connections. Based on a standard device network, rapidly check whether the connection states and methods of PCIe cables among multiple engines are correct.

2.5.3 Specifications

None

2.6 Data Migration

2.6.1 Background

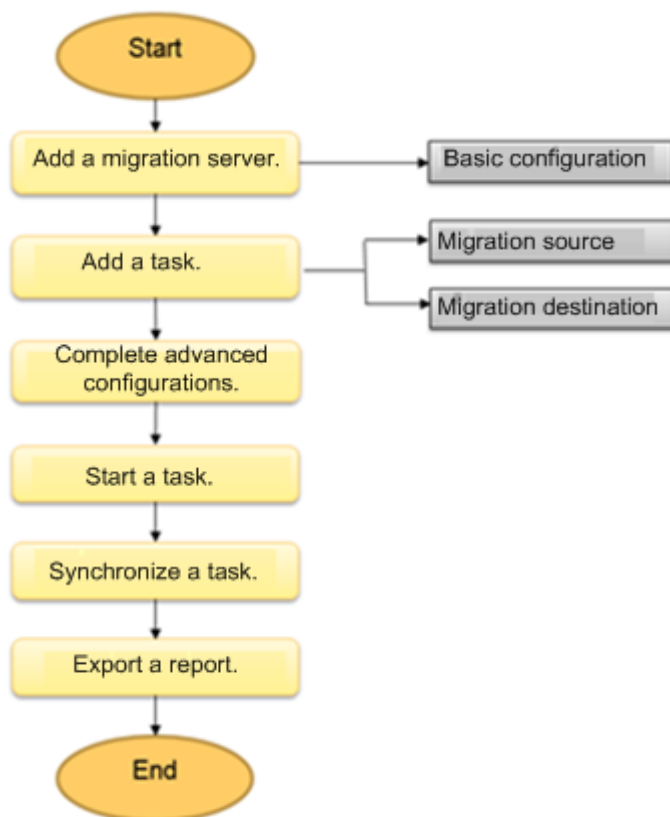
Data migration refers to the scenarios where data is migrated. In a broad sense, server migration, storage migration, and application migration all belong to data migration. Data migration in this section occurs during storage product replacement.

Data migration is more than migrating data from one place to another. Before performing enterprise-level data migration, many factors must be considered to strike a balance among data security, compatibility, downtime, and third-party software and hardware skills.

Huawei provides MigrationDirector for NAS and MigrationDirector for SAN tools for data migration. The tools enable automatic migration, improve overall data migration efficiency, and simply the operations of data migration engineers.

2.6.2 Specific Solution and Feature Description

MigrationDirector for NAS migration process is as follows:

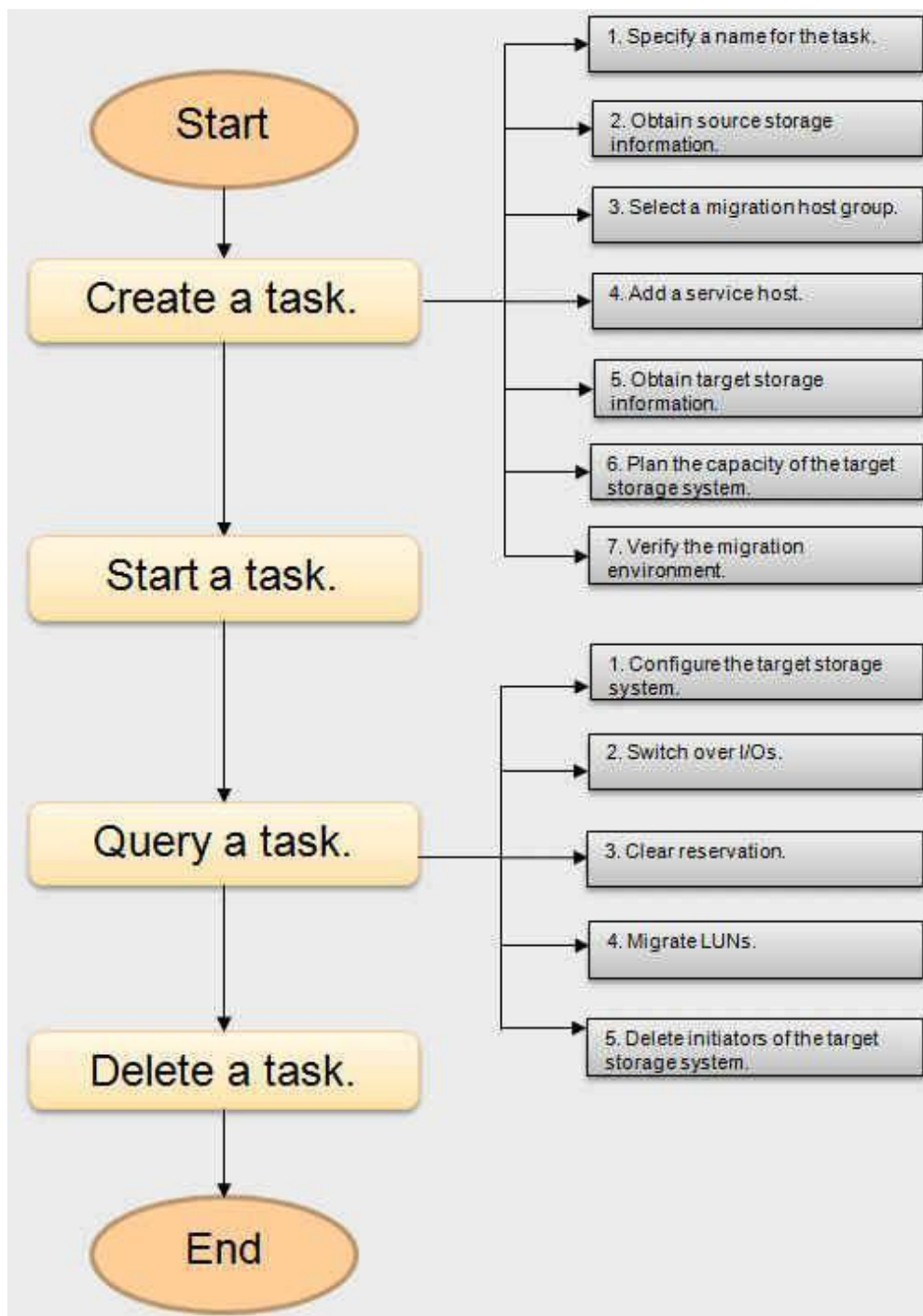


Data migration of NAS file systems is a type of migration on the file system level, allowing data to be migrated between NAS storage arrays of different vendors. Data in files can be replicated to new storage systems using file replication tools. Since these files comply with the CIFS or NFS protocol, differences in model and version metadata of different brands can be masked. Therefore, this solution is suitable for migrating NAS storage devices of both Huawei or non-Huawei vendors.

The NAS migration solution has the following characteristics:

- In this solution, data can be migrated between storage arrays of different vendors on mainstream operating systems such as Windows, AIX, HP-UX, SUSE Linux, and Red Hat Linux.
- This solution supports network file systems such as NFS and CIFS.
- The data replication is performed by the data migration software on the server. This will cause great pressure on the service system during the data migration. This solution also consumes plenty of server CPU and memory resources.
- During the data migration, services need to be offline for a short period of time.
- File migration software is required. If such software is not installed in the current environment, install it.
- Regardless of the source storage, the destination storage must be compatible with hosts.

MigrationDirector for SAN migration process is as follows:



The heterogeneous virtualization function of Huawei OceanStor series storage systems is composed of SmartVirtualization and SmartMigration features.

The data migration solution based on SmartVirtualization can migrate data from a storage array from a third-party vendor or Huawei to a new storage array of Huawei. In the solution, LUNs mapped to the source storage are taken over during the initial data migration phase and LUNs on remote storage arrays are initialized into external device LUNs (eDevLUNs) that can be managed on local storage arrays. Value-added functions such as LUN migration of SmartVirtualization enable data to be quickly migrated between source storage arrays and local storage arrays. Heterogeneous takeover

temporarily interrupts services; while, data replication has no impact on the normal operating of services.

The SAN migration solution has the following characteristics:

- In this solution, data is migrated between SAN storage arrays of different vendors in Windows, AIX, HP-UX, Solaris, SUSE Linux, Red Hat Linux, or other mainstream operating systems.
- During the migration, data is copied through the new Huawei storage array without affecting service systems. No CPU or memory resources of the server are consumed.
- During data migration, services are not interrupted but storage access performance is slightly affected.
- There is no need to install any extra software or agent in the existing storage environment, and data is migrated fast and conveniently.

2.6.3 Specifications

Supported operating systems

Migration Server Operating System	Supported Version
Windows	Windows 7 SP1
	Windows Server 2008 R2 SP1
	Windows Server 2012 R2
Linux	SUSE 10/11
	RHEL 5/6
	CENTOS 4/5/6

NAS migration specifications

File System Specification	
Online Capacity Expansion of File Systems	Supported
Maximum Capacity Per File System	255 TB
Number of File Systems	Maximum 256
Size Limit of a Single File	Maximum 64 TB
Maximum Number of Subdirectories Under a Single Directory	32,000
Longest Path	4 Kbyte
File Name Length	255 bytes
Directory Depth	256 levels
Maximum Length of a File System Name	Maximum 16 English characters
Maximum Number of Files Per File System	1 billion

Maximum Number of Files Per Directory	100,000
--	---------

2.7 One-click Device Archive Collection

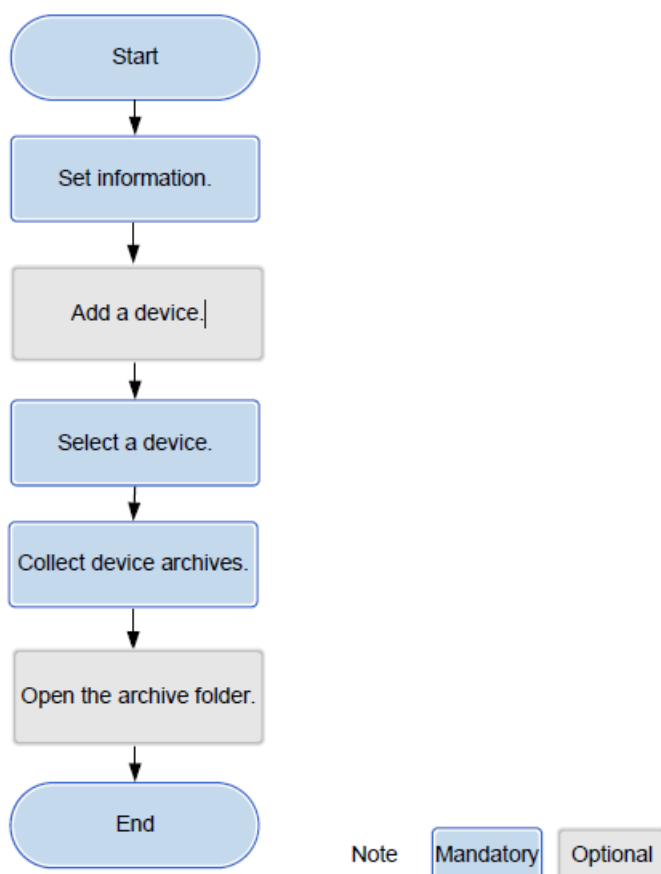
2.7.1 Background

The device archive collection tool collects information about device configuration and deployment and generates device archives for future maintenance.

2.7.2 Specific Solution and Feature Description

The information about storage device configuration is collected during the device archive collection. Before each maintenance operation is complete, the device archive collection tool is used to collect information and generate device archives for future maintenance.

The following figure shows the process of device archive collection.



Device archives include the following configuration information and operating status of managed objects:

- Summary: the device information, including model, version, number of controllers, storage pool, disk domain, number of LUNs, and license.
- System Info
 - The control board information, including ID, version, health status, operating status, location, cluster role, and electronic label.
 - The interface board information, including ID, version, health status, operating status, location, cluster role, and electronic label.
 - The BBU information, including the enclosure ID, BBU ID type, version, health status, operating status, controller ID, power status, number of charging and discharging times, remaining days, and electronic label.
 - The power module information, including the enclosure ID, power ID type, version, health status, operating status, manufacturer, and production date.
 - The fan module information, including enclosure ID, fan ID type, level, location, health status, operating status, and electronic label.
 - The expander backplane information, including ID, type, version, health status, operating status, and electronic label.
 - The management port information, including the controller ID, MAC address, and IP address.
 - The serial port information, including the controller ID, port ID, link status, type, and health status.
 - The management serial port information, including the controller ID, port ID, link status, type, and health status.
 - The iSCSI port information, including ID, health status, operating status, type, working mode, working rate, MAC address, IP address, and error packet statistics, and SFP information (including the manufacturer information, temperature, and receive and transmit optical power).
 - The Fibre Channel port information, including ID, health status, operating status, type, WWN, rate, link events and error packet statistics, and SFP information (including the manufacturer information, temperature, and receive and transmit optical power).
 - The FCoE port information, including ID, health status, operating status, type, WWN, rate, error packet statistics, and SFP information (including the manufacturer information, temperature, and receive and transmit optical power).
 - The SAS port information, including ID, role, type, health status, operating status, and link error statistics.
 - The PCIe and IB port information.
- Disk Domain Info

The disk domain information, including ID, name, tier, health status, operating status, capacity, and member disk information (ID, slot, WWN, capacity, type, and sector size).

- LUN info

The LUN information, including ID, name, types, storage pool ID, health status, operating status, capacity, working controller, owner controller, WWN, value-added feature information (SmartQos, SmartCache, SnapShot, and LUN copy), Remote Replication, Mirror, DST, DIF, Write Policy, Prefetch, Compression, Deduplication, and Retention configuration information.

- SmartQoS Info

- The SmartQoS Policy details, including ID, name, health status, operating status, types, policy enabling, configuration information (IOPS, BandWidth, Latency, Control Type, Priority, and Schedule), and working LUN list.

- The SmartQos Template details, including ID, name, health status, operating status, types, policy enabling, configuration information (IOPS, BandWidth, Latency, Control Type, Priority, and Schedule), and working LUN list.
- The SmartTier information, including migration speed, storage pool, enabling status, migration mode, operating status, global migrated data amount, and migrated data amount of tier 0, tier 1, and tier 2.
- RSS Info (Value-added service information)
 - The clone details, including limit number of clone groups, number of created clone groups, limit number of clone pairs, and number of created clone pairs.
 - The LUN copy information, including limit number of LUN copies, number of created LUN copies, and LUN copy details (ID, name, status, types, number of target LUNs, copy speed, status, progress, start and end time).
 - The source LUN information of the specific LUN copy, including the source LUN ID, name, capacity, status, type, LUN WWN, Array WWPN, and IP.
 - The target LUN information of the specific LUN copy, including the target LUN ID, name, capacity, status, type, LUN WWN, Array WWPN, and IP.
 - According to the device and feature support of different versions, the configuration and status information of snap, mirror, remote replication, active-active features are included.
- FS Info

The file system details, including limit number of file systems, file system ID, name, storage pool ID, type, capacity, block size, health status, operating status, working controller, owner controller, owner pair ID, cache, Snapshot, Clone, Compression, Deduplication, WORM, Quota, and SmarCache information.

- Mapview Info
 - The mapping view information, including host, port, PortGroup, HostGroup, LunGroup, and MapView configuration.
 - The number of hosts and the host information, including ID, name, OS type, owner host group ID and name, host port WWN and type, and multipathing software type.
 - The number of port groups and the port group information, including ID, name, port list, and owner mapping view ID.
 - The number of host groups and the host group information, including ID, name, host port list, and owner mapping view ID.
 - The number of LUN groups and the LUN group information, including ID, name, LUN list, and owner mapping view ID.
 - The number of mapping views and the mapping view information, including ID, name, mapping attributes, HostGroup ID, PortGroup ID, LunGroup ID, and InBand LUN ID.
- Disk Info
 - The basic information about disks, including ID, health status, operating status, types, capacity, role, owner disk domain ID, speed, and SN.
 - The member disk information, including ID, slot, health status, operating status, types, capacity, owner disk domain ID, multipathing information, speed, port IP address, PBC, and electronic label.

2.7.3 Specifications

None

2.8 SmartConfig

2.8.1 Introduction

SmartConfig is a piece of software installed on hosts for storage device management to simplify operations and improve usability of storage devices. It rids users of complex operations in enterprise-level storage management. You can flexibly and efficiently divide disk resources in storage devices into disks and mount them to hosts, and use them like local disks.

2.8.2 Function Features

Installation and Deployment

- SmartConfig for Windows

In the decompressed directory, double-click **OceanStor_SmartConfig_Setup.exe** to install the software.

- SmartConfig for Linux

Upload the SmartConfig installation package to any directory on the Linux operating system, and then run **tar -vxf <installation package name>** to decompress the package.

Resource Allocation

Perform the following steps to allocate resources:

Step 1 Add storage devices.

Step 2 Create a disk.

Step 3 Format the disk.

----End

2.8.3 Specifications

Table 2-1 Supported operating systems and compatible browsers

Host Operating System	Windows	Windows Server 2008 R2 Enterprise Edition SP1 (32/64 bit)
		Windows Server 2012 (32/64 bit)
	Linux	RedHat Enterprise Linux 5 to 7
		SUSE Enterprise Linux 10 to 11
Compatible Browser	Internet Explorer 10 to 11	
	Google Chrome 27 to 53	
	FireFox 25 to 48	

2.9 DeviceManager

2.9.1 Introduction

DeviceManager is GUI-based single-device management software for Huawei storage products, providing good user experience with consistent GUI styles. DeviceManager supports device login, fault management, configuration management, user authentication, performance management, and security management for storage devices, and provides RESTful APIs for Huawei or third-party NMS.

DeviceManager application scenarios are as follows:

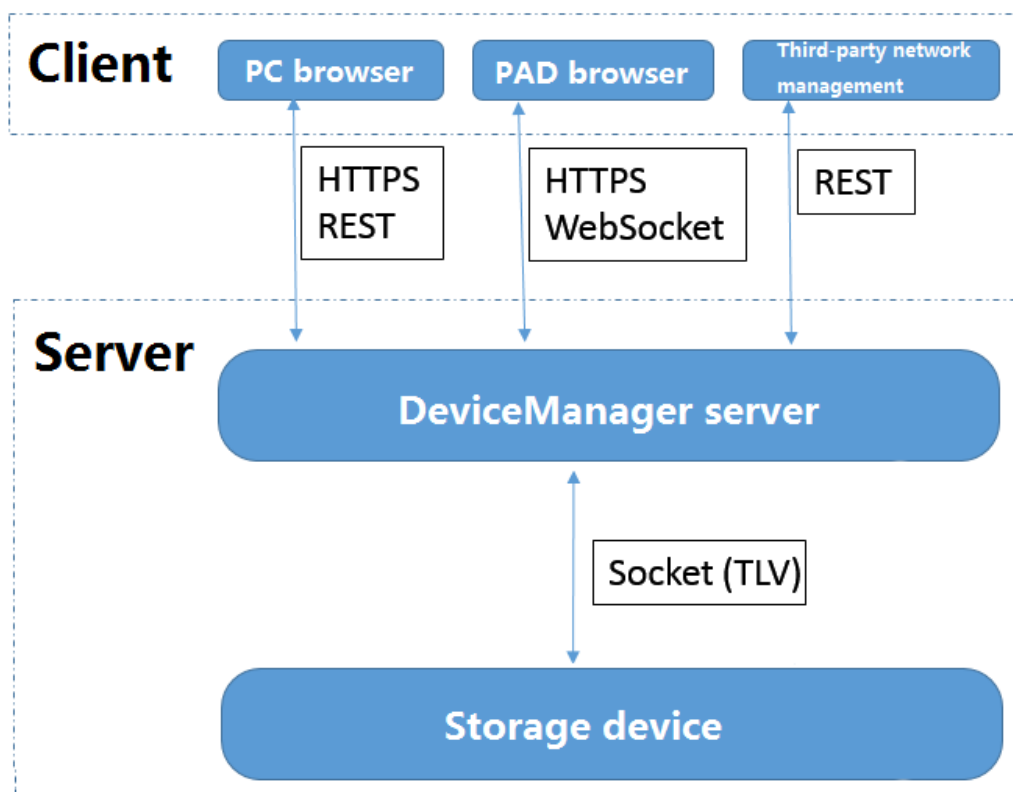
- Management of OceanStor storage devices

DeviceManager can manage storage arrays and provide device login, fault management, configuration management, user authentication, performance management, and security management for OceanStor storage, helping minimize the management cost.

- Supporting access of upper-layer NMS or service platforms

DeviceManager provides RESTful interfaces for upper-layer NMSs such as SMI-S, VASA, and eSight.

Figure 2-1 DeviceManager architecture



2.9.2 Function Features

Batch Configuration

Batch configuration, a function provided by DeviceManager, employs configuration files to batch divide storage resources to simplify resource management, reduce management time, and significantly improve the storage resource configuration efficiency.

The batch configuration procedure is as follows:

- Step 1** Write CLI commands to be executed and parameters and separate them with semicolons (;). Save the commands and parameters in .conf files.
- Step 2** Log in to the DeviceManager as a super administrator. Click **Provisioning** on the right of the home page. On the displayed page, click the icon of batch configuration.
- Step 3** Select the files to be uploaded and then upload them.
- Step 4** The batch configuration is performed in sequence of CLI commands. Then, the execution result is displayed.

----End

Configuration Wizard

Supporting applications including email boxes, databases, and virtual machines, the storage system automatically offers storage management best practices based on service configurations.

According to the different types of applications, storage resources can be created based on the applications or procedure of configuring basic storage services. Generally, storage resources are created based on the procedure of configuring basic storage services. When the configurations about Microsoft Exchange, VMware, Hyper-V, Oracle, or SQL Server are involved, the storage resource creation wizard can be used. Then, you only need to ensure the availability of a storage pool that meets the specific application requirements. The LUNs, LUN groups, and host groups can be configured automatically, which reduces the time for planning and configuration and helps improve configuration efficiency.

2.9.3 Specifications

DeviceManager supports the following browsers:

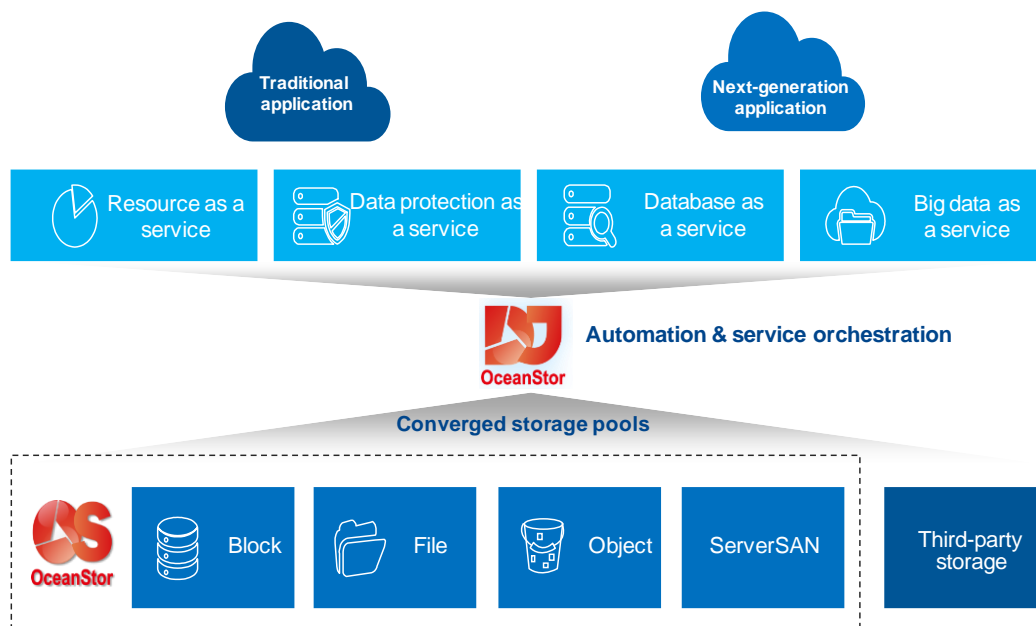
- Internet Explorer 8 and later versions
- Firefox 25 and later versions
- Chrome 27 and later versions
- Safari 5.5 and later versions

2.10 DJ

2.10.1 Introduction

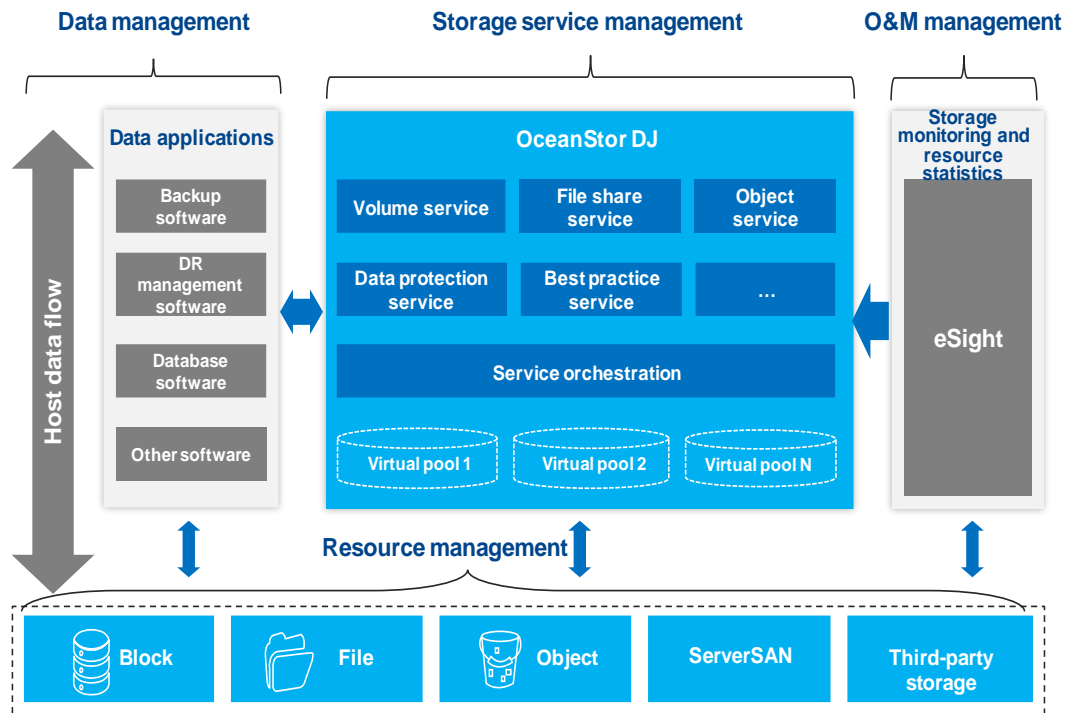
OceanStor DJ is a piece of service-driven storage control software. It masks underlying storage devices and describes services in the customer-friendly language, enabling users who do not understand storage terminologies to easily apply for appropriate storage resources.

Figure 2-1 OceanStor DJ service positioning



OceanStor DJ centrally manages storage resources, orchestrates service catalogs, and provides storage services and data application services on demand, which improves the operation efficiency of data centers. The industry has proposed the idea of control plane-based storage resource pool management in outband mode to take over various existing storage devices of enterprises, provide good expandability, and simplify the O&M of IT departments. That is, management channels are used to achieve storage resource virtualization, automatic configuration, and data protection as a service to resolve customer problems, without changing the existing data channels. With control plane-based storage resource pool management, vendors separate storage policy management from hardware and focus on customer requirements for storage features. Customers can consolidate multiple types of storage resources on multiple storage devices based on their needs instead of adding storage functions on a storage device. Software can support and use various features of all storage hardware.

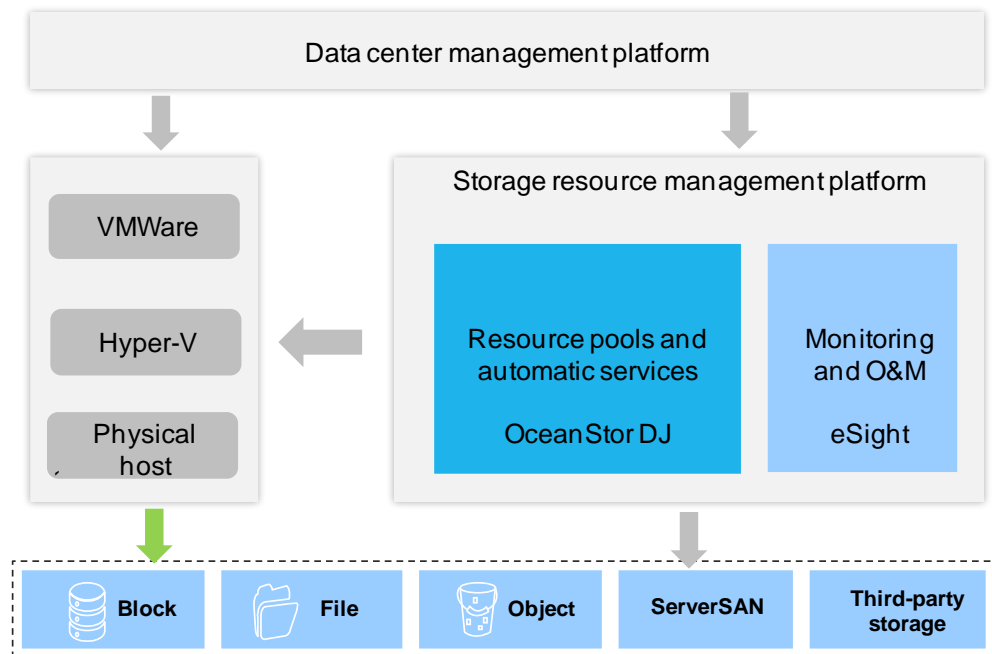
Figure 2-2 OceanStor DJ service capability



OceanStor DJ provides resource pools and automatic storage services in the following two scenarios:

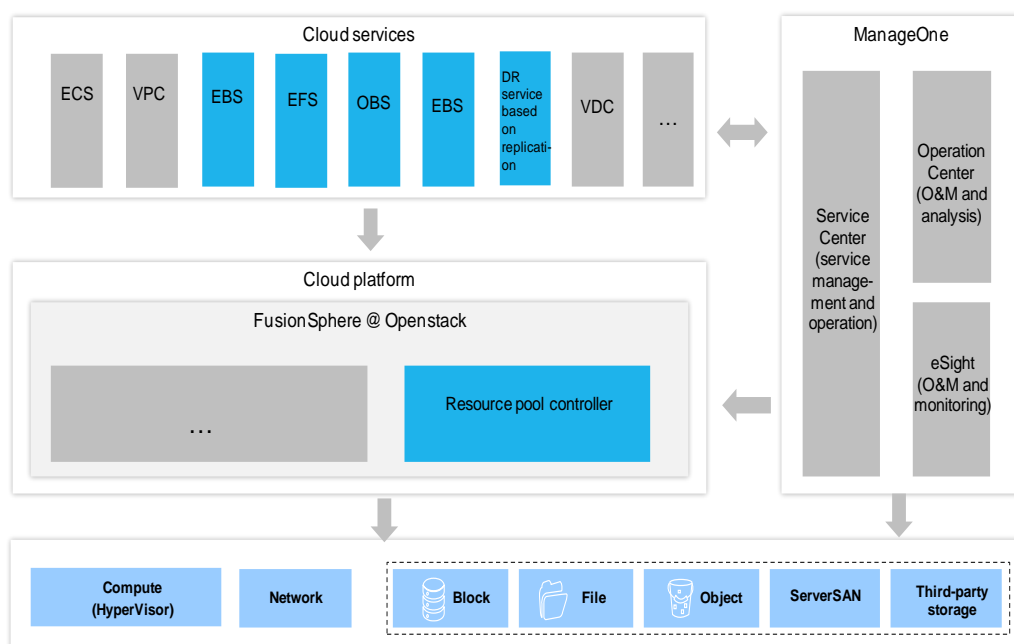
- Scenario 1: Independent software products, supporting STaaS solution

Figure 2-3 Independent software products



- Scenario 2: Storage resource pools and service components in cloud solutions

Figure 2-4 Storage resource pools and service components in cloud solutions



OceanStor DJ has the following characteristics:

- Supports storage resource virtualization based on the control plane and virtual resource pool establishment according to customer requirements.
- Allows administrators to configure management policies for storage and data services.
- Supports progressive construction of storage and data services.
- Supports globally automatic management.
- Provides users with various self-service portal interfaces or APIs.
- Supports the seamless expansion of the storage infrastructure architecture, improving reliability or performance (such as QoS and SLA settings)
- Allows users to monitor and manage storage resource and cost expenditure in an open and transparent manner.

2.10.2 Function Features

Installation and Deployment

The three-node OceanStor DJ cluster supports the physical machine and virtual machine environment as well as one-click installation.

One-click concurrent installation is supported for the three nodes in the cluster. To install the three nodes, users only need to enter required data in the installation planning tool to generate an installation configuration file. During the installation, no manual intervention is required.

OceanStor DJ can be deployed using OceanStor Toolkit.

Alarm Management

OceanStor DJ supports alarm management. It automatically reports detected faults and rectifies them. If a fault cannot be automatically rectified, users can view uncleared alarm information and clear it by performing recommended actions. If an alarm has been handled, users can manually clear it.

OceanStor DJ supports northbound SNMP and can report alarms to a third-party alarm management platform. SNMP supports connectivity tests.

OceanStor DJ supports alarm exporting. Exported alarms can be easily viewed and analyzed.

OceanStor DJ can manage only alarms of its own but cannot manage alarms of storage devices. Alarms of storage devices are managed by eSight or a third-party alarm management platform.

Parameter Configuration and Maintenance

OceanStor DJ supports system parameter configuration on the CLI.

OceanStor DJ supports system maintenance on the CLI. On the CLI, users can view the running status and details of all nodes and services in the system. When exceptions occur, users can restart services or perform active/standby switchovers (only for active/standby services such as GaussDB and RabbitMQ) to quickly recover services.

Health Check

To ensure long-term stable operation of the OceanStor DJ system, maintenance engineers can use the health check tool OceanStor Toolkit to periodically check the system, generate the check result report, detect faults in the system, and rectify the faults by performing recommended actions.

Information Collection

OceanStor DJ allows users to use the information collection tool OceanStor Toolkit to export logs. By viewing and analyzing the exported logs, users can obtain the system running status and rectify potential faults to ensure normal operation of the system.

Running Status and Operation Logs

OceanStor DJ supports running status logs and operation logs.

Running status logs record the real-time running status of processes in the system. When the size of the running status log file reaches a specified value, the file is compressed and backed up. The log backup file is used to track historical process execution information.

Operation logs record user operations on the system. When operation logs accumulate to a specified count, they are exported and saved in a local file with one or more copies. The local file is used to track historical user operation information.

Running status logs and operation logs can be backed up to a third-party FTP or NFS backup server.

NTP Time Synchronization

OceanStor DJ automatically synchronizes system time among the three nodes. It can also use an external NTP server as the clock source for time synchronization.

2.10.3 Specifications

Deployment mode

OceanStor DJ can be deployed on a single-node or a three-node cluster. The single-node deployment is not recommended because of its low reliability.

Installation specifications

The size of installation package is not greater than 2 GB. The installation duration is not longer than 2 hours.

Upgrade specifications

Online upgrade is supported. The upgrade duration is not longer than 2 hour.

Log storage duration

Operation logs and running logs during OceanStor DJ running phase can be automatically dumped to the external storage provided by customers. Local operation logs and running logs can be stored for six months.

3 Routine Maintenance

- 3.1 Overview
- 3.2 One-click Device Health Check
- 3.3 Performance Statistics and Optimization

3.1 Overview

During routine maintenance, use the inspection tool from Toolkit to check the health status of the device. Use SystemReporter to check the performance data or locate performance problems.

3.2 One-click Device Health Check

3.2.1 Background

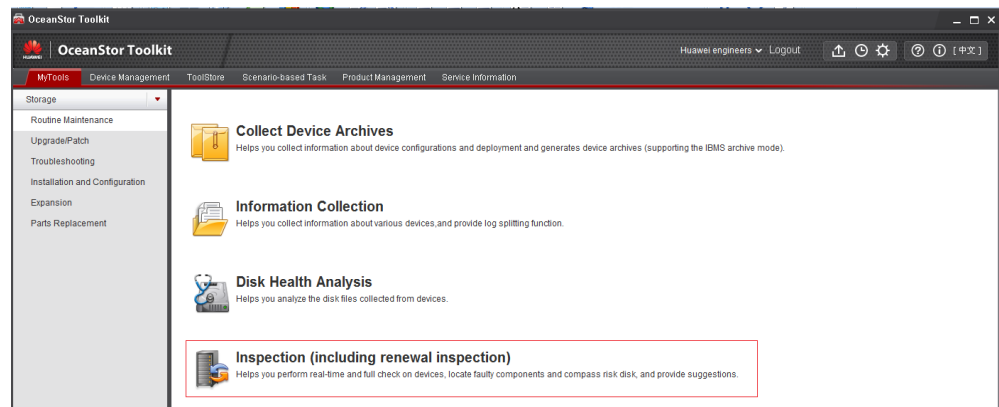
Inspection (including renewal inspection) supports five types of inspections: real-time inspection, site-deployment inspection, renewal inspection, CompassDisk inspection, and precaution inspection. Scheduled inspection and remote inspection are also supported. Inspection (including renewal inspection) is a tool that can customize policies. It comprehensively checks the health status of the software and hardware configuration and service running, and helps users identify device risks in a timely manner. Then, the tool offers well-illustrated rectification suggestions or case documents to provide guidance for troubleshooting. The inspection tool is designed according to the wizard-based operation process. The exported inspection reports are displayed in graphics, which makes the reports easy to read.

Scheduled inspection can inspect the device periodically. By using the scheduled inspection, the inspection report is automatically sent to the specified mail box, which is convenient for the administrator or customers to check the latest device health status in real time. Remote inspection supports checking the health status of devices at each site on a unified management interface.

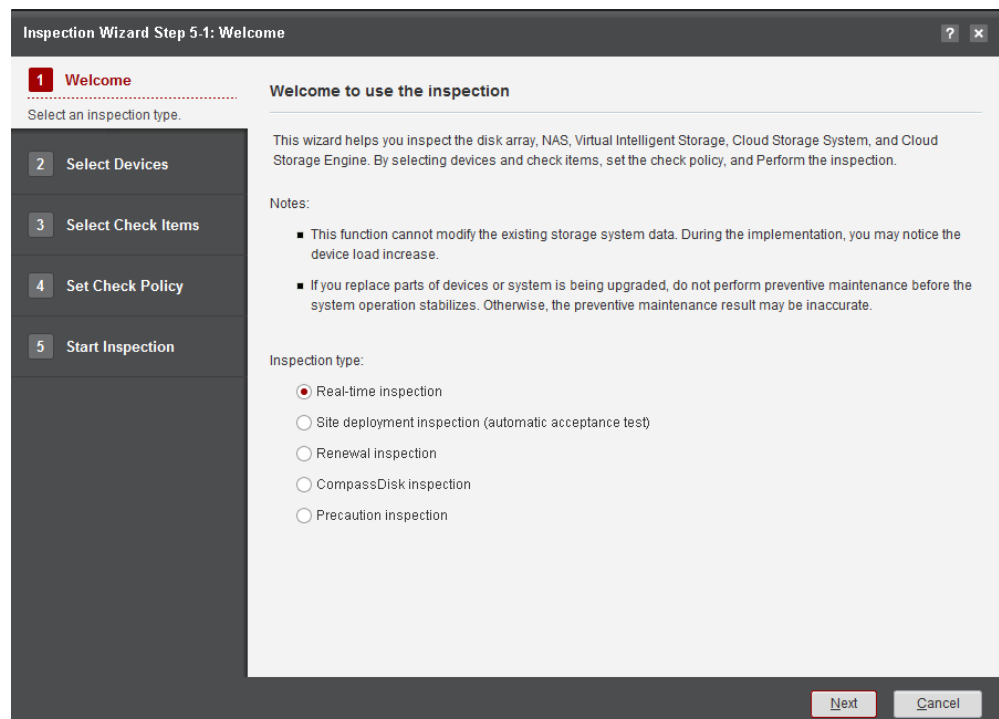
3.2.2 Specific Solution and Feature Description

Inspection (including renewal inspection)

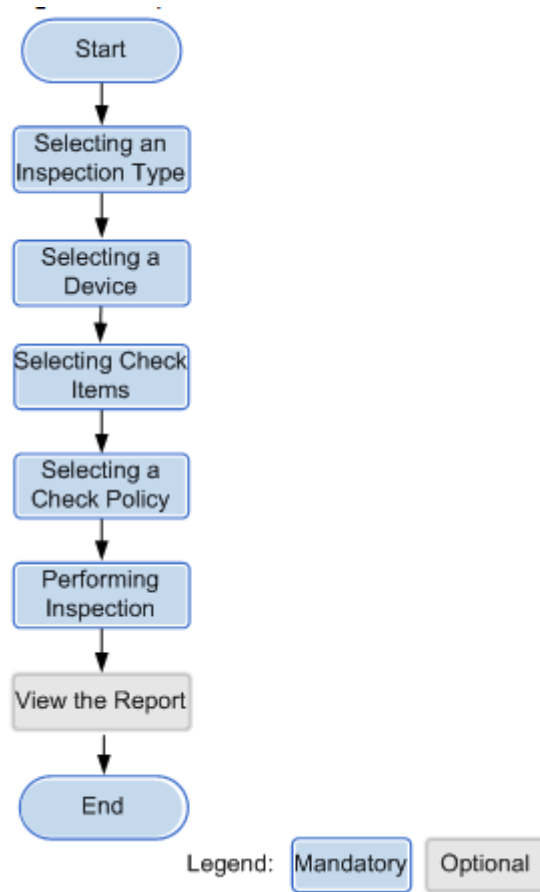
1. Start **Inspection (including renewal inspection)**, as shown in the following figure:



2. Select an inspection type.



3. The inspection procedures are as follows:

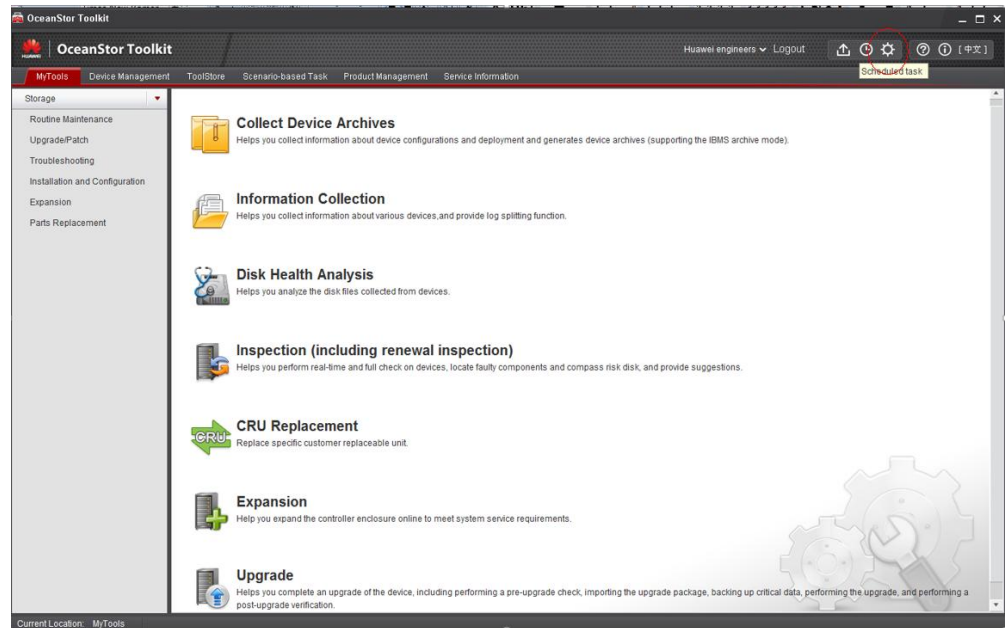


4. View the inspection report, and rectify the faults.

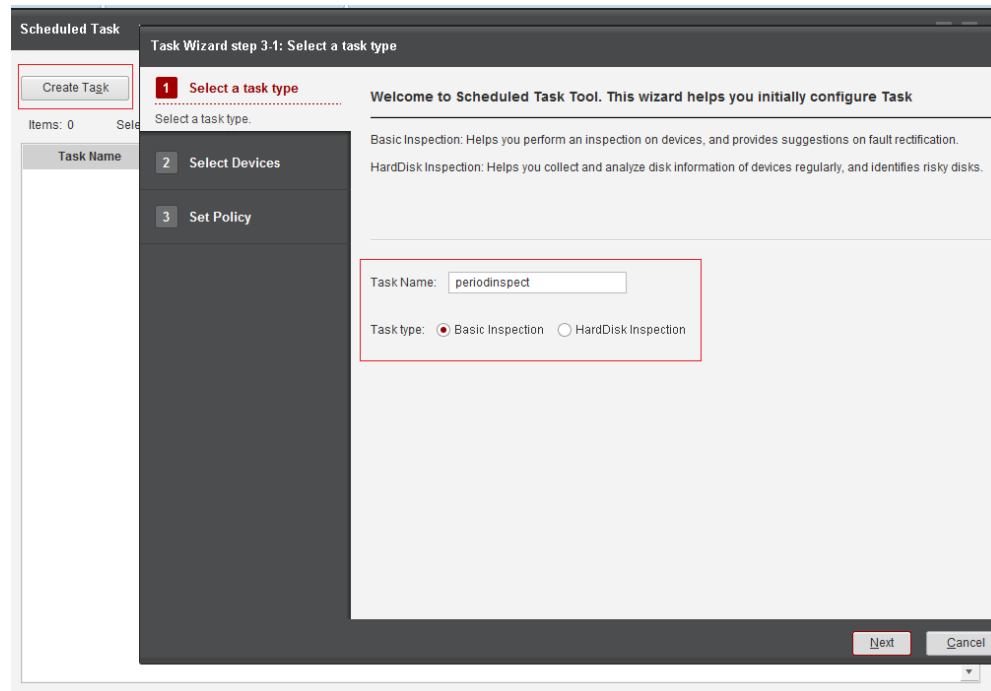
Optical module status	
Original Information	<pre> show port fibre_module PortID Health Status Running Status Type Working Rate (Mbps) Vendor Model SN ----- ENG0_A3.P0 Normal Link Up Multi Mode 12000 FINISAR CORP FCBG410QB1C15 DQP00J3 ENG0_A3.P1 Normal Link Up Multi Mode 12000 FINISAR CORP FCBG410QB1C15 DQN000V ENG0_A4.P1 Inconsistent Link Down Multi Mode 8000 JDSU F1RXPLVCSH423N CA49YK2XE ENG0_B2.P0 Normal Link Down Multi Mode 8000 AVAGO AFBR-57D7AF2 AA1207A303U ENG0_B2.P1 Normal Link Down Multi Mode 8000 AVAGO AFBR-57D7AF2-QL AA1231A0EST ENG0_B2.P2 Normal Link Down Multi Mode 8000 AVAGO AFBR-57D7AF2-QL AD1212A04SW ENG0_B3.P0 Normal Link Up Multi Mode 12000 FINISAR CORP FCBG410QB1C15 DQ0000W ENG0_B3.P1 Normal Link Up Multi Mode 12000 FINISAR CORP FCBG410QB1C15 DQ0000R ENG0_B4.P1 Normal Link Down Multi Mode 8000 AVAGO AFBR-57D7AF2 AA1145A3V3R ENG0_B4.P2 Normal Link Down Multi Mode 8000 AVAGO AFBR-57D7AF2-HW1 AD1243A0B54 admin:/> </pre>
Check Method	Step 1 Log in to the device Step 2 Run the show port fibre_module command.
Check Criteria	1. If optical module cannot be detected, it is normal. 2. If health status is normal, it is normal. 3. Otherwise, it is abnormal.
Recovery Suggestion	1. If the optical module status is abnormal, resolve this issue. For details, see the case . 2. If you have any questions, contact technical support engineers.
Check Result	Not passed The health status of port [ENG0_A4.P1] is abnormal (Health Status:Inconsistent) SN(BOM Code/Item) of hardware [ID: ENG0_A4.P1]:Unknown

3.2.2.2 Scheduled Task

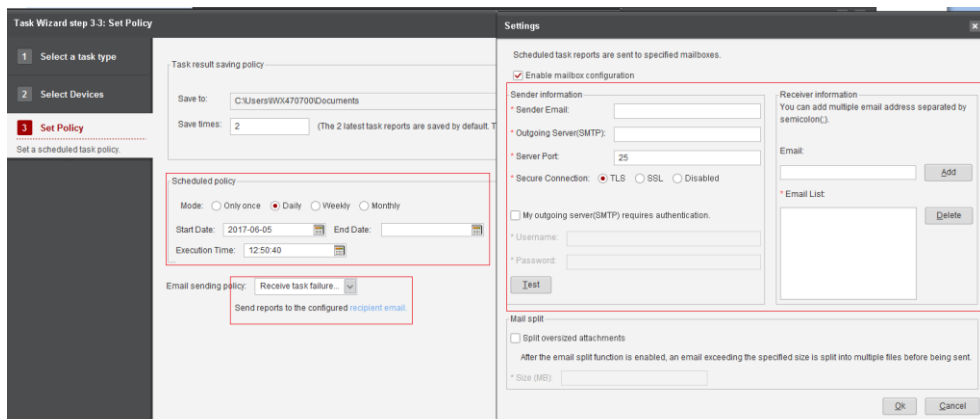
1. Start **Schedules task**, as shown in the following figure:



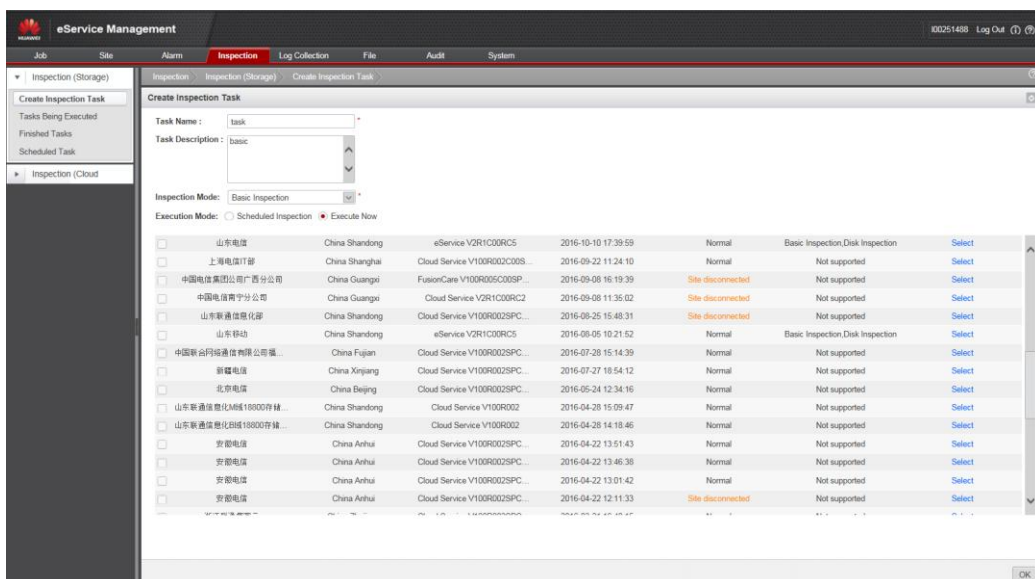
2. Scheduled task type can be set to **Basic Inspection** and **HardDisk Inspection** (disk health analysis), as shown in the following figure:



3. Scheduled task policies and inspection reports can be configured as follows:



3.2.2.3 Remote Inspection



3.2.3 Specifications

The number of inspection items in different versions varies slightly, and is generally about 40. In scenarios with common service pressure, the inspection takes about one to ten minutes. The inspection report of a single device is smaller than 3 MB. A maximum of 256 devices can be managed concurrently, and a maximum of 10 devices can be inspected concurrently.

3.3 Performance Statistics and Optimization

3.3.1 Background

OceanStor SystemReporter is a system performance analysis tool for storage systems. It provides functions of real-time monitoring, historical trend analysis, and capacity forecast

based on data collection, archive, analysis, and forecast. By using OceanStor SystemReporter, users can intuitively learn about storage system performance with ease, and optimize storage systems in time.

3.3.2 Feature Description

- 1. Real-time monitoring**

Users can view the real-time data within the last hour, helping users learn about the storage performance status in real time.
- 2. Historical monitoring**

By analyzing historical performance data, users can monitor the past performance and service pressure of a storage device, and locate performance faults of the device. Historical data is stored for one year.
- 3. Capacity trend**

Users can analyze the capacity data of a storage device, and predict capacity usage. This function provides references for users to work out better plans for using resources. Capacity data is stored for one year.
- 4. Performance threshold-crossing alarms**

Users can set performance threshold-crossing alarms according to service requirements to detect storage performance problems in time. Alarms can be sent through emails or short messages.
- 5. Performance hotspot statistics**

Users can view the system usage based on hotspot statistics.
- 6. Data export**

Users can create scheduled tasks of performance and capacity statistics analysis to export performance or capacity reports. The reports can be sent to specified mailboxes.
- 7. Offline performance file analysis**

If the storage device is not registered to SystemReporter, users can import the performance files of the device to SystemReporter for analysis.

3.3.3 Specifications

Real-time performance data collection

Sampling duration: 5s, 10s, 30s, and 60s

Data storage duration: 1 h

Historical performance data collection

Sampling duration: 5s, 1 min, 2 min, 5 min, 10 min, 30 min, and 60 min

Data storage duration: 1 year

4 Troubleshooting

4.1 Overview

Huawei storage products can detect hardware faults in advance, automatically check abnormalities, and report alarms. On single-device management software DeviceManager or infrastructure management software eSight, users can view the alarms. Then, users can locate the faults according to the device performance data and topology information. Finally, the system abnormalities are packed by using one-click information collection function for the use of Huawei Technical Support Center. Huawei storage systems support Dial in and Dial out functions. These functions provide support service of 7 x 24 h monitoring and troubleshooting for users.

Introduction to Dial in: Huawei Technical Support Center uses eService system to remotely access devices, implement remote troubleshooting, and check health status, ensuring the device stable running.

Introduction to Dial out: Alarms are reported to the remote maintenance center in real time, providing 7 x 24 h monitor to users' devices. When the device reports alarms, the eService system automatically creates orders, and locates faults. If necessary, with the authorization of customers, you can remotely access to customers' devices using the Dial in function for troubleshooting.

4.2 Hardware Fault Prediction

4.2.1 Background

Fault identification and replacement in advance can reduce service downtime, significantly preventing service interruption caused by explosive faults in product final phases.

4.2.2 Specific Solution and Feature Description

1. BBU module life alarms are supported. The system performs the check discharge test every three months. This is to test whether the BBU power backup capability meets the system requirements. If the discharged power is lower than the threshold (the threshold is set to power that can be used for at least 3 months), alarms are reported. The report notifies users that the BBU is about to expire, and users need replace the BBU based on their time. This function solves the service performance deterioration problems caused

by simultaneous BBU failures within a short period, ensuring the continuity of user services.

2. Fan module alarms are supported. The system checks the deviation between the control speed and actual rotational speed of the fan every few seconds. If the deviation exceeds the preset range, the fan module is faulty. To ensure the system heat dissipation, the fan operates at full speed. During this period, the system heat dissipation is not affected, and the system can run properly. Users can arrange time to replace the faulty fan.
3. Memory fault alarms are supported. The system periodically collects statistics of correctable errors on each memory page. When the error number exceeds a threshold, this page will be isolated to ensure the running of the system. When the number of isolated pages exceeds a specified threshold, the system generates an alarm that the controller is faulty (the error is caused by the memory). In this case, the service can continue to run. Based on this alarm, users can replace the controller during non-peak hours.
3. Link subhealth alarms are supported. System links include FC links, SAS links, IB links, network links, and PCIE links. When the link bit error rate (BER) the protocol-defined rate, the system will report BER alarms. In this case, the communication performance will be affected. The direct manifestation is that the bandwidth decreases and the latency increases. But this does not affect user service continuity. At this time, users can contact the technical support personnel to diagnose the links through the CLI command in advance, and repair in non-peak hours, ensuring stability of user service.
5. Hard disk alarms are supported. The system monitors the running status of the array disk and IO processing. In scenarios where the IO errors, IO times out, or the hard disk is about to expire, the system immediately starts the built-in online fault prediction model, meet model statistics conditions. The system determines the error type of the disk: slow disk, impending failure, or IO timeout disk. Then the system handles the errors and reports alarms according to the policy. This can avoid single point failure on services and ensures service continuity.

4.2.3 Specifications

The hardware fault prediction of the storage system supports BBU module life alarms, fan module alarms, memory fault alarms, hard disk alarms, and link subhealth alarms.

4.3 Fault Detection

4.3.1 Background

When a system fault occurs, affected physical or logical objects must generate the corresponding alarm to notify the administrator to perform the troubleshooting.

Fault detection includes alarm reporting, alarm clearance, alarm masking by alarm ID or object, and error code.

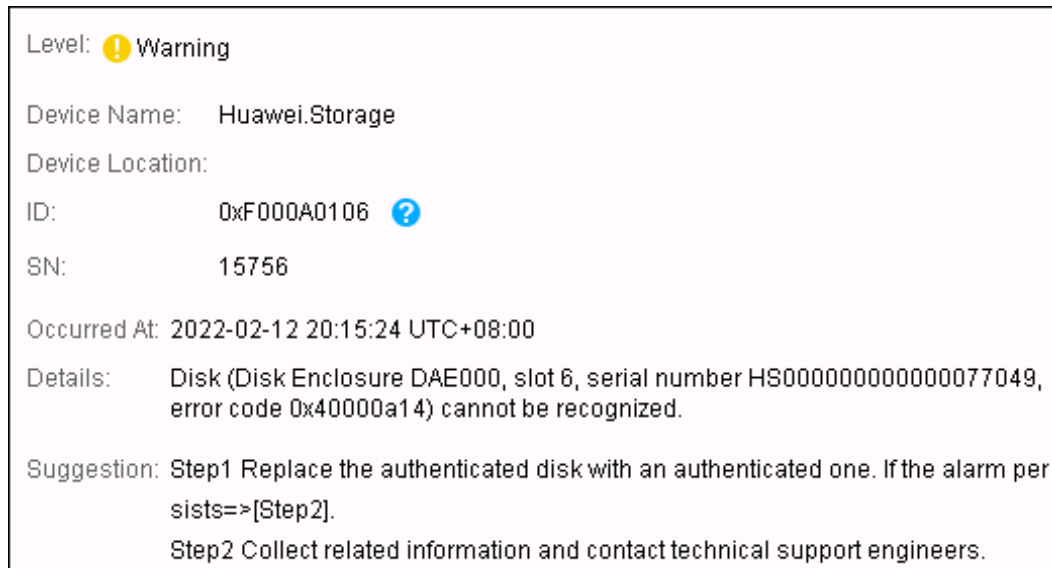
4.3.2 Specific Solution and Feature Description

Alarm: According to the alarm severity, the alarm falls into three levels: important, emergent, and general. The generated alarms can be transferred to users by email, SMS, or syslog.

Alarm masking: Users can mask unnecessary alarms by alarm ID or object. Currently, alarm masking by object is allowed only by command on the CLI mode.

Fault code: An alarm may be generated by various causes. Therefore, in alarm details, a fault code is added to display the detailed fault cause. The meaning of the fault code can be found in the product error code. For details, see the following figure.

Figure 4-1



Frequently-occurring alarm: In scenarios where the object changes frequently, and alarms are required to be sent in this changing status, frequently-sent/cleared alarms will affect user experience.

Set the alarm to frequently-occurring alarm. That is, when an alarm is generated, the alarm is delayed compared with the user configuration time. If the cleared alarm is not received within this period, the alarm will be reported to users.

Root alarm: For an object with logical relationship, such as a disk enclosure with N disks, if the disk enclosure is faulty, the corresponding disks are faulty. When the disk enclosure and disks report alarms, root alarm can establish root relationship based on the ID of the two alarms. If the parent alarm exists and has the same parameters with the child alarm within configured time, the child alarm will be suppressed. If the child alarm is not cleared with the clearance of the parent alarm, the child alarm will be reported to users.

4.3.3 Specifications

Alarm: Currently, the number of uncleared alarms is 10000. The same alarm or alarms with the same locating parameter will be deduplicated. The locating parameter is an alarm parameter. An alarm can be identified by specifying several locating parameters as features.

Event: System operation logs, events, and cleared alarms are put into the event information. The current maximum specifications are 50000 pieces, including uncleared alarms. If the number of events is more than 50000, 10000 pieces are deleted each time until the number is less than 45000. If customers want to save the deleted events, configure the FTP/SFTP to dump the information. When the events exceed 50000 pieces, the extra event information will be dumped to the FTP/SFTP server.

Alarm masking: At present, the alarm masking by alarm ID or object supports a maximum of 200 pieces.

Root alarm: At present, a maximum of 200 root alarm rules are supported.

4.4 Call Home

4.4.1 Background

As a remote maintenance expert system for Huawei's IT products, eService Client, called Call Home, monitors device alarms in 7/24 mode. Whenever an alarm is detected, it automatically notifies Huawei technical support engineers so that instant help can be provided for customers. Supporting device log backhaul, eService Client also provides a set of customer-based controllable and secure remote access technologies to enable Huawei engineers to quickly access the devices, thereby effectively facilitating fault handling and recovery.

4.4.2 Specific Solution and Feature Description

1. Active monitoring for device alarms. eService Client provides 24/7 monitoring of device alarms. When a fault occurs on a device, it automatically notifies Huawei technical support center and dispatches a trouble ticket to the involved engineer. This helps customers locate and resolve problems in a timely manner. Two channels are supported:
 - Email channel. The customer needs to have a mail server.
 - HTTPS channel. The customer does not need to provide the mail server, as long as eService Client can access to the external network (Http/Socks proxy).
2. Log express. To enable device logs to analyze and locate faults, frontline technical support engineers (or customers) can use eService to upload the collected log package to the background in one-click mode. Maintenance engineers download the package and use it for analysis and locating in the background. Email channel and HTTPS channel uploading are both supported.
3. Remote health check. Huawei engineers can initiate a remote inspection and log collection task at a site through eService cloud. Then, inspection report and device log package are automatically uploaded. The inspection policy can be configured, such as periodical inspection.

4.4.3 Specifications

1. Within 10 minutes, Huawei technical support engineer automatically detects site faults and performs required actions.
2. Within 5 minutes, eService Client collects the logs and uploads the 8 MB logs.
3. Within 10 minutes, Huawei technical support engineer can automatically obtain remote inspection results and handle problems.

4.5 One-click Fault Data Collection

4.5.1 Background

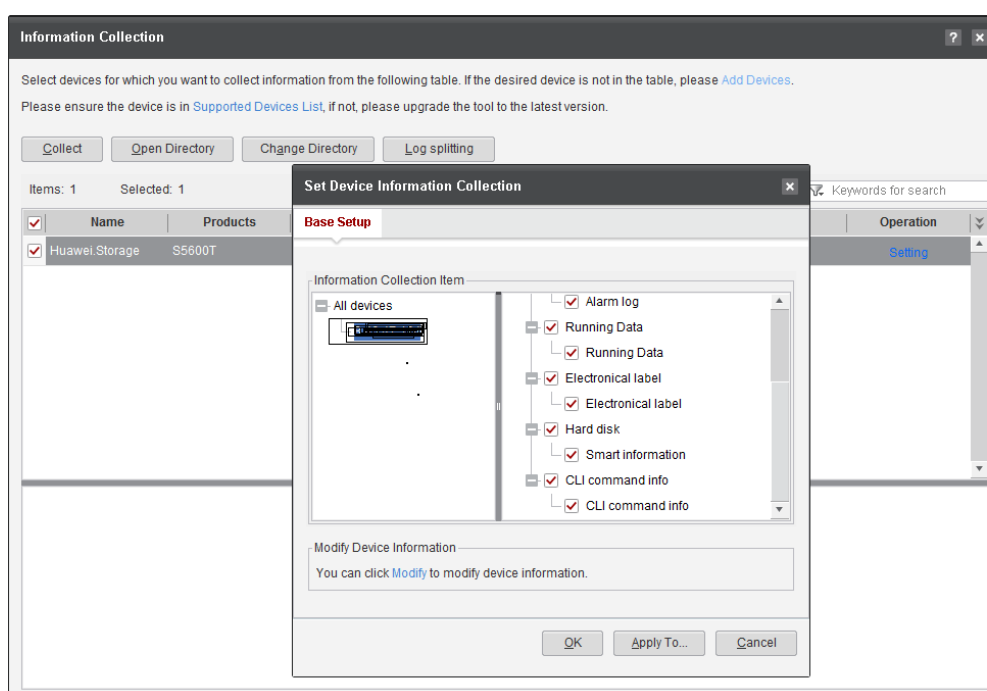
The information collection tool provides one-click collection of device logs and configuration information. This tool supports information collection in batches, customized collection items, collected data compression, collection progress display, log collection for N8000 devices in a specific period, and SMART information collection.

The tool can perform the following operations:

- Add a device.
- Set information collection.
- Collect information.
- Split logs.
- Open the directory of collected information.
- Change the directory of the collected information.

4.5.2 Specific Solution and Feature Description

The information collection tool supports collecting system logs, alarm logs, configuration information, electronic labels, and CLI command output, and disk Smart information.



4.5.3 Specifications

- Log storage duration

The operation logs, run logs, and debug logs generated during the operating phase of a storage device are stored in the independent log space of the device. Generally, those logs can be retained for six months.

Operation logs and run logs can be automatically dumped to external devices using SFTP or FTP. The storage duration of dumped logs depends on the storage space size of external devices.

- Log collection

When the service load is not heavy, information collection takes around 30 minutes. The size of the collected log package varies with the device running time, usually about 5 MB – 50 MB. The high-end information log package may exceed 100 MB as it contains SVP logs. A

maximum of 256 devices can be managed concurrently, and a maximum of 10 devices can be collected concurrently.

4.6 End-to-End Visual Fault Management

4.6.1 Background

As an IT infrastructure, storage devices may be maintained by each administrator of enterprises. With the increase of demands on data storage, a large number of storage systems are required. To ensure system reliability, the management of storage systems becomes more and more complicated and enterprises are faced with the following challenges:

- Complicated and time-consuming detection of storage performance problems
- Difficult detection of storage faults and long-time rectification

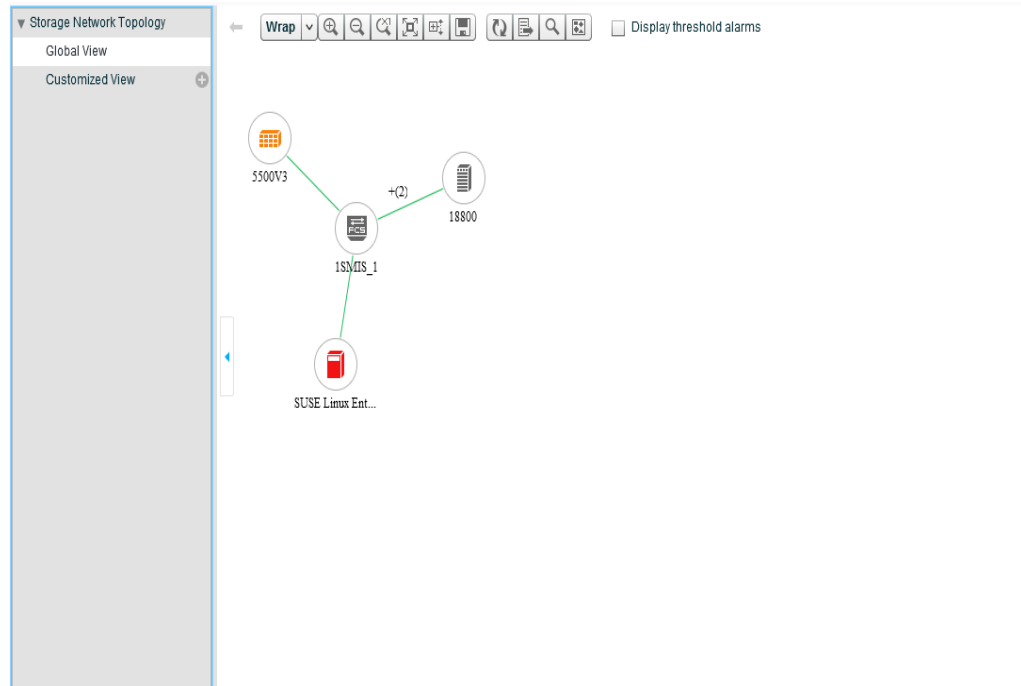
To cope with the preceding challenges, Huawei has provided a solution for ICT infrastructure management, which is called the eSight system. eSight storage serves as a component in the system and implements lifecycle management. When locating the storage-related problems, eSight supports displaying links among hosts, switches, and storage devices and performance analysis, and helps users to perform end-to-end visual fault management.

4.6.2 Specific Solution and Feature Description

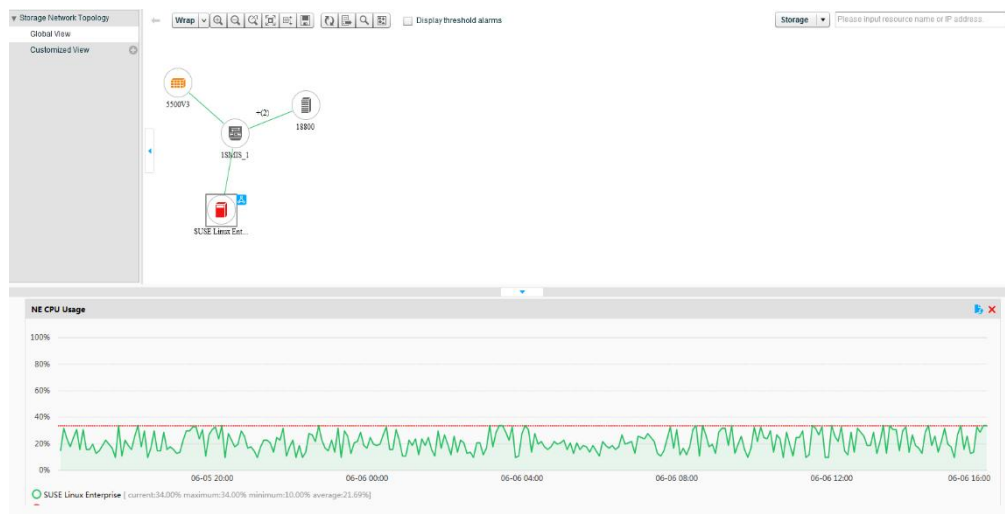
eSight provides the storage network analysis, serving as a professional monitoring and analysis tool dedicated to SAN/NAS storage network environments. The storage network analysis function can be used to automatically discover SAN and NAS topologies, monitor SAN and NAS alarms, and monitor storage path performance. The topologies are global or customized. The provided NE topologies, host path graphs, and historical and real-time performance graphs help analyze NEs at different levels.

In global view, you can perform operations on NEs, check basic properties of links and ports on the storage network, and the threshold alarms of port links and devices, and perform network-wide fault analysis and location.

In customized view, you can create, delete, and adjust topologies based on storage devices, hosts, or virtual resources. In addition, you can perform corresponding operations on NEs.

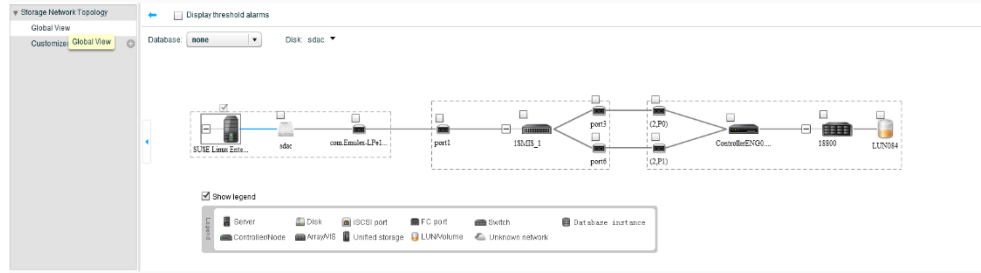


Select devices and links that support historical and real-time performance view.



In the topology view, if further analysis is required, you can select a host and go to the host path graph to analyze.

The host path graph displays the mapping among the host, Oracle database applications, disks, ports, switches, disk arrays, storage controllers, storage devices, and LUNs. You can view the historical and real-time performance of NEs and links in a host path graph.



You can select multiple components to analyze corresponding performance indicators.



4.6.3 Specifications

Node	Indicator
Host	CPU and memory usage
Disk	Read and write response time, read/write bandwidth, read/write IOPS, I/O waiting time, and I/O operation time percentage
Fibre channel port	Uplink and downlink traffic (bit/s), total traffic (bit/s), uplink and downlink bandwidth usage, and total bandwidth usage
Switch port	Error statistics, sending and receiving usage, sending/receiving rate and bandwidth usage, and buffer credits
Front-end host port	Read/write bandwidth, read/write bandwidth usage, write/read latency, read/write IOPS, and port usage
Controller	CPU/memory usage, read/write bandwidth, read/write IOPS, latency, and queue length
Storage device	CPU usage, read/write bandwidth, read/write IOPS, and latency
LUN	Read/write bandwidth, read/write IOPS, latency, and read cache hit ratio

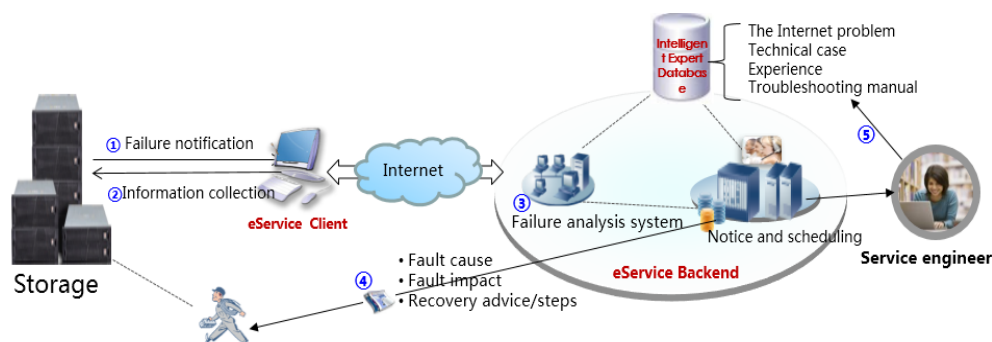
4.7 Intelligent Fault Analysis System

4.7.1 Background

In the complex fault scenarios, various types of logs with a large amount of information intensify O&M difficulty. Heavily relying on personnel skills and long recovery time bring huge pressure to maintenance engineers. Huawei intelligent storage fault analysis system is provided to achieve fast fault location and demarcation, reduce the fault location time, lower maintenance skill requirements, shorten the fault recovery duration, and improve customer satisfaction.

4.7.2 Specific Solution and Feature Description

Alarms, logs, error codes, and performance data collected using the information collection tool are used to facilitate fast fault location and demarcation with the comprehensive expert knowledge base, including technical cases about online problems, R&D and service experience, and tool-based troubleshooting guide and provide effective handling suggestions/procedures.



1. Report live-network faults.
2. Use the information collection tool to collect the log information (automatic or manual).
3. The intelligent fault analysis system analyzes faults and provides analysis results based on the fault symptoms, information collection results, and expert knowledge base.
4. The technical support engineer performs recovery based on analysis results.

4.7.3 Specifications

Benefiting from this system, the abnormal reset, startup failure, hardware fault and performance-related problems on the live network can be automatically located, and analysis results can be provided within 30 minutes.

4.8 Remote Access

4.8.1 Background

If Huawei engineers need to remotely access the customer's site for fault location and rectification, log in to the iRAD platform, and use the eService remote access function for remote access operation.

The eService remote access function supports Internet and Telephone Modem channels. For users who do not install eService in advance, a lightweight client version is provided for you to achieve fast remote access.

4.8.2 Specific Solution and Feature Description

Remote desktop access support establishing IP security channel based on the Internet and telephone line to enable local and remote desktop sharing and text communication.

Internet-based IP security channels are encrypted at the transmission layer/application layer based on the TLS/SSH/HTTPS to ensure the security of the access channel, supporting remote desktop communication by using the secure Socket channel. Telephone line-based IP channels are established based on the PPP/SLIP.

The dedicated local area network is established through Modem dial-up to provide remote desktop.

4.8.3 Specifications

You can access the customer sites for troubleshooting within 1.5 minutes.

4.9 Metadata Recovery

4.9.1 Background

Metadata refers to the data used to describe and organize the data space. Based on the industry-leading disk virtualization technology (RAID 2.0), Huawei enterprise storage systems support both SAN and NAS and a series of value-added features, which require support of the metadata. Therefore, metadata reliability is an important part of the entire storage system reliability. Once metadata is damaged due to software bugs and human error, the metadata recovery function enables you to quickly and accurately recover the metadata to prevent long-time service interruption and data loss.

4.9.2 Specific Solution and Feature Description

According to the system logical layers, metadata recovery includes metadata in the disk domain, LUN metadata, and metadata in the file system.

Metadata recovery in the disk domain: Recovery based on backup metadata and online consistency check is both used to achieve fast and accurate recovery.

The details are as follows:

Name	Principle	Application Scenario	Advantage
Metadata recovery in the disk domain	<ol style="list-style-type: none"> 1) Metadata changes caused by real-time backup additions, deletions, and modifications. 2) After the metadata is damaged, use the backup data to quickly recover the metadata. 3) After the recovery is complete, enable the online metadata consistency check function to ensure metadata consistency. 	Disk domain	The volume of metadata initiated by background task in the disk domain is small, and does not change frequently. It is suitable to use the traditional backup solution to recover metadata. This solution is mature and reliable, providing fast recovery and accurate results.

LUN metadata recovery: Recovery based on backup metadata and scanning, and online consistency check are used to achieve fast and accurate recovery.

Name	Principle	Application Scenario	Advantage
LUN metadata recovery	<ol style="list-style-type: none"> 1) Metadata changes caused by real-time backup additions, deletions, and modifications. 2) After the metadata is damaged, use the backup data to quickly recover. For those who have no backup, use scanning to recover. 3) After the recovery is complete, enable the online metadata consistency check function to ensure metadata consistency. 	Thick LUN, Thin LUN	Metadata in Extent layer of Thick LUN and Thin LUN have the features for backup. Therefore, metadata in Extent layer can be quickly and accurately recovered using the backup data. Thin LUN Grain contains a large amount of data which change frequently. Considering these and overall performance, the scanning recovery technology is used.

Metadata recovery in the file system: Recovery based on consistency point rollbacks and scanning, and online check are used to achieve fast and accurate recovery.

Name	Principle	Application Scenario	Advantage
Metadata recovery in the file system	<p>1) Scan all documents/directories on the logical linear space in the POOL, and reconstruct all the metadata in the file system based on these INODEs.</p> <p>2) Attempt to roll back all metadata in the file system to the consistency point before the latest consistent point, and then use the online check function to check whether the metadata is still damaged. If yes, you need to continue the rollback or use the scanning-based recovery mode.</p>	File system	In the scenarios where different metadata is damaged and host services scenarios, two recovery modes are available. Scanning-based recovery ensures that all metadata can be recovered after being damaged. The recovery based on consistency point rollbacks offers fast recovery in minutes.

4.9.3 Specifications

Metadata is 100% repairable after damage.

4.10 FRU/CRU Replacement

4.10.1 Background

To facilitate component maintenance, and reduce the impact of manual replacement on the services, field replacement unit (FRU)/customer replacement unit (CRU) replacement tool provides step-to-step guidance to ensure that components are successfully replaced.

4.10.2 Specific Solution and Feature Description

CRUs: BBU, expansion module, fan module, hard disk module, optical module.

FRUs: BBU, expansion module, fan module, hard disk module, interface module, front-end cable, AOC cable, SAS cable, management cable, controller module, system enclosure, optical module, assistant cooling unit, and data switch.

The FRU/CRU replacement tool provides the following features:

Select components: Select the components to be replaced, preferably faulty components.

Check before replacement: Check whether the conditions for component replacement are met, and whether online replacement affects services. If the conditions are not met, an error message is displayed with recommended actions.

Replace components: Click **Replacement Guide** on the tool page, and perform the replacement following the steps provided in *Replacement Guide*. Check after the replacement:

Check whether new components are running properly. If not, an error message is displayed with recommended actions.

Replacement completed: The replacement is completed.

4.10.3 Specifications

None

4.11 Backup and Recovery Configuration

4.11.1 Background

When using the NMS (such as Device Manager) to create a hard disk domain or storage pool for a device, some configuration information is generated and stored in the internal database of the array. When the device needs to be restarted or powered off unexpectedly, the data in the database is used to restore interrupted services.

The configuration data in the database is crucial to service recovery. Usually, before a few key operations, such as system upgrade, capacity expansion, and spare part replacement, you need to back up the configuration data, so that when exceptions occur, you can use the backup data to restore services. In daily use, you can periodically back up configuration data in case of emergency.

4.11.2 Specific Solution and Feature Description

There are two methods available for backing up configuration data: backup and recovery, and export and import.

For the backup and recovery method, configuration data is backed up to the reserved partition in the device. Then, data is recovered directly from the reserved partition.

For the export and import method, configuration data is exported to an FTP server. Then, data is imported to the device from the FTP server.

4.11.3 Specifications

	Command	Parameter
Backing up configuration data	backup configuration_data	None
Restoring configuration data	restore configuration_data	None
Exporting configuration data	export configuration_data	ip indicates the FTP or SFTP server address. user indicates the user name for logging in to the FTP or SFTP server. password indicates the password for logging in to the FTP or SFTP server. db_file indicates the stored path and file name on

		<p>the server.</p> <p>port indicates the port number on the server.</p> <p>protocol indicates the type of transfer protocols.</p> <p>Clean_device_file indicates whether to delete the configuration file that resides in the storage system memory after the configuration file is exported to a server.</p>
Importing configuration data	import configuration_data	<p>ip indicates the FTP or SFTP server address.</p> <p>user indicates the user name for logging in to the FTP or SFTP server.</p> <p>password indicates the password for logging in to the FTP or SFTP server.</p> <p>db_file indicates the stored path and file name on the server.</p> <p>port indicates the port number on the server.</p> <p>protocol indicates the type of transfer protocols.</p>

5 Upgrade and Capacity Expansion

5.1 Overview

The upgrade involves a series of operations with the change of software version, including solution design, preparations, implementation, and verification. Capacity expansion is to add the controller, disk enclosure, or hard disk for meeting service capacity or performance requirements, including solution design, preparations, implementation, and verification. This section describes each of the two parts in detail.

5.2 Upgrade

5.2.1 Background

Huawei enterprise storage version is divided into R version, SPC version, and hot patch version. R version enables you to add a function. SPC version is used to rectify defects within a period, and hot patch version is used to rectify a particular defect.

R version and SPC version are both upgraded following the online microcode upgrade procedure. During the upgrade, temporary performance degradation may occur.

The hot patch version is upgraded following the microcode patch upgrade procedure. The upgrade has no impact on host services.

5.2.2 Specific Solution and Feature Description

1. Online upgrade flowchart

- Upgrade method:

OceanStor Toolkit is provided to perform one-click upgrade on Huawei enterprise storage systems, simplifying the upgrade to the maximum extent.

Specifically, select some controllers to stay offline, and switch the services on these controllers to other controllers, and then perform the upgrade. After the upgrade is complete, these controllers take over the services. Then, upgrade other controllers in the same way.

- Steps

In OceanStor storage systems, four controllers in an engine can be divided into two planes: plane X and Y. Assuming that the controller A and C belong to plane X, and

controller B and D belong to plane Y, Online system upgrade is performed in the following two batches:

The first batch: upgrade the controllers of plane Y. If the controllers of plane Y fail to be upgraded, suspend the upgrade and choose rollback or allow the maintenance engineer to rectify the fault before you can continue the upgrade. If the controllers of plane Y are upgraded successfully, switch services carried on the controllers of plane X service to controllers of plane Y. Then, continue the second batch upgrade.

The second batch: upgrade the controllers of plane X. If one of the controllers fails to be upgraded, suspend the upgrade and isolate the controller or allow the maintenance engineer to rectify the fault before you can continue the upgrade. Set the controller experiencing upgrade failure to be in isolated state, and continue the upgrade. After the upgrade is complete, notify the system to rectify the isolated controller.

- Upgrade impact

Service switchover impact

The controller stops accepting service requests and then starts the service switchover procedure. During the switchover process, the controller returns the busy state to I/Os delivered to the controller (the returned state varies with operating systems). After services have been switched over, the UltraPath software delivers these I/Os to other controllers. It takes about one second to complete a service switchover.

Impact on performance

During the upgrade, 50% controllers of each engine can accept I/Os so that the performance pressure is lower than 50% of the maximum performance.

- Restrictions

To perform an online upgrade, states of disk arrays and multipath redundancy must be normal and service loads must be light. Before an upgrade, the system automatically checks whether conditions of disk arrays for online upgrade are met. If not, online upgrades cannot be performed.

Check items are as follows:

- System state: Check whether there are faults or alarms in the system. If yes, online upgrades cannot be performed.
- Version compatibility: Check whether the target version is supported by the online upgrade.
- System resources: Check whether system resources are enough for an upgrade.
- Service pressure: Check whether the service pressure is significant. If yes, online upgrades cannot be performed.
- Upgrade package: Check whether the upgrade package is correct and complete.
- System redundancy: Check whether there are required redundant key components and host paths.
- Online upgrades cannot be performed in the case of single path.

2. Hot patch upgrade process

OceanStor Toolkit one-click upgrade can be used for both patch upgrades and online upgrades.

Working principle of hot patches: Replacing defect codes without interrupting the running of storage systems is called hot patch upgrade. Hot patch upgrades do not require offline controllers. When the hot patch upgrade is adopted, defects of current microcode version can be rectified without impairing services.

- Upgrade procedure:

- i. Import the hot patch package to the disk driver.
 - ii. Activate the hot patch. That is, replace the defect codes.
 - iii. Check whether the hot patch status is normal to ensure that new codes have taken effect.
- Upgrade impact
None
 - Restrictions
The controller status is normal.
1. Rollback and troubleshooting
During the online upgrade process, if a fault occurs and the upgrade stops, the Toolkit tool displays the retry and rollback buttons. Under such circumstances, users can rectify the fault and click the retry button to resume the upgrade process. Alternatively, users can click the rollback button to perform online rollback.
When the storage device of a later microcode version is in normal use (not in the upgrade process) and the storage device needs to roll back to the source version, users only need to deliver the one-click rollback command on OceanStor storage to roll back the microcode version. Currently, microcode rollback does not support online rollback.
- Rollback method: The CLI command can be used to perform microcode rollback. One CLI command is required to complete the version rollback operation.
Rollback of multipathing software refers to re-installation of the multipathing software.
 - Steps of microcode rollback: Stop all services and run the rollback command. > Enable the system to load the old version. > Restart all controllers.
 - Impact: Services are interrupted.
 - Restrictions of rollback: Features of the new version must be deleted before rollback is performed.

5.2.3 Specifications

Online upgrade duration: 60 minutes

I/O congestion duration for online upgrades: 1s

5.3 Capacity Expansion

5.3.1 Background

With the continued development of enterprise information systems and the ever-increasing expansion in the scale of services, massive information volumes have caused a ceaseless increase in data accumulation. The initial configuration of storage systems is often not enough to meet these demands and therefore, storage system capacity expansion has become a key issue in system administration. Huawei enterprise storage system provides the online expansion function, which enables storage capacity expansion without interrupting ongoing services.

5.3.2 Specific Solution and Feature Description

Currently, the capacity of storage system can be expanded using the following methods: adding disks, adding disk enclosures, adding controllers, and adding links. You can choose a

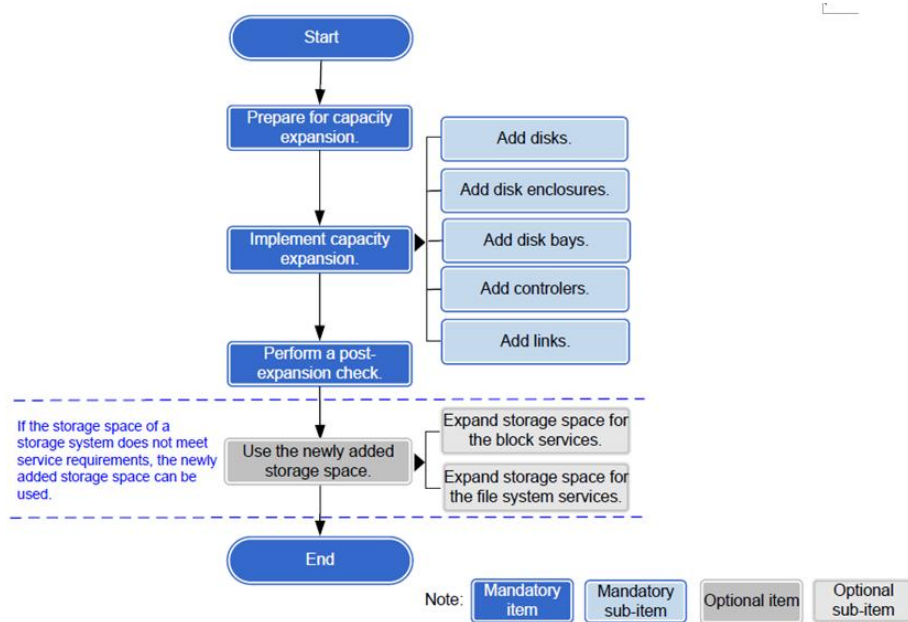
capacity expansion method based on capacity expansion requirements. Table 5-1 describes the characteristics and application scenarios of the capacity expansion methods.

Table 5-1 Characteristics and application scenarios of capacity expansion methods

Capacity Expansion Method	Characteristics	Application Scenario
Adding disks	<ul style="list-style-type: none"> No need to stop services Easy to operate Fast Cost-effective 	The storage system has enough empty disk slots to satisfy your capacity expansion requirements.
Adding disk enclosures	<ul style="list-style-type: none"> No need to stop services Large-capacity 	<p>The storage system does not have enough empty disk slots, or the total capacity of the empty disk slots is not enough to satisfy your capacity expansion requirements.</p> <p>For example, 5 TB of capacity is required but only 2 TB is available after disks are added to all free disk slots.</p>
Adding controllers	<ul style="list-style-type: none"> No need to stop services Large-capacity Enhanced system performance 	<ul style="list-style-type: none"> The storage system does not have enough empty disk slots and disk enclosure slots, or the total capacity of the empty disk slots and disk enclosure slots is not enough to satisfy your capacity expansion requirements. The storage system does not meet service performance requirements.
Adding links	No need to stop services	Links of the storage system do not meet service reliability requirements.

Huawei enterprise capacity expansion provides scenario-based capacity expansion tools through OceanStor Toolkit and provides step-by-step instructions on how to perform capacity expansion. Capacity expansion procedure includes preparing for capacity expansion, performing capacity expansion, checking after capacity expansion, and using the newly added storage space.

Figure 5-1 shows the capacity expansion flowchart.

Figure 5-1 Capacity expansion process

Preparing for the Capacity Expansion

Make preparations before capacity expansion. Specifically, you need to collect information about the live network, plan for capacity expansion, prepare capacity expansion tools, perform a pre-expansion check, determine the time to perform capacity expansion, and back up the storage system configuration data before capacity expansion.

2. Collect information about the live network.

Live network information is required for preparing capacity expansion plans and installing hardware for capacity expansion. Live network information includes information about the storage system and application servers.

3. Plan for capacity expansion.

A capacity expansion plan varies with different capacity expansion methods. Before performing capacity expansion, make feasible and efficient plans based on the compatibility of added hardware as well as the operating status of the storage system.

4. Prepare auxiliary materials and software tools.

Preparing auxiliary materials and software tools ensures smooth capacity expansion.

5. Perform a pre-expansion check.

Before capacity expansion, check the health status of storage systems and the status of application servers. Capacity expansion can be smoothly performed only when the storage system is working correctly. If you encounter any problem that cannot be resolved during capacity expansion, contact Huawei technical support.

6. Determine the capacity expansion time.

Expanding system capacity at an appropriate time reduces risks associated with the expansion process.

7. Export storage system configuration data.

Export all configuration data before capacity expansion or storage system upgrades to restore the system in case that the expansion or upgrade fails.

8. (Optional) Configure switches manually.

When controllers are added on switch-connection networks and Toolkit is used to perform capacity expansion, Toolkit automatically configures switches. If onsite conditions of users cannot meet the requirements of switch configuration through Toolkit, you can manually configure switches in batches or independently for each port.

9. (Optional) Initialize the system.

If controllers are to be added, you need to initialize the system. To initialize the system, you need to configure the IP address of management ports on the original storage system, initialize the IBC account, clear configuration information of the controller to be expanded, and configure the IP address of management ports on the switch as well as information about SSH login user.

Performing Capacity Expansion

You can use a capacity expansion method based on your service and capacity requirements.

1. Adding disks

Expanding capacity by adding disks is simple, fast, and cost-effective, suiting application scenarios where a small amount of capacity needs to be added. The process for adding disks includes installing disks and checking the status of newly added disks.

2. Adding disk enclosures

Adding disk enclosures help expand capacity on a large scale, suiting application scenarios where a large amount of capacity needs to be added. The process for adding a disk enclosure includes installing a disk enclosure, connecting cables, powering on the disk enclosure, and confirming the status of the disk enclosure.

3. Adding controllers

You can add controllers to improve system performance if capacity expansion cannot meet increasing requirements of service data.

4. Adding links

You can add interface modules to add links to enhance the system reliability and security by link redundancy.

Performing A Post-expansion Check

After capacity expansion is completed, check the status of the storage system and verify services. Check the statuses of controllers, disks, and LUNs as well as the overall system status in a similar way to the pre-expansion check. In addition, verify services to ensure that all services are running correctly.

5.3.3 Specifications

OceanStor series storage can be expanded storage systems.

6 Disaster Recovery and Backup

6.1 BCManager eBackup

6.1.1 Introduction

BCManager eBackup is a backup software product designed for Huawei FusionSphere and VMware vSphere virtualization platforms as well as cloud platforms. By using VM snapshot, storage snapshot, and changed block tracking (CBT) technologies, eBackup provides comprehensive protection for data on VMs. With highlights such as ease-of-use and cost-effectiveness, it meets backup requirements of a large number of VMs.

Figure 6-1 Product positioning

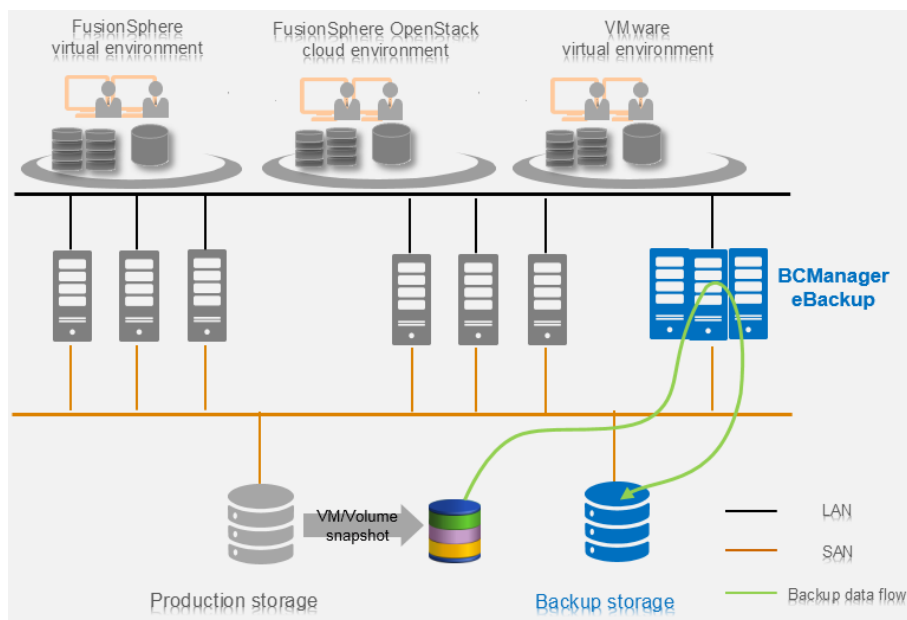
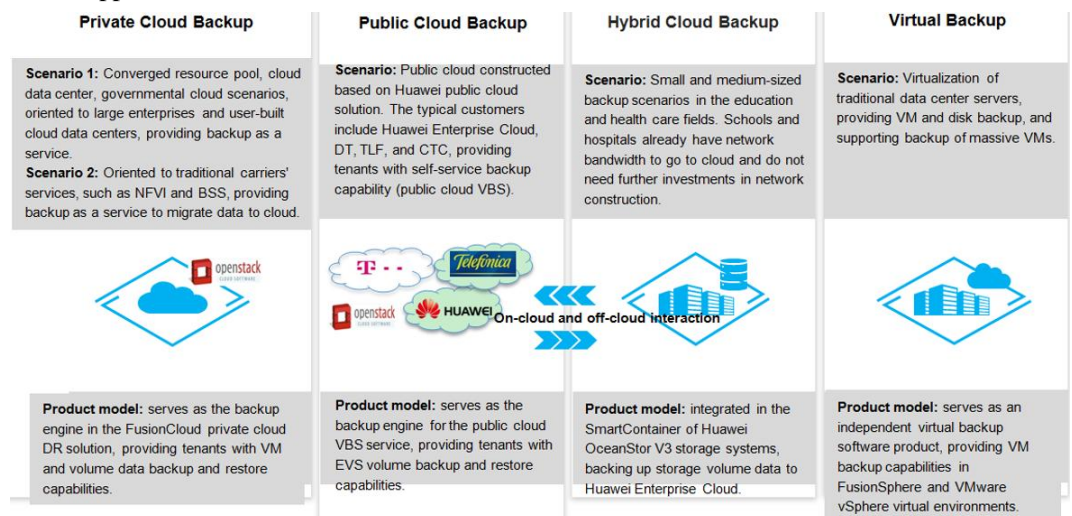


Figure 6-2 Application scenarios

6.1.2 Function Features

- Installation and initial configuration

BCManager eBackup can be installed by installing software or importing the VM template. That is, you can manually execute the installation script to perform one-click installation. Or you only need to import the VM template to perform installation because the software is pre-installed in the VM template. BCManager eBackup provides manual script for the initial configuration of software, which can be installed using the preceding two methods.

- Alarm management

BCManager eBackup supports alarm management. It automatically reports detected faults and rectifies them. If a fault cannot be automatically rectified, users can view uncleared alarm information and clear it by performing recommended actions. If an alarm has been handled, users can manually clear it.

BCManager eBackup supports the import of alarms for the convenience of viewing and analyzing.

- Configuration and maintenance

BCManager eBackup supports initial configuration and configuration adjustment by executing scripts.

BCManager eBackup provides GUI and CLI to configure and adjust system running parameters.

- Preventive maintenance inspection

To ensure long-term stable operation of the system, maintenance engineers can use Toolkit to periodically check the system and rectify faults based on the check results.

- Information collection

BCManager eBackup allows users to use an information collection tool Toolkit to export logs. By viewing and analyzing the exported logs, users can understand the system running status and rectify potential faults to ensure normal system operation.

- Run logs and operation logs

BCManager eBackup supports run logs and operation logs.

Run logs record the real-time running status of processes in the system. When the run log file reaches a specified size, it is compressed and backed up. The backup file is used to track historical process execution information.

Operation logs record user operations in the system. When operation logs accumulate to a specified count, they are exported and saved in a local file with one or more copies. The local file is used to track historical user operation information.

- NTP time synchronization

BCManager eBackup automatically synchronizes system time on the Backup Server and Backup Proxy nodes (As an internal NTP server, Backup Server provides clock synchronization services for the Backup Proxy node). In addition, Backup Server uses an external NTP server as a clock source for time synchronization.

6.1.3 Specifications

- Deployment mode

Backup Server of BCManager eBackup supports deployment on a single node or HA deployment on two nodes, while Backup Proxy of BCManager eBackup supports deployment on up to 64 nodes.

- Installation specifications

The size of BCManager eBackup installation package is equal to or smaller than 300 MB and the duration for installing the overall system is equal to or less than four hours.

- Upgrade specifications

BCManager eBackup supports offline upgrades and the upgrade lasts equal to or less than one hour.

- Log storage duration

Run logs and operation logs generated during the operating phase of BCManager eBackup can be automatically dumped. Local operation logs and run logs can be saved for six months.

6.2 BCManager eReplication

6.2.1 Introduction

BCManager eReplication is designed to manage DR services of data centers for enterprises. Its high application-aware capability and the value-added features of Huawei storage products ensure service consistency during DR, simplify DR service configuration, support the monitoring of DR service status, and facilitate data recovery and DR tests.

6.2.2 Function Features

- Installation and initial configuration

BCManager eReplication can be installed by installing software or importing the VM template. That is, you can install the command wizard. Or you only need to import the VM template to perform installation because the software is pre-installed in the VM template.

Users are instructed to enter the initial configuration information during the installation of BCManager eReplication and the import of VM template.

- Alarm management

BCManager eReplication supports functions, such as alarm statistics, alarm notification, and alarm dumping. After browsing the alarm information, the network administrator can take measures in time to make sure that the system runs properly. If a fault cannot be automatically rectified, users can view uncleared alarm information and clear it by performing recommended actions. If an alarm has been handled, users can manually clear it.

- Configuration and maintenance

BCManager eReplication supports reconfiguration on the system through scripts.

BCManager eReplication provides GUI and CLI to configure and adjust system running parameters.

- Preventive maintenance inspection

To ensure long-term stable operation of the system, maintenance engineers can use Toolkit to periodically check the system and rectify faults based on the check results.

- Information collection

BCManager eReplication allows users to use an information collection tool Toolkit to export logs. By viewing and analyzing the exported logs, users can understand the system running status and rectify potential faults to ensure normal system operation.

- Run logs and operation logs

BCManager eReplication supports run logs and operation logs.

Run logs record the real-time running status of processes in the system. When the run log file reaches a specified size, it is compressed and backed up. The backup file is used to track historical process execution information.

Operation logs record user operations in the system. When operation logs accumulate to a specified count, they are exported and saved in a local file with one or more copies. The local file is used to track historical user operation information.

- NTP time synchronization

BCManager eReplication Server uses an external NTP server as a clock source for time synchronization.

6.2.3 Specifications

- Deployment mode

BCManager eReplication can be deployed in centralized or distributed manners.

Centralized deployment: A BCManager eReplication Server is deployed on an independent server at the disaster recovery site or on a VM to manage production and disaster recovery resources. The BCManager eReplication Server deployed on the disaster recovery site must be able to communicate properly with the production site network.

Distributed deployment: Two BCManager eReplication Servers are deployed on the server of production site and the server or VM of the disaster recovery site to manage disaster recovery resources. The BCManager eReplication Server deployed at the production site must communicate properly with the BCManager eReplication Server deployed at the DR site.

- Installation specifications

The size of the BCManager eReplication Server installation package is equal to or smaller than 300 MB and the duration for installing the overall system is equal to or less than one hour.

The size of BCManager eReplication Agent installation package is equal to or smaller than 400 MB and the duration for installing a single host is equal to or less than one hour.

- Upgrade specifications

The BCManager eReplication Server supports offline upgrades and the upgrade lasts equal to or less than one hour.

BCManager eReplication Agent supports offline upgrades and the upgrade lasts equal to or less than one hour.

- Log storage duration

Run logs and operation logs generated during the operating phase of BCManager eReplication can be configured to enable dumping. Local run logs can be saved for 40 days and a maximum of 200,000 local operation logs can be saved.

7 Interfaces and the Ecosystem

7.1 Overview

This chapter describes interfaces used by Huawei enterprise storage in the operation and maintenance, including CLI, SNMP, REST, SMIS, and OpenStack.

7.2 CLI

7.2.1 Introduction

CLI indicates command-line interface. It is an interface where users can enter the executable instruction after prompts. The mouse cannot be used on CLI. Only the keyboard can be used to enter the command. The computer receives commands and executes them.

CLI is considered to be less user-friendly than graphical user interface (GUI). Software with CLI requires users to memorize the operation commands. However, comparing with GUI, CLI saves computer resources. Under the premise of memorizing commands, the user using CLI can operate faster than using GUI. Therefore, CLI is also available in the GUI operating system. After logging in to the CLI, you can query, set, manage, and maintain the storage system. The usage and use skills of the CLI can help you use the CLI more easily and quickly.

7.2.2 Function Features

- **Command management at different levels**
CLI categorizes commands into different levels based on the user level. The user logs in to the system must have the permission to see the corresponding command list. Huawei enterprise storage supports the three levels of super administrator, administrator, and read-only user.
- **Command views**
CLI distinguishes different command views based on the application scenarios, including the user view, engineer view, and developer view. Users under different views have different operation permissions.
- **Automatic command completion**
When entering CLI commands, the user can press Tab or the space. The available command fields will be automatically displayed. If the command field can be unique, the system automatically completes the whole field value.

- Intelligent error check
If the user enters an incorrect command or parameter, CLI can identify the incorrect character and mark it with "^" for users to correct it.
- Online help
You can run the **help obj** command to obtain help information about the command and view the command definition and instruction.
- Command filter
You can run the **filterRow** and **filterColumn** command to filter the search results and only view the required data.
- Historical command record
You can run the **show cli history** command to view information about commands that have been executed. You can use up and down navigation keys to quickly enter commands that have been executed before the current session.
- Shortcut keys
You can use shortcut keys to operate quickly. The following table lists the shortcut keys.

Function	Shortcut Key	Description
Move	↑	Moves to the previous command saved in the system
	↓	Moves to the next command saved in the system
	←	Moves the cursor forward one character
	→	Moves the cursor backward one character
	Ctrl+←	Moves the cursor forward one field
	Ctrl+→	Moves the cursor backward one field
	Ctrl+S	Moves the cursor forward to the command beginning
	Ctrl+E	Moves the cursor backward to the command end
Delete	Ctrl+C	Jumps to the next line
	Ctrl+D	Deletes the character where the cursor stays
	Ctrl+K	Deletes all characters on the right of the cursor, including the character where the cursor stays
	Backspace	Deletes the character to the left of the cursor
Page	Enter	Turns to the next line
	Space	Turns to the next page
	Shift+G	Turns to the last page

7.2.3 Specifications

The user can log in to a maximum of four CLIs on each controller node.

7.3 SNMP

7.3.1 Introduction

Simple network management protocol (SNMP) consists of a group of network management standards. SNMP includes an application layer protocol, a database schema, and a group of resource objects. This protocol can be used in the network management system to detect whether devices connected to the network have any problem causing management concerns. This protocol is a part of the Internet protocol cluster defined by the Internet Engineering Task Force (IETF). SNMP aims to manage software and hardware platforms of various manufacturers on the Internet. Therefore, the Internet management architecture has a great impact on SNMP. The third version of SNMP has been released. Its function is greatly improved than before.

SNMP is a network management standard based on the TCP/IP protocol suite. It is designed to manage network nodes, such as servers, workstations, routers, and LAN switches, on IP networks. SNMP can improve network administrators' efficiency of managing networks, detect and solve network problems, and plan the network expansion. Network administrators can also use SNMP to receive notification and alarms on the network nodes and to know problems occur on the network.

The network managed by SNMP consists of three parts:

- The managed device
- The SNMP agent
- The network management system (NMS)

Their relationship is as follows.

- Every managed device in the network has a management information base (MIB) for collecting and saving the management information. The NMS can obtain the information through the SNMP. The managed device, also known as the network unit or network node, can be a router, switch, server, or host supporting SNMP.
- The SNMP agent is a network management software module on the managed device. It has information about local device management, can transfer the information into a format compatible with SNMP, and send the information to the NMS.
- The NMS monitors the managed devices by running applications. In addition, the NMS provides a large number of handling processes for the network management and provides the required storage resources.

7.3.2 Function Features

There are three widely used SNMP versions: SNMPv1, SNMPv2, and SNMPv3.

SNMPv1

The structure of management information (SMI) of SNMPv1 defines standard management objects based on the ASN.1 standard. This version is easy to implement and is widely accepted in the industry. But one of its disadvantages is the poor security. The only security mechanism is based on the community strings which are like common passwords consisting of characters.

SNMPv2

The second version of the SMI is described in RFC 2578. It is enhanced on the basis of the first SMI version, such as the IP addresses and counters.

The SNMP runs at the seventh layer of the OSI model. In the first version, five core protocol data units (PDUs) are specified:

- GET REQUEST
- GET NEXT REQUEST
- GET RESPONSE
- SET REQUEST
- TRAP

Other PDUs are added in the second version, including:

- GETBULK REQUEST
- INFORM

SNMPv3

The third version of the SNMP is defined by RFC 3411-RFC 3418. The security and remote configurations are strengthened in this version.

The third version of the SNMP provides important security functions:

- Information integrity: ensure that the packets are not modified during the transfer.
- Authentication: authenticate that the information is from the correct source.
- Encapsulation encryption: avoid being snooped by unauthorized sources.

SNMPv3 defines the user-based security model and uses the shared key to authenticate the packets.

The following security levels are introduced to the SNMPv3.

- noAuthNoPriv: no authentication is required and no privacy (encryption) is provided.
- authNoPriv: authentication based on HMAC-MD5 or HMAC-SHA. No encryption is provided.
- authPriv: in addition to the authentication, the CBC-DES encryption algorithm is used as the privacy protocol.

7.3.3 Specifications

The SNMP interface is compatible with early versions.

The RFC regulations supported by the SNMP are as follows.

RFC #	Title
3410	Introduction and Applicability Statements for Internet Standard Management Framework
3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
3413	Simple Network Management Protocol Applications
3414	User Based Security Model (USM) for SNMPv3

3415	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
3416	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
3417	Transport Mappings for the Simple Network Management Protocol (SNMP) (UDP only)
3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
3584	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
3826	The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model

7.4 REST

7.4.1 Introduction

RESTful Applications Programming Interfaces (APIs) are open APIs provided by Huawei OceanStor DeviceManager based on Representational State Transfer (REST). Third-party developers can use RESTful APIs to access OceanStor DeviceManager open resources, such as alarms, performance data, and resource allocation information.

7.4.2 Function Features

Huawei has limitation on the security of storage REST interfaces. Only Hypertext Transfer Protocol Secure (HTTPS) is supported. First you need to configure security certificates on the server. By default, the temporary self-signed certificate is delivered with the device. The enterprise users need to use their own certificates to replace the temporary certificate. For details, see the related management guide of storage devices. CipherSuite is an important parameter that needs to be negotiated during the SSL handshake. Currently, cipher suite algorithms supported by REST interface servers of Huawei storage systems are upgraded from AES128-SHA, AES128-SHA256, AES256-SHA256, AES256-SHA, DHE-RSA-AES128-SHA, and DHE-DSS-AES128-SHA to ECDHE-RSA-AES128-SHA256 and ECDHE-RSA-AES128-SHA.

To invoke a RESTful API except the authentication API, you must obtain the API invocation permission first. Otherwise, an authentication error is returned, and the API fails to be invoked. Therefore, the first step of using the interface is to invoke the authentication API to authenticate. For details, see the description of the authentication API.

After the authentication, add the client cookie returned for this request to the header file of all requests and send the header file to the client. Besides, add the value of **iBaseToken** returned for this request to the header file of all subsequent requests with the **iBaseToken** as the key. Otherwise, the background authentication fails.

7.4.3 Specifications

RESTful APIs provide the Object Performance Indicators appendix. When you query the performance indicator of an object, refer to this appendix.

RESTful APIs also provide the error code appendix of all requests. If different error codes are returned for one RESTful API, you need to handle with the same logic. Do not handle different error codes differently. Otherwise, error code changes may bring compatibility problems.

Do not use parameters that are not included in the documents and parameters that are marked as discarded.

7.5 syslog

7.5.1 Introduction

Syslog protocol is a standard that forwards system log information over an IP network. It is developed by the Berkeley Software Distribution Research Center of University of California during a TCP/IP system implementation. Now it has become an industry standard protocol for recording device logs. Syslog records all events in the system. The management personnel can master the system situation by checking the system logs. The system log records system related events and application running events in the syslog process. Devices where the syslog protocol runs can communicate after they are properly configured. By analyzing these network behavior logs, you can track and obtain device and network situations.

7.5.2 Function Features

Currently, the storage array can dump system alarms and events to the syslog servers.

7.5.3 Specifications

Currently, info, warning, major, and critical information can be forwarded through the syslog server. A maximum of 4 syslog servers can be configured, and the type of alarms dumped to the syslog server can be flexibly configured.

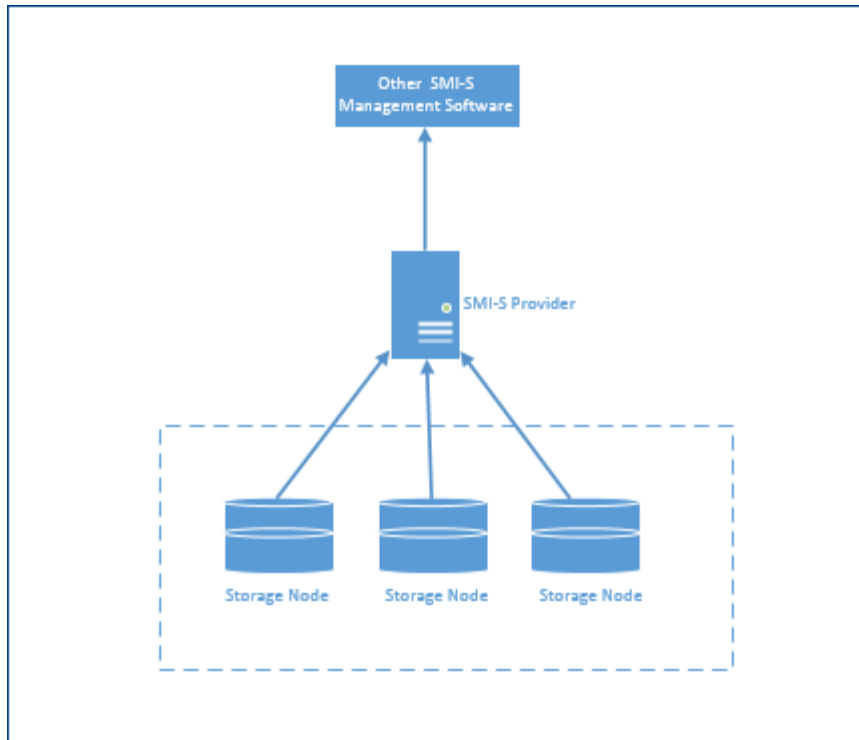
7.6 SMIS

7.6.1 Introduction

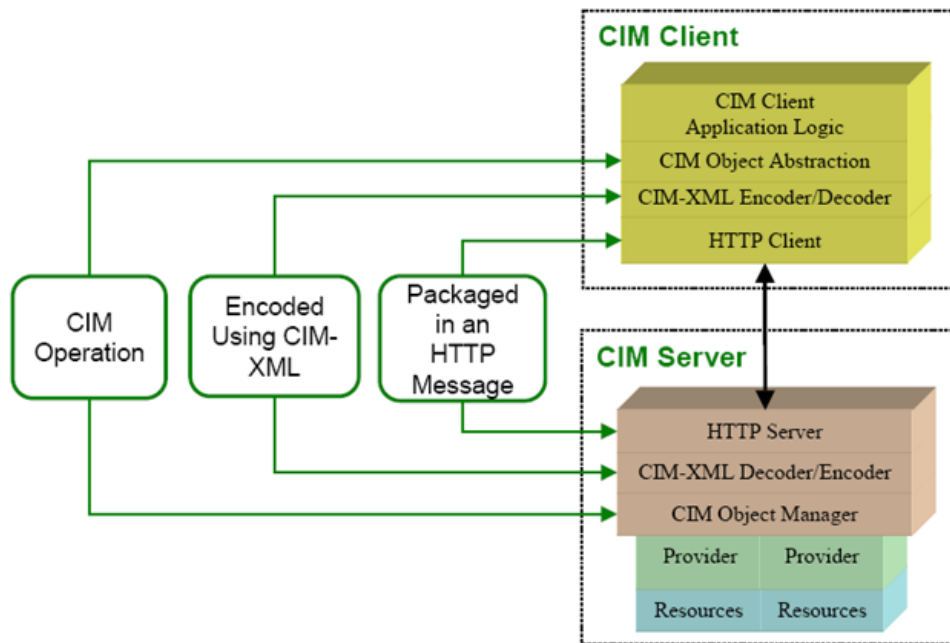
Storage Management Initiative – Specification (SMI-S) is a set of standards set by Storage Networking Industry Association (SNIA) for the management of storage network consisting of devices from multiple vendors. It defines unified interfaces to solve the problem that network management software cannot manage devices from different vendors.

7.6.2 Function Features

eSDK SMI-S is the SMIS-S service developed based on the open-source software OpenPegasus. The third-party storage management software can use the eSDK SMI-S service to manage Huawei storage devices as the network elements.



OpenPegasus is a C++ implementation of the WBEM framework. The following figure shows the overall architecture.



eSDK SMI-S features.

Supported Profiles	lArray
---------------------------	--------

	ISelf-Container NAS IServer
Supported Subprofiles and Packages	IBlock Services ICopy Services IDisk Drive Lite IFC Target Ports iSCSI Target Ports ISoftware IMasking and Mapping IGroup Masking and Mapping IMultiple Computer System IPhysical Package IJob Control IReplication Services IAutomated Storage Tiering IIndication IBlock Server Performance IExtent Composition IFile Server Manipulation IFile System IFile System Manipulation IFile Storage INAS Network Port IFile Export IFile Export Manipulation

eSDK SMI-S features that are supported by OceanStor 9000 series.

Supported Profiles	ISelf-Container NAS IServer
Supported Subprofiles and Packages	IMultiple Computer System IPhysical Package IBlock Service IFile Server Manipulation IFile System IFile System Manipulation IFile Storage INAS Network Port IFile Export IFile Export Manipulation

7.6.3 Specifications

None

7.7 OpenStack

7.7.1 Introduction

As the most active initiative to build open source software for creating and managing public and private clouds, OpenStack provides complete infrastructure as a service (IaaS) solutions. OpenStack enables any enterprise or individual to build private clouds to provide services within an enterprise, or to build public clouds to provide cloud services for external users. The OpenStack Foundation now enjoys over 160 members, including industry-leading vendors.

On October 23, 2012, Huawei announced its accession to the foundation. Since then, Huawei has made its efforts to accelerate the development of the OpenStack. Among these efforts, one is that Huawei's united storage series and OceanStor 18000 series all support OpenStack.

7.7.2 Function Features

OpenStack stores computing cloud data requiring permanent storage in volumes which are carried by logical unit numbers (LUNs).

Creating a volume

The procedure for creating a volume in storage drivers is as follows:

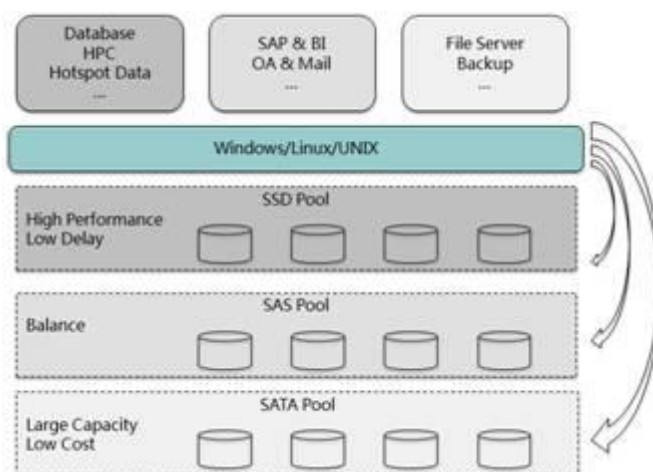
- The scheduler forwards the request for creating a volume to the storage driver.
- The storage driver obtains the specific LUN type and attributes.
- The storage driver creates the specific LUN in the storage system.

Volumes created by Huawei storage drivers provide better flexibility and availability, satisfying the requirements of cloud computing for optimized services:

- Users can configure the LUN type created by the storage nodes based on specific services. For key and high-performance services, configure traditional LUNs to ensure the performance of key services. For non-key services and services allocated with large initial capacity, configure Thin LUNs to reduce investment and increase the storage space usage.
- The attributes (such as stripe depth, prefetch policy, and data write policy) of newly created LUNs can be specified to meet services' requirements on block storage performance in computing clouds.

Note: Multiple service systems may be deployed in a customer's computing cloud, and each of them may require different storage performance, as shown in the following Figure 7-1. To satisfy these requirements, the virtualized resource pools must be able to provide differentiated volumes. The current version of Huawei storage driver adopts a global configuration policy. This policy can satisfy the storage requirements in monotonous service scenarios, but cannot meet those in mixed service scenarios. The next version will allow dynamic configurations of LUN attributes based on the volume type. After these attributes, such as SmartThin, SmartCache, and SmartTier, are configured, the storage performance will be greatly enhanced.

Figure 7-1 Storage requirements in mixed services



Deleting a volume

The procedure for deleting a volume in storage drivers is as follows:

- Cinder-api forwards the request for deleting a volume to the storage driver.
- The storage driver deletes the specific LUN in the storage system.

Mounting a volume

The storage driver attaches a volume for OpenStack by maintaining the mapping between the computing nodes and the LUNs of the storage system. The procedure for mounting a volume in storage drivers is as follows:

- Cinder-api forwards the request for mounting a volume to the storage driver.
- The storage driver creates a mapping between the specific LUN and computing nodes of the instance in the storage system.
- The storage driver returns the information about the target ports connected to the computing nodes.

- Based on the returned information, the computing nodes obtain the mapped block storage and attach it to the VM instance.

Huawei storage drivers automatically maintain the mapping between the computing nodes and the storage system. The current policy for attaching volumes provides the following benefits:

- Simplifying configurations: Unified storage ports used by computing nodes in iSCSI simplify the configuration of storage networks.
- Ensuring performance: Independent storage ports configured in computing nodes in iSCSI prevent the storage ports from becoming a performance bottleneck.

Note: The next version will support autozoning and port load balancing strategies in FC SAN.

Unmounting a volume

The procedure for unmounting a volume in storage drivers is as follows:

- Cinder-api forwards the request for unmounting a volume to the storage driver.
- The storage driver removes the mapping between the LUN and the computing nodes.

Volume cloning

Huawei storage drivers support volume cloning by copying data in the storage system, remarkably reducing host performance consumption and bandwidth consumption of the storage network. The procedure for cloning a volume is as follows:

- Cinder-api forwards the request for cloning a volume to the storage driver.
- The storage driver creates a LUN and copies the source LUN data to the new LUN using the LUN copy function.

QoS

Huawei storage drivers support the integration of the SmartQoS feature into the storage system. The integration procedure is as follows:

- The administrator creates a QoS specification using the Cinder CLI. The specification parameters can be defined by the storage vendors. Parameters supported by Huawei storage drivers are **maxIOPS/minIOPS**, **maxBandWidth/ minBandWidth**, and **latency**.
- The administrator associates the QoS specification to the volume type using the Cinder CLI.
- Tenants choose a specific volume type while creating a volume.
- If the storage driver detects that a volume is associated with the QoS specification when a volume is being created, the driver will create a SmartQoS policy group, configure it based on the QoS specification, and add the newly created LUN to the SmartQoS policy group.

Snapshot Management

In OpenStack clouds, snapshot management enables backup and replication of storage data by providing interfaces for creating volume snapshots, deleting volume snapshots, and separating volumes from snapshots.

Creating a snapshot

The storage driver uses the Huawei virtual snapshot technology to meet the requirements of OpenStack on snapshots. The procedure for creating a volume snapshot is as follows:

- Cinder-api forwards the request for creating a volume snapshot to the storage driver.

- The storage driver creates and activates the specific virtual LUN snapshot in the storage system.

Huawei storage system creates snapshots using the virtual snapshot technology. This feature brings the following benefits:

- High speed: The storage system can create a volume snapshot within a short time.
- Low usage of the storage space: No complete data replication is required, saving the storage space.

When instance snapshots are used to store real-time data of a running VM in OpenStack, the instance snapshots are created in a different manner due to different boot modes of instances. For example, if a VM is started from an image stored in Glance, the instance snapshot is created as the instance image copy. Likewise, when a VM instance is started from an attached volume, the instance snapshot is created as the volume snapshot. Testing results show that when a VM instance is started from attached volumes, the virtual snapshot technology can greatly save time in creating instance snapshots. The following table compares time consumed in creating VM instance snapshots when a VM is started from the image and from the attached volume.

Table 7-1 Comparison of time consumed in creating instance snapshots

System Type	Time (The instance VM is started from the image.)	Time (The instance VM is started from the attached volume of the OceanStor T series.)
Ubuntu Precise i586 (208 MB)	5 min	1 sec
Cirros 0.3.0 i586 (9 MB)	10 sec	1 sec

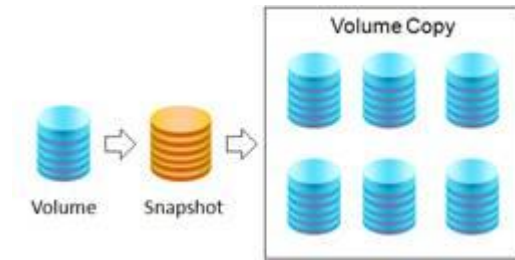
Deleting a snapshot

The procedure for deleting a volume snapshot is as follows:

- Cinder-api forwards the request for deleting a volume snapshot to the storage driver.
- The storage driver deletes the specific virtual snapshot in the storage system.

Separating a volume snapshot

Separating a volume snapshot means to separate a volume that has the same data with a snapshot from the snapshot. The following figure shows several data volumes of the same content separated from data volume snapshots. Separating volumes using snapshots enables data backup and distribution for OpenStack. A VM instance system existing in data volumes can support large-scale deployment of virtual environments.

Figure 7-2 Separating a volume snapshot

The storage driver separates volume snapshots using the LUN copy function of the Huawei storage system, satisfying the requirement of OpenStack. The procedure for separating a volume snapshot is as follows:

- Cinder-api forwards the request for separating a volume snapshot to the storage driver.
- The storage driver creates a LUN in the storage system.
- The storage driver copies all the data from the source snapshot to the new LUN.

7.7.3 Specifications

None

7.8 Easy to Be Integrated

7.8.1 Introduction

The compatibility involves various fields, including the operating system, HBA, switch, backup and archive software, network management software, and virtual gateway.

7.8.2 Function Features

Major operating systems

Windows

Linux: SUSE/Red Hat

IBM AIX

Oracle Solaris

HP-UX

Mac OS

VM:

VMware

Hyper-V

XenServer

The HBA and switch type:

Original manufacturer:

FC (QLogic, Emulex, LSI, Brocade, ATTO and more)

iSCSI (QLogic and more)

Original equipment manufacturers (OEMs):

IBM, HP, DELL, SUN, HUAWEI

Major management software

Windows: SCVMM, SCOM

BMC: PATROL, BAO, BCO

HP: SE, OM, SIM, NNM

IBM: Tivoli OMNIBus

CA: Spectrum

Major backup software

Commvault: Simpana

Symantec: NetBackup

Veeam: Veeam Backup & Replication

IBM: TSM

7.8.3 Specifications

Compatibility query:

<http://3ms.huawei.com/> > DOCUMENTS > By Product Line > IT Solutions > Storage > Validation & Certification


The screenshot displays the Huawei 3MS website interface. At the top, there are navigation tabs for HOME, DOCUMENTS (selected), CASE, HI, KA, IMSS, Minisite, and My 3MS. A search bar is present with a 'Search' button and a link to 'Advanced Search'. Below the navigation, a breadcrumb trail reads 'Directory > Storage > Validation & Certification'. On the left, a sidebar menu shows a tree structure under 'Storage', with 'Validation & Certification' expanded to show sub-items like 'Test & Reports', 'Product Certification', and 'Compatibility List'. The main content area is titled 'By Product' and features a search box, a 'Search' button, and a 'Database' tab. Below the search area, there are buttons for 'All Documents', 'Chinese', 'English', and 'Others'. A pagination bar shows 'Total: 153' and page numbers '1', '2', '3', '4', '5', '11', and 'Next'. At the bottom, there is a 'Create DOC' button, a dropdown menu set to 'All Documents', and an 'Order By' dropdown set to 'Release Date'.





<http://support-open.huawei.com/ready/> > Interoperability Center > Storage Interoperability

OceanStor Interoperability Navigator

Please click the **Q** icon, then double click the components which you need to query in the expanded panel, you can get the compatibility information after click the submit button.






If you have any question or opinion please feedback to IT-OPENLAB@huawei.com

Search for a component 

Component Type	Component	
OceanStor Storage System	OceanStor 5300 V3	
Server Model		
Operating System		

Guides Dictionary

Guides

- Microsoft Windows 
- Suse Linux Enterprise 
- Red Hat Linux 
- IBM AIX 
- VMware ESX 

More

A Acronyms and Abbreviations

Acronym and Abbreviation	Full Name
FRU	Field Replaceable Unit
CRU	Customer Replaceable Unit
CLI	Command Line Interface
OPEX	Operating Expense
SNMP	Simple Network Management Protocol
REST	Representational State Transfer
SMI-S	Storage Management Initiative specification